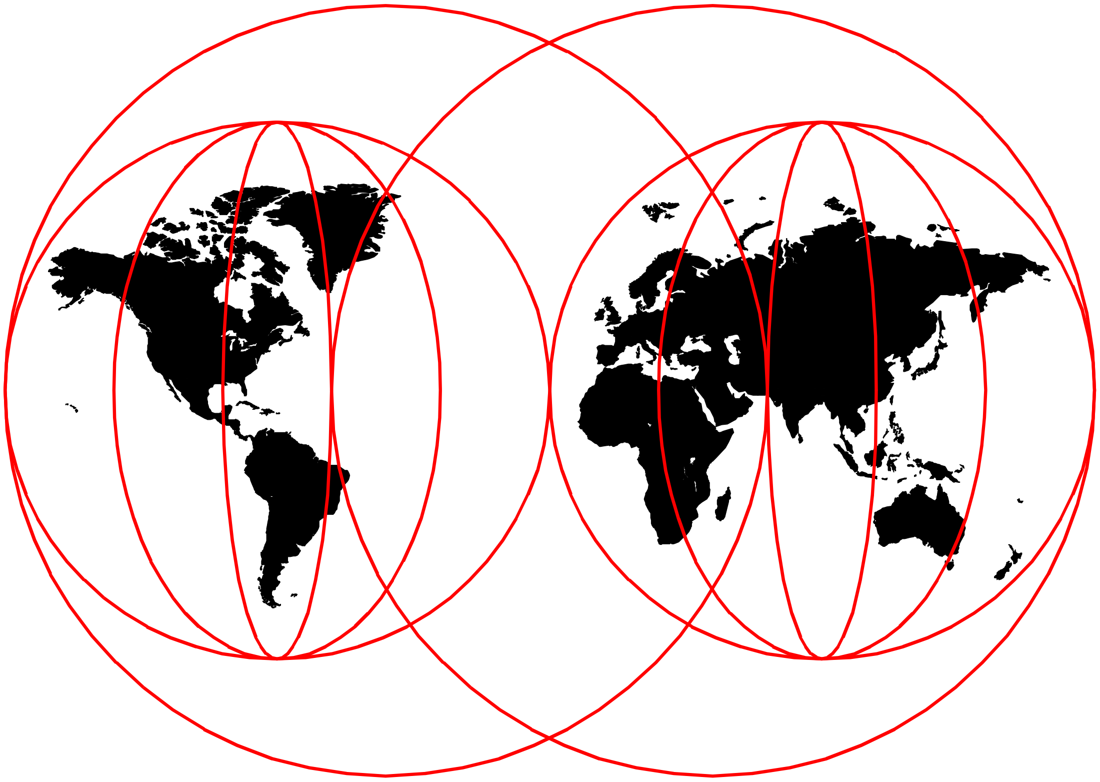
AS/400 Internet Security: Developing a Digital Certificate Infrastructure

Thomas Barlen, Colin Grierson, Benoît Grimée, Yukihiro Minote



International Technical Support Organization

www.redbooks.ibm.com

SG24-5659-00

International Technical Support Organization

SG24-5659-00

AS/400 Internet Security: Developing a Digital Certificate Infrastructure

February 2000

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix F, “Special notices” on page 403.

First Edition (February 2000)

This edition applies to Version 4 Release 4 Modification 0 of the Operating System/400 - 5769-SS1.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JLU Building 107-2
3605 Highway 52N
Rochester, Minnesota 55901-7829

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Preface

This redbook is the first publication that shows in a complete picture how digital certificates can be used for security on the AS/400 system.

One of the reasons why many customers should consider using digital certificates is to secure their Internet and intranet applications. Everybody knows that nowadays almost every Internet application requires a user ID and password to get access to it. And of course it is very likely that one user never gets a single user ID for different applications, which means a user has to remember several user IDs and passwords. The worst case is that users start to write down their passwords, which weakens the security policies that are in place. The answer to get rid of many user IDs and passwords is using digital certificates.

For applications and servers that already support client authentication through digital certificates, there is no need to use User IDs and passwords anymore. A single certificate issued by a well-known Certificate Authority can serve as an identifier of an entity for many applications.

This redbook describes what you can do with digital certificates on the AS/400 system. It explains how to set up the various servers and clients to use certificates. Further it provides information and sample code of how to use AS/400 system APIs to manage and use digital certificates in user applications.

It also gives a basic introduction to the terms and technologies used when dealing with digital certificates and the Secured Socket Layer protocol.

Some knowledge of the IBM HTTP Server for AS/400 is assumed.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Rochester Center.

Thomas Barlen is an Advisory International Technical Support Specialist for AS/400 systems at the International Technical Support Organization, Raleigh Center. He writes extensively and teaches IBM classes worldwide on all areas of AS/400 communications. Before joining the ITSO in 1999, he worked in AS/400 software support in IBM Germany. He has over 10 years of experience in AS/400 networking and system management as well as LAN and WAN network design and implementation.

Colin Grierson is a programmer, analyst, and technical consultant for Systems Advisory Services in New Zealand, primarily an outsourcing company using AS/400s. Colin has 20 years of experience in programming and business analysis mainly working on S/38 and AS/400 systems. He holds a degree in mathematics from Auckland University. His areas of expertise include programming, business analysis, and security. He has written applications in RPG/400, Cool 2E (previously Synon/2), and AS400 CL.

Benoît Grimée is a Senior Consultant for SkillTeam S.A. in Luxembourg. He has 11 years of experience in software development, of which he worked three years in Java development and two years as a Security Senior developer. He holds a degree as a Civil Engineer from UCL, Belgium. His areas of expertise include

Lotus Notes/Domino Internet and intranet, Java, and security application development. He has written extensively on Internet transactional systems. In particular he has developed and implemented cryptography solutions for online banking applications.

Yukihiro Minote is an Advisory IT specialist in IBM Japan. He has 11 years of experience in the AS/400 system area. He joined IBM Japan in 1988. His areas of expertise include network (APPN HPR and TCP/IP), security, and performance. He provides technical support to general AS/400 customers, IBM sales representatives, and IBM Business Partners. Currently, his focus is on AS/400 Internet technologies, especially Web server security and WebSphere.

Thanks to the following people for their invaluable contributions to this project:

Marcela Adan, Bob Maatta, Kris Peterson
International Technical Support Organization, Rochester Center

Gail Christensen, Martin Murhammer, Tate Renner, Shawn Walsh
International Technical Support Organization, Raleigh Center

Mark Bauman, Kathleen Bies, Patrick Botz, Jim Fall, Jai Goradia, Kent Hofer, Beth Hoffman, Bill Lynch, Ramy Mehta, Barb Smith, Jeff Thelen, Daryl Woker, John Wolfe, Carol Woodbury, Ravi Yamdagni
IBM Rochester Development

Martin Barbeau
IBM Canada

Mark Pottorff
IBM Rochester Partners in Development

Erika Alejandra Monjaraz Cuadra
IBM Mexico, AS/400 Test Team

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Please send us your comments about this or other Redbooks in one of the following ways:

- Fax the evaluation form found in “IBM Redbooks evaluation” on page 415 to the fax number shown on the form.
- Use the online evaluation form found at `http://www.redbooks.ibm.com/`
- Send your comments in an Internet note to `redbook@us.ibm.com`

Part 1. Introduction

Chapter 1. Introduction to digital certificates

Digital certificates were created to serve several roles in current and foreseeable computing environments, where large numbers of entities communicate in a complicated web.

A single digital certificate can be used by an entity to identify itself to a number of other parties. Identification can be done automatically and securely. This is much more convenient and more secure than having to have multiple user names and passwords as is often the case now.

Digital certificates include a public and private key pair that can be used to set up secure connections across an untrusted network, as well as being used to securely identify an entity. Secure Sockets Layer (SSL) protocol, the IPSec protocols used to build Virtual Private Networks (VPN), and several other secure Internet protocols use digital certificates to initiate secure communications.

This chapter introduces terms that are commonly used when talking about digital certificates, how they work and where they are used. For a complete and detailed description of public key infrastructures, refer to *Deploying a Public Key Infrastructure*, SG24-5512.

1.1 Terms

Once you dive into the world of Internet or intranet security, you will encounter a lot of new phrases and terms. The following list introduces common terms associated with digital certificates. They will provide you with a good foundation for understanding digital certificates.

Authentication

Authentication is the function of proving the identity of an entity.

AS/400 DCM

The AS/400 Digital Certificate Manager (DCM) is an application for managing digital certificates. It includes the ability to create and store certificates on the AS/400, to validate certificates, and to associate certificates with user profiles and applications.

Certificate

The term certificate is just a short form of digital certificate. Sometimes it is also referred to as a digital ID. But all terms mean the same: an electronic form of identification. Refer to 1.2, “What are digital certificates?” on page 6 for further information about digital certificates.

Certificate Authority (CA)

A CA is an organization that issues digital certificates. Companies such as VeriSign and Thawte are examples of Internet Certificate Authorities. A digital certificate will be issued from a Certificate Authority when the required information is given to them, a fee is paid, and the information passes their security checks. You may choose to set up a Certificate Authority on your AS/400 and issue certificates to entities you communicate with. In the wider community a certificate is only likely to be accepted if it has been issued by a well-known and trusted CA.

Certificate handle

The certificate handle on the AS/400 system is an identifier that uniquely identifies a certificate. It is available through the following application programming interfaces (APIs):

- QsyParseCertificate()
- QSYPARSC
- QsyListUserCertificates()
- QSYLISTUC
- QsyListVldlCertificates()
- QSYLISTVC()

The certificate handle is 40 bytes in length and is a combination of 2 hashes done against unique parts of the certificate.

Certification Practice Statement

The Certification Practice Statement (CPS) contains the terms and conditions under which a CA issues certificates. It includes, for example, how the CA validates certificate requests. A CPS should be examined carefully before requesting or accepting a certificate issued by that CA. For example, it contains information to determine what parts of the identity of the person that requested the certificate were verified for the fee that was paid.

Certificate Revocation List

A Certificate Revocation List (CRL) is a list of certificates that are no longer valid and should not be accepted. If a CA maintains a CRL it is responsible for keeping it up to date and for making the CRL available to the appropriate entities.

A CRL contains a list of certificate serial numbers and revocation dates.

Note

The AS/400 DCM does not maintain a CRL.

Challenge phrase

A challenge phrase is a sentence or a word used like a password to protect your digital certificate against unauthorized action. The challenge phrase is needed by most CAs to validate requests to revoke, renew, or replace a digital certificate. It is requested to be specified during a certificate request.

Digital signature

A digital signature is a method used to enable checking that data has not been modified while on transit and to prove the identity of the entity that created the signature. To create a digital signature for some data, a hash of the data is made and then encrypted with the signer’s private key. The encrypted hash, the signer’s identity, and the hashing method are used to form the digital signature.

Later another party can repeat the hash method on the data, use the signer’s public key to decrypt the original hash, and compare the results. If they match, the party can be sure that the data has not been changed and that the signer was the entity that created the digital certificate.

Distinguished Name (DN)

A DN is the name of an entity stored as a list of attributes and values, for example:

- Country: New Zealand
- State or province: King country
- Locality or city: Taihape
- Organization name: University of Taihape
- Organizational unit: Sheep shearing
- Common name: Fred Dagg

The DN of an entity must be unique in the CA that issues a certificate.

A number of attributes, including those used above, are defined in RFC 2459. RFC stands for *Request for Comments,* which can be accessed through `http://www.rfc-editor.org/`. Others may be used by CAs but may not be universally accepted. For example, zip code is not accepted on some older browsers.

The AS/400 DCM allows values to be given for the attribute’s zip code (this will be removed in a future release), country, state or province, locality, organization name, and organization unit. For client certificates, the common name is the name of the user profile requesting the certificate.

Entity

An entity is a person, organization, or machine that can participate in a communications network.

Hash

Hashing functions are used to ensure message integrity. The message sender applies a hashing function, which is a mathematical algorithm, to the message to create a message digest. The message digest along with the original message will then be sent to the receiver, who applies the same algorithm to the message and compares the two digests. If they are identical, it proves that the message has not been tampered with during transmission. Ideally if one bit in the message is altered in the original data approximately half the bits in the hash or digest will change.

Key escrow authority

This is a trusted organization that will hold copies of private keys and release them only to authorized parties. This institution is required by some governments.

Man in the middle

This is used to describe the situation where a third party, X, is in a position to intercept and relay communications between two other parties. Party X is then in a position to mount several types of security attacks.

Public key/private key

This is a pair of keys that can be used to encrypt data in such a way that data encrypted by the private key can only be decrypted by the public key and vice versa. Generally one of the keys is made publicly available and the other is kept private and secure. These keys are also called asymmetric keys.

Smart card

A smart card is a physical device, typically a card with an embedded processor and memory. It can be used to hold a person's private key and, provided the correct PIN or password has been given, to perform encryption or decrypting functions using this key. Because the key never leaves the smart card when using this option, it can strengthen your security system.

Well-known CA

A CA that is widely known and trusted, for example, VeriSign, American Express, and Thawte. The certificates of many well-known CAs are preloaded into applications such as the Netscape browser so that secure transmissions can be established immediately with servers having certificates signed by these CAs.

1.2 What are digital certificates?

A digital certificate, sometimes known as a digital ID, is a form of personal identification that can be verified electronically. It is used as a form of identification for individual persons and other entities, such as servers. A digital certificate can be compared with a passport. The authenticity of the data in a passport is validated by the issuing bureau. Usually this bureau is operated by the government. Similar to passports, digital certificates are issued by a Certificate Authority (CA). CAs are entities that are entrusted to properly issue certificates and have control mechanisms in place to prevent fraud. An individual may have many certificates from many different CAs, just as we have many forms of personal identification. Just as you trust a passport more than a membership card as personal identification, you will trust a certificate issued by a well-known CA more than one issued by an unknown CA. A certificate is normally created in a standardized format. It is the X.509 format that is described in RFC 2459. A certificate typically holds:

- A serial number.
- The name of the entity it was created for in DN format.
- The public key of the certificate.
- The period for which the certificate is valid.
- The name of the CA that issued the certificate in DN format.
- Additional information placed by the CA that issued the certificate. Generally this further describes the entity and specifies how the certificate may be used. For example, there is a standard extension used to restrict the function of certificates to roles such as a normal user, a server, or a CA that is almost always present. Aliases of the user name, which are generally their e-mail or TCP/IP addresses, are often stored using another standard extension.
- A digital signature from the CA that issued the certificate. This can be used to prove the validity of the certificate.

The corresponding private key of the certificate's public key is held by the entity to whom the certificate was issued and sometimes other trusted parties, such as a key escrow authority.

- The private key must be kept secure. This is done by storing the key together with a password in an encrypted form and accessing the key via an application that requires the password to establish authority. Another method of securing the private key is to use a smart card that uses a personal identification number (PIN).

1.3 Uses for digital certificates

Digital certificates can be used for authentication, for convenience, to secure information being transmitted across an untrusted network, and to establish the ownership and integrity of information you receive.

Authentication

To positively identify an entity, certificates have advantages over other methods, such as a user name and password.

- Digital certificates are innately more secure than names and passwords, because possession of the private key and knowledge of the password to unlock it from the certificate store are needed to use them.
- Unlike a password, a private key never needs to be transmitted and hence is much less likely to be discovered. If smart cards are used, the system can be even more secure because physical possession of an object is required.
- The process of validating an entity by using a certificate is secure, whereas a name and password must cross a network and can be intercepted.
- One certificate can be used to identify an entity to many other entities, regardless of the level of trust in the other entities, because the private key is kept secure. Digital certificates eliminate the need for many user names and passwords.
- Certificates are not vulnerable to “man in the middle” attacks.

Note

Of course, even certificates can be misused. For example, if Anita gives Colin the password to her browser’s certificate store, Colin could use Anita’s private key just as if he were Anita. The actual owner, in this example Anita, must use reasonable care to protect her password that allows use of her private key.

Convenience

In many cases when initiating communication, an entity’s certificate can be automatically presented for identification and authentication. This can be hidden so that all a person needs to do is unlock his private key at the beginning of the day or insert a smart card into a reader instead of having to give a name and password every time he establishes a session with a server. If he typically has many sessions during a day with many different servers, this can be a significant advantage.

Secure transmitted data

Digital certificates are used as the basis for Secured Socket Layer (SSL), which is a method of encrypting data sent across TCP/IP networks. SSL can be used by most of the services that run across TCP/IP to ensure others cannot intercept or modify data. For example HTTP, Telnet, Lightweight Directory Access Protocol

(LDAP), Distributed Data Management (DDM), all the Client Access Express APIs, and AS/400 Toolbox for Java functions can use SSL.

Note

To establish a secure SSL connection, only the server needs to possess a certificate. SSL is frequently used by HTTP servers, and generally the client browsers do not possess a certificate. However, the CA that signed the HTTP server's certificate must be known to the client browsers.

Digital certificates can be used for authentication by Virtual Private Networks (VPNs). Like SSL, VPNs encrypt data to ensure privacy and integrity, but do this at a lower layer than SSL so that applications, such as HTTP and Telnet do not need modification.

Establishing ownership and integrity of data

An entity can use its private key to digitally sign data to be sent to another party. When the data and digital signature are received, the recipient can use them to verify that the data has come from the correct entity and that it has not been modified.

In some cases, data must be signed before it will be accepted. Later, if necessary, the ownership of the data can be proved.

1.4 Obtaining a new certificate

Today all Certificate Authorities have slightly different procedures for processing a request to create a new digital certificate, but the basic steps involved are always the same.

1. The client user enters the Web application of a Certificate Authority (CA) and selects the option to get a certificate.
2. A form has to be filled out by the user. In most cases the following information is requested:
   - Name.
   - E-mail address.
   - Country, locality or city, organization, organizational unit.
   - Zip code.
   - Challenge phrase.
   - Other optional information, such as a birth date in case a client certificate is requested.
   - Payment information, if it is not a free trial or intranet certificate. Of course the payment information will not be included in the certificate when it is issued.

The actual information to be provided to the Certificate Authority may vary from CA to CA.

Note

The zip code field is not always requested in a certificate request. Sometimes the zip code, when filled in, leads to problems with some browsers. For example, the Netscape Communicator terminates abnormally when the certificate contains a zip code. This problem is solved with Netscape Communicator 4.7.

3. After the form is filled out, the client user has to submit the request. At this time the client, for example Netscape Communicator, is requested to create the private key. The request to create the private key is indicated by a message.
4. After the private key is created, the CA gives directions on how to proceed to get the certificate to your client. In many cases, the client user gets an e-mail indicating how to receive the certificate into the client.
5. Depending on the class of the certificate requested, the CA validates the data provided in the request and creates the certificate. After the certificate is received, it can be used immediately.

An example of a client certificate request is shown in Appendix C, “Obtaining a digital certificate” on page 387.

1.5 Designing a certificate infrastructure

It is extremely important to thoroughly plan your certificate infastructure. Before you start requesting certificates and using them in your environment, you have to answer some fundamental questions. The most important questions are:

- What functions will certificates be used for?
- Who will issue certificates?
- How will requests for new certificates be validated?
- What mechanisms will be put in place so that certificates can be used to control access to applications?
- How do you administer the certificates, validate and execute change requests, and handle lost, compromised, and undesirable certificates?

1.5.1 Deciding when to use certificates

This section examines the situations where digital certificates can be used.

1.5.1.1 Serving Secured Socket Layer (SSL)

You will need a certificate for the HTTP server to use SSL for secure communications.

If your site will be available to the public, your certificate should come from a well-known CA. If you create your own CA and use it to sign your own server certificates then users who visit your site will receive a series of questions asking if they trust you and if they will accept your certificate. This can confuse and worry your visitors. Server certificates signed by well-known CAs are accepted automatically.

If your site will only be used within your intranet, you can create your own server certificate using your local CA. In this case you can distribute your CA's certificate to each employee's browser or train employees to install the certificate in their own browsers.

1.5.1.2 Client authentication

You can use certificates to identify clients so they do not have to give user names and passwords. If you do this you need to consider the mechanisms your applications will use to decide which certificates can be accepted. These are discussed in Chapter 4, “Securing the HTTP Server for AS/400” on page 35 and Chapter 6, “Enabling SSL on AS/400 standard server applications” on page 187.

1.5.1.3 Digital signatures

You can use certificates to sign documents you create and to validate signatures on documents you receive. This requires an application to make each user’s public key accessible to the people who need to validate signatures. One way to make public keys available to all users is to publish them in a directory and access them through the Lightweight Directory Access Protocol (LDAP). You also need routines for signing and for verifying signatures. Currently the AS/400 does not have APIs to do these functions.

1.5.2 Deciding who issues the certificates

You could decide to operate your own Certificate Authority (CA) to issue certificates and trust certificates only from this CA. Alternatively, you could accept certificates issued by any well-known CA, once the certificate and associated entity have passed your security checks.

Digital certificates are intended to be a universal identification mechanism. Issuing separate certificates for small localized applications and forcing people to have mulitple certificates defeats the purpose of having a certificate as a universal identification mechanism. If this happens, you end up in a situation similar to having multiple user IDs and passwords.

If each application that will use certificates keeps its own list of certificates that it will accept, or shares a common list, then there is no advantage in issuing your own certificates.

If you have an application running on multiple systems and it has a simple authorization scheme, then issuing your own certificates and having the application accept only your certificates is a simple and effective way of implementing a secure environment. However, this method does not work well in situations where there are multiple applications and multiple levels of access within applications. In this case you need other methods to distinguish different levels of access.

It is possible to place additional information within a certificate, particularly if you do not require the certificates to be used outside of your organization, and to use this information to control access. This option was designed with the idea of industry segments agreeing on a need and a format to meet that need. To do this you will probably have to modify your CA to insert the additional information when creating the certificate. It is not really suitable for holding authorizations because if a change is required, which frequently happens with authorizations, a new certificate must be issued.

Note

The AS/400 DCM does not allow additional information to be placed into certificates.

As you can see, there are a lot of considerations that have to be taken into account when making the decision to use a well-known CA or a private CA to issue certificates.

Generally a well-known CA is useful when:

- You are serving SSL to the Internet
- You are serving SSL to an intranet and do not want to have to train users how to receive your CA certificate into their browsers.
- You do not want to operate your own CA.
- You want to accept certificates that users already have.
- The number of certificates to be issued is large and you do not want the job of having to validate the information people give.

For larger organizations that have to obtain many certificates, the cost factor may influence their decision as well. In this case, it is worthwhile to consider operating your own CA. Other reasons to justify the operation of a local CA are:

- You want to operate your own CA to control the issuing process.
- You want to identify users in advance.
- Trust is based on organization.

Note

The only way to create client user certificates using the AS/400 DCM is for the user to come to the DCM using a browser. The user has to enter the AS/400 system user name and password, and then request a certificate. The user profile must exist in advance. There is no way to create a certificate on behalf of another entity, nor to modify the creation of the certificate by using an exit program or something similar. When the certificate has been created, it is automatically associated with the user name that was given.

If the level of trust of a Certificate Authority is an issue, you have to refer to the CA’s Certification Practice Statement (CPS). The CPS contains the terms and conditions under which a CA operates. For example, it describes how certificates are issued, validated and revoked.

1.5.3 Validating requests to enable access to an application

When an entity requests access to an application, the same validation process must be followed regardless of the method of authentication that will be used. However, if a certificate has been given, it may be used to help validate the identity of the entity. If the request is approved, the certificate must be stored and associated with the application.

1.5.4 Using client certificates to control access on the AS/400 system

On the AS/400, the simplest way to control access is to associate a certificate with a user profile and to use the normal AS/400 security control mechanisms. If this is used, it should be the most secure system, as it provides control no matter how a user accesses the system. When you decide to associate client certificates with AS/400 user profiles, be sure to set the password expiration period to *NOMAX and the password to *NONE. Otherwise, an Internet user might not be able to access the application due to password expiration. And of course, you do not want to be bothered with passwords anymore when using certificates instead.

Another mechanism that is suitable when certificates are not associated with user profiles is validation lists. These are AS/400 objects, of the type *VLDL, that can hold lists of objects such as certificates. APIs are available to, for example, add a certificate to a validation list, check if a certificate is on a list, or remove a certificate from a list. Validation lists can be used to hold a list of certificates that an application will accept. When defining a protection setup for the AS/400 HTTP server, you can name one or more validation lists to be checked in order to validate a certificate.

Of course, you could set up your own system to control access, but there should be a compelling reason to do this.

1.5.5 Administering certificates

Users, and their certificates, are ever changing. You must issue certificates to new users, renew expired certificates, refuse certificates that have been revoked, and reissue certificates that need changes. This is an important area and procedures must be designed carefully and enforced. We introduce the issues here, but for a detailed discussion see the redbook *Deploying a Public Key Infrastructure*, SG24-5512.

It is very important that you design and implement the logistics well. If your security system prevents people from doing their normal work, they will collaborate to find ways around the system, and may seriously compromise your system's security in the process. A security system functions best if it is easy and comfortable for people to use.

1.5.5.1 Certificate Revocation Lists (CRLs)

Since certificates are possessed by entities outside of your system you cannot take them back once they have been issued.

A CRL is used to hold a list of revoked certificates that should not be accepted. Generally each CA will maintain and publish a CRL of certificates they have issued that are now revoked.

If you are accepting certificates and using their existence to allow an entity access to a sensitive application, then you will need to check that certificates are still valid before allowing access to an application. To do this you need to check the CRLs of all the CAs from which you trust certificates.

Currently, you can set up jobs to download the various CRLs on a daily or weekly basis and combine them into a single list that can be easily checked. The structure of CRLs is very simple, so it would not be difficult to combine them. However, checking the combined list would have to be done by your application, or by a common application gateway. At V4R4 there is no built-in support for checking CRLs, nor can you combine the CRLs into a list and have the HTTP server validate the client certificate.

1.5.5.2 Issuing certificates

You must consider the process for issuing certificates to new users so that it can be done in a timely manner that does not prevent them from working. You must also consider what information is to appear on the certificate, how it will be used, and how it will be validated and by whom. This is particularly important if you are going to use the contents of a certificate to control access to applications. If you are using certificates only for identification, the above considerations are less important; however, you must then consider how you will handle the logistics of controlling access to applications.

1.5.5.3 Storing certificates

If you use certificates to identify users within your company you will need to consider how to store, back up, and secure them. Storing certificates on a PC ties a person to one PC and if the PC is unavailable, the person cannot access her certificate. You might want to store certificates on a local file server, so that they are accessible to the people who need them - but not to everyone. When laptops are used you will need to export copies of the user's certificates to her laptop. In all cases you should try to make sure that users secure the certificates with a non-trivial password. You may also consider exporting copies of certificates to a secure repository in case people lose their certificates or forget the passwords needed to unlock it.

1.5.5.4 Renewing certificates

All certificates must have an expiration date. When this date has passed the certificate becomes unusable. When this happens, you have to replace your CA, server, and user certificates with new ones.

The well-known CA certificates have long lifetimes and are replaced well in advance of their expiration. As long as users keep their browsers reasonably up to date they should have no problems. On the AS/400 as long as you keep your operating system up to date you should have copies of the certificates of the well-known CAs. However you have to manually ensure that the correct applications trust the new certificates. This should be done on a regular basis, at least every six months.

If you create your own CA and use it to issue certificates you should ensure the CA certificate has a much longer lifetime than the certificates it signs. This allows you to switch to a new CA certificate well before the old one expires. It also ensures that all certificates issued by the old CA will expire before the old CA certificate expires.

If you are using a server certificate from a well-known CA, there is no problem with simply swapping it for a new certificate the CA has issued. This is because the CA ensures their CA certificate always expires later than the certificates it has signed.

If you are using your own CA to create and sign server certificates, there should be no problem with swapping an old certificate for a new one signed by the same CA certificate. However, when you create a new CA certificate and switch to using a server certificate signed by the new CA certificate, entities accessing your system will need to obtain a copy of the new CA certificate.

Replacing user certificates should be done before the certificate expires. If there are mechanisms to control the applications a certificate has access to, the access authorities of the old certificate must be copied to the new certificate. If you have a repository holding a list of entities and their public keys, this must be updated. If entities have distributed their public key to other entities to use when sending them encrypted documents, the new public key must be sent.

You will probably need to set up some reminder system to ensure that the various tasks are done at the correct times. To give an example, the CA should be valid for at least twice as long as the certificates that it issues, and the CA should stop issuing certificates when it is half way to its expiration date. This would mean a certificate issued on the last day that the CA is used to issue certificates would still expire before the CA does. DCM attempts to help with this by decreasing the time that its issued certificates are valid - since less time is left for the CA to be valid, certificates are issued for a smaller validity period.

1.5.5.5 Changing existing certificates

This is essentially the same as replacing a certificate when it expires. The only difference is likely to be that the urgency is much greater. This is particularly so if the certificate contents, such as company and division, are being used to control access to applications.

1.5.5.6 Using certificates to directly control access to applications

We do not recommend using the existence of a certificate, or the attributes on a certificate, such as company and division, to control access to sensitive applications, because:

- A field in a certificate might not be validated. Being able to use the private key for a certificate verifies that the certificate belongs to whomever presented it, but does not verify that all fields in the certificate are validated or even that the organization name was entered with the same punctuation or abbreviations as one might expect.
- Validating and creating certificates may take time, particularly if you are using another company, such as VeriSign. This could prevent users from working, for example, when their job role has changed and they need a new or changed certificate to gain proper access to applications.
- Working with CRLs is complex and seldom immediate. This makes it difficult to keep your system secure if you want to prevent entities accessing applications they have had access to.
- Using the contents of one certificate may be good to manage access to one application. But when developing more, or changing applications, you probably have to change all user certificates again.

For sensitive applications it is more sensible to use certificates for identification only. Use associated user profiles or validation lists for controlling access to applications.

1.6 Summary

Provided the following is true, digital certificates can be used to set up a friendly system to authenticate users and to secure transmitted data:

- The Certificate Authority must be trustworthy.
- The information given when a certificate is requested must have been verified. Certificates have to be issued only to entities that are trustworthy for the functions the certificate will authorize them to.
- The private key must have been distributed in a secure manner if this is needed to be done.
- The private key must have been kept secure:
  - Using a password
  - Using a smart card and PIN
  - When unlocked at a workstation, the workstation must have been kept secure.
- The CA must be promptly informed of lost, compromised, or unwanted certificates.
- The CA must immediately update its CRL whenever informed of a compromised, lost, or unwanted certificate.
- Servers must consult an up-to-date copy of the CRL before accepting a certificate as valid.
- The rest of the business infrastructure, physical security, procedures, and people must all be secure.
- The length of the keys used in the certificate must be long enough to deter attack.
- Most of the potential exposures are procedural and must be addressed when designing the system.

People must be properly trained, so they understand the need for security and what they need to do. The procedures implemented must be easy to follow and convenient so that people have no reason not to use them.

Chapter 2. Secured Sockets Layer protocol overview

This chapter introduces the Secure Sockets Layer (SSL) protocol. SSL is commonly used to secure communication between TCP/IP applications, such as HTTP and Telnet.

2.1 Overview

The explosive growth of the Internet and its increasing use for commerce has meant that more and more information is being being sent that is either confidential or must not be changed. The Internet as an open network has had some facilities for protecting data, but they did not meet the security requirements for modern data communication. Hence there was a demand for developing a protocol for secured communications over an IP-based network.

Cryptographic protection is needed to protect data from being read while in transit. Because of the number of parties communicating across the Internet it is impractical to have to securely exchange code books or any other shared secrets in advance of starting secure communications. A method is needed that can establish secure communications immediately. SSL is the answer.

SSL also ensures protection against modification of the data sent.

Because of the anonymity of the Internet, a method is required to enable parties to authenticate each other so they can be sure with whom they are communicating. SSL provides this function also.

For a protocol like SSL to be useful, it must be widely adopted so that the effort made in setting up systems that use SSL is not wasted. SSL is an open protocol so any company can refer to it and make use of it. SSL has become the de facto security standard for the Internet.

However, applications must be written to support SSL.

2.1.1 History of the SSL protocol

SSL was developed by Netscape and RSA in 1994. Version 1.0 was designed but never implemented in a real product. The protocol was revised and extended to form SSL V2.0. Netscape and RSA implemented this in their products and marketed it in 1995. Soon other vendors started using SSL in their own products. SSL V2.0 became the de facto industry standard and today is widely used in many applications to establish secure connections.

However, SSL V2.0 had some security weaknesses and some missing functionality, such as client authentication. In 1996 Netscape revised the SSL protocol and published SSL V3.0. This fixed some problems found in SSL V2.0 and included extensions such as client authentication and additional methods of enciphering data. Currently some products still support only V2.0. Applications that are using a common function set of Version 2.0 and Version 3.0 can operate with products that only support Version 2.0. But problems can arise if you are designing an application that requires V3.0 functions.

SSL support was originally implemented on the AS/400 system with V4R1.

Note

Netscape has committed to keep its specification open. It has submitted SSL V3.0 as a draft to the Internet Engineering Task Force (IETF), which is working to standardize it. The new standard is called the Transport Layer Security (TLS) protocol. This was recently published as an IETF Internet draft RFC 2246, called the TLS Protocol Version 1.0.

2.1.2 Basic concepts of SSL

The SSL protocol provides an end-to-end encrypted communication session. It is nested between the transport and application layer as shown in Figure 1:

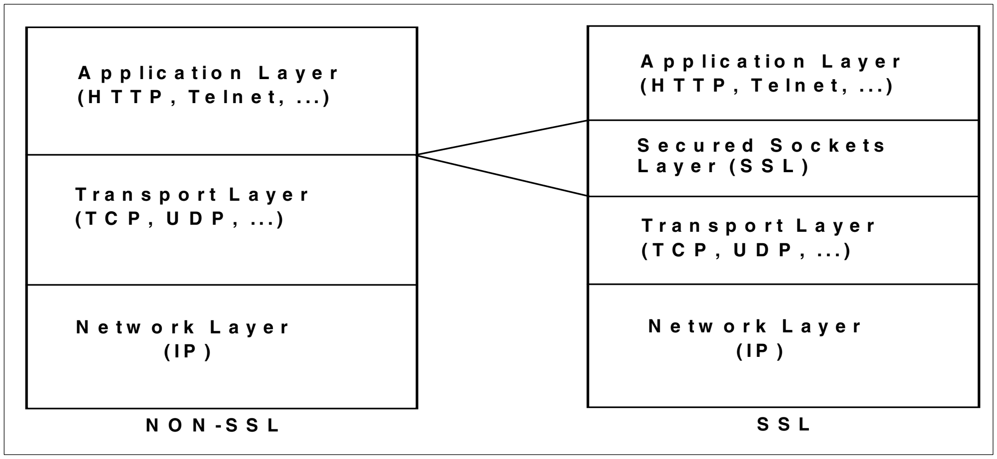


Figure 1. Protocol layers

The SSL protocol supports both reliability and privacy. This is achieved by the following functions:

Data encryption and decryption This is to ensure that no one can read transmitted data that someone might intercept somewhere between the sender and receiver.

Data integrity This is to ensure that no one is able to manipulate transmitted data between the sender and receiver. Message Authentication Codes (MACs) are used so that any changes to data can be detected and rejected.

Authentication This allows each party to verify the identity of the other if required. Digital certificates are used to provide this function. In SSL V2.0, only server authentication is supported. SSL V3.0 supports both server and client authentication. However, these functions are optional.

Actually the SSL protocol is not just a single protocol. Instead it consists of two protocols. These are:

SSL record protocol The SSL record protocol sits on top of the transport layer and is used for encapsulation of various higher-level protocols.

SSL handshake protocol The SSL handshake protocol operates on top of the SSL record layer. It allows the client and server to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol receives or transmits data.

2.2 How certificates are used within the SSL protocol

In this section we explain how certificates are used within the SSL protocol.

- Data encryption and decryption

  A secret key is generated for each session and used to encrypt and decrypt data. Secret keys have much better performance than public/private keys. However, to generate a secret key in a secure manner, the public and private keys in the server's certificate are required. One party, normally the server, sends its certificate to the client first. At this time the server might also request a certificate from the client. Next the client creates the secret key, encrypts it with the other party's public key, and sends the encrypted key back. The first party uses its private key to decrypt the secret key. From then on, the secret key is used because encryption techniques with shared secret keys require much less computation than those using public/private key pairs. The secret key automatically expires after a specific time. The SSL V3.0 draft suggests a maximum lifetime of 24 hours. After the session has expired a complete handshake has to be performed again.

- Data integrity

  To detect any changes to data between the sender and receiver, message digests are used. A message digest is a secure hash that is built from the original data processed with an authentication algorithm, such as MD5 or SHA. The hash itself is encrypted and added to the sent data. When received, the hash can be decrypted and compared with a newly calculated hash. If the two differ, the data has been changed and should be requested again. When possible, public and private keys are used to encrypt the hash since these provide better authentication than symmetric key encryption.

- Authentication

  Each party can use the other's certificate to verify its identity. The SSL protocol has flexibility in this and authentication will only be implemented if it is needed. Authentication allows you to check that the other party's certificate is valid and that it is really the party with whom you are communicating. You may want to build functions into your application to recognize certificates you have received before and treat them differently. You may also want to accept only certificates that have previously been registered.

2.3 SSL handshake

Before data can be sent or received over a connection protected by the SSL protocol, a session must be established. SSL requires a certain method of establishing a secured connection. This method of exchanging specific messages prior to the user session is called the *SSL handshake*. Digital certificates play an important role within the SSL handshake, which has to flow in a predefined order using standard formats.

The handshake protocol is responsible for negotiating a Cipher Spec and generating a shared secret key. The Cipher Spec defines what kind of encryption (for example, DES, RC, RC4) and authentication (for example, MD5, SHA) algorithms can be used for the communication session. Currently there are two versions, Version 2.0 and Version 3.0, of the SSL protocol available, but only Version 3.0 supports client authentication.

Figure 2 shows the flow of the SSL handshake using a server certificate only:

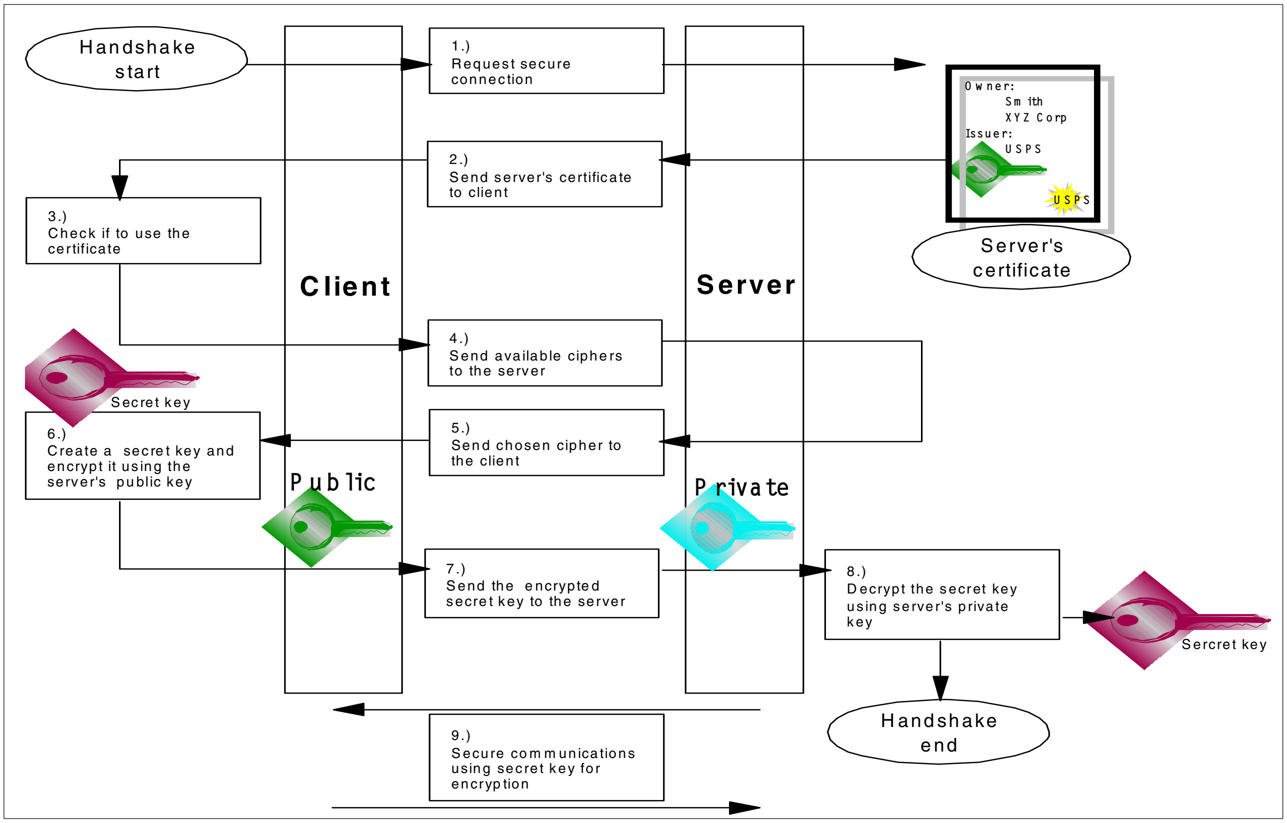

Handshake start
1.) Request secure connection
Owner: Smith XYZ Corp
Issuer: USPS
USPS
Server's certificate
2.) Send server's certificate to client
3.) Check if to use the certificate
Client
Server
4.) Send available ciphers to the server
Secret key
5.) Send chosen cipher to the client
6.) Create a secret key and encrypt it using the server's public key
Public
Private
7.) Send the encrypted secret key to the server
8.) Decrypt the secret key using server's private key
Sercret key
Handshake end
9.) Secure communications using secret key for encryption

Figure 2. SSL handshake with server certificate only

1. The client sends a request to connect to an SSL-enabled server. This is done by sending the request to a specific port used for secure connections. Normally this is the well-known port number for the secure version of the protocol being used. When using HTTP, the request is initiated through the URL starting with *https*. The request is also called the *Client Hello* message. This message is also used to exchange attributes, such as protocol version, session ID, and so on.
2. The server sends back its *Server Hello* message and its certificate.
3. The client checks if the certificate was issued by a CA it trusts. If so it checks that the certificate is valid. If either of these checks fails the client can cancel the connection or choose to proceed without authentication.

4. The client tells the server what ciphers, or types of encryption keys, it can use for communication.
5. The server chooses the strongest common cipher and informs the client about its selection.
6. Using that cipher, the client generates a session key (an encryption key to be used only for this session) and encrypts it using the server's public key.
7. The client sends the encrypted session key to the server.
8. The server receives the session key and decrypts it using its private key.
9. This completes the handshake and henceforth the client and server use the session key to encrypt and decrypt the data they send and receive.

For more information about the SSL protocol and the SSL handshake, refer to the SSL 3.0 Internet draft at `http://www.netscape.com/eng/ssl3/index.html`.

2.4 SSL support on the AS/400 system

Since SSL first became available with OS/400 V4R1, more functions have been added to V4R3 and V4R4. In the meantime, most of the TCP/IP servers on the AS/400 system support SSL V3.0 with server authentication only. The HTTP server for AS/400 supports both client and server authentication. Table 1 shows the SSL capabilities of the AS/400 TCP/IP server applications:

Table 1. SSL capabilities of AS/400 TCP/IP server applications

Server application	**Server Authentication**	**Client Authentication**
Client Access Express (1)	X	
Management Central	X	
DRDA/DDM	X	
Host On-Demand	X	
HTTP Server for AS/400	X	X
Java applications	X	
LDAP	X	
Telnet (2)	X	

(1) Client Access Express allows SSL protection based on single remote connections. User-written applications that use Client Access Express APIs can also be protected by SSL.

(2) Currently the IBM eNetwork Personal Communications product and the 5250 emulation of the Client Access Express product support the configuration for SSL connections.

2.4.1 Requirements for using SSL on the AS/400 system

To use SSL with the AS/400 system, the following license programs must be installed:

- Digital Certificate Manager (DCM), option 34 of OS/400 (5769-SS1)

- TCP/IP Connectivity Utilities for AS/400 (5769-TC1)
- IBM HTTP Server for AS/400 (5769-DG1)
  Even if you do not want to use the IBM HTTP Server for AS/400 as a Web server for your applications, it has to be installed to provide access to the AS/400 Tasks page. This page is the entry point for the Digital Certificate Manager.
- One of the IBM Cryptographic Access Provider products: 5769-AC1 (40-bit), 5769-AC2 (56-bit), or 5769-AC3 (128-bit). The bit size for these products indicates the varying sizes of the digital keys that they are capable of employing during symmetric encryption. A higher bit size generally results in a more secure connection. Export constraints indicate *data encryption key* sizes are the 128-bit (RC2 and RC4), 56-bit (DES), and 40-bit (RC2 and RC4). Key encrypting keys and authentication key sizes are the RSA 2048-bit, 1024-bit,and 512-bit. Keys and key sizes are used by SSL when agreeing on a common cipher suite between the server and the browser. A larger key size does not necessarily mean a higher level of symmetric encryption. A server with AC3 may have a server certificate that has a 1024-bit key, but if the browser supports only 40-bit encryption, 40-bit will be used. A server with AC3 may have a server certificate that has a 512-bit key, but if the browser supports 128-bit encryption, 128-bit will be used. The 5769-ACx products are not in a direct relationship with the browser crypto strength. When creating certificates, the key size (such as 512/1024/2048) has to be selected. Some of these products are not available in all areas due to government export regulations. Currently the IBM Cryptographic Access Provider product 5769-AC3 is available only in the US and Canada.
- If you want to use SSL with any Client Access Express component, including Operations Navigator, you must also install at least one of the AS/400 Client Encryption products: 5769-CE1 (40-bit), 5769-CE2 (56-bit), or 5769-CE3 (128-bit). Client Access Express and Operations Navigator need one of these products to establish a secure connection. As with the Cryptographic Access Provider products, the bit size for these products indicates the varying sizes of the digital keys that they employ for data encryption. Some of these products also are not available in all areas due to government export regulations. If the PC has CE1 (40-bit encryption) and the AS/400 system has AC3 (128-bit encryption), the level of encryption for that PC would be 40-bit. However, another PC could have CE2 (56-bit encryption) installed and that level of encryption between the AS/400 system and PC would be 56-bit. You might use this option for PC users in different countries who are connecting to a central AS/400 to meet the various country import/export requirements.

Note

You do not need to install a Client Encryption Product to use the PC5250 emulator that is shipped with the eNetwork Personal Communications product. Personal Communications has its own built-in encryption code.

2.4.2 Setting up applications to use SSL with certificates

New AS/400 applications by default are not enabled to use SSL. You have to perform several tasks in order to enable SSL with certificates for an application. First of all, the prerequisite license programs must be installed. The following list shows the various steps involved to enable SSL for an AS/400 application:

1. Register the application using the Registration Facility. IBM standard applications, such as Telnet server, DDM server, and so on, are registered automatically. User applications must be registered using the Register Application For Certificate Use (QsyRegisterAppForCertUse, QSYRGAP) API. When registering a user application, the following parameter can be specified, whereby all parameters are optional except the application ID:
   - Application ID
   - Exit program name
   - Application description or message file and message ID for the application description
   - Limit CA certificates trusted
   - Multithreaded job action
   - Threadsafe
2. After the application is registered, you need to use Digital Certificate Manager (DCM) to associate a server certificate with the application. Every time a client requests an SSL session for this particular application, the AS/400 system sends the server certificate that is associated with it back to the requester for server authentication. This allows you to use different server certificates for different server applications.
3. Specify which Certificate Authority the application trusts. If client authentication is on or required, the application trusts only certificates that were issued by CAs that are marked as trusted CAs. You can set which of the available CAs are trusted by the application. If the application does not support client authentication, then this step is not required

How to enable SSL for a user application is covered in Chapter 8, “Sample application: using APIs with ILE RPG” on page 295 and Chapter 9, “Sample application: using certificates in Java” on page 337.

Detailed steps on how to enable SSL with certificates for AS/400 standard applications are shown in Chapter 6, “Enabling SSL on AS/400 standard server applications” on page 187.

Chapter 3. Introducing digital certificate management APIs

The AS/400 system offers a large variety of functions that allow you to install, configure and manage your system. Of course there are situations where standard management functions cannot be used or do not exist. For example, user applications often require special functions. The AS/400 system uses application programming interfaces (APIs) to provide the needed functionality and flexibility for those applications. This chapter introduces AS/400 APIs that can be used to work with digital certificates. It also introduces AS/400 validation lists as they pertain to digital certificates.

3.1 Validation lists

Validation lists were introduced on the AS/400 system with Version 4 Release 1. They have an object type of *VLDL and are used to store data, such as certificates, user names, and passwords.

- The contents of validation lists are case sensitive. This can be important for user names and passwords.
- The HTTP server can refer to validation lists to check for valid Internet users using names and passwords or by using certificates.
- Entries stored on a validation list must have an entry ID (or key) and may have unencrypted data, encrypted data, and additional attributes.
- Accessing validation list entries by entry ID or key is fast.
- Certificates are assigned a 40-byte handle, which is then used as the entry ID, or key, in a validation list.
- Certificate data is encoded in Abstract Syntax Notation 1 Distinguished Encoding Rules (ASN.1 DER) format, and is stored as an additional attribute of the validation list entry.

The HTTP Configuration and Administration utility has some basic options for managing user names and passwords on validation lists and for displaying certificates on validation lists. These are under the category Internet Users on the navigation panel. However, the primary interfaces to validation lists are APIs, except for the commands to create and delete them. We discuss validation lists only as they relate to the use of certificates. For details of all the validation list APIs, see *OS/400 Security APIs V4R4*, SC41-5872.

3.2 Managing digital certificates with APIs

The AS/400 Digital Certificate Manager (DCM) centralizes management functions for digital certificates on the AS/400 system. It can be used to operate your own Certificate Authority (CA), to manage server certificates, or create and register user certificates for AS/400 user profiles. However, if you want to manage client certificates in user applications, you have to use application programming interfaces (APIs). They can be used, for example, to:

- Check for client certificates in validation lists.
- List client certificates.
- Add certificates into validation lists.

- Register applications for certificate use.

See Chapter 8, “Sample application: using APIs with ILE RPG” on page 295 for examples of how APIs may be used to construct an application using certificates to provide security.

Table 2 shows an overview of the available APIs with a brief description of each API. Refer to *OS/400 Security APIs V4R4,* SC41-5872 for detailed information on these APIs.

Table 2. Digital certificate management APIs overview

API name	**OPM name** **ILE name**	**Description**
Add User Certificate	QSYADDUC QsyAddUserCertificate	Associates a certificate with an OS/400 user profile. Note that while a user profile may have many certificates associated with it, each certificate may be associated with only one user profile.
Add Validation List Certificate	QSYADDVC QsyAddVldlCertificate	Adds a certificate to a validation list. Validation lists may have many certificates and certificates may be added to many validation lists.
Check Validation List Certificate	QSYCHKVC QsyCheckVldlCertificate	Checks if a certificate is in a validation list.
Deregister Application for Certificate Use	N/A QsyDeregisterAppForCertUse	Removes an application and all associated certificate information from the registration facility.
Find Certificate User	QSYFNDCU QsyFindCertificateUser	Returns the user profile, if any, that is associated with a given certificate.
Find Validation List Entry	QSYFDVLE QsyFindValidationLstEntry	Given a validation list entry key, returns the validation list entry data and attributes.
Find Validation List Entry Attributes	N/A QsyFindValidationLstEntryAttrs	Finds an entry in a validation list object and the attributes associated with the entry.
Find First Validation List Entry	N/A QsyFindFirstValidationLstEntry	Returns the validation list entry data for the first entry in the list.
Find Next Validation List Entry	N/A QsyFindNextValidationLstEntry	Given a validation list entry key, returns the validation list entry data for the next entry in the list.
List User Certificates	QSYLSTUC QsyListUserCertificates	Creates a list of the certificates associated with a user profile and puts this into a user space.
List Validation List Certificates	QSYLSTVC QsyListVldlCertificates	Creates a list of the certificates in a validation list and puts this into a user space.

API name	OPM name ILE name	Description
Open List of User Certificates	QSYOLUC N/A	Creates a list of the certificates associated with a user profile and returns this in a variable.
Parse Certificate	QSYPARSC QsyParseCertificate	Parses a certificate and returns the internal fields in a variable.
Register Application for Certificate Use	QSYRGAP QsyRegisterAppForCertUse	Registers an application entry with the registration facility. This is a requirement to use SSL for application access.
Remove User Certificate	QSYRMVUC QsyRemoveUserCertificate	Removes the association of a certificate from a user profile.
Remove Validation List Certificate	QSYRMVVC QsyRemoveVldlCertificate	Removes a certificate from a validation list.

Notes

APIs are available for either or both the Original Programming Model (OPM) and Integrated Language Environment (ILE) environments. APIs for OPM have names such as QSYFDVLE. APIs for ILE have names such as QsyRemoveVldlCertificate. See 8.5.2, “Differences between procedures and programs” on page 318 for a discussion of the differences between using OPM and ILE APIs.

3.2.1 API usage scenarios

This section introduces two possible scenarios where APIs can be used to manage and process digital certificates within user applications.

3.2.1.1 Scenario 1: Certificate use in an Internet application

An application is created that will be made generally available from the Internet. Security is important and certificates have been chosen as the means of authenticating users. SSL will be used to secure the communications.

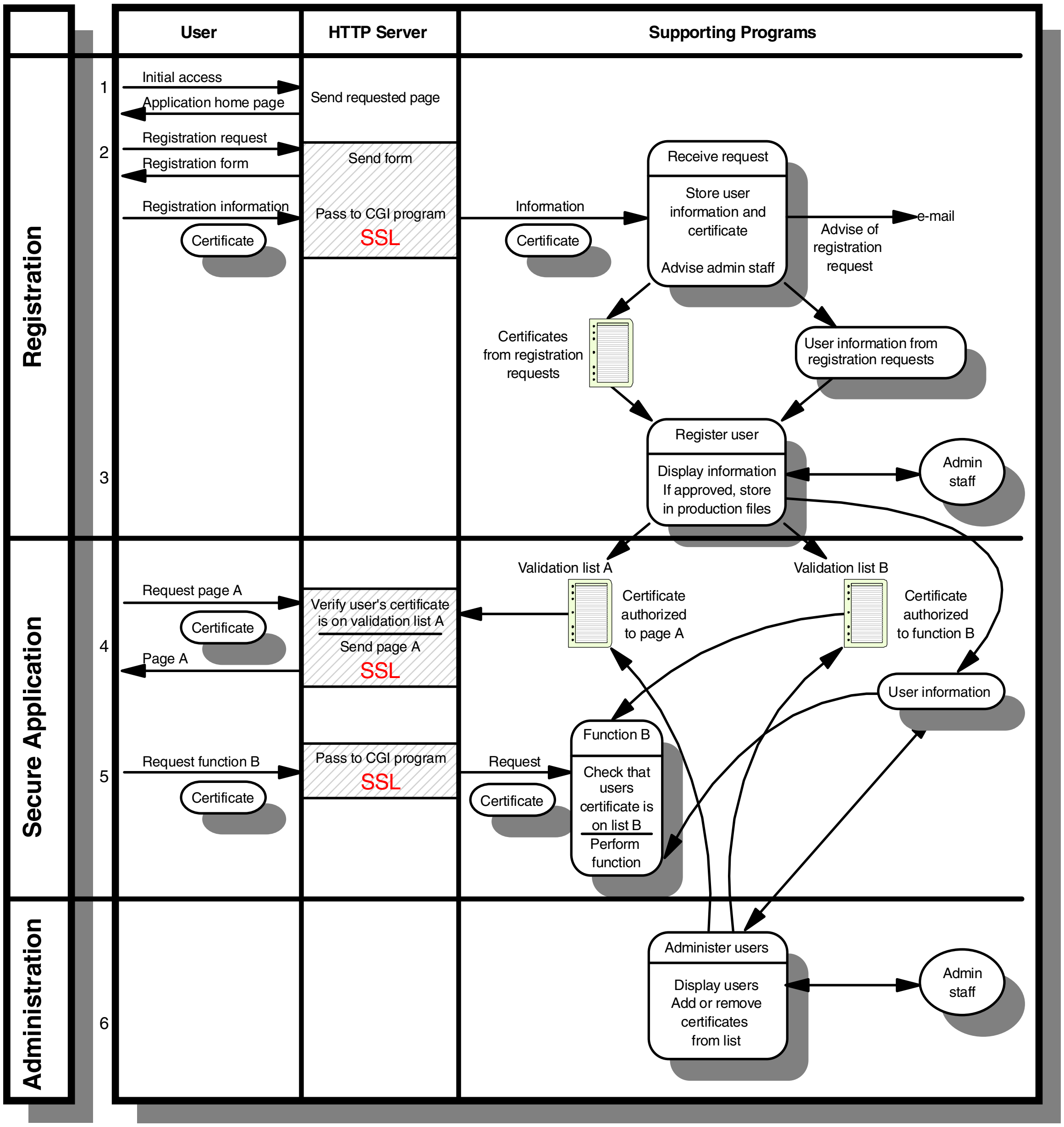


Figure 3. Validation list usage example

1. Initial access

   The home page will be unsecured. From there new users can choose to register and existing users can enter the application. Existing users can also enter the application directly.

2. Registration

   The secure HTTP server will be used to establish an SSL connection. This requires a certificate only on the server. Because the system is to be generally available, the secure HTTP server will use a certificate obtained from a well-known CA. SSL client authentication will be required so that the user will need to present a valid certificate to proceed. If they have no certificate, the application will deny access and the user must obtain a certificate first.

The user requests a registration form that may contain information such as address, phone number, credit card information, and so on, and returns this along with their certificate.

The API QsyParseCertificate would be used to parse a certificate and obtain its contents. However, you can retrieve many certificate values from environment variables when using the HTTP server. In this case you do not need to call the parse API. QsyAddVldlCertificate would be used to add certificates to the validation list holding certificates from registration requests.

3. The user information and certificate are held pending verification by the administration staff. When verified the user will be notified and their information stored in a database in the normal way. Their certificate will be added to a validation list, or lists, corresponding to the applications they are allowed to use.

   The API QSYFDVLE would be used to retrieve a certificate from the validation list holding certificates from registration requests. QsyRemoveVldlCertificate would be used to remove it from this list. QsyAddVldlCertificate would be used to add it to the appropriate production validation lists.

4. Entering the application

   The secure HTTP server is used to establish an SSL connection. Because the system is to be generally available, the HTTP server will use a certificate obtained from a well-known CA.

   The HTTP server can be configured to protect pages based on the user certificates contained in a validation list. This will be used to control access to simple HTML pages.

5. If programs must check a user’s authority to perform a function, they can use the API for checking the existence of the user’s certificate within the appropriate validation list.

   The API QsyCheckVldlCertificate would be used to check if a certificate is on a particular validation list and hence if a client is authorized to the application requested.

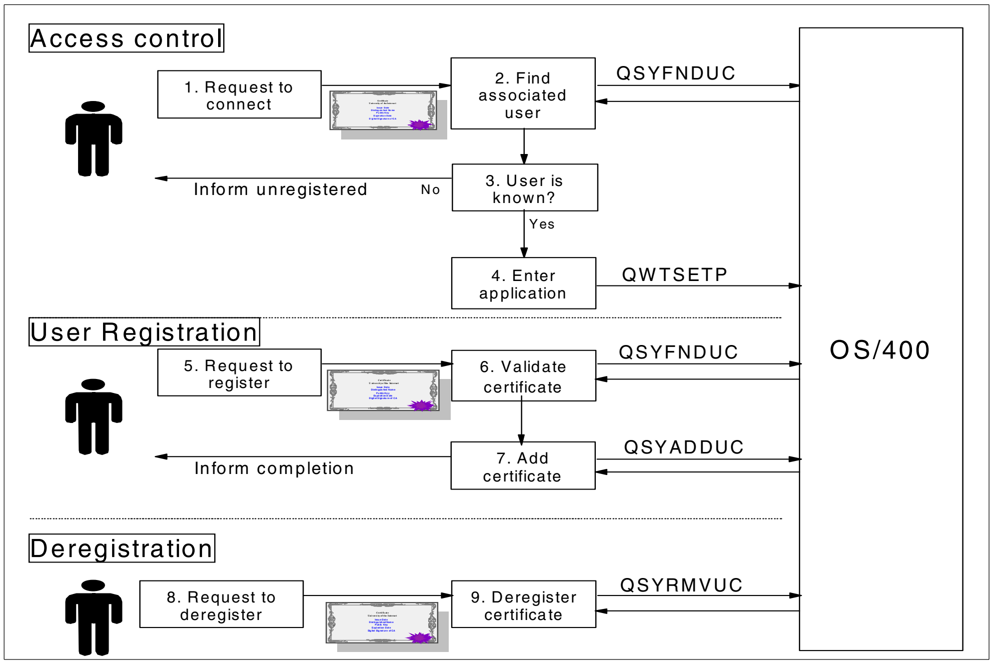
6. User management

   An application will be created to list users and allow authorities to be added or removed as required. This will work from the user details held in the database because database files are more suited to query type functions than the lists created by APIs. However, APIs will be used to add and remove entries from the validation lists used for controlling access.

   The API QSYFDVLE would be used to retrieve a certificate from one of the production validation lists holding certificates. QsyRemoveVldlCertificate would be used to remove it from lists. QsyAddVldlCertificate would be used to add it to lists.

3.2.1.2 Scenario 2: Use within an intranet

A client/server application has been created to run within an intranet of a large company. The communication protocol used between the clients and the server is TCP/IP, using SSL to secure the data. SSL client authentication will be used to determine the users and associate them with an AS/400 user profile. User access to functions will be controlled using the standard AS/400 authority mechanisms. Because the AS/400 security mechanisms are flexible, well understood, and comprehensive this is a very good way of controlling access, particularly if the application has complex authorization requirements.



1. A user connects to the system. A secure SSL connection is established and both server and client authentication are performed.

   Because this is an intranet application the server certificate could be created by the local CA using DCM. In this case the CA's certificate would need to be distributed to all the client devices, or a mechanism created so that it can be sent to the application on the client when the client first connects.

2. The client's certificate is passed to the application, which uses the QSYFNDUC API to check if it is associated with a user profile.

3. If the certificate is not associated with a user profile, or is not acceptable for any other reason, the user is sent an appropriate message and asked to register or take whatever other action is appropriate.

4. The application starts a new thread, or new job, to process the user's requests. The QWTSETP API is used to change the user profile under which the job is running to be the user profile associated with the user's certificate. This API requires a profile handle as an input parameter that can be obtained using the QSYGETPH API. Henceforth the application will have the authorities appropriate to that user profile.

5. A user requests to register. To do this he must provide a certificate and whatever details are required by the application's administrator.

6. The application for processing registration requests notes the information provided and stores this so the administrator can check it. One of the checks is that the certificate is not already associated with a user profile. This can be achieved by using the QSYFNDCU API.

7. If the registration is accepted, the application uses the QSYADDUC API to associate the user's certificate with the appropriate user profile as specified by the administrator. A message is sent to the user informing him that he may now use the application.
8. The user presents his certificate and requests to deregister from the application. This may be the case when the user wants to use a new certificate.
9. The application uses the QSYRMVUC API to remove the association of the certificate with the user profile.

Part 2. Using digital certificates with AS/400 license programs

Chapter 4. Securing the HTTP Server for AS/400

This chapter discusses HTTP server directives that relate to protecting single files or entire directories on the AS/400 system. These directives ensure communication integrity, communication privacy, and client authentication. The focus is on directives that use certificates and these will be discussed in detail. Other directives relevant to the topic will be discussed briefly so you can understand the options available and how they fit together.

We are assuming familiarity with the HTTP server in general and with the concepts of using digital certificates. You should also be familiar with the common directives used in HTTP server configurations.

We are also assuming the HTTP Configuration and Administration utility, not the AS/400 system command `WRKHTTPCFG`, will be used for creating and maintaining server configurations. The HTTP Configuration and Administration utility can be accessed from the AS/400 Tasks page. The utility ensures directives have the correct syntax and are in the correct sequence. With `WRKHTTPCFG`, you enter the directives manually, so the syntax and sequence of the directives are not verified.

The following publications contain further information about the topics covered in this chapter:

HTTP Server for AS/400 Webmaster's Guide V4R4, GC41-5434

Web Programming Guide V4R4, GC41-5435

OS/400 TCP/IP Configuration and Reference V4R4, SC41-5420

4.1 The HTTP Configuration and Administration utility

The HTTP Configuration and Administration utility can be used to configure an HTTP server. The various configurations shown in this chapter are created using the HTTP Configuration and Administration utility.

This utility is started through the AS/400 Tasks page. The following steps show you how to start this utility:

1. Start a Web browser and enter either of the following URLs to access the AS/400 Tasks page:

   `http://as400name:2001/`

   The port number 2001 is used to access the AS/400 HTTP *ADMIN server instance with the HTTP protocol. The URL value `as400name` represents the AS/400 host name or IP address.

   `https://as400name:2010/`

   The port number 2010 is used to connect to the secured (SSL) port of the HTTP *ADMIN server instance. Prior to use the SSL port for accessing the AS/400 Tasks page, you have to enable SSL for this server instance.

   Ensure that the ADMIN server instance is up and running. With OS/400 V4R4 the ADMIN server instance is running under the QHTTPSVR subsystem. You can also use the `NETSTAT *CNN` command to verify that at least port 2001 is in the Listen state.

2. When prompted, enter the user profile and password.
3. On the AS/400 Tasks page click **IBM HTTP Server for AS/400**.
4. On the IBM HTTP Server for AS/400 page click **Configuration and Administration** to start the HTTP Configuration and Administration utility.

4.2 Planning the security setup for the HTTP Server

Before you start to configure protection setups for your HTTP server, you have to designate the level of protection you need to secure your application resources. This level depends basically on the type of application you are planning to run on your HTTP server. The planning process involves the following steps to be performed:

1. Identify the URL to protect

   The design of the application directory structure is essential for setting up the URL protection. A good structure of the application directory paths can simplify the protection setup. Always put resources related to a single application in one directory. An example of a good directory structure would be:

   ```
   /webserver/public/appl1
   /webserver/public/appl2
   /webserver/private/appl3/dtagrp1
   /webserver/private/appl3/dtagrp2
   /webserver/private/appl4
   ```

   The previous example shows a flat (horizontal) directory structure. All applications are kept separate, which allows you to easily configure a protection setup for all or each individual application. A separate pass directive should be used for each application directory. Also use the pass or map directives to hide the directory structure as much as possible.

   The following example shows a vertical directory structure that makes the protection setup more difficult and should, if possible, not being used:

   ```
   /webserver/public/appl1/appl2
   /webserver/private/appl3/dtagrp1/dtagrp2
   ```

   In the previous example you would have to use multiple pass directives to protect the various subdirectories of, for example, the appl3 directory. It would also be necessary to put the pass directives in a certain order to achieve the desired level of protection.

2. Select a security model

   You have to select the proper security model for protecting application resources on the AS/400 system. To decide what model to choose, you may have to examine what the application does. For example, if you run the company payroll application, you will allow access only to those users that have an AS/400 user profile on the server system, and access is restricted to intranet users only. But if you run an online order application, you have to open the access to the Internet as well and allow registered Internet users access to it. So, the selection is driven by the application and is based on the following criteria:

   a. Who is allowed to access the application?

   - Users that have a user profile on the AS/400 system on which the application is running on.
   - Users that are registered as Internet users. In this case the user does not have an AS/400 user profile, but is registered in an AS/400 validation list.
   - All users have access to the application, so that no users need to be registered at all.

   b. Where are users allowed to access the application from?

   - From the intranet.
   - From the Internet.
   - From both the intranet and Internet.

3. If you are hosting a public Internet application, you do not have to restrict application access to certain users. But we suggest that you run the HTTP server under a certain user profile. By default, the HTTP server uses the QTMHHTTP or QTMHHTP1 user profile to access the application data. Running an HTTP server under a specific application user profile allows you to restrict access to only the data that is related to this particular application. Refer to 4.4, "AS/400 system authorities" on page 39 for further information about using different user profiles for different applications.

4. If you need to limit access to intranet or extranet applications, you have to determine how to identify and authenticate users. You have three choices to authenticate and identify users:

   a. The basic authentication scheme, which uses a user ID and password to authenticate a user. Using this method, the browser prompts the client user to enter a valid user ID and a password to gain access to the application. Based on the HTTP server configuration, the user ID can be a real AS/400 user profile or an Internet user name that is registered in a validation list.

   b. Using the SSL protocol with client certificates. This method requires the HTTP server to be configured for SSL. You have the choice of making client authentication with digital certificates optional or mandatory. If you choose optional authentication and the client user does not provide a certificate or provides an invalid one, the user is then, based on the configuration, prompted for a user ID and password. If you require a client certificate for authentication and the user fails to present a valid certificate, the access will be rejected. You can also determine which client certificates you will accept:

      1. Valid certificates that are associated with an AS/400 user profile.
      2. Valid certificates that are stored in a validation list.
      3. Valid certificates that match one or more attributes of a certificate, such as the common name (CN), the organization (O), the organizational unit (OU), and so on.
      4. All valid certificates. In this case a user gets access to the application if the Certificate Authority (CA) that issued the client certificate is registered as a trusted root. Also, the certificate must not have expired.

   c. Using an IP address to identify clients. IP addresses are specified on mask subdirectives to limit access to application resources. This method can be used to limit access to browsers from certain IP addresses. In combination with authentication, it limits access to identified users from a specific IP address.

These methods can be used separately or together. For security reasons we do not recommend that you rely solely on the IP address to identify and authenticate users. But in conjunction with one of the other options it may be useful.

Another method to further limit the access to a subset of identified users is using group files. Used on mask subdirectives you can limit access to a group of identified users for certain application resources. Access Control Lists (ACLs) can also be used to restrict access to certain directories or single files within a particular directory. Refer to 4.8, “Access control lists (ACLs) and group files” on page 49 for further information on ACLs and group files.

Based on scenarios, the remaining sections of this chapter show you how to setup the various levels of protection for the HTTP server.

4.3 The request routing directives Map, Pass, Fail, and Exec

All the HTTP server directives shown in this section are used to process Uniform Resource Locator (URL) requests. A URL is a kind of path that can consist, for example of a protocol (for example, HTTP, FTP), a host name, a directory path, a file name, and parameters. For example:

```
http://www.redbooks.ibm.com/abstracts/sg245404.html
```

The request processing directives contain a template. This template is the directory and file name part of the URL, in this example `/abstracts/sg245404.html`. The directory is not necessarily an existing directory. The replacement path, which is another parameter on the request routing directives (except the Fail directive), can be used to map the directory from the URL request to an existing directory. This allows you hide your internal directory structure from the outside world.

When setting up routing directives, try to ensure that only those directories required for serving HTTP can be reached.

Map directives modify URLs received and can be used to hide parts of your directory structure.

Fail directives reject URLs received and can be used to prevent access to parts of your directory structure.

Pass directives accept, and possibly modify, URLs received for HTML pages.

Exec directives accept, and possibly modify, URLs received for CGI-BIN programs.

The request routing directives are executed in the order they appear in the configuration. Generally you will place Fail directives first, then Map directives, and finally Pass and Exec directives. Putting the Fail directives first ensures that a request for which a Fail directive is defined will instantly be declined before processing any other directive. For example, you create a Pass directive that allows access to a directory /webserver/customer/*. Further you create a Fail directive for the URL request /webserver/customer/customer.html that should deny requests for the customer.html page. If you would place the Pass directive first and the Fail directive second and an URL request /webserver/customer/customer.html comes in, the access would be granted. The reason is that the URL request matches the Pass directive and the HTTP server stops processing after the first match. The Fail directive would never work. So it is important to ensure that for every request that should be denied, a proper Fail directive is placed before any other Pass, Map or Exec directives.

Examples

- PASS /*

  On its own `Pass /*` allows access to your entire file system, provided that the user has the required AS/400 object authorities. This could be very dangerous and should never be used on its own or without a proper Map directive. Ensure that you always specify a replacement path on a Pass directive.

  PASS /* /customer/sales/*

  `Exec /*` on its own should not be used for the same reason. The Exec directive allows you to run Common Gateway Interface (CGI) programs.

- It is always advisable to narrow down the routing requests as much as possible. For example, if all the files for serving HTTP are inside `/apps/internet/http`, use one of the following approaches to allow proper access:

  ```
  MAP /* /apps/internet/http/*
  PASS /*
  ```

  or

  ```
  PASS /* /apps/internet/http/*
  ```

  This allows URLs to be of the form Your.DNS.name/file.html instead of Your.DNS.name/apps/internet/http/file.html.

- Consider using FAIL directives to block access to directories and file systems that you know should not be accessed by HTTP. These may not be necessary if your Pass directives are configured correctly, but they will prevent your entire system from being open to the public.

  ```
  FAIL /QSYS.LIB/*
  FAIL /QDLS/*
  FAIL /private/*
  PASS /* /apps/internet/http/*
  ```

- Consider your directory design before starting to implement a system using the HTTP server. Make sure it is simple enough to limit access to the appropriate directories. This will reduce the chance of errors now, and later as you develop your application.

4.4 AS/400 system authorities

The various HTTP directives for protecting directories and files only control access through the HTTP server. You should also put in place AS/400 system authorizations to protect your HTTP server applications from users who can access the AS/400 system in other ways.

When serving static Web pages, the HTTP server runs, by default, under the user profile QTMHHTTP. The user profile QTMHHTP1 is used by default for running CGI programs.You could make this the only user profile, except for the system owner, that can access the directories holding the files used by the HTTP server. However, you can use the Userid directive to change the user profile that the HTTP server uses. This may be useful if you have multiple HTTP instances serving different applications. This allows you to run each server instance under a different user profile. You can also set up directory protection so that URL requests are running under a specific application user profile or the client profile. Normally the user profiles used by the HTTP server should have no password so that they cannot be used to sign on to the AS/400 system.

You can also change the user profile used for specific URLs. This is discussed in more detail in 4.7, “The protection directive” on page 42.

Use a separate directory or library for each group of documents with similar access and authority requirements. This will make it simpler to secure the system later.

4.5 Methods

Methods are the types of functions the HTTP server can perform when processing HTML.The common methods that are relevant to security are:

GET This allows the server to get files and serve them to a client or to call a program and return the output to a client. GET is enabled for the HTTP server by default.

HEAD This allows the server to get an HTML file heading section and serve it to a client. HEAD is enabled by default.

POST This allows data to be sent (posted) to CGI-BIN programs. POST is disabled by default.

PUT This allows the HTTP server to receive files and write them to a directory or library. PUT is disabled by default. The PUT method is used by some programs, such as Netscape Composer, for publishing HTML documents.

DELETE This allows the HTTP server to delete files from a directory or library. DELETE is disabled by default.

PUT and DELETE directives are very rarely used and the IBM HTTP Server for AS/400 has only recently supported them. If you enable these directives, you should be extra careful that only the appropriate directories are accessible. You should use AS/400 system authorities to ensure that only the appropriate files can be replaced or deleted. You may also consider using access control lists as described in 4.8, “Access control lists (ACLs) and group files” on page 49.

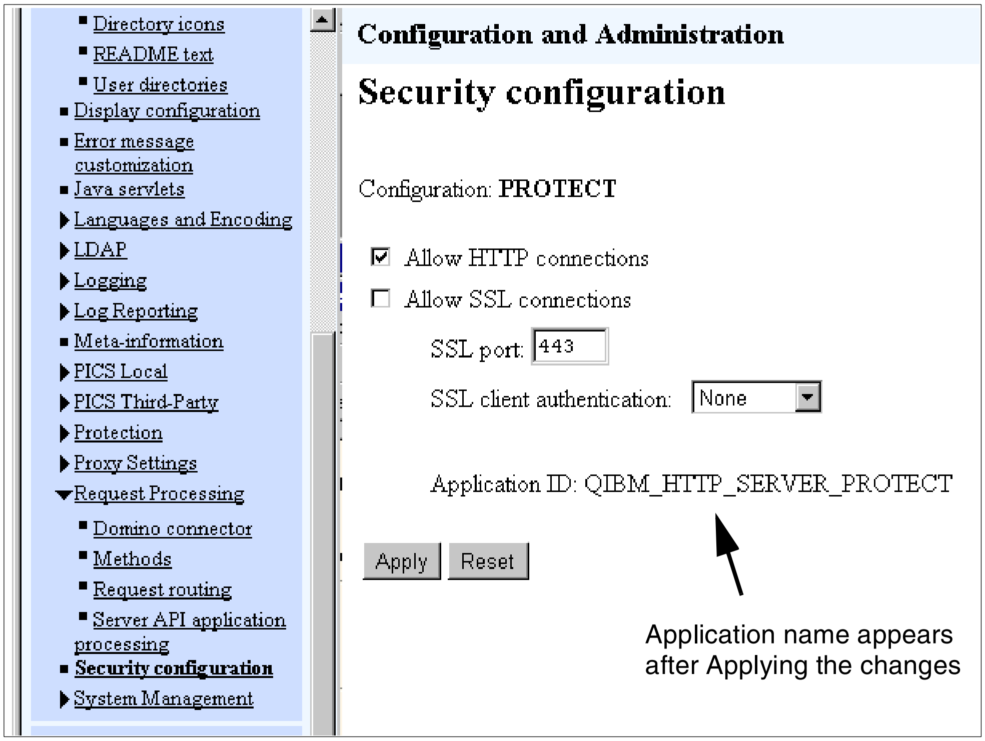
4.6 The Security directives

The Security directives allow you to specify if either normal HTTP requests, SSL requests or both will be accepted and served by an HTTP server instance.

You should use the HTTP Configuration and Administration utility to configure the Security directives rather than using the command `WRKHTTPCFG`. The HTTP

Configuration and Administration utility takes care of all required changes. For example, the utility enrolls your configuration in the DCM so that you can assign a server certificate. The alternative is to create a program to call the API provided to enroll applications in DCM.

To display the security configuration panel start the HTTP Configuration and Administration utility and click **Security configuration** in the navigation panel.



Configuration and Administration

Security configuration

Configuration: **PROTECT**

☑ Allow HTTP connections

□ Allow SSL connections

SSL port: 443

SSL client authentication: None

Application ID: QIBM_HTTP_SERVER_PROTECT

Application name appears after Applying the changes

Figure 4. Security configuration panel

Usually clients initially contact you using HTTP. Later the client may switch to SSL if secure communication is required. This depends on the HTTP server side. So normally HTTP connections are allowed. However, if you use SSL a lot, it may simplify your configuration and security to have one server instance for only HTTP connections and another for only SSL connections. By default, client SSL requests are processed through the well-known port 443. If you are using a different port for SSL, you have to ensure that all URL requests to that server contain the appropriate SSL port.

- When using a single server instance for both HTTP and SSL, a file or directory can be accessed by using either the HTTP or SSL protocol. If you want to ensure that a file or directory is only accessed using SSL with client certificates, SSL client authentication has to be enabled and a protection directive defined. Depending on your directory structure, and the files that require SSL protection, you may need many protection directives.
- If you have one server instance dedicated to HTTP and another for SSL, you can use the request routing directives to ensure each server instance can only access the appropriate files and directories. Using separate server instances and request routing directives are simpler than the protection directives to control whether files can be accessed through the HTTP or SSL protocol.

If you allow SSL connections you can choose that client authentication is not done, is optional, or is required.

- If client authentication is not performed, users do not need certificates to connect to your site. However, the communications can still be protected by SSL and the clients can use the server’s certificate to authenticate the site.
- If client authentication is optional, users will be asked to present a certificate when they first connect to your site. However, certificates given will not be validated and the connection will still be made if they do not give a certificate. If you are using a protection set up with AuthType set to Cert_Or_Basic and the client certificate is, for example not valid, the user gets a password prompt. If this authentication also fails, access will be denied.
- If client authentication is required users must present a valid certificate. Note that expired certificates are not considered valid certificates. Self-signed certificates and certificates issued by a CA that is not trusted are also not considered valid certificates.

If you allow SSL connections and have defined the proper security directive, the application ID of the HTTP server instance appears after you click **Apply**. This application ID is also added to the list of secured applications in DCM, which is required to assign a server certificate to that server instance. Next a server certificate needs to be assigned to the HTTP server instance using the Digital Certificate Manager. An example of this is given in 5.6.1.5, “Associate the certificate with a secure application” on page 155.

Note

Copying an existing configuration that uses SSL does not register the server configuration as a secure application. You must use the HTTP Server's Security Configuration panel, ensure the settings are correct, and click the **Apply** button to do this.

4.7 The protection directive

Protection directives allow you to protect specific URLs. They contain sub-directives that define several security-related functions including client authentication, the user profile to process requests, and the methods that may be used in processing a request.

Protection directives are used to protect files or directories by requiring client authentication of some sort and by restricting the HTTP methods available to certain clients.

4.7.1 Protection directive structure

The first part of the directive is a URL template, for example /private/*. The rules in the protection directive are applied to all URLs that match the template.

Note

Protection directives must be placed before the directives they protect, such as Pass, Exec, or Proxy. The configuration utility does this.

First a URL is compared to the templates on the protection directives. Next Map, Fail and other directives are processed. If the URL is accepted and there was a match on a protection directive, the rules of the directive are applied.

If multiple protection directives match a URL the last matching directive is used.

The second part of the directive is either a pointer to a previously defined protection setup or the rules to be applied. If you are using the same rules for several URL templates it is a good idea to define them just once in a protection setup and then refer the protection directives to it. We recommend that you always use named protection setups. When you create another document protection that requires the same set of rules at a later time, you can simply refer to the named protection setup and do not have to define all rules again.

If a protection directive includes the rules to be applied, it is called an inline, or document-specific, protection directive.

The final part of the directive is optional and is the server's IP address or host name. This can be used to restrict a protection directive to just one of the local interfaces on which the URL request comes in.

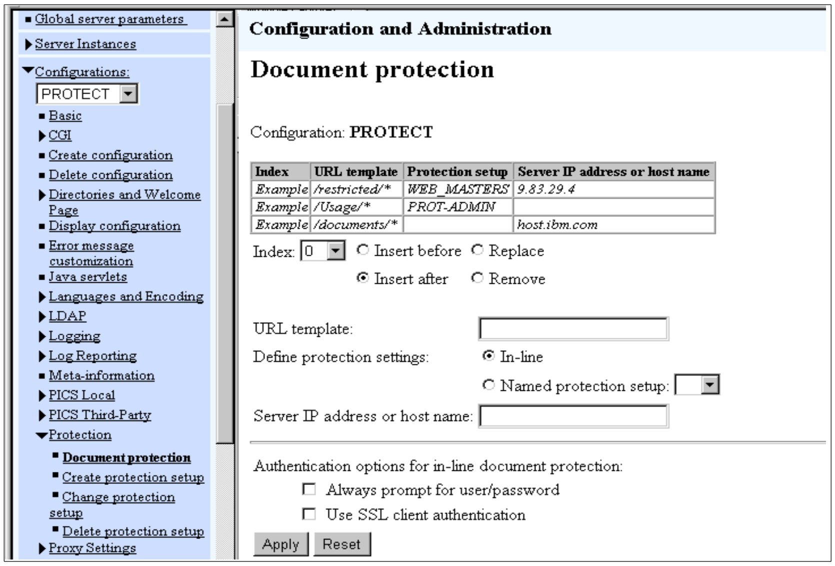
Following is an example of a protection directive:

```
Protect /private/* {
      SSL_ClientAuth client
      ACLOverride Off
      Mask Anybody@(*)
      UserID %%SERVER%%
}
```

4.7.2 Defining an inline protection directive

The Protect directive can be complex. Therefore, we recommend the use of the HTTP Configuration and Administration utility to define your protection directives.

To display the protection directive panels first click **Protection** in the navigation panel. Then click the protection option you want, in this case **Document protection**.



Configuration and Administration

Document protection

Configuration: PROTECT

Index	URL template	Protection setup	Server IP address or host name
Example	*/restricted/**	*WEB_MASTERS*	*9.83.29.4*
Example	*/Usage/**	*PROT-ADMIN*	
Example	*/documents/**		*host.ibm.com*

Index: 0 ○ Insert before ○ Replace

● Insert after ○ Remove

URL template:

Define protection settings: ● In-line

○ Named protection setup:

Server IP address or host name:

Authentication options for in-line document protection:

□ Always prompt for user/password

□ Use SSL client authentication

Figure 5. Document protection window

This displays three examples of protection setups and any protection setups you have created. You can chose to replace or remove an existing protection setup, or you can create a new protection directive. If you create a new protection setup you must specify the index position to control where the new protection setup is inserted in relation to other ones that already exist.

Note

If you are using the HTTP Configuration and Administration utility to make major changes in a protection directive it is safest to first remove the directive and then insert it again. When we were testing and used the Replace option sometimes parts of the old directive did not get removed properly and caused confusing problems.

Provide the URL template for the directory or files that are protected by this protection directive.

You can choose to define all the protection options to be used by the Protect directive or refer to a named *protection setup* if you have previously defined one. In this case there is no further configuration to do. Named protection setups are discussed in 4.7.3, “Named protection setups” on page 48.

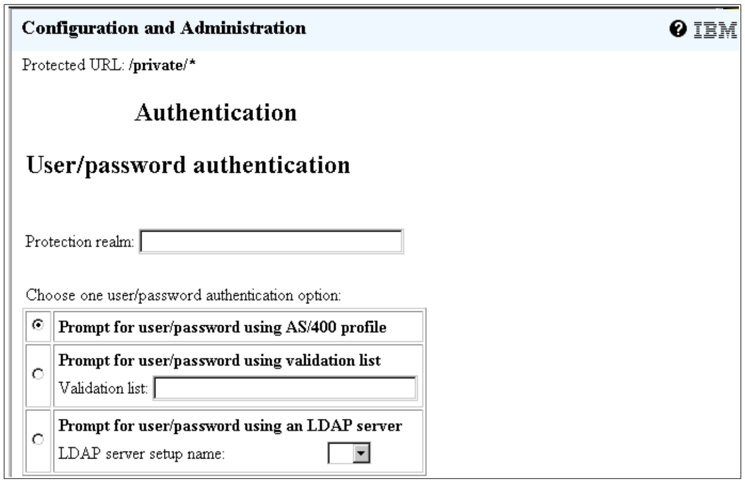
You can specify the server IP address or host name of a local IP interface. In this case the Protect directive will be activated only by URLs that come from this interface. This, for example, is useful when you want to protect directories only from Internet users but do not want protection for intranet users.

4.7.2.1 Authentication options

The options **Always prompt for user and password** and **Use SSL client authentication** as shown in Figure 5 on page 44 allow you to control how clients are authenticated. You can choose either or both of these.

User name and password

If you select **Always prompt for user and password** then when the Protect directive is activated the client will see a prompt asking for a user name and password. When you click **Apply** in the window shown in Figure 5 on page 44 you see the following window:



Configuration and Administration

Protected URL: **/private/***

Authentication

User/password authentication

Protection realm:

Choose one user/password authentication option:

● **Prompt for user/password using AS/400 profile**

○ **Prompt for user/password using validation list**
Validation list:

○ **Prompt for user/password using an LDAP server**
LDAP server setup name:

Figure 6. User/Password authentication

Whatever you type in the Protection realm field is the name that will appear on the title of the prompt displayed to the user.

Note

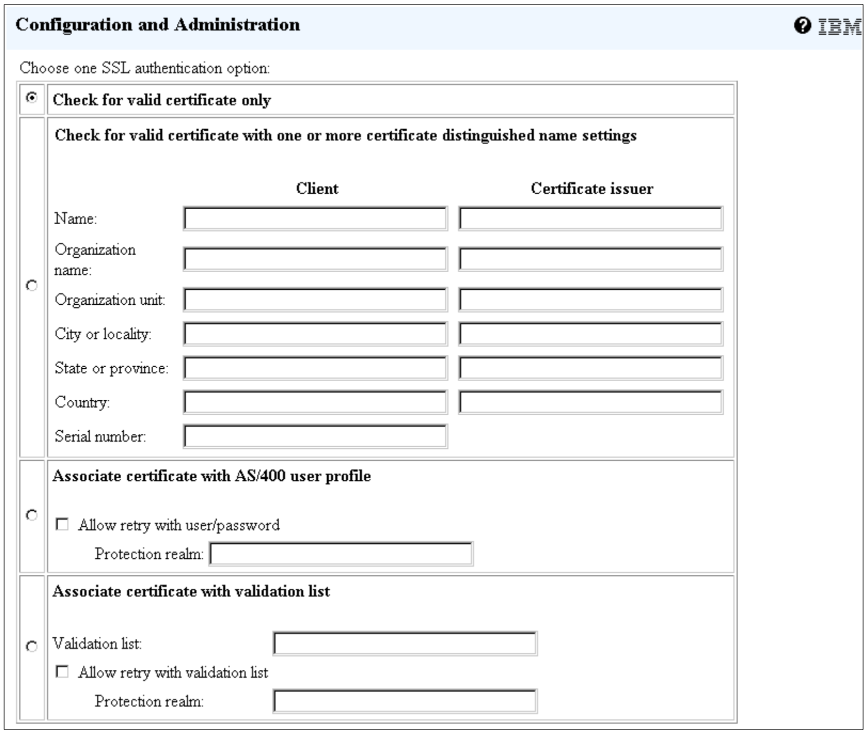
Only one word is displayed. The HTTP server configuration utility allows you to enter several words for the realm. But only the first word is displayed. To show a realm composed of several words, the words need to be connected. Using underscores is one way to do it. For example Order_inquiry_login. If you defined a realm using spaces between words, the configuration using the `WRKHTTPCFG` command shows the appropriate Server_ID statement in error.

You can choose whether to require AS/400 user profile, validation list entry, or LDAP user names and passwords to authenticate users.

Using an AS/400 user profile has the advantage that you can exploit the authority that has been given to it. Validation lists may be useful for clients coming from the Internet, where there is no reason to create a new user profile for each client. LDAP directories allow you to consolidate directories for several systems onto one server. Later we will give examples of using user profiles and of using validation lists. Validation lists and LDAP provide some advantages when defining Internet users on more than one system. However, LDAP directories are outside the scope of this book.

SSL client authentication

If you select **Use SSL client authentication** then you must have enabled SSL processing and specified that client authentication is required or optional. These are described in 4.6, “The Security directives” on page 40. When you click **Apply** you see the following panel.



Configuration and Administration

Choose one SSL authentication option:

● **Check for valid certificate only**

○ **Check for valid certificate with one or more certificate distinguished name settings**

	Client	Certificate issuer
Name:		
Organization name:		
Organization unit:		
City or locality:		
State or province:		
Country:		
Serial number:		

○ **Associate certificate with AS/400 user profile**

□ Allow retry with user/password

Protection realm:

○ **Associate certificate with validation list**

Validation list:

□ Allow retry with validation list

Protection realm:

Figure 7. SSL client authentication

Select **Check for valid certificate only** if possession of a valid certificate is all that is required to grant access. The actual request for the certificate occurs when SSL is first initiated, so all we are really doing is ensuring that SSL is used to access the files protected by this Protect directive.

Note

If SSL is enabled but client authentication is turned off in the server security directives, then the SSL client authentication options in the Protect directive have no effect. No error messages appear and no protection is in place. Testing is the only way to ensure that no problems such as this one exist in your system.

Select **Check for valid certificate with one or more certificate distinguished name settings** when you want to use some of the certificate attributes to control access to the files protected by this Protect directive. For example you may want to accept only certificates issued by your CA with the client's organizational unit "Human resources". The value specified here must exactly match the value in the certificate, including upper and lower case characters.

Select **Associate certificate with AS/400 user profile** when you want to accept only certificates that are associated with AS/400 user profiles. You can use this to restrict the certificates accepted to only those you have previously registered and associated with a user profile. You can also exploit the authorities on user profiles to control the parts of the application that the clients can access. See 5.8, "Working with user certificates in DCM" on page 175 for information on registering client certificates and issuing new certificates for clients.

- You can choose to prompt for a user name and password if the client's certificate is not associated with an AS/400 user profile. In this case you should also give the protection realm, for example the name to appear on the prompt for name and password the client will see.

Select **Associate certificate with validation list** when you want to accept only certificates that are present in a validation list.

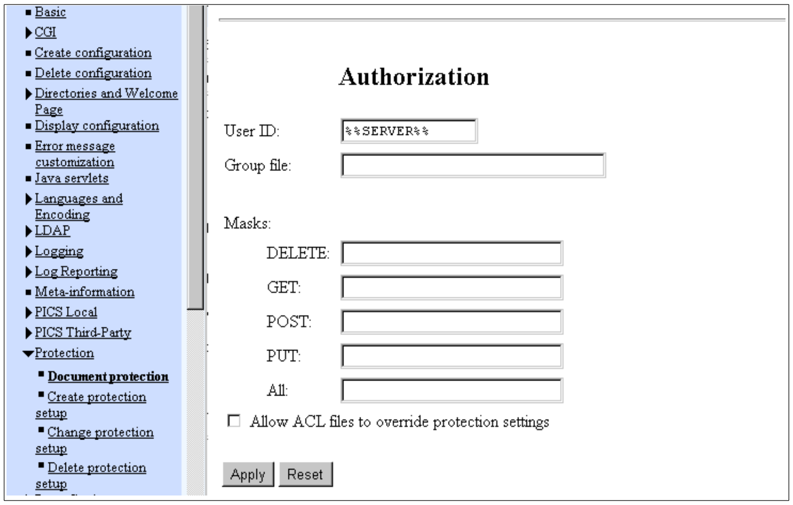
- You must name the validation list, or several lists separated by commas, to be checked.
- You can choose to prompt for a user name and password if the client's certificate is not in the specified validation lists. The same lists will be checked for the user name and password. In this case you should also give the protection realm, for example the name to appear on the prompt for name and password the client will see.

Both User/password and SSL client authentication

You can select both to prompt for a user name and password and to do SSL client authentication. In this case the User/password options all appear and the SSL options to check for a valid certificate only and to check distinguished name settings appear.

4.7.2.2 Authorization options

Further down the window of the client authentication options, shown in Figure 6 on page 45 and Figure 7 on page 46, are more options that allow you to control the methods that can be performed on a specific URL.



Authorization

User ID: %%SERVER%%

Group file:

Masks:

DELETE:

GET:

POST:

PUT:

All:

□ Allow ACL files to override protection settings

Figure 8. Protect directive authorization options

User ID

Completing the User ID field allows you to specify the user profile that will be used to process the request. That means, if the HTTP server receives a request where the URL template matches this particular Protect directive, the process user profile is switched to the user ID specified in this parameter. All further authority checks are performed using this user ID.

- The default is %%SERVER%%, which means the user profile that is running the HTTP server job is used. By default this is QTMHHTTP.

- You can specify a specific user profile name of an existing AS/400 user profile.
- If you are using AS/400 user profiles for authentication then you can specify %%CLIENT%% to use the client's user profile, either from the user name given or from the user profile associated with their certificate. By using this option you can exploit existing AS/400 authorization schemes to control access to your files.

Group file

The Group file field is optional. You can name a file that has entries grouping users by name or by location. The groups defined can then be used to mask access methods or by an access control list. Group files and access control lists are discussed in more detail in 4.8, "Access control lists (ACLs) and group files" on page 49.

Masks

The masks subdirective is used to control certain HTTP requests, such as GET, POST, DELETE or against ALL methods. This allows you to restrict specific methods to, for example, certain users. You can directly enter names and locations or you can use groups defined in the group file.

Allow ACL files to override protection settings

Access control lists (ACLs) are used to limit access to specific files. ACLs can be used to process requests for specific files differently from other files in the same directory. They can also be used to allow a Web administrator to delegate authorization to a non-Web administrator. They contain information about the files that can be accessed, the methods that can be used, and the users to which this applies. ACLs are discussed in 4.8, "Access control lists (ACLs) and group files" on page 49.

Normally the mask rules in a Protect directive are applied and then the rules in an ACL, if one is present, are also applied. If you choose to allow ACL files to override protection settings, and an ACL is present, the mask rules in the Protect directive are ignored, and only the ACL rules are applied.

4.7.3 Named protection setups

A named protection setup has the same options as the previously discussed inline Protect directive. However, instead of specifying a URL template, it is given a name. Using this approach, Protect directives can refer to the setup by name instead of repeating the options.

Figure 9 is an example of a named protection setup and a Protect directive that refers to it.

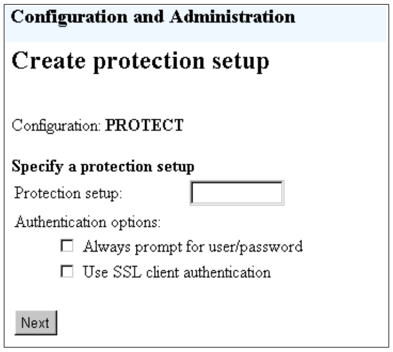
```
Protection CERTAU {
      PasswdFile %%SYSTEM%%
      ACLOverride Off
      DeleteMask All@(*)
      PostMask All@(*)
      PutMask All@(*)
      GetMask All@(*)
      AuthType Cert_Or_Basic
      ServerID CERTAU_Retry
      UserID %%SERVER%%
}
.
.
.Protect /certau/* CERTAU
```

Figure 9. Named protection setup

To create a named protection setup perform the following steps:

1. Start the HTTP Configuration and Administration utility.
2. Click **Protection** to expand its options.
3. Click **Create protection setup** in the navigation panel under **Protection**. The following configuration window appears. Give the protection setup name, select the desired authentication option and click **Next.**

.



Configuration and Administration

Create protection setup

Configuration: **PROTECT**

Specify a protection setup

Protection setup:

Authentication options:

□ Always prompt for user/password

□ Use SSL client authentication

Figure 10. Named protection setup

The same configuration options appear and must be completed as when you configure an inline protection as shown in 4.7.2, “Defining an inline protection directive” on page 43.

4.8 Access control lists (ACLs) and group files

Group file

A group file is a file that defines groups of users in the format group-name:users.

Group-name can be any name.

Users is a list of user entries separated by commas.

Each user entry can be a user name, an IP address template such as 172.16.24.*, or a group name already defined in the file.

Any user names given must exist either as an AS/400 user profile or a user in a validation list or LDAP directory that is used for authentication.

Group files are used to define groups of users with similar authorities. Protection directives and ACLs can then refer to the group name instead of having to list all the users. A sample scenario of using group files is shown in 4.20.4, “Using a group file” on page 100.

Note

Group files are cached by the AS/400 HTTP server. If you change a group file’s contents you must restart any HTTP server instance for your changes to become effective.

Access control lists

An access control list (ACL) is a list of rules defining the methods specified users may use on specified files.

ACLs can be used only in the "Root" (/) file system, QLanSrvr, QOpenSys, and QDLS.

ACLs are held in files named www_acl. When the HTTP server is accessing a file, and a protection setup has been activated, and an ACL is present in the same directory as the file, then the ACL will be processed.

Normally, first the rules that limit usable methods in the Protect directive, are applied. After the Protect directive rules are applied, the rules in the ACL are processed. However, a protection setup can specify that if an ACL is present, only the rules in the ACL are to be applied.

An ACL contains a list of entries of the format:

File : Methods : Users

File Defines a full file name or a template containing a wildcard character *.

Methods Specifies an HTTP request method name or several request method names separated by commas.

Users Defines a list of user entries.
Each user entry can be a user name, an IP address template such as 172.16.24.*, or a group name from the group file named in the Protect directive.
Any user names given must be present in the directory used for user authentication by the Protect directive, AS/400 user profiles, or validation lists, or an LDAP directory.

We do not recommend using ACLs if you can achieve the same result using AS/400 system authorities or validation lists.

- It is best to make your controls visible, but in as few places as possible.
- ACLs are not very visible. This could cause some hard-to-find problems, especially for novice users who might not know that ACLs even exist.
- If an ACL is somehow deleted, the system will continue to work without the necessary protection. Detecting a missing ACL takes considerable time.

- If you have multiple directories that are accessible through HTTP servers, you will need multiple ACLs. However, this increases administration effort as well as the likelihood of errors.
- ACLs protect files only from access through the HTTP server. AS/400 system authorities can protect files regardless of how they are accessed.

An example of using a group file and an ACL is given in 4.20, “Scenario 6: Using an access control list and a group file” on page 95.

> **Note**
>
> - User names in validation lists can include spaces and other special characters. We have tried *, !, and), and these work without problems. However, when we tried a group file that included user names with spaces, the group file did not load properly.
>
>   This problem has been fixed with the following PTFs:
>
> | | |
> |---|---|
> | VRM430 | SF57103 |
> | VRM440 | SF58303 |
>
> - If you are using ACLs, then your default HTTP server job user profile needs at least read authority to all directories that contain ACLs. This may be changed in the future, so that the HTTP server switches the user to the user profile specified in the UserID directive.

4.9 Case sensitivity

A very important subject when designing your HTTP server setup is the case sensitivity of server directives, such as Pass, Map, Protect, and so on. Originally the AS/400 HTTP server processed URLs in a case-sensitive manner.

Sometimes it was not desirable to process requests in a case-sensitive manner. Therefore, new PTFs were released in the second half of 1999 to disable the case sensitivity. The PTFs for the various releases are:

SF58363	VRM410
SF58331	VRM420
SF58140	VRM430
SF58236	VRM440

Uppercase and lowercase letters are now treated equally. For example, uppercase ’M’ is equal to lowercase ’m’.

4.9.1 Possible incompatibilities you may see

So, what does that mean to you? Well, most likely, nothing. But there are some subtle incompatibilities that this may introduce. The best way to illustrate this is with an example using the following configuration file directives (just the Protect and some request routing directives are shown):

```
Protect /WWW/PRIVATE.HTML Default
Protect /Case/Private.html Default
Protect /CGI-BIN/PRIVATE Default
```

```
Pass /WWW/* /MYDIR/*
Pass /Case/* /QOpenSys/*
Map /CGI-BIN/* /QSYS.LIB/QSYSCGI.LIB/*.PGM
Exec /QSYS.LIB/QSYSCGI.LIB/*
```

Users of this example would see the following differences:

1. If you use case-insensitive file systems, your Web users will be able to reach your URLs independent of the case of the URL they enter on their browser. So, if you had a file named /MYDIR/WELCOME.HTML in the root file system (which is case insensitive), and they entered http://mysite.com/www/Welcome.html, they would have seen error 403 (forbidden by rule). With this change, they will now see the welcome page. So, they will now get the document you would likely want them to see anyway.
2. If you use case-sensitive file systems such as QOpenSys, the case sensitivity of the file name still matters to the file system, but the case of the URL will no longer matter. So if you had a file named /QOpenSys/Welcome.html in QOpenSys file system, which is case sensitive, and they entered http://mysite.com/CASE/WELCOME.HTML, they would have seen error 403 (forbidden by rule). With this change, they will now see error 404 (not found). This may mean that you will get questions on why they are seeing something different.
3. For your CGI programs, including Net.Data (which is a CGI program), your Web users will be able to run your CGI programs independent of the case of the URL they enter on their browser. So, if you had a program in the QSYSCGI library named PUBLIC, and they entered /cgi-bin/public, they would have seen error 403 (forbidden by rule). With this change, they will now be able to run the CGI program. This is probably what you want to happen.

In the following you see what happens to the protected resource in the example:

1. If you use case-insensitive file systems, your Web users will be able to reach your URLs independent of the case of the URL they enter on their browser. So, if you had a file named /MYDIR/PRIVATE.HTML in the root file system (which is case insensitive), and they entered http://mysite.com/www/Welcome.html, they would have seen error 403 (forbidden by rule). With this change, they will now be prompted for authentication (based on your protection setup). So, if they enter the correct authentication information, they will now get the document you would likely want them to see.
2. If you use case-sensitive file systems (such as QOpenSys), the case sensitivity of the file name still matters to the file system, but the case of the URL will no longer matter. So if you had a file named /QOpenSys/Private.html in the QOpenSys file system (which is case sensitive), and they entered http://mysite.com/Case/PRIVATE.HTML, they would have seen error 403 (forbidden by rule). With this change, this will now be prompted for authentication (based on your protection setup). And then assuming they enter the correct authentication information, they will now see error 404 (not found). This may mean that you will get questions on why they are seeing something different.

   However, if you did have a file named /QOpenSys/PRIVATE.HTML, they will get a different document. This may not be what you want.

3. For your CGI programs, including Net.Data (which is a CGI program), your Web users will be able to run your CGI programs independent of the case of the URL they enter on their browser. So, if you had a program in the QSYSCGI library named PRIVATE, and they entered /cgi-bin/private, they would have seen error 403 (forbidden by rule). With this change, they will now be prompted for authentication (based on your protection setup). So, if they enter the correct authentication information, they will be able to run the CGI program.

Now, let us assume that you had previously understood that URLs were case sensitive, and you chose to make the case of a letter mean something, then you will likely have a problem after you load this PTF. The following example shows the impact after the PTF is applied:

```
Protect /WWW/P* Default
Protect /CGI-BIN/P* Default
Pass /WWW/P* /MYDIR/PRIVATE/*
Pass /WWW/p* /MYDIR/PUBLIC/*
Map /CGI-BIN/P* /QSYS.LIB/QSYSPRIV.LIB/*.PGM
Exec /QSYS.LIB/QSYSPRIV.LIB/*
Map /CGI-BIN/p* /QSYS.LIB/QSYSPUBLIC.LIB/*.PGM
Exec /QSYS.LIB/QSYSPUBLIC.LIB/*
```

Assume that you chose to use capital *P* as the first letter for your private resources and lowercase *p* as the first letter for your public resources. With this PTF change, the server will now perform authentication (based on your protection setup) for all URLs that start with either lowercase p or uppercase P. So, your Web users that only access public resources will now need a user ID and password to get to your Web site.

Also, if you had two documents named /MYDIR/PRIVATE/WELCOME.HTML and /MYDIR/PUBLIC/WELCOME.HTML, all of your users that have valid authentication will see the first document and no one will see the second one. The same logic applies to the CGI programs. This is not likely to be acceptable.

4.9.2 How do I make it work as before?

So, what do you do if your Web server configuration is going to run into one of these incompatibilities? You have to add a new directive, RuleCaseSense On, to your Web server configuration file. This directive will cause the Web server to again treat all URLs as case sensitive. If you choose to do this, you must be very careful with your protect and request routing configuration file directives, especially if you are protecting only part of your Web site or you protect different parts of your Web site with different protection characteristics. You should follow these guidelines to be safe:

- Separate your files into separate directories or members into QSYS files so that all of the files in any particular directory or members in the QSYS file have exactly the same security characteristics. Perform the same task with your CGI programs, separating them into different QSYS libraries so that all of the programs in any particular QSYS library have the exact same security characteristics.
- Make sure that each Protect directive for a URL or set of URLs also has a unique request routing directive for that protected URL or set of URLs. Also, make sure none of the other request routing directives in the configuration file

will match the protected URL or set of URLs. For the Protect and request routing directives:

- Make sure that if there is no wild card (*) in the URL of the Protect directive, then there had better not be a wild card (*) in the corresponding request routing directive (except for the Exec directive, which must have a wild card (*) as the last character; however, it must follow the full program name).
- If there is a wild card (*) in the URL of the Protect directive, then the placement of the wild card (*) in the URL of the corresponding request routing directive should be in exactly the same place. Never move the wild card (*) to the left in the Request Routing URL.

If you are doing client authentication by prompting for name and password and are using AS/400 user profiles, then the names and passwords are not case sensitive. However, if you are holding the names and passwords in validation lists then both the names and passwords are case sensitive and may contain spaces and other special characters.

4.10 TCP port numbers

The default port numbers used by HTTP servers are 80 for HTTP, and 443 for HTTPS. These are the well-known port numbers that all browsers use by default. You should use these ports for pages that users initially request.

Only one HTTP server instance at a time can listen to a single port. If you have multiple servers, for ease of configuration, testing, performance, and so on, then you have to use other port numbers.

- The valid range of port numbers is 1 through 65535.
- Port numbers up to 1024 are reserved for standard TCP/UDP functions.
- Port numbers 8080 and 8008 are the usual numbers for proxy servers.

For testing, port numbers are not a problem, as you know the numbers and only you need to know. However, for production systems you normally do not want your users to have to know specific port numbers. The exception to this might be a secure system with few users. In this case you might use a non-standard port number to make it less likely for other people to ever encounter your system. However, you should also take action to really make the system secure.

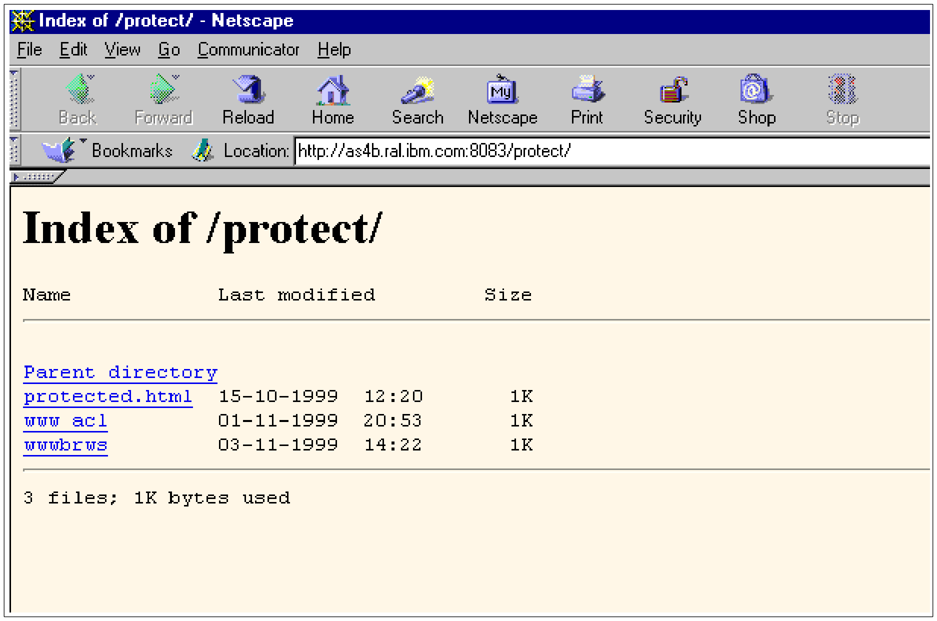
The normal method of working with multiple server instances, all serving the Internet, is to have one server instance to receive the initial URLs and redirect them to the port of the appropriate server instance. The dialog will then proceed on the new server’s port. All subsequent URL requests that are requested through relative links, use the same IP address and port number of the server.

For example. `Redirect   /inquiry/*   http://my.dns.name:8081/inquiry/*`

In our examples, because we are testing, we are using non-standard port numbers.

4.11 Directory browsing

You can choose to allow your directory contents to be displayed. In this case when a user enters a URL such as `http://as4b.ral.ibm.com:8083/protect/` the contents of the directory the URL is mapped to will be displayed. For example:


Index of /protect/ - Netscape
File Edit View Go Communicator Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Shop
Stop
Bookmarks
Location: http://as4b.ral.ibm.com:8083/protect/

Index of /protect/

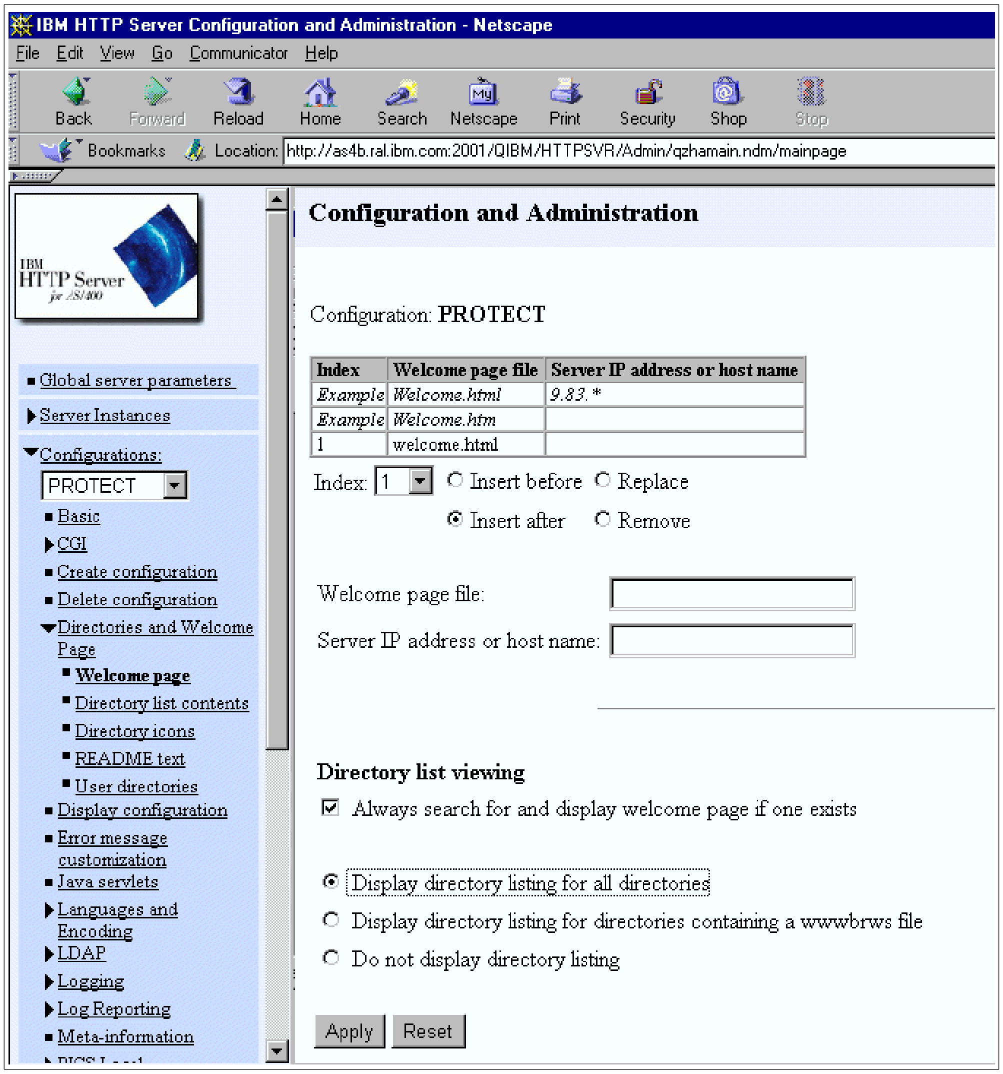
```
Name               Last modified         Size

Parent directory
protected.html   15-10-1999  12:20       1K
www acl          01-11-1999  20:53       1K
wwwbrws          03-11-1999  14:22       1K

3 files; 1K bytes used
```

Figure 11. Directory list

Before you allow directory browsing you should have a good reason for doing so. Sometimes file names are suggestive or if a person knows your business the existence or size of a file may be significant. The default is not to display directories.

You can use the HTTP Configuration and Administration utility to specify that directories will be displayed. To set the directory browsing options perform the following steps:

1. Start the HTTP Configuration and Administration utility.
2. Expand **Directories and Welcome Page**.
3. Click **Welcome page** to display the welcome page configuration window as shown in Figure 12 on page 56.


IBM HTTP Server Configuration and Administration - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://as4b.ral.ibm.com:2001/QIBM/HTTPSVR/Admin/qzhamain.ndm/mainpage
IBM HTTP Server for AS/400
Global server parameters
Server Instances
Configurations:
PROTECT
Basic
CGI
Create configuration
Delete configuration
Directories and Welcome Page
Welcome page
Directory list contents
Directory icons
README text
User directories
Display configuration
Error message customization
Java servlets
Languages and Encoding
LDAP
Logging
Log Reporting
Meta-information
Apply
Reset

Configuration and Administration

Configuration: PROTECT

Index	Welcome page file	Server IP address or host name
Example	*Welcome.html*	*9.83.**
Example	*Welcome.htm*	
1	welcome.html	

Index: 1 ○ Insert before ○ Replace

● Insert after ○ Remove

Welcome page file:

Server IP address or host name:

Directory list viewing

☑ Always search for and display welcome page if one exists

● Display directory listing for all directories

○ Display directory listing for directories containing a wwwbrws file

○ Do not display directory listing

Figure 12. HTTP configuration welcome page options

- You can always display a directory if requested.
- You can display a directory when requested only if a file named wwwbrws is present in the directory. The contents of the file are not relevant, just its existence.
- You can never display directories.

If you specify a welcome page to be displayed as well as to display directories then the welcome page will be displayed if one is present in a directory. The directory list will only appear if there is no welcome page in the directory requested.

If you choose to display directories there are a number of options to specify what information is to be displayed and how it is to appear. These can be specified by clicking **Directory list contents** and **Directory icons**.

4.12 Testing

You must carefully test your HTTP server configuration and AS/400 authorities to ensure people can access what they should be able to access and nothing else.

- Test that what should be allowed is.
- Test that what should not be allowed is not.
- Try hard to break your system security. Be inventive. Try odd cases and combinations. The objective is to find problems. All of them.

If you change your HTTP server instance configuration, always remember to restart the server using the AS/400 system command `STRTCPSVR *HTTP RESTART(*HTTP) HTTPSVR(-name-)`. Forgetting to do this can cause confusion and you may have to spend unreasonable time troubleshooting. Changing some directives like the Port directive require the server to be completely stopped and then started for the change to take effect. For these kind of changes, a restart will not reset the server. Refer to "Using server directives in a configuration file" in the *HTTP Server for AS/400 Webmaster's Guide V4R4*, SC41-5434 to see the full list of directives this applies to.

If you are using group files and change the group file contents you should also restart the HTTP server instance. The server holds a copy of the group file and only loads this once.

If you want to repeat a test on your browser requiring client authentication you must close your browser completely and restart it. If you do not do this, the browser will use the previous client authentication.

If your testing involves changing page contents, you should turn off caching on your browser; otherwise, the browser is likely to display the previously cached copy of pages, which can also be confusing.

4.13 HTTP configuration scenarios

In this section we use a very simple application and secure it in various ways to illustrate the points discussed previously. There is a directory holding files accessible to the public, from which the welcome page is being displayed. There is a directory holding sensitive files which we will secure.

Our application directory structure is as follows and resides in the root directory:

```
HTTP
├─Protect
│  └─protected.html
└─Public
   ├─redlogo.gif
   ├─secured.html
   └─welcome.html
```

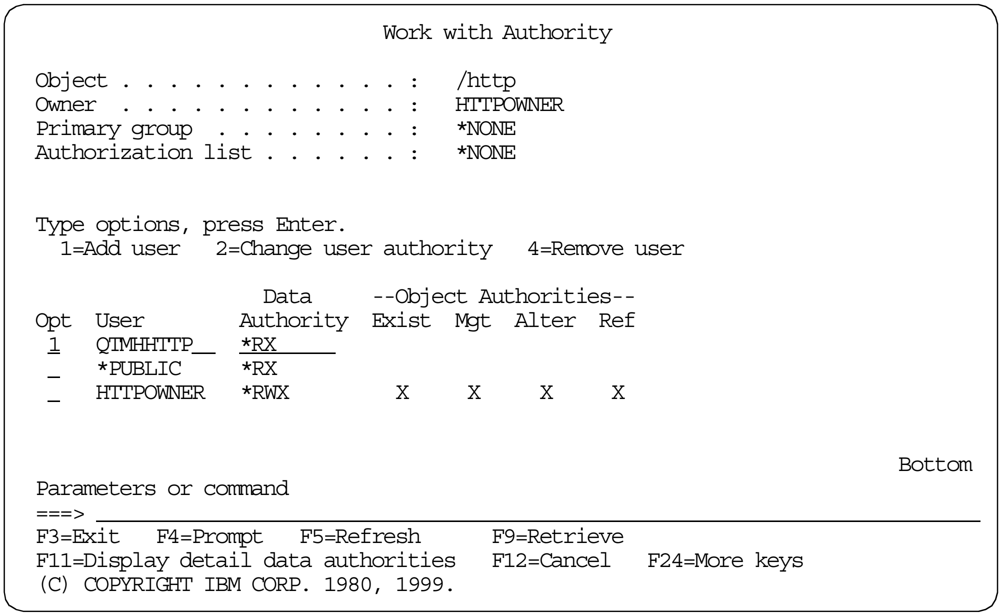
Figure 13. Application directory structure

Directory authorities

One of the requirements is to limit directory access as much as possible. Therefore, public authority is revoked from the HTTP directory, and read and execute authority granted to the default HTTP server user profile QTMHTTP. Our policy is to never give public authority to a library or directory unless it holds objects for all users on the AS/400 system. The HTTP directory only contains objects to be served by the HTTP server and so should not be accessible to the public.

To make the required changes to the object authorities, perform the following steps:

1. Enter the AS/400 system command `WRKAUT '/HTTP'` to display and work with the authorities to the HTTP directory.

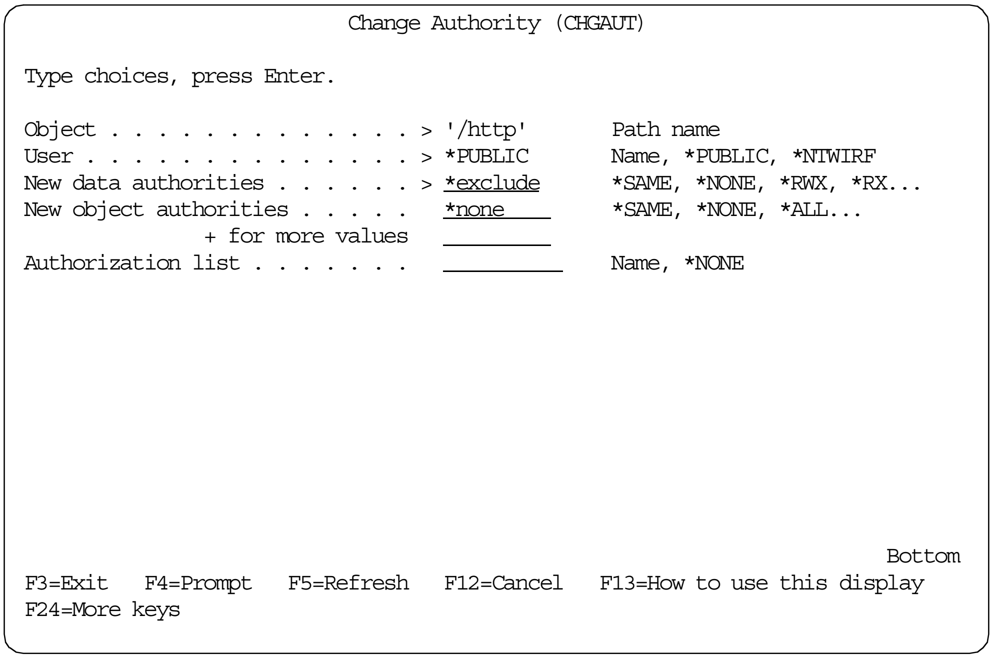


```
                           Work with Authority

 Object . . . . . . . . . . . . :   /http
 Owner  . . . . . . . . . . . . :   HTTPOWNER
 Primary group  . . . . . . . . :   *NONE
 Authorization list . . . . . . :   *NONE


 Type options, press Enter.
   1=Add user   2=Change user authority   4=Remove user

                     Data     --Object Authorities--
 Opt  User         Authority  Exist  Mgt  Alter  Ref
  1   QTMHHTTP__   *RX____
  _    *PUBLIC     *RX
  _   HTTPOWNER    *RWX         X     X     X     X


                                                                   Bottom
 Parameters or command
 ===> ____________________________________________________________________
 F3=Exit   F4=Prompt   F5=Refresh      F9=Retrieve
 F11=Display detail data authorities   F12=Cancel   F24=More keys
 (C) COPYRIGHT IBM CORP. 1980, 1999.
```

Figure 14. Directory authorities

Use option `1` to add the new user `QTMHHTTP` and specify `*RX` for the authorities.

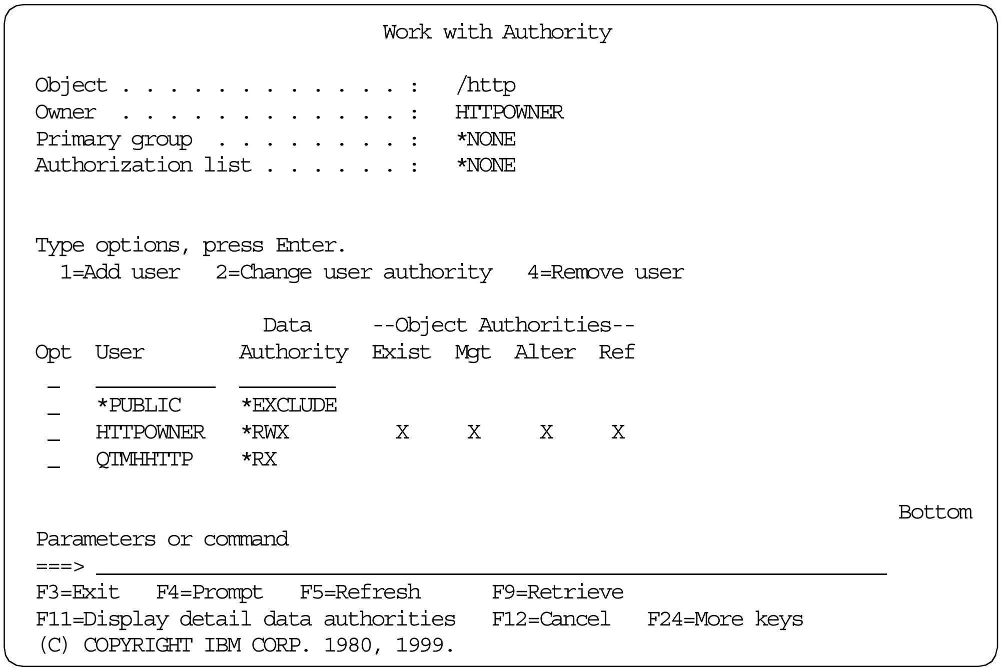
2. Press Enter to save your input.
3. Select option 2 next to user `*PUBLIC` and press Enter to work with the public authorities for the HTTP directory.



```
                             Change Authority (CHGAUT)

Type choices, press Enter.

Object . . . . . . . . . . . . . . > '/http'       Path name
User . . . . . . . . . . . . . . . > *PUBLIC       Name, *PUBLIC, *NTWIRF
New data authorities . . . . . . . > *exclude      *SAME, *NONE, *RWX, *RX...
New object authorities . . . . .     *none         *SAME, *NONE, *ALL...
               + for more values     _________
Authorization list . . . . . . .     __________    Name, *NONE










                                                                        Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 15. Public authorities to HTTP directory

4. Specify `*exclude` for the data authorities and `*none` for the object authorities.
5. Press Enter to save the changes.
6. Press F5 to refresh the display and verify that the changes are correct.



```
                             Work with Authority

Object . . . . . . . . . . . . :   /http
Owner  . . . . . . . . . . . . :   HTTPOWNER
Primary group  . . . . . . . . :   *NONE
Authorization list . . . . . . :   *NONE


Type options, press Enter.
  1=Add user   2=Change user authority   4=Remove user

                   Data     --Object Authorities--
Opt  User        Authority  Exist  Mgt  Alter  Ref
 _   __________  ________
 _   *PUBLIC     *EXCLUDE
 _   HTTPOWNER   *RWX         X     X     X     X
 _   QTMHHTTP    *RX

                                                                        Bottom
Parameters or command
===> __________________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh     F9=Retrieve
F11=Display detail data authorities   F12=Cancel   F24=More keys
(C) COPYRIGHT IBM CORP. 1980, 1999.
```

Figure 16. HTTP directory authorities.

Subsequent objects created in the HTTP directory automatically get these authorities.

HTTP server configuration

The HTTP server configuration is created using the HTTP Configuration and Administration utility and is as follows:

```
Configuration: PROTECT

BindSpecific Off
Port 8083
UserID %%SERVER%%
DNS-Lookup Off
Imbeds Off SSIOnly
AlwaysWelcome On
Welcome welcome.html
DirAccess Off
Pass /protect/* /http/protect/*
Pass /* /http/public/*
```

- We have chosen to use port 8083 for our testing. To access our server instance we will need to give URLs such as `http://our.dns.name:8083/file.html`.
- The directive `UserID %%SERVER%%` is the default and states that the user profile of the HTTP server job will be used to access directories and files. In other words the user QTMHHTTP must be authorized to the directories and files that will be used.
- Further it is specified to look for a welcome page named welcome.html if a URL request does not name a file.
- We have specified that directories are not to be displayed.
- Any URL starting with `/protect/` will be accepted and internally changed to start with `http/protect/`.
- Any other URLs will be accepted and changed to start with `http/public/`.

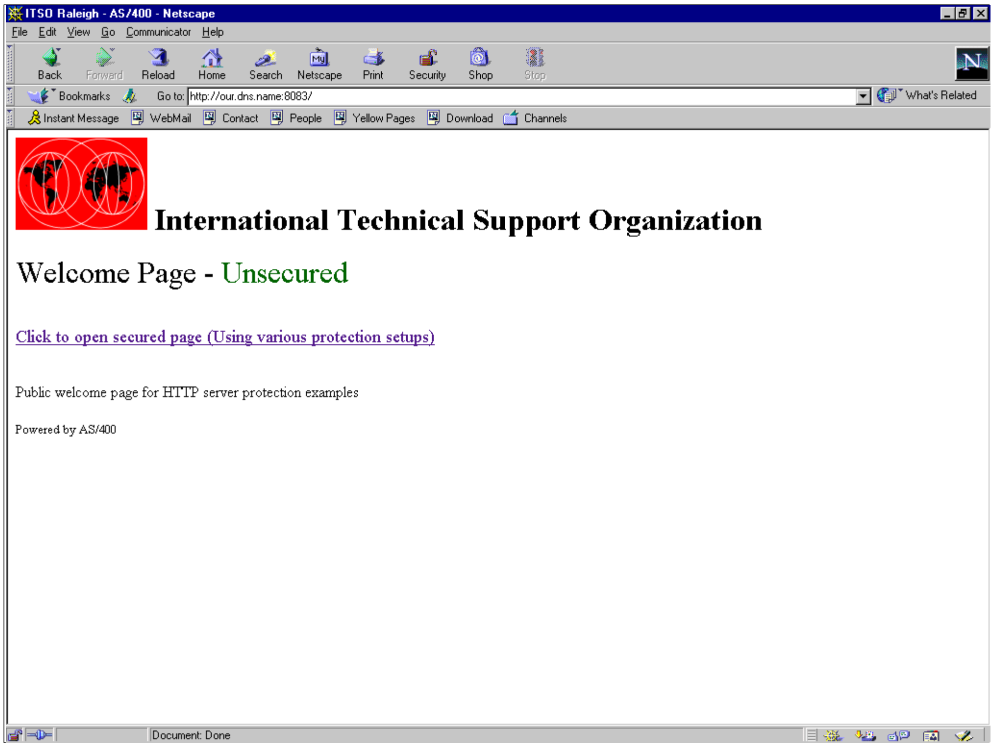
Welcome page

The welcome page used in the scenarios contains essential information. Figure 17 shows the HTML source of the welcome page.

```
<html>
<head><title>ITSO Raleigh - AS/400</title></head>
<body>
<img SRC="redlogo.gif" height=96 width=137>&nbsp;
<font size=+3><b>International Technical Support
Organization</b>&nbsp;&nbsp;</font>
<p><font size=+3>Welcome Page - <font color="#006600">Unsecured</font></font>
<br>&nbsp;
<p><font size=+1><a href="/protect/Protected.html">Click to open secured
page (Using various protection setups)</a></font>
<p><br>
<p>Public welcome page for HTTP server protection examples
<p><font size=-1>Powered by AS/400</font>
</body>
</html>
```

Figure 17. Welcome page source

The welcome page appears as follows.


ITSO Raleigh - AS/400 - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks
Go to: http://our.dns.name:8083/
What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
Document: Done

International Technical Support Organization

Welcome Page - Unsecured

Click to open secured page (Using various protection setups)

Public welcome page for HTTP server protection examples

Powered by AS/400

Figure 18. Welcome page

4.14 Scenario 1: Secure transmission using SSL

This scenario uses SSL to ensure the privacy and integrity of files sent from the protected directory. No client authentication is in place.

This scenario would be appropriate when the following conditions are important:

- We must ensure the privacy of information sent between the server and the client.
- Clients need to be able to authenticate the server site.

This scenario might be appropriate for an application such as supplying prices on request. The information is not private but it is important that clients are able to authenticate your site and that what you send is not modified during transmission.

Another very common example is accepting payment by credit card over the Internet. Clients need to be able to authenticate your site and you must ensure the privacy of the payment details the client sends to you.

4.14.1 Scenario objectives

The objectives of this scenario are:

- Change the server configuration to enable SSL.
- Change the link properties on the welcome page to use the HTTPS protocol for accessing the secured page.

Note:

- The files in the protected directory are not secured; anyone can access them.
- SSL is not enforced. A URL such as http://`our.site.dns/protect/protected.html` will be accepted and the file will be sent using HTTP instead of SSL.

4.14.2 Modifying the link to the secured page

The following step changes the link information for requesting the file Protected.html. To change the link information, you can use an HTML design tool or an ordinary editor, such as Windows Notepad. This scenario uses an editor.

1. Start an editor and open the file welcome.html and locate the following statements:

   ```
   <p><font size=+1><a href="/protect/Protected.html">Click to open secured
   page (Using various protection setups)</a></font>
   ```

2. Change the href option to reference the new link information as shown in the following statement.

   ```
   <p><font size=+1><a
   href="https://our.dns.name:4433/protect/Protected.html"> Click to open
   secured page (Using various protection setups)</a></font>

   <p><br>
   ```

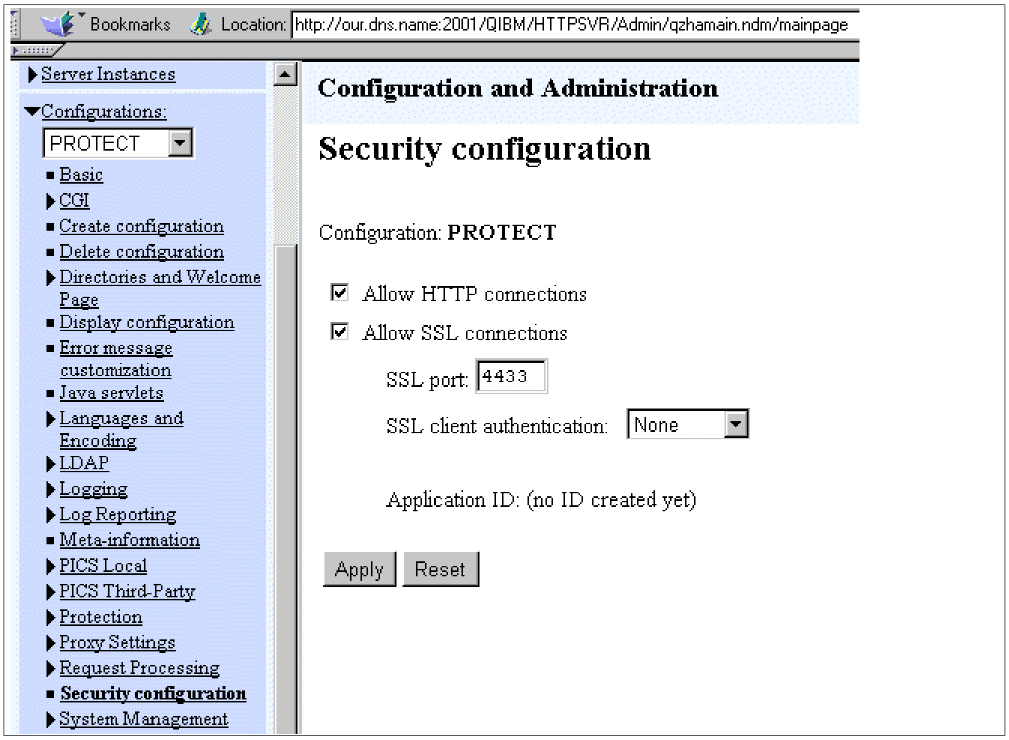
This will use the secure protocol HTTPS on port 4433 instead of the same protocol and port as had been used to serve the welcome page, HTTP on port 8083. Note that the link information is changed from a relative link to an absolute link.

4.14.3 Enabling SSL

SSL must be enabled using port 4433 in order to use the link to the secure page. If you do not enable SSL and you click this link, you get no response from the server and the browser waits until it times out or the request is cancelled.

Perform the following steps to enable SSL for the HTTP server instance used in this scenario:

1. Start the HTTP Configuration and Administration utility.
2. Click **Security configuration** in the navigation panel. The security configuration window appears.



Configuration and Administration

Security configuration

Configuration: **PROTECT**

☑ Allow HTTP connections

☑ Allow SSL connections

SSL port: 4433

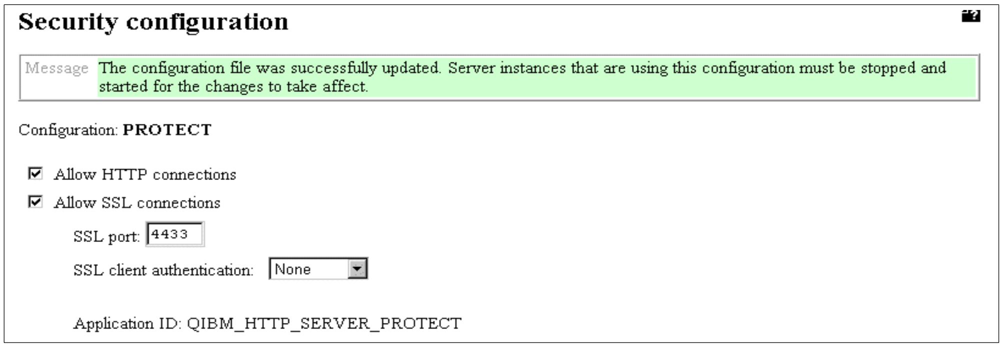
SSL client authentication: None

Application ID: (no ID created yet)

Figure 19. Security configuration for SSL

3. Allow SSL connections and change the SSL port from 443 to 4433.
4. Click the **Apply** button.

   The completion message and the Application ID appears.



Security configuration

Message The configuration file was successfully updated. Server instances that are using this configuration must be stopped and started for the changes to take affect.

Configuration: **PROTECT**

☑ Allow HTTP connections

☑ Allow SSL connections

SSL port: 4433

SSL client authentication: None

Application ID: QIBM_HTTP_SERVER_PROTECT

Figure 20. Security configuration for SSL after application ID assignment

The following directives have been added to the HTTP configuration.

```
NormalMode On
# Do not change or delete the following AppName directive
AppName QIBM_HTTP_SERVER_PROTECT
SSLMode On
SSLPort 4433
SSLClientAuth Off
```

5. Go to the DCM and assign a server certificate as explained in 5.6.1.5, “Associate the certificate with a secure application” on page 155. Because this

application will be made available on the Internet, it uses a server certificate from a well-known CA.

6. Finally restart the HTTP server instance so that the new configuration becomes effective. You have to end and restart the HTTP server instance to activate the changes. If you just restart the server with the command `STRTCPSVR *HTTP RESTART(*HTTP) HTTPSVR(PROTECT)` the port 4433 is not going to the listen state. Perform the following commands to activate the changes:

```
ENDTCPSVR SERVER(*HTTP) HTTPSVR(PROTECT)
```

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(PROTECT)
```

4.14.4 Testing the system

After the configuration is done and the server is restarted, test the new configuration and verify that you get the intended results.

1. Open a browser and request the welcome page using the URL `http://our.dns.name:8083/`.
2. Click the welcome page link **Click to open secured page (Using various protection setups)**. The secured page appears.

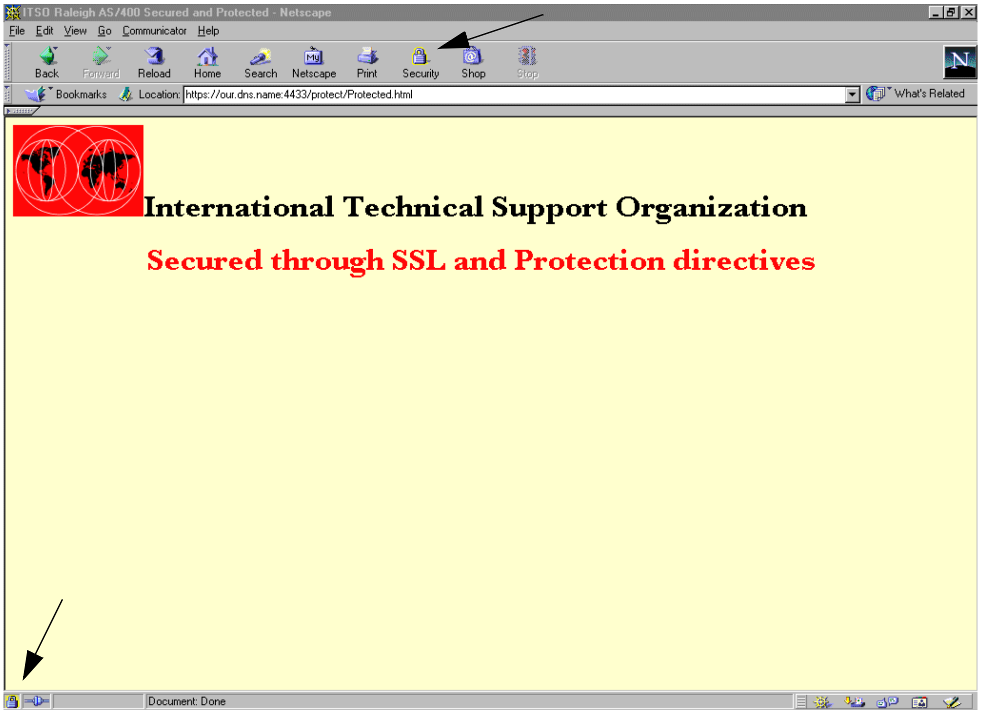
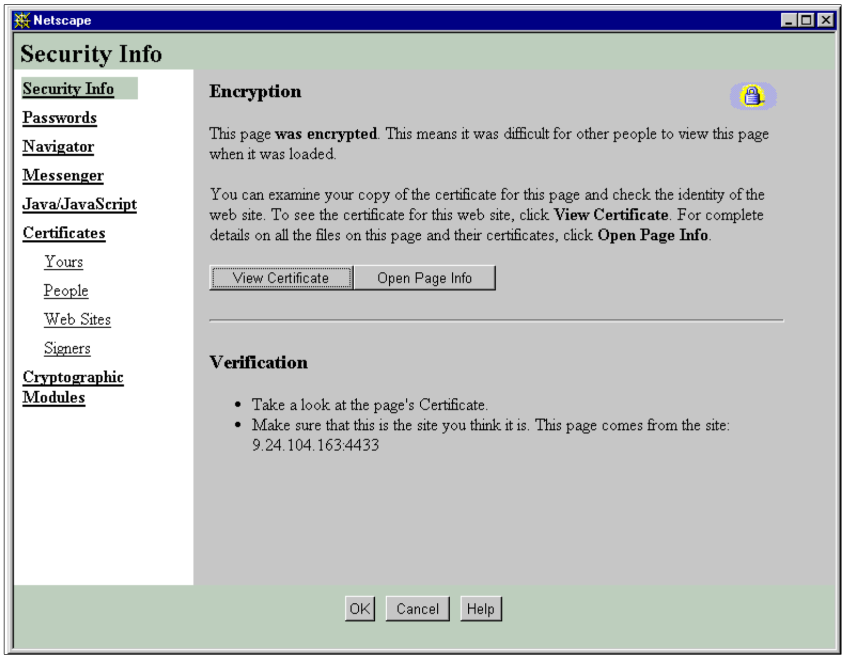

ITSO Raleigh AS/400 Secured and Protected - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: https://our.dns.name:4433/protect/Protected.html
What's Related
International Technical Support Organization
Secured through SSL and Protection directives
Document: Done

Figure 21. Secured page

Note the closed padlocks that appear in the tool bar and at the bottom left. This is how Netscape Communicator shows that the connection is using SSL. To view the security information held on the Netscape Communicator browser, click either of the padlock icons.



Encryption

This page **was encrypted**. This means it was difficult for other people to view this page when it was loaded.

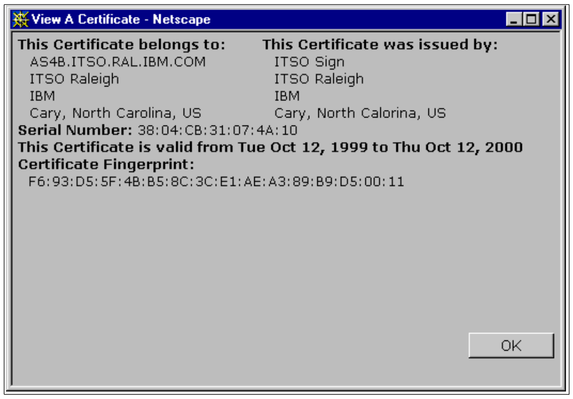
You can examine your copy of the certificate for this page and check the identity of the web site. To see the certificate for this web site, click **View Certificate**. For complete details on all the files on this page and their certificates, click **Open Page Info**.

Verification

- Take a look at the page's Certificate.
- Make sure that this is the site you think it is. This page comes from the site: 9.24.104.163:4433

Figure 22. Netscape security information panel

From this panel you have a number of options related to security. To view the server’s certificate click the **View Certificate** button.



```
This Certificate belongs to:        This Certificate was issued by:
  AS4B.ITSO.RAL.IBM.COM               ITSO Sign
  ITSO Raleigh                        ITSO Raleigh
  IBM                                 IBM
  Cary, North Carolina, US            Cary, North Calorina, US
Serial Number: 38:04:CB:31:07:4A:10
This Certificate is valid from Tue Oct 12, 1999 to Thu Oct 12, 2000
Certificate Fingerprint:
  F6:93:D5:5F:4B:B5:8C:3C:E1:AE:A3:89:B9:D5:00:11
```

Figure 23. Netscape certificate information display

The server certificate credentials are shown.

This concludes scenario 1, in which you have seen how to enable SSL on the HTTP Server for AS/400.

4.15 Scenario 2: Client authentication using AS/400 user name/password

This scenario uses client authentication by prompting users for a name and password. Checking is done against the user profiles on the AS/400 system.

This scenario would be appropriate when the following conditions are important:

- Your application needs to be restricted to registered users.

- The user who accesses your HTTP application already has an AS/400 user profile or can wait while one is being created for them.
- You want to use AS/400 authorities to control access to your application or within your application.

An existing application, which you have Web enabled for your employees to access using an intranet or the Internet, would fit this scenario.

4.15.1 Scenario objectives

The objectives of the second scenario are:

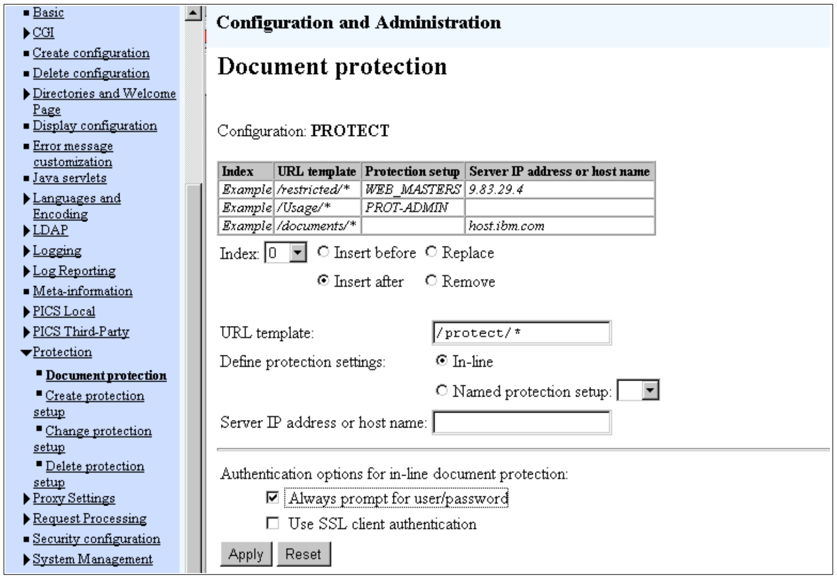
- Authenticate clients that connect by prompting for an AS/400 user profile name and password.
- Control access to parts of the application based on user profile authority.

The scenario discussed in 4.14, “Scenario 1: Secure transmission using SSL” on page 61 will be the starting point. We add client authentication by prompting for user name and password and use AS/400 authorities to control the access to the application. SSL will be used to secure communications. This is very desirable in the user name and password dialog. Later, depending on the application, we could revert to HTTP because this has lower overheads and gives better performance. But this of course always depends on the data to be transmitted.

4.15.2 Client authentication

To request client authentication a Protect directive needs to be added to the HTTP server configuration. To add the directive used in this scenario, perform the following steps:

1. Start the HTTP Configuration and Administration utility.
2. On the navigation panel, expand **Protection** and then click **Document protection**. The Document protection window appears.



Configuration and Administration

Document protection

Configuration: PROTECT

Index	URL template	Protection setup	Server IP address or host name
Example	*/restricted/**	*WEB_MASTERS*	*9.83.29.4*
Example	*/Usage/**	*PROT-ADMIN*	
Example	*/documents/**		*host.ibm.com*

Index: 0 ○ Insert before ○ Replace

● Insert after ○ Remove

URL template: /protect/*

Define protection settings: ● In-line

○ Named protection setup:

Server IP address or host name:

Authentication options for in-line document protection:

☑ Always prompt for user/password

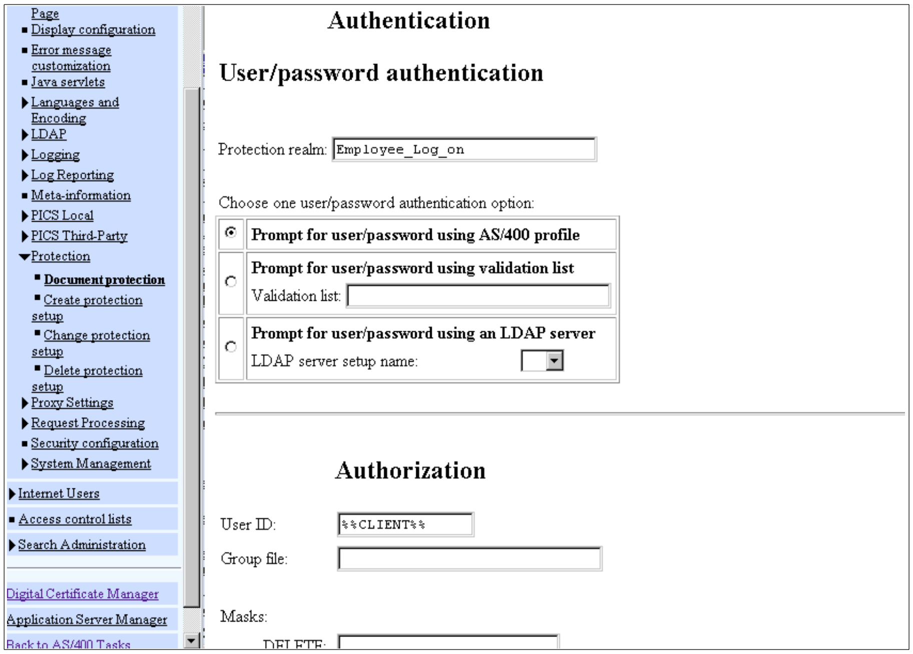
☐ Use SSL client authentication

Apply Reset

Figure 24. Client authentication using name and password

Define a Protect directive with the URL template `/protect/*` that matches everything in the protected directory and its subdirectories.
Select **Always prompt for user/password**.

3. Click **Apply**. The User/password authentication panel appears.



Authentication

User/password authentication

Protection realm: Employee_Log_on

Choose one user/password authentication option:

● Prompt for user/password using AS/400 profile

○ Prompt for user/password using validation list
Validation list:

○ Prompt for user/password using an LDAP server
LDAP server setup name:

Authorization

User ID: %%CLIENT%%

Group file:

Masks:

DELETE:

Figure 25. Client authentication part 2

Give the text to appear in the user name and password prompt, `Employee_log_on`, remembering to link the words so they are all displayed.

4. Leave the default selection to Prompt for user/password using AS/400 profile.

5. Set User ID to `%%CLIENT%%` so that the user profile given by the client when they log on is used by the HTTP server job to access files. This allows us to use AS/400 system authorities to control what users can access.

6. Click **Apply**. The protection directives are created and our configuration appears as follows:

```
Configuration: PROTECT
Protect /protect/* {
      PasswdFile %%SYSTEM%%
      ACLOverride Off
      DeleteMask All@(*)
      PostMask All@(*)
      PutMask All@(*)
      GetMask All@(*)
      AuthType Basic
      ServerID Employee_log_on
      UserID %%CLIENT%%
}
BindSpecific Off
Port 8083
UserID %%SERVER%%
DNS-Lookup Off
Imbeds Off SSIOnly
AlwaysWelcome On
Welcome welcome.html
DirAccess Off
Pass /protect/* /http/protect/*
Pass /* /http/public/*
NormalMode On
# Do not change or delete the following AppName directive
AppName QIBM_HTTP_SERVER_PROTECT
SSLMode On
SSLPort 4433
SSLClientAuth Off
```

7. Use the AS/400 system command `STRTCPSVR *HTTP RESTART(*HTTP) HTTPSVR(PROTECT)` to restart the HTTP server instance with the new configuration. If the server instance PROTECT was not already running use the command `STRTCPSVR *HTTP HTTPSVR(PROTECT)` to start it.

4.15.3 AS/400 system authorities

You must now grant the employees who are to use the application authority to the directory PROTECT. Say the system is a human resources application. Create a user profile HMNRSCAUT which gets authority to all the objects needed to access the application. Make HMNRSCAUT a group profile for the users of the application.

1. On an AS/400 system command line, use the following commands:

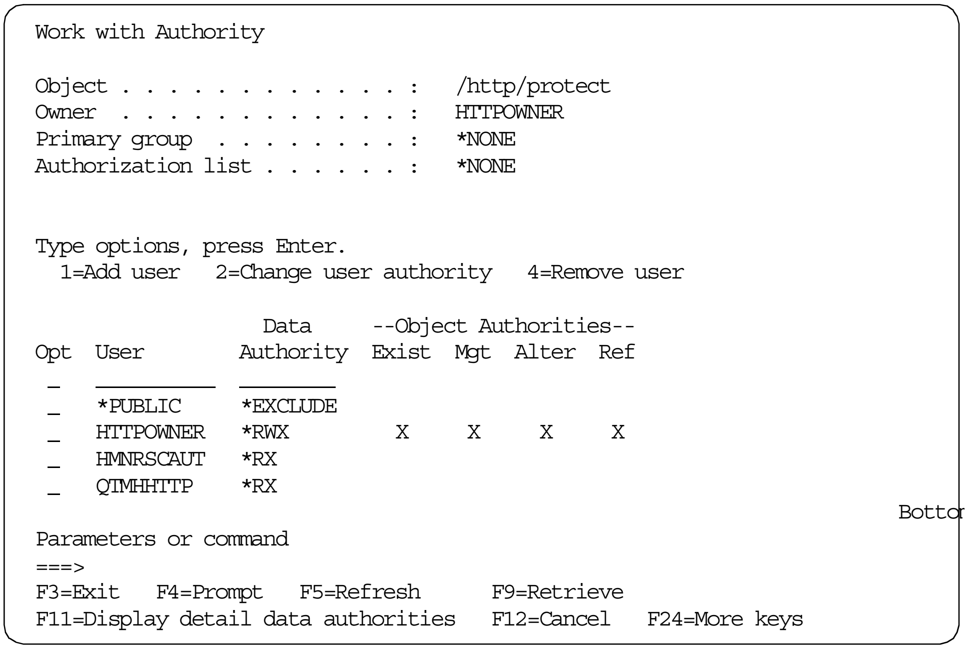
```
CRTUSRPRF USRPRF(HMNRSCAUT) PASSWORD(*NONE) TEXT('Human Resources System
group authorities')
CHGAUT OBJ('http') USER(HMNRSCAUT) DTAAUT(*RX)
CHGAUT OBJ('http/protect') USER(HMNRSCAUT) DTAAUT(*RX)
CHGAUT OBJ('http/public') USER(HMNRSCAUT) DTAAUT(*RX)
CHGAUT OBJ('http/protect/*') USER(HMNRSCAUT) DTAAUT(*RX)
CHGAUT OBJ('http/public/*') USER(HMNRSCAUT) DTAAUT(*RX)
```

These commands:

- Create the user profile `HMNRSCAUT`. We use `PASSWORD(*NONE)` so that it cannot be used to sign on.

- Grant HMNRSCAUT authority to the directories HTTP, PROTECT, and PUBLIC.
- Grant HMNRSCAUT authority to everything in the directories HTTP/PROTECT and HTTP/PUBLIC.

2. Use the command WRKAUT '/http/protect' to display the authorities to the protected directory so you can verify they are as they should be.



```
Work with Authority

Object . . . . . . . . . . . . :   /http/protect
Owner  . . . . . . . . . . . . :   HTTPOWNER
Primary group  . . . . . . . . :   *NONE
Authorization list . . . . . . :   *NONE


Type options, press Enter.
  1=Add user   2=Change user authority   4=Remove user

                   Data     --Object Authorities--
Opt  User        Authority  Exist  Mgt  Alter  Ref
 _   __________  ________
 _   *PUBLIC     *EXCLUDE
 _   HTTPOWNER   *RWX         X     X     X     X
 _   HMNRSCAUT   *RX
 _   QTMHHTTP    *RX
                                                                           Botto
Parameters or command
===>
F3=Exit   F4=Prompt   F5=Refresh      F9=Retrieve
F11=Display detail data authorities   F12=Cancel   F24=More keys
```

Figure 26. Authorities on protected directory

QTMHTTP is the default user profile used by the HTTP server job. It should not have authority to the protected directory.

3. Type option 4 beside the QTMHHTTP user profile and press Enter. Press Enter again to confirm. The Work with Authority display reappears and QTMHHTTP no longer has authority to the directory. Press Enter again to exit the display.
4. Use the command CHGAUT OBJ('/http/protect/*') USER(QTMHHTTP) DTAAUT(*NONE) OBJAUT(*NONE) to remove authority from QTMHHTTP to all objects in the protected directory.
5. Make HMNRSCAUT a group profile of the users who should access the human resources system. We use the following commands:

```
CHGUSRPRF USRPRF(ITSOCOLIN) GRPPRF(HMNRSCAUT)
CHGUSRPRF USRPRF(ITSOTOM) SUPGRPPRF(HMNRSCAUT)
```

User profile ITSOTOM already had a group profile, so the HMNRSCAUT user profile must be specified as a supplemental group profile. However, the effect is the same.

4.15.4 Ensuring SSL connections

This scenario does not enforce an SSL connection to the secured pages. A user could give a URL such as http://our.dns.name:8083/protect/protected.html and obtain the pages using HTTP instead of SSL.

We can enforce SSL by having a dedicated HTTP server instance or by using SSL client authentication together with a protection directive.

The pages in this secure system will normally be requested by using links defined on, for example, the welcome page. These links specify SSL, so it is not likely that pages will be requested using HTTP. However, this is a weakness in the configuration.

4.15.5 Testing the system

As previously mentioned, testing an application, especially when deployed on the Internet is essential. The test, if possible, should stress any kind of user requests or attacks to access your application. The testing performed for this scenario is as follows:

4.15.5.1 Try a valid user name and password

1. On a browser use the URL `http://our.dns.name:8083` to display the welcome page.
2. Click the link to the protected page and the prompt for user and password appears.

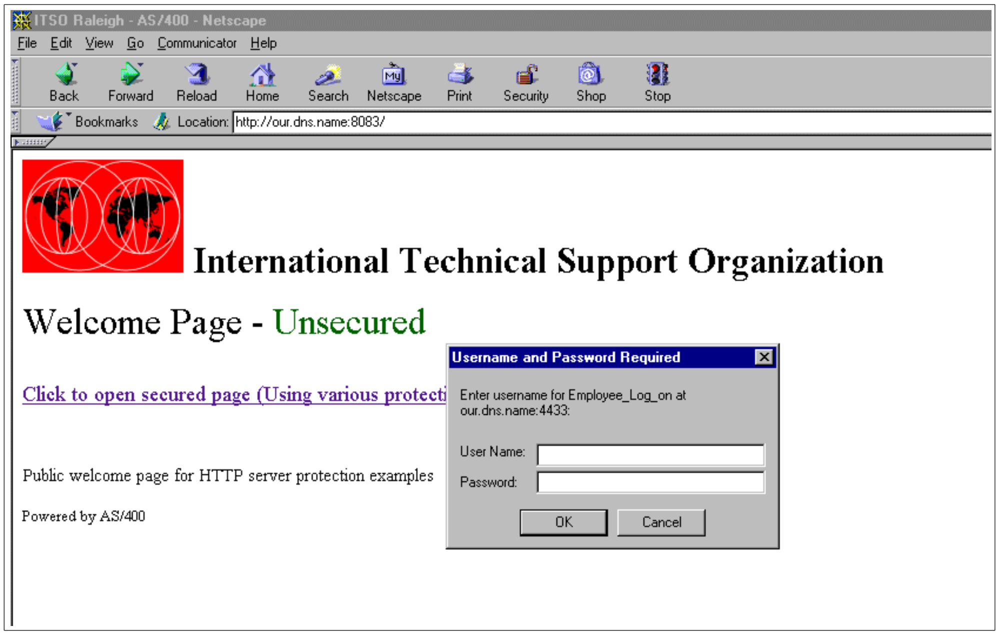
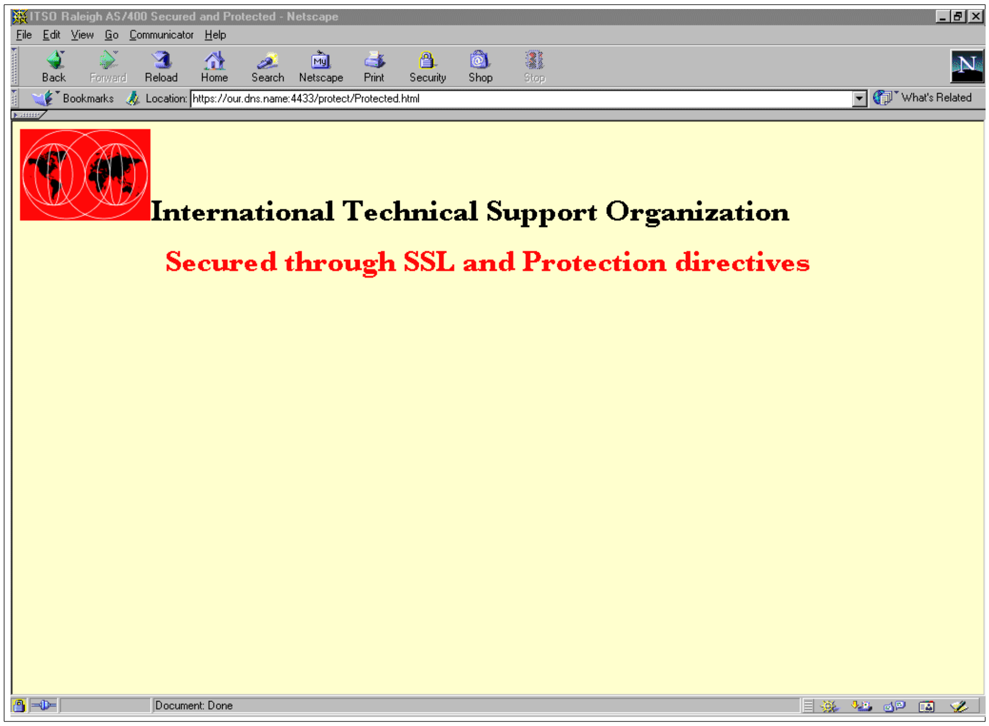

ITSO Raleigh - AS/400 - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://our.dns.name:8083/
International Technical Support Organization
Welcome Page - Unsecured
Click to open secured page (Using various protecti
Public welcome page for HTTP server protection examples
Powered by AS/400
Username and Password Required
Enter username for Employee_Log_on at our.dns.name:4433:
User Name:
Password:
OK
Cancel

Figure 27. User and password prompt

3. We enter user `ITSOCOLIN` and its password, then click **OK**.

   The secure page appears with padlocks closed to indicate SSL has been used for the connection.The SSL connection is established before prompting for the password and so the password dialog is protected.



Location: https://our.dns.name:4433/protect/Protected.html

International Technical Support Organization

Secured through SSL and Protection directives

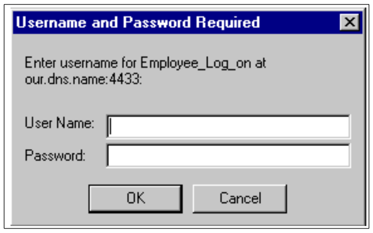
Figure 28. Secured page. SSL and User/password

4.15.5.2 Try a nonexistent user, bad password, and unauthorized user

1. Close the browser and restart it so you can log on as another user.

2. Enter the URL our.dns.name:8083 to display the welcome page.

3. Click the link to the protected page. The prompt for user and password appears.



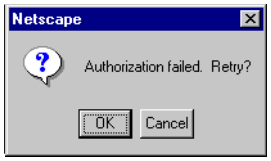
Enter username for Employee_Log_on at our.dns.name:4433:

User Name:

Password:

Figure 29. User and password prompt

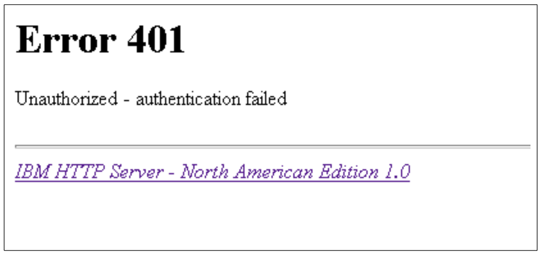
4. Enter `ITSOFRED`, which does not exist. The Authorization failed panel appears as follows:



Authorization failed. Retry?

Figure 30. Authorization failed

5. Click **Cancel**. The following error message appears:



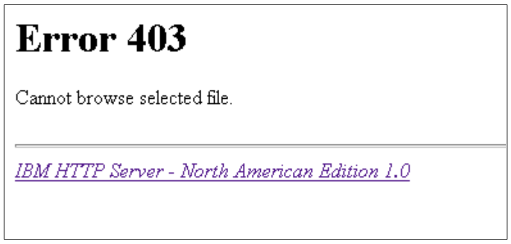
Error 401

Unauthorized - authentication failed

IBM HTTP Server - North American Edition 1.0

Figure 31. Unauthorized - authentication failed

6. Click your browser's **Back** icon to redisplay the welcome page, then click the link to the protected page so the prompt for user and password appears.
7. We enter the user name `ITSOMINOTE`, which does exist, and give the wrong password. This also gets the Authorization failed panel as in Figure 30.
8. We try `ITSOMINOTE` with the correct password. The following error message appears.



Error 403

Cannot browse selected file.

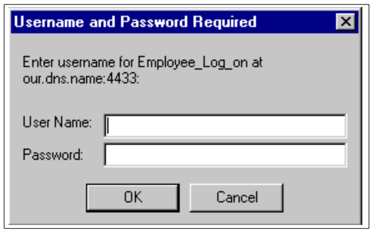
IBM HTTP Server - North American Edition 1.0

Figure 32. Not authorized

This is correct. `ITSOMINOTE` is not in the group profile `HMNRSCAUT` and so is not authorized to this application.

4.15.5.3 Try a disabled user and a user with an expired password

1. On the AS/400 system, change a valid user to status disabled. We will change `ITSOCOLIN` using the command `CHGUSRPRF ITSOCOLIN STATUS(*DISABLED)`
2. Close the browser and restart it so you can log on as another user.
3. Use the URL our.dns.name:8083 to display the welcome page.
4. Click the link to the protected page. The prompt for user and password appears:



Username and Password Required

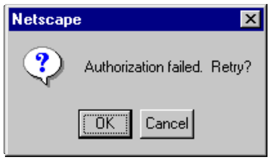
Enter username for Employee_Log_on at our.dns.name:4433:

User Name:

Password:

Figure 33. User and password prompt

5. Enter the user name and password and click **OK**. The Authorization failed panel appears as follows.

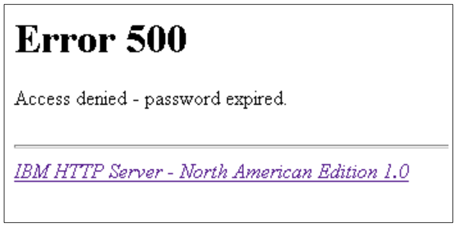


Authorization failed. Retry?

Figure 34. Authorization failed

6. Click **OK**.
7. On the AS/400 system change the user to status enabled and set the password to be expired. We will change `ITSOCOLIN` using the command `CHGUSRPRF ITSOCOLIN STATUS(*ENABLED) PWDEXP(*YES)`
8. Enter the user name and password and click **OK**. The following panel appears.

.



Error 500

Access denied - password expired.

IBM HTTP Server - North American Edition 1.0

Figure 35. Password expired

9. On the AS/400 system change the user so the password is not expired. We will change `ITSOCOLIN` using the command `CHGUSRPRF ITSOCOLIN PWDEXP(*NO)`.
10. Close the browser and restart it.
11. Use the URL our.dns.name:8083 to display the welcome page.
12. Click the link to the protected page.
13. Enter the user name and password and click **OK**. The secure page appears.

These results are all as expected. This concludes scenario 2.

4.16 Scenario 3: Client authentication using certificates or name/password

Scenario 3 allows clients to use a certificate or a user name and password for authentication. For a certificate to be accepted it must be valid and associated with an AS/400 user profile. If no certificate is given or the one given is not associated with an AS/400 user profile, then an AS/400 user profile name and password must be given.

This scenario would be appropriate when the following conditions are important:

- Your application needs to be restricted to registered users.
- The users who will access your HTTP server application already have AS/400 user profiles or can wait while one is being created for them.
- You want to use AS/400 authorities to control access to your application or within your application.
- Users already have certificates or can easily obtain them.

- If you have a number of applications on separate systems and users find password maintenance annoying.

An existing application that is Web enabled for your employees to access using an intranet or the Internet would fit this scenario.

Allowing both certificates and user names with passwords to be used could be a good configuration while changing to certificate authentication only.

4.16.1 Scenario 3 objectives

The objectives of this scenario are:

- Authenticate clients with digital certificates associated with an AS/400 user profile.
- If no valid certificate is presented or the certificate is not associated with an AS/400 user profile, the user is prompted for an AS/400 user profile name and password.

The configuration created in scenario 2 will be our starting point. We will change the HTTP configuration so that SSL client authentication can be used.

We must have a procedure for obtaining certificates for our employees and for associating them with a user profile.

Note

It is possible to associate more than one certificate with a user profile. However, the implementation of this was not done with large numbers in mind.

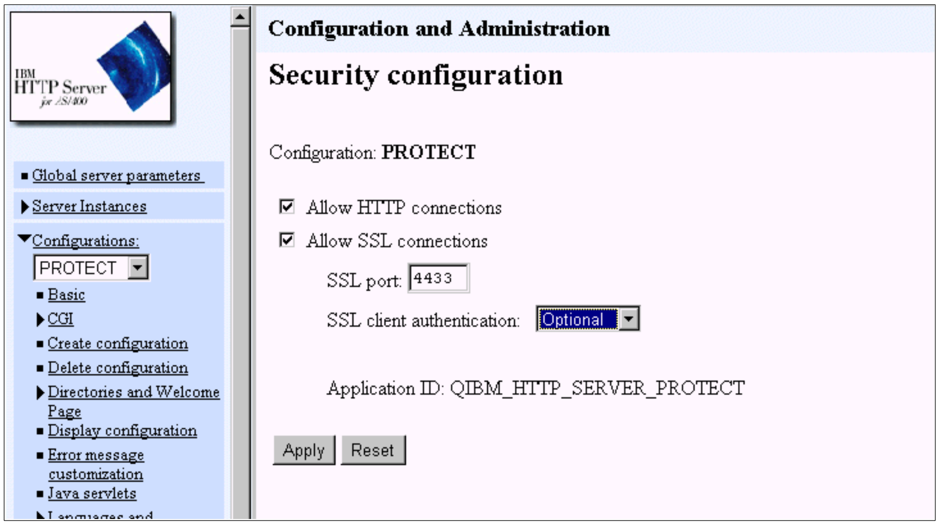
- Do not plan a system that will have many (for example, several hundred) certificates associated with the same user profile.
- Do not plan a system where it is likely that several people will try to register, or otherwise manage, certificates for one user profile at the same time.

Doing either of the preceding can cause occasional errors, frustration, and confusion. If you have a large number of certificates, use a validation list to group them and the user ID on a protection directive to name the user profile to process their requests.

4.16.2 Enabling client authentication for SSL

To enable client authentication with digital certificates for the HTTP server, perform the following configuration steps:

1. Click **Security configuration** on the navigation panel to display the Security configuration panel as follows.



Configuration and Administration

Security configuration

Configuration: PROTECT

☑ Allow HTTP connections

☑ Allow SSL connections

SSL port: 4433

SSL client authentication: Optional

Application ID: QIBM_HTTP_SERVER_PROTECT

Figure 36. Enabling SSL client authentication

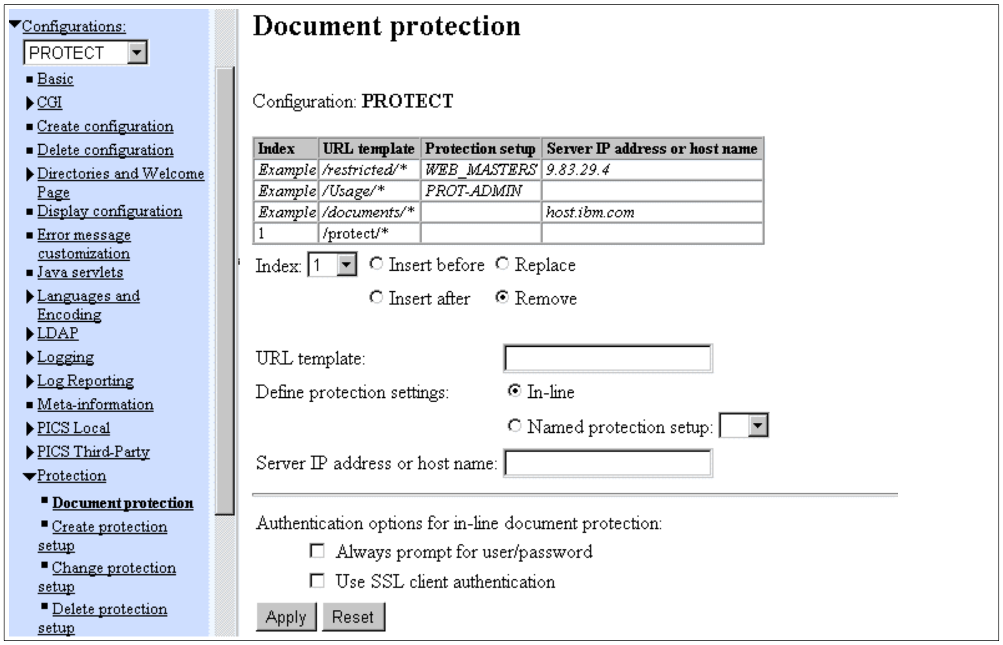
In the SSL client authentication drop-down, select **Optional**.

2. Click **Apply** to update the configuration. This adds the directive `SSLClientAuth On`.

4.16.3 Creating the protection setup

The protection directive used in this scenario allows both client authentication with certificates and with user profiles. The following steps show the steps to create the appropriate directive:

1. Start the HTTP Configuration and Administration utility.
2. Click **Protection** then **Document protection** in the navigation panel.



Document protection

Configuration: PROTECT

Index	URL template	Protection setup	Server IP address or host name
Example	/restricted/*	WEB_MASTERS	9.83.29.4
Example	/Usage/*	PROT-ADMIN	
Example	/documents/*		host.ibm.com
1	/protect/*		

Index: 1 ○ Insert before ○ Replace

○ Insert after ● Remove

URL template:

Define protection settings: ● In-line

○ Named protection setup:

Server IP address or host name:

Authentication options for in-line document protection:

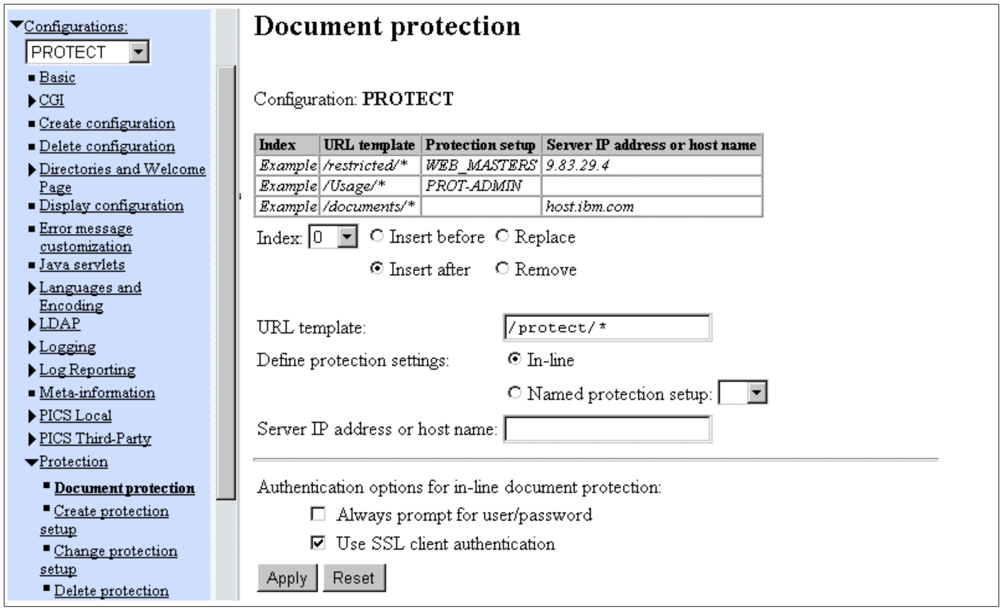
□ Always prompt for user/password

□ Use SSL client authentication

Figure 37. Removing the protection setup

Select index **1** and **Remove.**

3. Click **Apply**. This removes the old protection setup and cleans up the HTTP configuration.



Document protection

Configuration: **PROTECT**

Index	URL template	Protection setup	Server IP address or host name
Example	*/restricted/**	*WEB_MASTERS*	*9.83.29.4*
Example	*/Usage/**	*PROT-ADMIN*	
Example	*/documents/**		*host.ibm.com*

Index: 0 ○ Insert before ○ Replace

● Insert after ○ Remove

URL template: `/protect/*`

Define protection settings: ● In-line

○ Named protection setup:

Server IP address or host name:

Authentication options for in-line document protection:

□ Always prompt for user/password

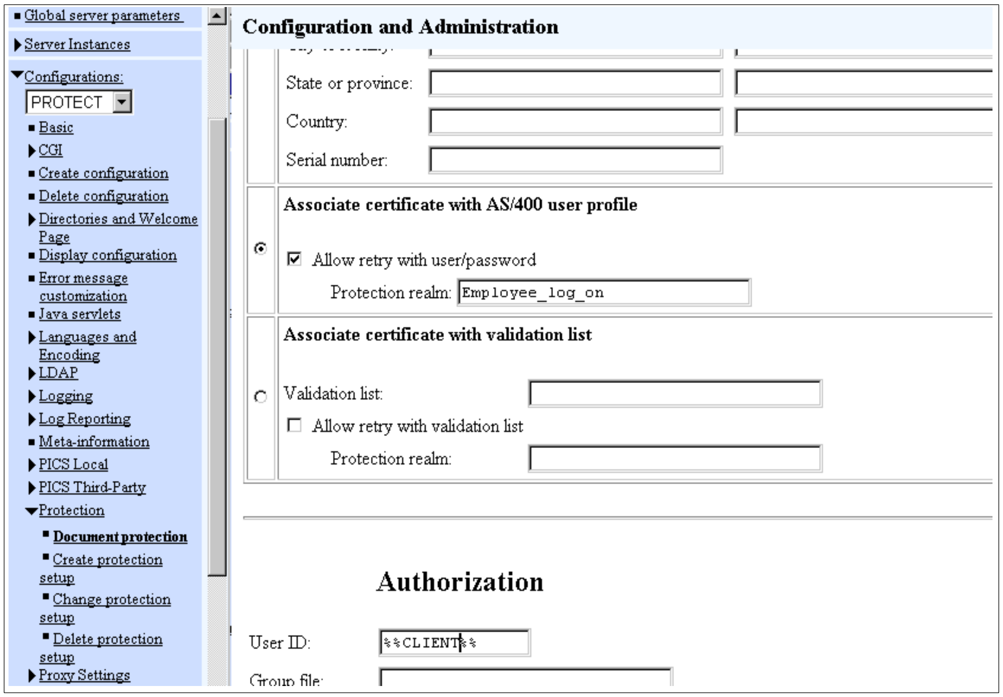
☑ Use SSL client authentication

Figure 38. Adding the new protection setup

4. Select **Insert after** and enter `/protect/*` for the URL template, then select **Use SSL client authentication.**

5. Click **Apply** to continue creating the new protection setup. The SSL authentication panel appears.

.



Configuration and Administration

State or province:

Country:

Serial number:

● Associate certificate with AS/400 user profile

☑ Allow retry with user/password

Protection realm: Employee_log_on

○ Associate certificate with validation list

Validation list:

□ Allow retry with validation list

Protection realm:

Authorization

User ID: %%CLIENT%%

Group file:

Figure 39. SSL authentication configuration options

6. Scroll down and select **Associate certificate with AS/400 user profile**.
7. Select **Allow retry with user/password** and enter the protection realm name `Emplotee_log_on`.

   This option enables the HTTP server to prompt the user for a user profile and password in case the user presents no valid or no associated certificate.
8. Change the user ID to `%%CLIENT%%` so that the client's user profile is used by the HTTP server. This means that the user profile that the presented certificate is associated with or the user profile entered in the prompt is used by the HTTP server to process client requests.
9. Click **Apply** to update the configuration.

   The HTTP server configuration now has protection directives as follows:

```
Protect /protect/* {
      PasswdFile %%SYSTEM%%
      ACLOverride Off
      DeleteMask All@(*)
      PostMask All@(*)
      PutMask All@(*)
      GetMask All@(*)
      AuthType Cert_Or_Basic
      ServerID Employee_log_on
      UserID %%CLIENT%%
}
```

10. Use the AS/400 system command `STRTCPSVR *HTTP RESTART(*HTTP) HTTPSVR(PROTECT)` to restart the HTTP server instance PROTECT with the new configuration.

4.16.4 Registering certificates to user profiles

The previous steps complete the HTTP configuration; however, we still have to obtain certificates for our employees and associate them with their user profiles. These processes are explained in detail in 5.8, “Working with user certificates in DCM” on page 175.

You can either create your own certificates for users or certificates can be obtained from a well-known CA, such as VeriSign, and registered to a user profile. In either case the certificate holder must use a browser to contact the DCM, log on with his or her user name and password, and follow the procedure to create a new certificate or register an existing certificate. The procedures are not complex, and users are familiar with using a name and password, so a small amount of training plus some good instructions should be all that is needed.

Another way of associating respectively registering certificates with AS/400 user profiles is using APIs within an application. Chapter 8, “Sample application: using APIs with ILE RPG” on page 295 explains how certificates are registered within an application.

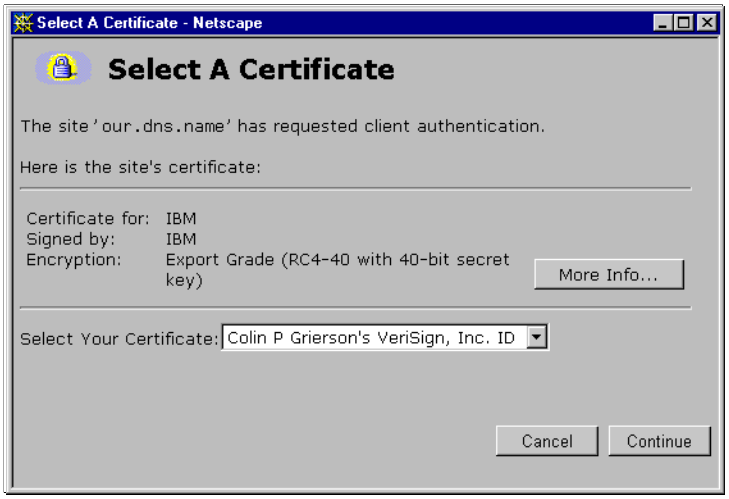
You will need to put some procedures in place to renew certificates before they expire. This topic is discussed in more detail in 1.5.5.4, “Renewing certificates” on page 13.

4.16.5 Testing our configuration

We have two certificates installed in our browser: Colin P Grierson’s VeriSign Inc. ID and Colin’s IBM ID. The VeriSign certificate has been registered to the user profile ITSOCOLIN. The certificate Colin’s IBM ID is not currently registered to a user profile.

4.16.5.1 Try a certificate for an authorized user

1. Start the browser and enter the URL `http://our.dns.name:8083/` to display the welcome page.
2. Click the link to the secured page. Netscape Communicator displays the following window asking for the certificate to use.



The site 'our.dns.name' has requested client authentication.

Here is the site's certificate:

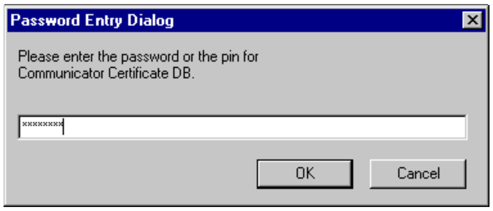
Certificate for: IBM
Signed by: IBM
Encryption: Export Grade (RC4-40 with 40-bit secret key)

Select Your Certificate: Colin P Grierson's VeriSign, Inc. ID

Figure 40. Presenting a user certificate

3. We select the VeriSign certificate associated with user profile `ITSOCOLIN` and click **Continue**.

4. The prompt for entering the certificate's password appears. Type the appropriate password and click **OK**.



Password Entry Dialog

Please enter the password or the pin for Communicator Certificate DB.

****

Figure 41. Password entry dialog prompt

The secured page appears.

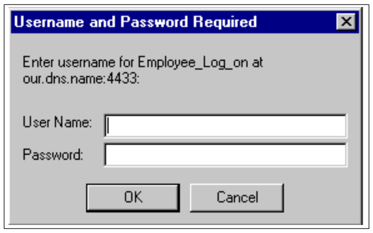
4.16.5.2 Try a certificate that is not associated with a user profile

1. Close the browser and restart it so that it will reestablish the SSL connection and ask for a certificate to use.

2. When the Select a Certificate panel, as shown in Figure 40, appears we select the certificate **Colin's IBM ID**, click **Continue**, and give the appropriate password for the certificate database and click **OK**.

3. The User name and password prompt appears. This is correct because the certificate Colin's IBM ID is not associated with any user profile.

.



Username and Password Required

Enter username for Employee_Log_on at our.dns.name:4433:

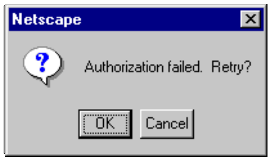
User Name:

Password:

Figure 42. Name/password prompt

4. We type `ITSOCOLIN` as the user and give his password and the secured page appears.

5. Repeat the above process and try a bad password, and a nonexistent user name. In both cases the Authorization failed panel appears as expected.

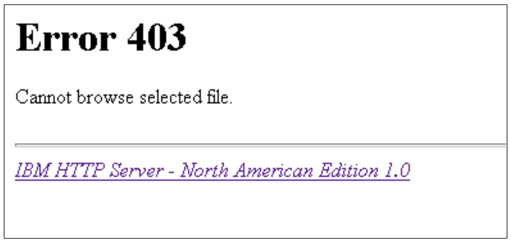


Netscape

Authorization failed. Retry?

Figure 43. Authorization failed panel

6. Try a valid user name that is not authorized to the application. We use `ITSOMINOTE`. Give the correct password. The following error message appears.



Error 403

Cannot browse selected file.

IBM HTTP Server - North American Edition 1.0

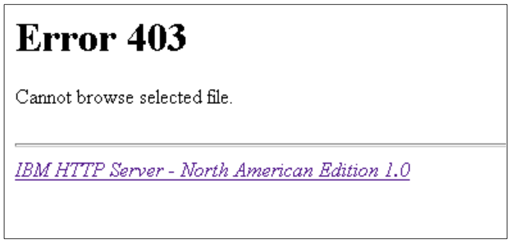
Figure 44. Not authorized

This is correct. ITSOMINOTE does not belong to the group profile HMNRSCAUT and so is not authorized to this application.

4.16.5.3 Try a certificate associated with a user who is not authorized

1. We use the AS/400 system command `CHGAUT OBJ('http/protect') USER(ITSOCOLIN) DTAAUT(*EXCLUDE) OBJAUT(*NONE)` to exclude user ITSOCOLIN from the directory http/protect.
2. Close the browser and restart it so that it will reestablish the SSL connection and ask for a certificate to use.
3. When the Select a Certificate panel, as in Figure 40, appears we select the VeriSign certificate associated with ITSOCOLIN, click **Continue**, type the password for the certificate and click **OK**.

.



Error 403

Cannot browse selected file.

IBM HTTP Server - North American Edition 1.0

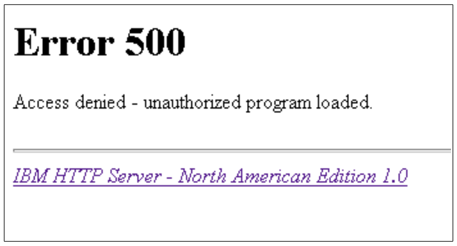
Figure 45. Unauthorized user profile

This seems reasonable to us. The certificate is associated with a user but the user is not authorized to access the files.

4. We use the AS/400 system command `CHGAUT OBJ('http/protect') USER(ITSOCOLIN) DTAAUT(*NONE) OBJAUT(*NONE)` to remove the exclusion of user ITSOCOLIN from the directory http/protect.

Try a certificate associated with a disabled user profile

1. We use the AS/400 system command `CHGUSRPRF ITSOCOLIN STATUS(*DISABLED)` to disable the user profile ITSOCOLIN.
2. Close the browser and restart it so that it will reestablish the SSL connection and ask for a certificate to use.
3. When the Select a Certificate panel, as shown in Figure 40, appears we select the VeriSign certificate associated with ITSOCOLIN, click **Continue**, type the password for the certificate and click **OK.**



Error 500

Access denied - unauthorized program loaded.

IBM HTTP Server - North American Edition 1.0

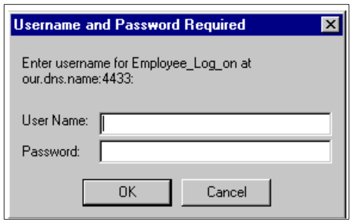
Figure 46. Disabled user profile

The message `Unauthorized program load` lets the user not assume that a disabled user profile causes this problem. So it is not very helpful. However, since the certificate is associated with an AS/400 user profile, the AS/400 system is treating the access request the same as it would be, for example, for an interactive sign-on with user name and password.

4.16.5.4 Try a certificate associated with a user with expired password

1. We use the AS/400 system command `CHGUSRPRF ITSOCOLIN STATUS(*ENABLED) PWDEXP(*YES)` to enable the user profile ITSOCOLIN and set its password to be expired.
2. Close the browser and restart it so that it will reestablish the SSL connection and ask for a certificate to use.
3. When the Select a Certificate window, as shown in Figure 40, appears we select the VeriSign certificate associated with ITSOCOLIN, click **Continue**, enter the password for the certificate and click **OK.**

.



Enter username for Employee_Log_on at our.dns.name:4433:

Figure 47. User name and password prompt

The user name and password prompt appears. The AS/400 system presents the user name / password prompt because the user profile associated with the presented certificate is not allowed to use the system without changing the password. So you have specify in the user profile for Internet users that the password never expires. How could an Internet user change the password without signing on?

1. Close the browser and restart it so that it will reestablish the SSL connection and ask for a certificate to use.
2. Click the link to the secured page.
3. When the Select a Certificate panel, as shown in Figure 40, appears, click **Cancel**.
4. The User name and password prompt appear as in Figure 42. Test an invalid user, an invalid password, and finally an authorized user with its password. The secured page appears.

This concludes the testing for scenario 3.

4.17 Scenario 3b: Client authentication using certificates only

This is almost the same as 4.16, “Scenario 3: Client authentication using certificates or name/password” on page 73 but we will remove the option to use a name and password to connect to the application.

This scenario would be appropriate when the following conditions are important:

- The conditions listed for scenario 3 are true and it is reasonable to use certificates.
- Your clients are mostly familiar with using certificates and not using a user name and password anymore.
- You require the superior authentication possible with certificates and will take the necessary steps to educate your clients in their use and to help your clients obtain certificates.

For example the Web-enabled application from scenario 3 may have been in use for some months. Your company policy is to give each employee a certificate and this is now complete. Few people are still using a name and password. We will check why they are still doing this. If they can start using certificates we will remove the option to give a user name and password.

4.17.1 Objective of scenario 3b

The objective of this scenario is to change the protection directive so using a user name and password is no longer allowed.

Leave the server SSL client authentication optional as there may be other applications that require SSL but not client authentication. If all your applications that use SSL also require client authentication using certificates, you should required SSL client authentication for the server.

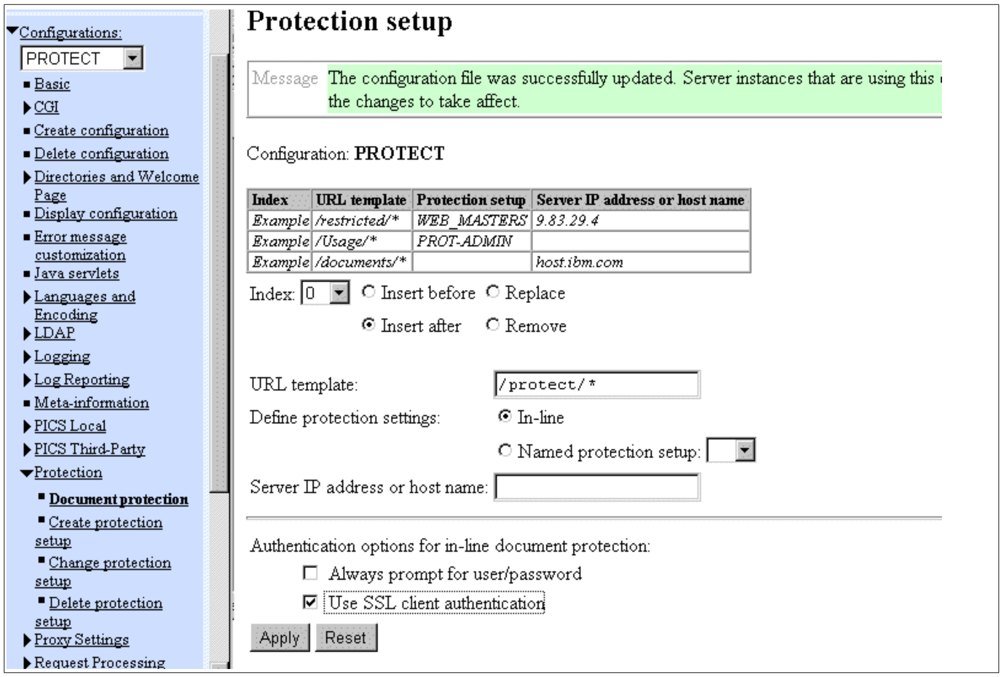
As stated above, the approach of enabling both client authentication with certificates and with user name and password is a good way for a smooth transition to using certificates only. Once you have provided certificates to all users, you can disable the authentication with user names and passwords. Of course, if there are still users authenticating themselves with user names and passwords but are in possession of a certificate, this is the method to force them finally to use certificates.

4.17.2 Creating the protection setup

The Protect directive for scenario 3b allows only client authentication using digital certificates. Authentication with user name and password is not allowed anymore. The following steps show how to set up the directive:

1. Start the HTTP Configuration and Administration utility.
2. Click **Protection** then **Document protection** in the navigation panel.
3. Select the index number of the existing `/protect/*` directive and click **Remove**.
4. Click **Apply**. This removes the old protection setup.

5. Select **Insert after** and enter `/protect/*` for the URL template, then select **Use SSL client authentication**



Protection setup

Message The configuration file was successfully updated. Server instances that are using this
the changes to take affect.

Configuration: **PROTECT**

Index	URL template	Protection setup	Server IP address or host name
Example	*/restricted/**	*WEB_MASTERS*	*9.83.29.4*
Example	*/Usage/**	*PROT-ADMIN*	
Example	*/documents/**		*host.ibm.com*

Index: 0 ○ Insert before ○ Replace

● Insert after ○ Remove

URL template: /protect/*

Define protection settings: ● In-line

○ Named protection setup:

Server IP address or host name:

Authentication options for in-line document protection:

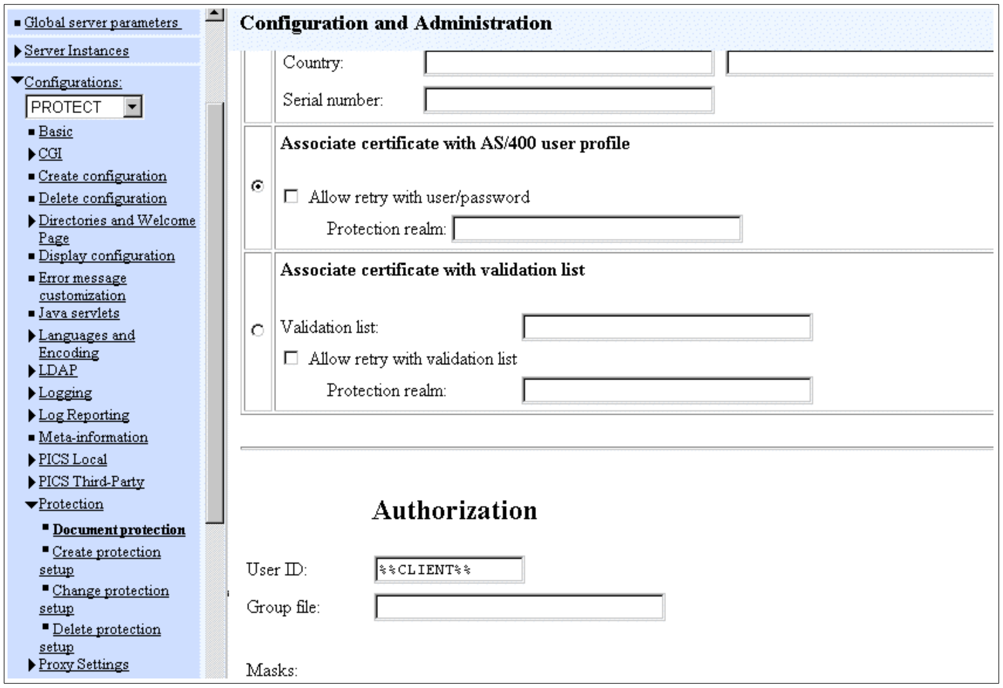
☐ Always prompt for user/password

☑ Use SSL client authentication

Figure 48. Protection setup scenario 3b - basic settings

6. Click **Apply** to continue creating the new protection setup. The SSL authentication panel appears

.



Configuration and Administration

Country:

Serial number:

● **Associate certificate with AS/400 user profile**

☐ Allow retry with user/password

Protection realm:

○ **Associate certificate with validation list**

Validation list:

☐ Allow retry with validation list

Protection realm:

Authorization

User ID: %%CLIENT%%

Group file:

Masks:

Figure 49. Protection setup scenario 3b - SSL authentication panel

7. Select **Associate certificate with AS/400 user profile** and change the user ID to `%%CLIENT%%` so that the client's user profile is used by the HTTP server.
8. Click **Apply** to update the configuration.

   The HTTP server configuration now has the protection directive as follows:

```
Protect /protect/* {
      PasswdFile %%SYSTEM%%
      ACLOverride Off
      DeleteMask All@(*)
      PostMask All@(*)
      PutMask All@(*)
      GetMask All@(*)
      AuthType Cert
      UserID %%CLIENT%%
}
```

9. Use the AS/400 system command `STRTCPSVR *HTTP RESTART(*HTTP) HTTPSVR(PROTECT)` to restart the HTTP server instance PROTECT with the new configuration.

4.17.3 Testing our configuration

We have two certificates installed in our browser: Colin P Grierson's VeriSign Inc. ID. and Colin's IBM ID. The VeriSign certificate has been registered to the user profile ITSOCOLIN. The certificate Colin's IBM ID is not currently registered to a user profile.

4.17.3.1 Try a valid certificate associated with a user who is authorized

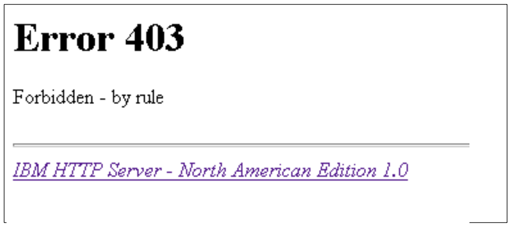
1. Display the welcome page and click the link to the secured page. The window appears asking for the certificate to use, as shown in Figure 40 on page 78.
2. We select the VeriSign certificate that is associated with user ITSOCOLIN, click **Continue**, enter the password for the certificate and click **OK**.

   The secured page appears.

4.17.3.2 Try a certificate that is not associated with a user profile

1. Close the browser and restart it so that it will reestablish the SSL connection and ask for a certificate to use.
2. When the Select a Certificate window, as shown in Figure 40, appears we select the certificate **Colin's IBM ID**, click **Continue**, enter the password for the certificate and click **OK**.

.



Error 403

Forbidden - by rule

IBM HTTP Server - North American Edition 1.0

Figure 50. Not associated with a user profile

Note

Actually the first time we tested this the secured page did appear. A little investigation found two problems.

The first problem was that we had not thought to verify the authorities to the protected directory in 4.15.3, “AS/400 system authorities” on page 68. The default HTTP server job user profile, QTMHHTTP, still had authority to the protected directory.

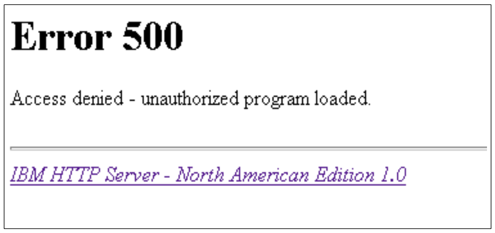
Second was that we had mistyped the URL template on the Protect directive and were not protecting our directory at all.

So we corrected the URL template, fixed the authorities, and repeated our testing. This proves that it is always important to carefully set up and test the implementation before going into production.

Try a certificate associated with a disabled user profile

1. We use the AS/400 system command `CHGUSRPRF ITSOCOLIN STATUS(*DISABLED)` to disable the user profile ITSOCOLIN.
2. Close the browser and restart it so that it will reestablish the SSL connection and ask for a certificate to use.
3. When the Select a Certificate window, as shown in Figure 40, appears we select the VeriSign certificate associated with ITSOCOLIN, click **Continue**, enter the password for the certificate and click **OK.**

.



Error 500

Access denied - unauthorized program loaded.

IBM HTTP Server - North American Edition 1.0

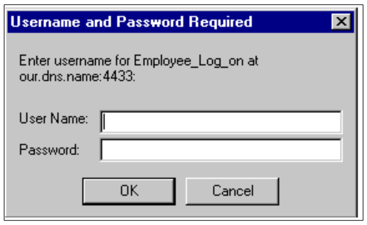
Figure 51. Disabled user profile

Refusing the connection is correct but the message `Unauthorized program loaded` is not very helpful.

4.17.3.3 Try an associated certificate with an expired password

1. We use the AS/400 system command `CHGUSRPRF ITSOCOLIN STATUS(*ENABLED) PWDEXP(*YES)` to enable the user profile ITSOCOLIN and set its password to be expired.
2. Close the browser and restart it so that it will reestablish the SSL connection and ask for a certificate to use.
3. When the Select a Certificate window, as shown in Figure 40, appears we select the VeriSign certificate associated with ITSOCOLIN, click **Continue**, enter the password for the certificate database and click **OK**.

.


Username and Password Required

Enter username for Employee_Log_on at our.dns.name:4433:

User Name:

Password:

Figure 52. Unknown user /password prompt

A prompt for user name and password appears. Giving a valid AS/400 user name and password results in the message `Authorization failed` so you cannot get anywhere.

From the configuration point of view the AS/400 system should not trigger the browser to present the prompt for user name and password. Since this phenomenon has no impact on the security functions itself, the OS/400 will be changed in a future so that the prompt will not appear anymore.

This concludes scenario 3b.

4.18 Scenario 4: Using distinguished name settings on certificates

In this scenario users are accepted if they have valid certificates with certain attributes.

This scenario would be appropriate when the following conditions are important:

- There are a large number of users who may access your application and they all have the same authorities within the application.
- There is no reason to create user profiles on the AS/400 system for users of your application. (Creating and maintaining user profiles is a bit of work. If some users come to your system only to use your HTTP application it would be an advantage not to have to create user profiles or otherwise register them.)
- Your company is in control of issuing the user’s certificates so that you can be sure the attributes on them are correct and can be used for your purposes.
- The certificate attributes you will be using to control access to your system do not change often.

These conditions might be true for a system in a large organization where a group of users, such as human resource managers, need to access a particular system. There would need to be an attribute of the user’s distinguished name, or the CA’s distinguished name, that can be used to identify the group.

4.18.1 Objectives of scenario 4

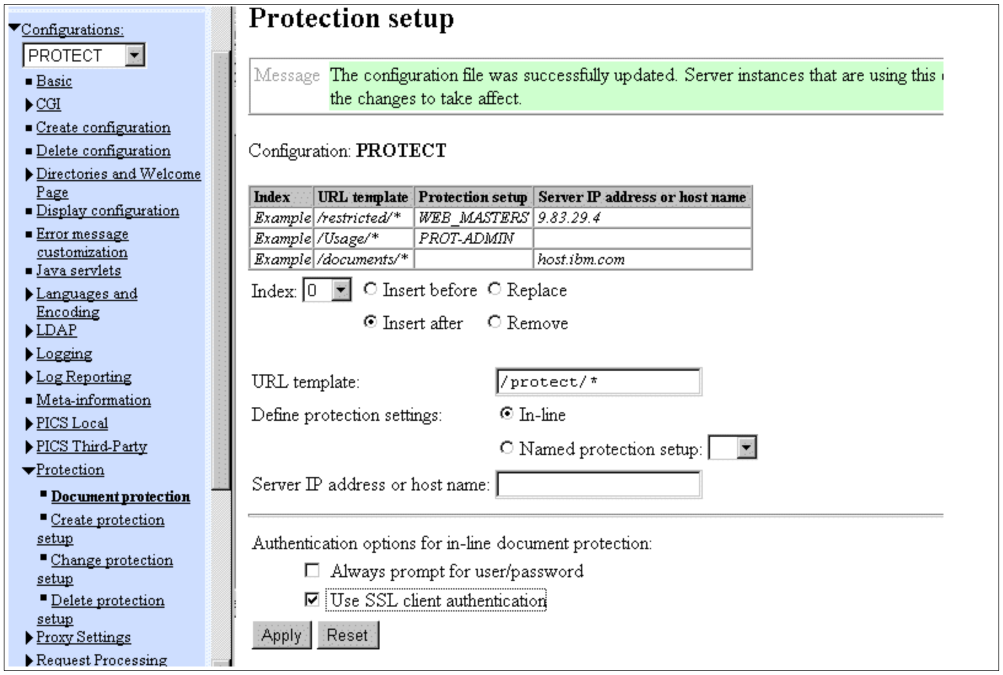
The objectives of this scenario are:

- Continue using SSL to protect the communications and use protection setups to ensure client authentication using certificates.
- Change the protection setup to allow certificates only with the correct attributes to access our application.

4.18.2 Creating the protection setup

The Protect directive used in this scenario will check for certain DN attributes in a certificate presented by a user. The following steps show how to define such a directive:

1. Start the HTTP Configuration and Administration utility.
2. Click **Protection** then **Document protection** in the navigation panel.
3. Select the index number of the existing `/protect/*` directive and click **Remove**.
4. Click **Apply**. This removes the old protection setup.
5. Select **Insert after** and enter `/protect/*` for the URL template, then select **Use SSL client authentication**.



Protection setup

Message: The configuration file was successfully updated. Server instances that are using this
the changes to take affect.

Configuration: **PROTECT**

Index	URL template	Protection setup	Server IP address or host name
Example	*/restricted/**	*WEB_MASTERS*	*9.83.29.4*
Example	*/Usage/**	*PROT-ADMIN*	
Example	*/documents/**		*host.ibm.com*

Index: 0 ○ Insert before ○ Replace

● Insert after ○ Remove

URL template: /protect/*

Define protection settings: ● In-line

○ Named protection setup:

Server IP address or host name:

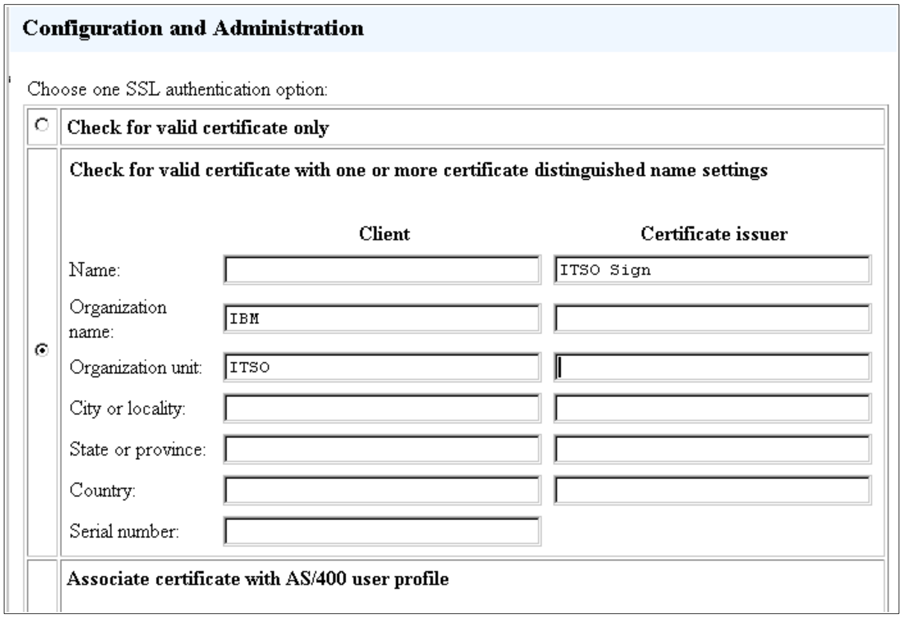
Authentication options for in-line document protection:

□ Always prompt for user/password

☑ Use SSL client authentication

Figure 53. Protect directive scenario 4 - basic settings

6. Click **Apply**. The configuration window for SSL client authentication appears.



Configuration and Administration

Choose one SSL authentication option:

○ **Check for valid certificate only**

● **Check for valid certificate with one or more certificate distinguished name settings**

	Client	Certificate issuer
Name:		ITSO Sign
Organization name:	IBM	
Organization unit:	ITSO	
City or locality:		
State or province:		
Country:		
Serial number:		

Associate certificate with AS/400 user profile

Figure 54. Use certificate DN settings

7. As shown in Figure 54, we specify settings to ensure the certificate has been issued by our company CA and has the correct attributes for accessing our application.

   Further down on the window set the user ID to `HMNRSCAUT`, so that the HTTP server will switch to use a user profile authorized to our application, then click **Apply**.

8. The HTTP server configuration now includes the protection directive as follows:

```
Protect /protect/* {
      OrgUnit ITSO
      Organization IBM
      IssuerCommonName "ITSO Sign"
      ACLOverride Off
      Mask Anybody@(*)
      UserID HMNRSCAUT
```

9. Use the AS/400 system command `STRTCPSVR *HTTP RESTART(*HTTP) HTTPSVR(PROTECT)` to restart the HTTP server instance PROTECT with the new configuration.

4.18.3 Testing our configuration

We have two certificates installed in our browser: Colin P Grierson's VeriSign Inc. ID. and Colin's IBM ID. The certificate Colin's IBM ID was issued by our test CA and should have the correct attributes to be accepted by the Protect directive. The VeriSign certificate should be rejected.

4.18.3.1 Try a valid certificate with the correct attributes

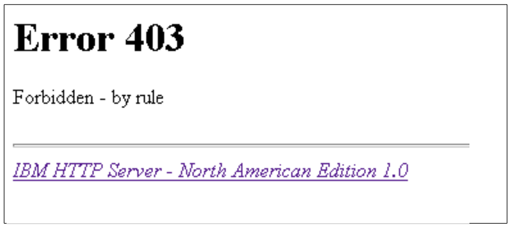
1. Display the welcome page and click the link to the secured page. The window appears asking for the certificate to use as shown in Figure 40 on page 78.

2. We select the certificate **Colin's IBM ID,** click **Continue**, enter the password for the certificate database and click **OK**.

The secured page appears.

4.18.3.2 Try a certificate that has no matching DN attributes

1. Close the browser and restart it so that it will reestablish the SSL connection and ask for a certificate to use.
2. When the Select a Certificate window, as shown in Figure 40, appears we select the VeriSign certificate, click **Continue**, enter the password for the certificate database, and click **OK**. The following error message appears:



Error 403

Forbidden - by rule

IBM HTTP Server - North American Edition 1.0

Figure 55. Invalid certificate rejected

This concludes scenario 4.

4.19 Scenario 5: Using validation lists

In this scenario we will use two validation lists to hold user names and passwords. These are used to control who can have access to our system.

Validation lists can also be used to hold certificates. When this is done users can use their certificates to identify themselves instead of a user name and password or they can use either with certificates and AS/400 user profiles. To receive certificates and put them into a validation list requires programming using the security APIs of the AS/400 system. An example of this is provided in Chapter 8, “Sample application: using APIs with ILE RPG” on page 295.

This scenario would be appropriate when the following conditions are important:

- The users who access your HTTP application do not need to access your AS/400 system in other ways and so do not need AS/400 user profiles.
- Users must be registered and approved before they can access the system.

A service provided through the Internet for which users are charged is a situation where using validation lists would be appropriate.

The HTTP Configuration and Administration utility has some facilities for managing user names and passwords on validation lists under the category Internet Users. The facilities are fairly limited and are not intended for managing a production system. Programming work is needed using APIs to register user certificates in validation lists. However, the configuration utility functions are perfect for doing testing as we are doing in this scenario. Details of the validation list API programs can be found in *OS/400 Security APIs,* SC41-5872.

4.19.1 Scenario 5 objectives

The objectives of this scenario are:

- Create two validation lists for holding user names and passwords.
- Create a named protection setup using the two validation lists.
- Create a Protect directive using the named protection setup.
- Authenticate users through user names and passwords.

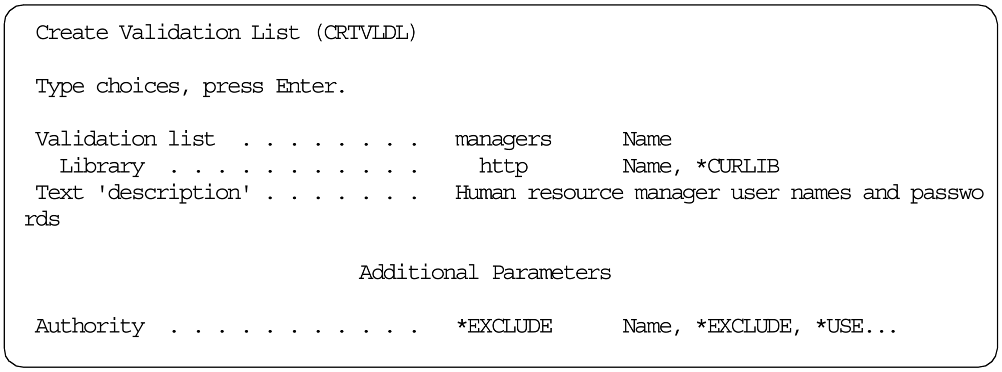
4.19.2 Creating and populating validation lists

A validation list is a multi-purpose object that has a structure to store unencrypted and encrypted data.

The following steps show how validation lists are created and Internet users added to them.

1. Create a validation list explicitly by using the AS/400 system command `CRTVLDL`.

   Following is the prompt for the Create Validation List command.



```
 Create Validation List (CRTVLDL)

 Type choices, press Enter.

 Validation list . . . . . . . .   managers      Name
   Library . . . . . . . . . . .     http        Name, *CURLIB
 Text 'description' . . . . . . .   Human resource manager user names and passwo
rds

                            Additional Parameters

 Authority . . . . . . . . . . .   *EXCLUDE      Name, *EXCLUDE, *USE...
```

Figure 56. Creating a validation list

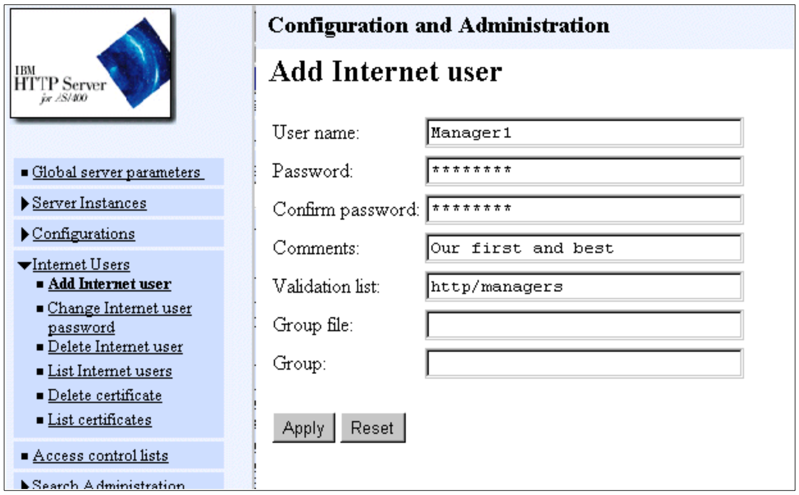
Validation lists can be created manually as shown in this scenario or are automatically created when adding Internet users.

2. Add a new user to the validation list created in the previous step.

Figure 57 is the configuration utility window for adding a user and password to a validation list.

To add a user, start the HTTP Configuration and Administration utility, then click **Internet Users** and then **Add Internet user** in the navigation panel.

.



Configuration and Administration

Add Internet user

User name: Manager1
Password: ********
Confirm password: ********
Comments: Our first and best
Validation list: http/managers
Group file:
Group:

Figure 57. Adding users to a validation list

We are adding Manager1 to our managers validation list. The group file options which are discussed in 4.20, “Scenario 6: Using an access control list and a group file” on page 95 are not used in scenario 5.

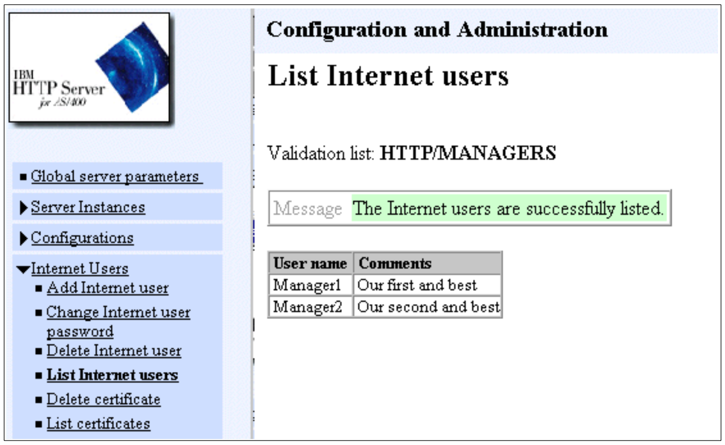
The configuration utility will create the validation list if it does not already exist. If you use this facility you should later sign on to the AS/400 system to set the object description of the validation list and to review the authority on it. Use the commands CHGOBJD and EDTOBJAUT to do this. Be sure to set the object description. All permanent objects should have a meaningful description.

- You should review the authorities to your validation lists.
- The default for public authority is *EXCLUDE.
- If you use the configuration utility to create a validation list it gives the QTMHHTTP user profile *USE authority to the new list.
- The user profile running the HTTP server job that need to access the list will need *USE or higher authority to the list. Other user profiles may need authority depending on your application design.

For this scenario, the validation lists STAFF and MANAGERS are created. Furthermore some test internet users have been added to the lists.

3. To display the users within the validation lists, select **Internet Users->List Internet Users**. Specify HTTP/MANAGERS for the name of the validation list.

   All defined Internet users are listed as shown in Figure 58.



Configuration and Administration

List Internet users

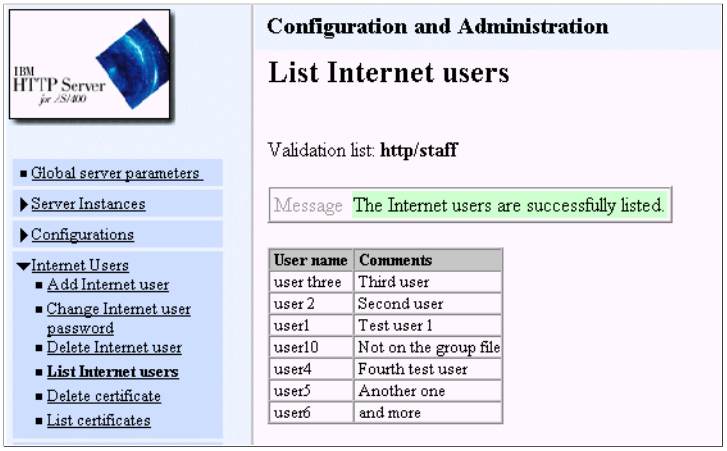
Validation list: **HTTP/MANAGERS**

Message The Internet users are successfully listed.

User name	Comments
Manager1	Our first and best
Manager2	Our second and best

Figure 58. Managers validation list

4. Repeat the previous step to display the users in the HTTP/STAFF validation list.



Configuration and Administration

List Internet users

Validation list: **http/staff**

Message The Internet users are successfully listed.

User name	Comments
user three	Third user
user 2	Second user
user1	Test user 1
user10	Not on the group file
user4	Fourth test user
user5	Another one
user6	and more

Figure 59. Staff validation list

We have authorized the QTMHHTTP user profile to our validation lists.

Note

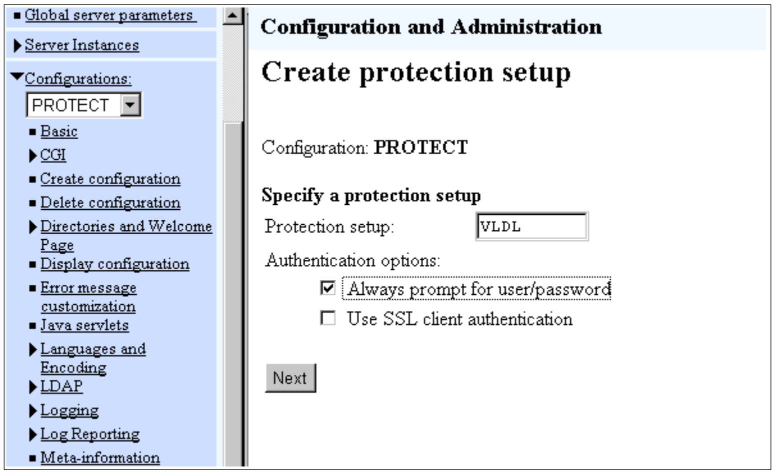
The user profile that needs authority to the validation list, or lists, is the user profile running the HTTP server instance, not the user profile named on the protection directive.

In our example the protection directive names HMNRSCAUT as the user profile but we do not need to give this user any authority at all to the STAFF or MANAGERS validation lists.

4.19.3 Creating a named protection setup

We will create a named protection setup that can be referred to many times within an HTTP server configuration. This could be useful when you have several directories or files you want to protect in the same way.

1. Click **Protection** and then **Create protection setup** in the configuration utility navigation panel.



Configuration and Administration

Create protection setup

Configuration: PROTECT

Specify a protection setup

Protection setup: VLDL

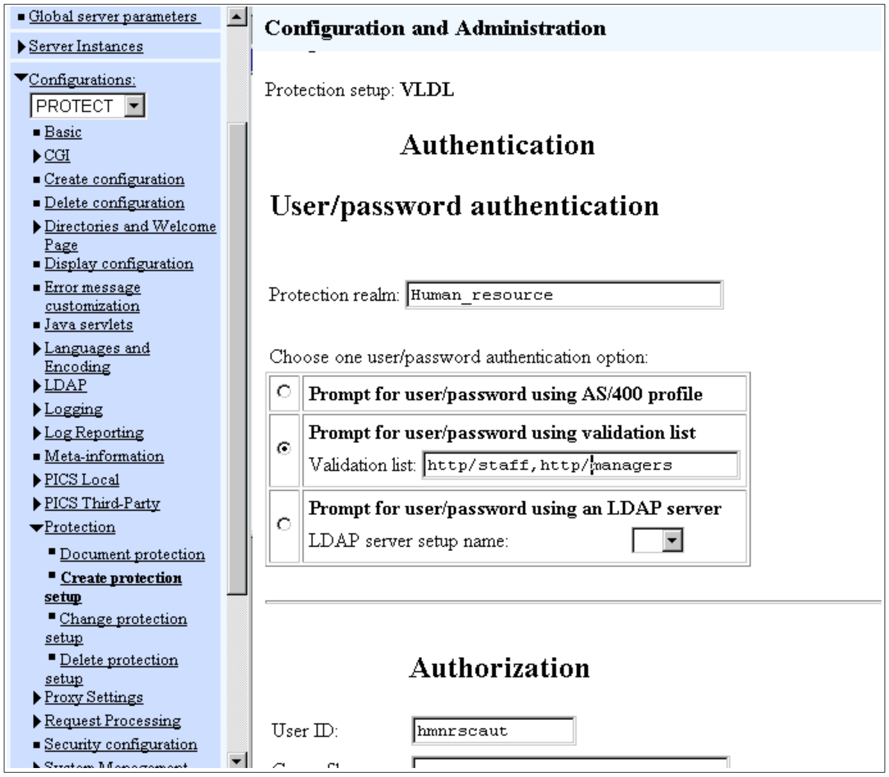
Authentication options:

☑ Always prompt for user/password

☐ Use SSL client authentication

Figure 60. Create a named protection setup

2. Type the name of the protection setup and select the desired type of client authentication. Click **Next**. The authentication options are shown.



Configuration and Administration

Protection setup: VLDL

Authentication

User/password authentication

Protection realm: Human_resource

Choose one user/password authentication option:

○ Prompt for user/password using AS/400 profile

● Prompt for user/password using validation list
Validation list: http/staff,http/managers

○ Prompt for user/password using an LDAP server
LDAP server setup name:

Authorization

User ID: hmnrscaut

Figure 61. Protection using a validation list

3. Select **Prompt for user/password using validation list** and type the validation list or lists to be checked for user names. In our case we have two validation lists so we enter them both, separated by a comma. Remember to include the library names, since these are required.

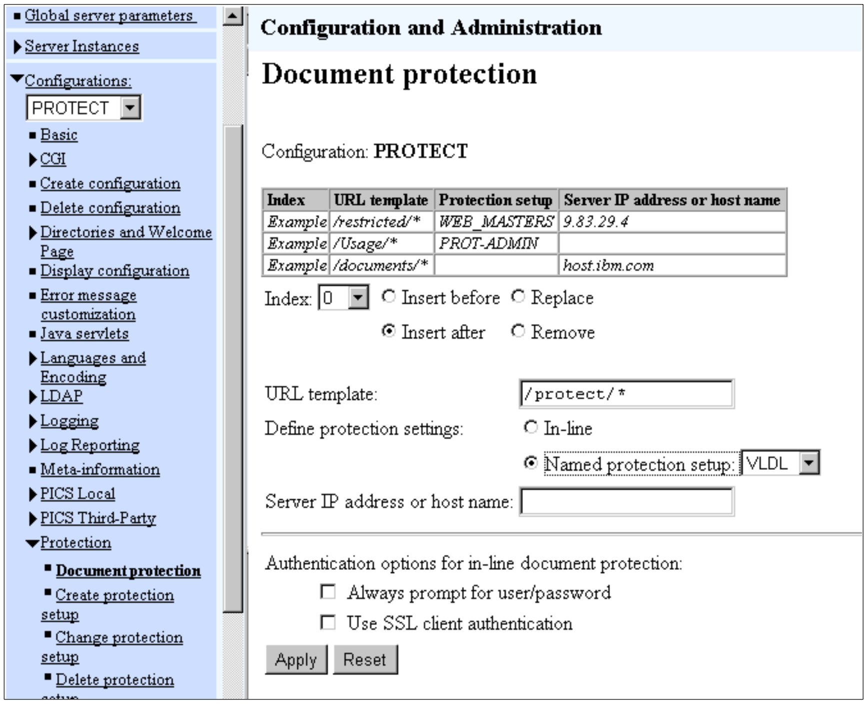
Enter the user profile name that will be used to access the protected application. Because only certain user profiles have access to the protected directory, we will use HMNRSCAUT for the user profile. The default value %%SERVER%% would refer to the default HTTP server job user profile, QTMHHTTP. This gives us another level of protection.

4. Click **Apply** to create the protection setup.

4.19.4 Create a Protect directive using a named protection setup

We will create a protection directive for our protected directory by referring to the named protection setup VLDL as shown in the following steps.

1. Click **Protection->Document protection** in the navigation panel to display the active protection setups.
2. If there are any protection setups that should not be in your configuration remove them. For this scenario we have removed the Protect directive for the URL template /protect/*.



Configuration and Administration

Document protection

Configuration: **PROTECT**

Index	URL template	Protection setup	Server IP address or host name
Example	*/restricted/**	*WEB_MASTERS*	*9.83.29.4*
Example	*/Usage/**	*PROT-ADMIN*	
Example	*/documents/**		*host.ibm.com*

Index: 0 ○ Insert before ○ Replace
● Insert after ○ Remove

URL template: /protect/*

Define protection settings: ○ In-line
● Named protection setup: VLDL

Server IP address or host name:

Authentication options for in-line document protection:
□ Always prompt for user/password
□ Use SSL client authentication

Apply Reset

Figure 62. Using a named protection setup

3. Define the URL template /protect/*. Then select in the Named protection setup: parameter the VLDL entry from the drop-down list.

   No further configuration needs to be done since all authentication options are already defined in the named protection setup.

4. Click **Apply** to create the Protect directive.

The configuration now includes the directives as follows:

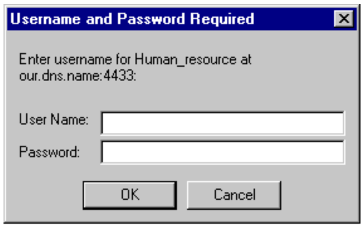
```
Protection VLDL {
      PasswdFile HTTP/STAFF,HTTP/MANAGER
      ACLOverride Off
      DeleteMask All@(*)
```

```
        PostMask All@(*)
        PutMask All@(*)
        GetMask All@(*)
        AuthType Basic
        ServerID Human_resource
        UserID hmnrscaut
}
Protect /protect/* VLDL
```

5. Use the AS/400 system command `STRTCPSVR *HTTP RESTART(*HTTP) HTTPSVR(PROTECT)` to restart the HTTP server instance PROTECT with the new configuration.

4.19.5 Testing the new configuration

1. Close and restart your browser to ensure to prompt for client authentication.
2. Display the welcome page and click the link to the secured page. The user name and password prompt appears.


Username and Password Required

Enter username for Human_resource at our.dns.name:4433:

User Name:

Password:

Figure 63. User name and password prompt

3. Try to perform the authentication with existing user names from both validation lists, with invalid user names, and with valid user names but wrong passwords.

Note

- User names are case sensitive.
- Passwords are case sensitive.
- User names can have spaces in them.
- Passwords can have spaces in them - you can use a phrase not just a word.

4.20 Scenario 6: Using an access control list and a group file

This scenario uses an access control list and a group file to limit access to files in the protected directory.

This scenario would be appropriate when the following conditions are important:

- You want to limit access to a large number of files in a directory and would require many protection directives to achieve this.
- The clients who can access your application are registered and managed on another system. The list of valid clients is periodically sent to your system.
- You wish to give some clients more access than others to files in your system. For example, you may wish to allow certain clients the ability to use the PUT directive to publish files to a directory on your system.

AS/400 system authorities and client authentication using AS/400 user profiles is a more secure way of doing this.

4.20.1 Objectives of scenario 6

The objectives of this scenario are:

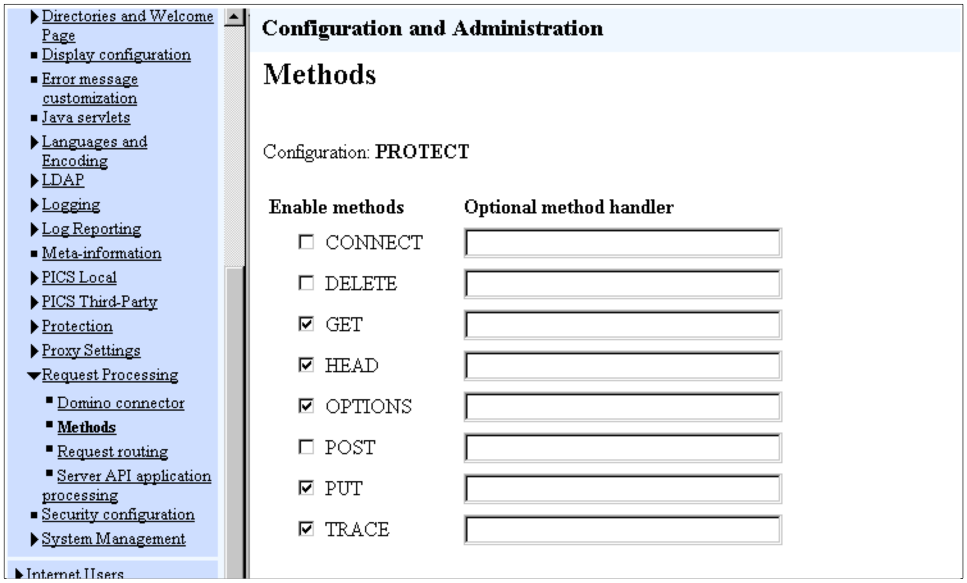
- Create and test several configurations using group files, protection setups masks, and access control lists.
- Use a Protect directive mask to control access to a directory.
- Create a group file and use this with Protect directive masks to control access to a directory.
- Create an access control list and use this to control access to files in a directory.

Scenario 6 will use scenario 5 as a base. The validation lists STAFF and MANAGERS hold all the valid client names and passwords.

4.20.2 Using a Protect directive mask

We enable the PUT directive for the HTTP server instance and use a Protect directive to limit its use to the PUT directory only.

1. Start the HTTP Configuration and Administration utility and expand Configurations.
2. Click **Request processing** and then **Methods** in the configuration utility navigation panel. The Methods configuration panel is displayed.



Configuration and Administration

Methods

Configuration: **PROTECT**

Enable methods	Optional method handler
☐ CONNECT	
☐ DELETE	
☑ GET	
☑ HEAD	
☑ OPTIONS	
☐ POST	
☑ PUT	
☑ TRACE	

Figure 64. Enabling PUT Method

3. Check next to PUT and then click **Apply** further down the window. The following directives are added to the HTTP server configuration:

```
Disable CONNECT
Disable DELETE
Disable POST
Enable GET
Enable HEAD
Enable OPTIONS
Enable PUT
Enable TRACE
```

The request methods configured through this step enable or disable the request methods for the entire server instance. However, methods that are disabled for the server instance cannot be enabled within a Protect directive. But methods enabled for a server instance can be disabled for a particular Protect directive.

4. Use the AS/400 system command `CRTDIR DIR('/http/put')` to create a new directory called PUT in the HTTP directory.
5. Use the AS/400 system command `CHGAUT OBJ('/http/put') USER(HMNRSCAUT) DTAAUT(*RWX) OBJAUT(*ALL)` to grant the AS/400 user profile HMNRSCAUT all authority to the directory http/put.
6. Add the routing directive `Pass /put/* /http/put/*` to the configuration so an Internet user can access the new directory. To add the Pass directive, click **Request processing->Request routing** within the configuration section of the HTTP Configuration and Administration utility.
7. Create a Protect directive to validate users and allow the use of the method PUT within the directory PUT.
   d. Click **Protection->Document protection** in the navigation panel.
   e. Type `/put/*` for the URL template, select **Always prompt for user/password**, and then click **Apply**.
   f. In the Protection setup window enter `Human_Rsc_Maint` for the Protection realm, select **Prompt for user/password using validation list**, and type `http/staff,http/managers` for the validation list. Set **User ID:** to `HMNRSCAUT`, then click **Apply**.

   The following directive is added to the configuration:

```
Protect /put/* {
      PasswdFile HTTP/STAFF,HTTP/MANAGERS
      ACLOverride Off
      DeleteMask All@(*)
      PostMask All@(*)
      PutMask All@(*)
      GetMask All@(*)
      AuthType Basic
      ServerID Human_resources
      UserID hmnrscaut
}
```

Note that the configuration utility defaults to creating Protect directives that allow all methods for all authenticated clients.

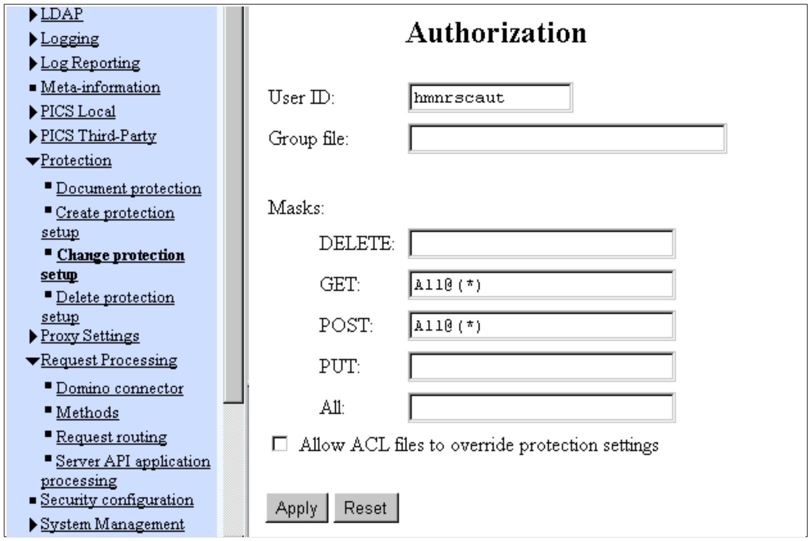
Preparing the test environment

For the application test, the named protection setup VLDL that is referred to in the Protect directive for the /protect/* directory must be changed. The changes are to disable the PUT and DELETE method as shown in the following steps:

1. Click **Protection->Change protection setup** in the navigation panel.
2. Ensure the correct protection setup is selected, in this case VLDL, and then click **Next**.

3. Ensure **Change current user/password authentication settings** is selected and then click **Next**.

4. Clear the input boxes beside the DELETE and PUT masks.



Authorization

User ID: hmnrscaut

Group file:

Masks:

DELETE:

GET: All@(*)

POST: All@(*)

PUT:

All:

□ Allow ACL files to override protection settings

Figure 65. Disabling DELETE and PUT

5. Click **Apply**.

   The named protection directive VLDL is now as follows:

```
Protection VLDL {
      PasswdFile HTTP/STAFF,HTTP/MANAGERS
      ACLOverride Off
      PostMask All@(*)
      GetMask All@(*)
      AuthType Basic
      ServerID Human_resource
      UserID hmnrscaut
}
```

6. Use the AS/400 system command `STRTCPSVR *HTTP RESTART(*HTTP) HTTPSVR(PROTECT)` to restart the HTTP server instance PROTECT with the new configuration.

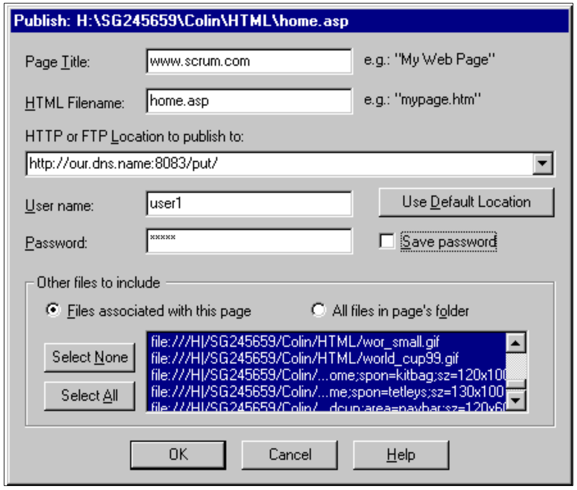
4.20.3 Testing the protection directive mask directive

Testing the PUT method requires an application that enables and build the correct data stream to be sent to the HTTP server. The Netscape composer uses the PUT method to publish objects, such as HTML pages, graphic files, and so on. In this scenario the Netscape composer is used to publish, which means to upload, HTML pages and it is presumed that the Netscape preferences are already configured.

4.20.3.1 Try publishing a document into the directory PUT

1. Open or create a Web page in Netscape composer.

2. Click the **Publish** icon.



Publish: H:\SG245659\Colin\HTML\home.asp

Page Title: www.scrum.com e.g.: "My Web Page"

HTML Filename: home.asp e.g.: "mypage.htm"

HTTP or FTP Location to publish to:

http://our.dns.name:8083/put/

User name: user1

Password: *****

□ Save password

Other files to include

● Files associated with this page ○ All files in page's folder

file:///H|/SG245659/Colin/HTML/wor_small.gif
file:///H|/SG245659/Colin/HTML/world_cup99.gif
file:///H|/SG245659/Colin/...ome;spon=kitbag;sz=120x100
file:///H|/SG245659/Colin/...me;spon=tetleys;sz=130x100
file:///H|/SG245659/Colin/...dcup;area=navbar;sz=120x60

Figure 66. Publishing from Netscape Composer

3. We set the URL to publish to `http://our.dns.name:8083/put/` and then click **OK**.

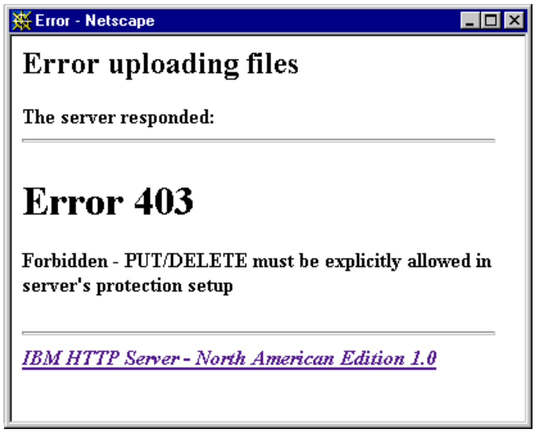
Note

When we tried to publish more than one file that did not exist on the AS/400 system, an error message was shown indicating an upload error. However, that had nothing to do with HTTP server configuration. When uploading just one file or updating existing files, all worked fine.

Looking at the directory /http/put we see one of the files we wanted to publish. That is enough to prove our Protect directives are working as desired.

4.20.3.2 Publishing document into PROTECT and PUBLIC directories

1. We set the URL to publish to `http://our.dns.name:8083/protect` and then click **OK**. This attempts to publish the files into the directory /http/protect, which does not allow the PUT request method. The following error message confirms our configuration.



Error - Netscape

Error uploading files

The server responded:

Error 403

Forbidden - PUT/DELETE must be explicitly allowed in server's protection setup

IBM HTTP Server - North American Edition 1.0

Figure 67. PUT not allowed

2. We set the URL to publish to `http://our.dns.name:8083/` and then click **OK**. This attempts to publish the files into the directory /http/public, which does not

have a protection directive in place. Again we receive the error message as shown in Figure 67.

Note

For the methods PUT or DELETE to be used they must be explicitly allowed using a Protect directive that matches the incoming URL. If no Protect directive matches a URL, PUT and DELETE cannot be used.

The HTTP Configuration and Administration utility defaults to explicitly allowing GET, POST, PUT, and DELETE. If you enable PUT or DELETE be very careful when you use the configuration utility to create Protect directives that you do not inadvertently allow PUT and DELETE where they should not be allowed.

4.20.4 Using a group file

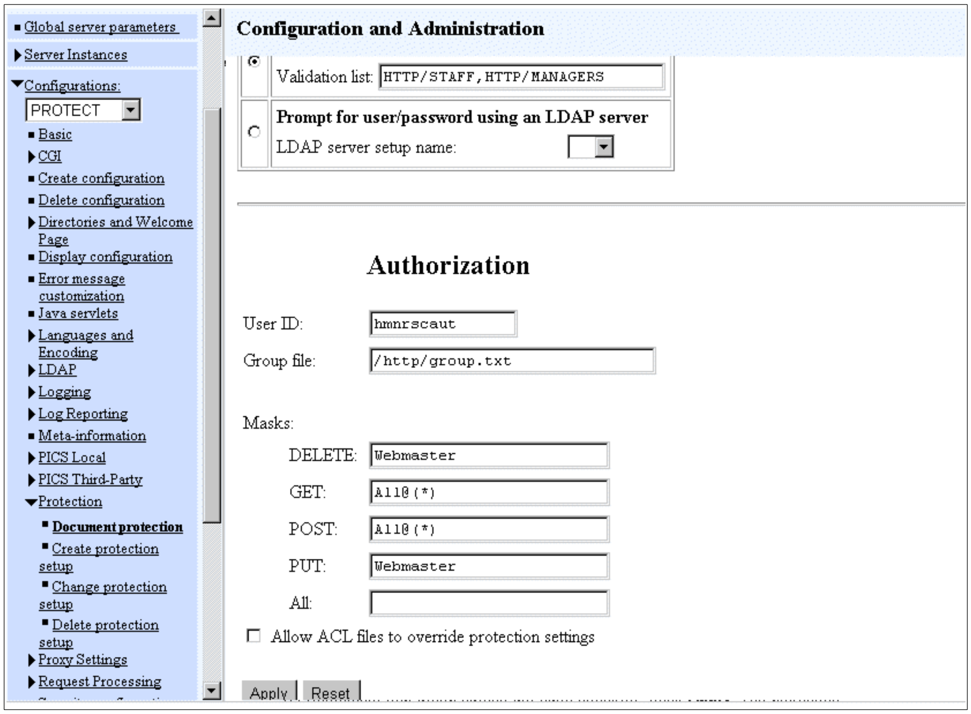
We will create a group file to allow us to group our clients in a number of ways. One of the groups will be Webmaster. We will change the Protect directive for the PUT directory so that only members of the Webmaster group can use the PUT directive there.

The HTTP Configuration and Administration utility has a facility for adding user names to group files. To add users to groups click **Internet Users->Add Internet user** in the navigation panel. We have used this to set up a simple group file as follows:

```
System1: user1, user2, userthree
System2: user4
System3: user5, user6
Webmaster: user1, Manager2
```

For more information about group files see *HTTP Server for AS/400 Webmaster's Guide,* GC41-5434.

1. Create a group file such as shown in this scenario.
2. Change the Protect directive for the URLs /put/* so that the PUT and DELETE directives are only allowed for the group Webmaster.



Configuration and Administration

● Validation list: HTTP/STAFF,HTTP/MANAGERS

○ Prompt for user/password using an LDAP server
LDAP server setup name:

Authorization

User ID: hmnrscaut

Group file: /http/group.txt

Masks:

DELETE: Webmaster

GET: All@(*)

POST: All@(*)

PUT: Webmaster

All:

□ Allow ACL files to override protection settings

Figure 68. Restrict DELETE and PUT to a group

3. Remember that group names are case sensitive. Click **Apply**. The Protect directive is now as follows:

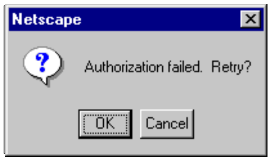
```
Protect /put/* {
      GroupFile /http/group.txt
      PasswdFile HTTP/STAFF,HTTP/MANAGERS
      ACLOverride Off
      DeleteMask Webmaster
      PostMask All@(*)
      PutMask Webmaster
      GetMask All@(*)
      AuthType Basic
      ServerID Human_resources
      UserID hmnrscaut
}
```

4. Use the AS/400 system command `STRTCPSVR *HTTP RESTART(*HTTP) HTTPSVR(PROTECT)` to restart the HTTP server instance PROTECT with the new configuration.

Testing our configuration

1. Close Netscape Composer and Navigator, then restart it so it performs the client authentication procedure.

2. Attempt to publish to directory `PUT` with user name `user7`, which does not exist. The authorization failed message appears as follows:



Authorization failed. Retry?

Figure 69. Authorization failed

3. Click **OK** then try user name `user2`, which does exist but is not in the group Webmaster. Again the authorization panel appears as in Figure 69.
4. Click **OK** then try user name Manager2, which is in the group Webmaster. This time files are published.

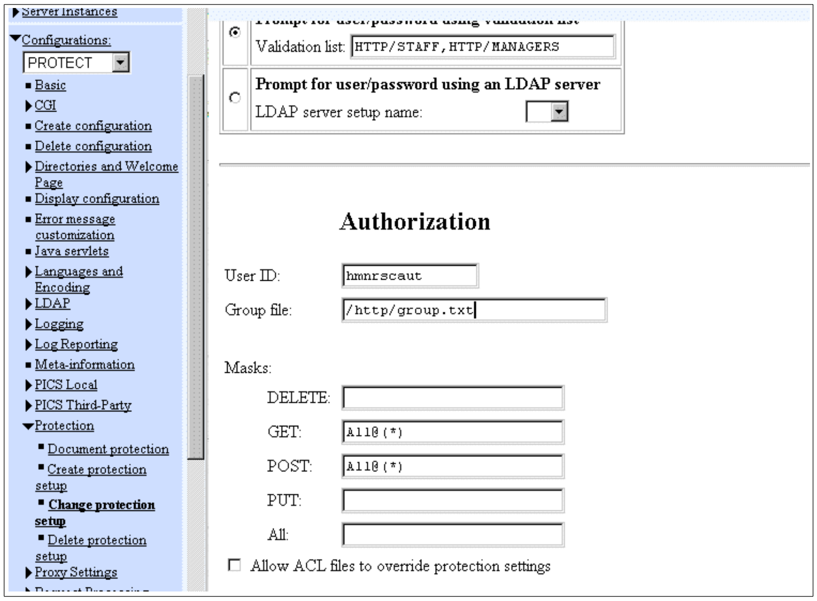
4.20.5 Using an Access Control List

ACLs let you control file access at a very detailed level. Generally you should try to avoid this by designing your directories to hold files with similar security needs.

We will set up a very simple ACL to control access to our protected file. Much more complex control is possible combining files, methods, and users or groups of users.

Change the named protection setup VLDL to name our group file /http/group.txt.

1. Click **Protection->Change protection setup** in the navigation panel.
2. Ensure the correct protection setup is selected, in this case VLDL and then click **Next**.
3. Ensure **Change current user/password authentication settings** is selected and click **Next**.
4. Enter the name `/http/group.txt` in the group file parameter.



● Validation list: HTTP/STAFF,HTTP/MANAGERS

○ **Prompt for user/password using an LDAP server**
LDAP server setup name:

Authorization

User ID: hmnrscaut

Group file: /http/group.txt

Masks:

DELETE:

GET: All@(*)

POST: All@(*)

PUT:

All:

□ Allow ACL files to override protection settings

Figure 70. Disabling DELETE and PUT

5. Click **Apply**.

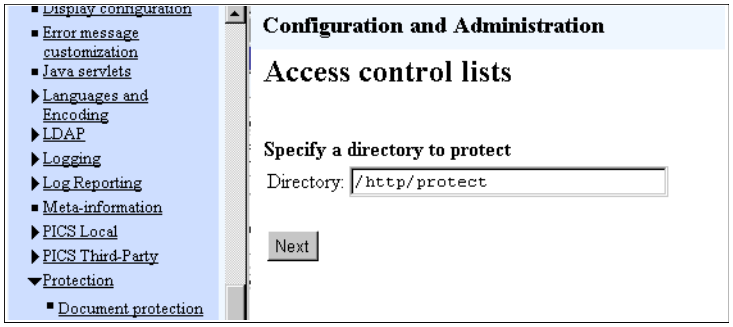
   The named protection directive VLDL is now as follows:

```
Protection VLDL {
      GroupFile /http/group.txt
      PasswdFile HTTP/STAFF,HTTP/MANAGERS
      ACLOverride Off
      PostMask All@(*)
      GetMask All@(*)
      AuthType Basic
```

```
        ServerID Human_resource
        UserID hmnrscaut
    }
```

Our ACL will have one entry restricting access to the file protected.html to the group Webmaster.

1. Click **Access control lists** in the navigation panel of the HTTP Configuration and Administration utility.



Configuration and Administration

Access control lists

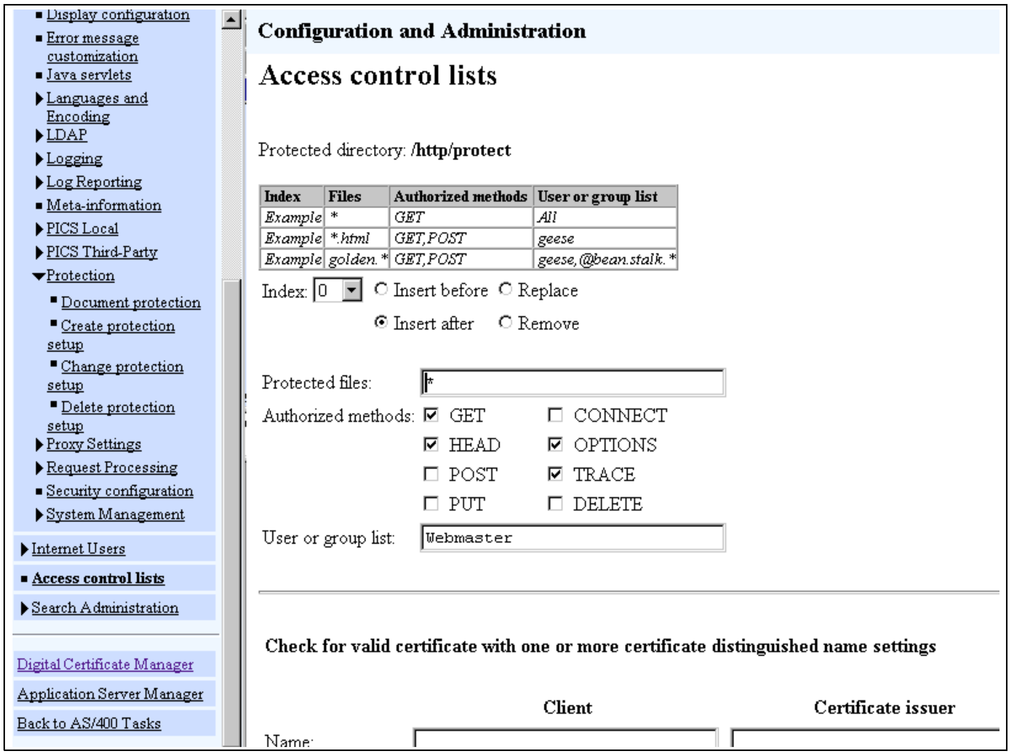
Specify a directory to protect

Directory: /http/protect

Figure 71. Defining an access control list.

Enter the name of the directory to protect, in this case `/http/protect`.

2. Click **Next**.



Configuration and Administration

Access control lists

Protected directory: **/http/protect**

Index	Files	Authorized methods	User or group list
Example	*	*GET*	*All*
Example	*.html	*GET,POST*	*geese*
Example	golden.*	*GET,POST*	*geese,@bean.stalk.**

Index: 0 ○ Insert before ○ Replace

● Insert after ○ Remove

Protected files: *

Authorized methods: ☑ GET ☐ CONNECT

☑ HEAD ☑ OPTIONS

☐ POST ☑ TRACE

☐ PUT ☐ DELETE

User or group list: Webmaster

Check for valid certificate with one or more certificate distinguished name settings

	Client	Certificate issuer
Name:		

Figure 72. Defining an access control list 2

Enter `*` to select all files. Select the methods that are enabled by default: `GET`, `HEAD`, `OPTIONS`, and `TRACE`. Finally enter the name of the group to have access to the selected files using the selected methods, in this case `Webmaster`.

3. Click **Apply**.

Testing the configuration

1. Close your browser and restart it so authentication will be done.
2. In this case the server does not need to be ended and started again, since ACLs are not cached.
3. Try to access the secured page using a user name in the group Webmaster. The secured page appears.
4. Try to access the secured page using a valid user name that is not in the group Webmaster. The secured page appears even if it should not.

Important

When we saw the phenomenon that the page was served even if it should not have been, we investigated further. Enabling an error log, repeating the process, and examining the log made us no wiser. So we worked through the HTTP service trace (see 4.21, “Troubleshooting - HTTP service trace” on page 104). In the trace we saw that the HTTP server job is not authorized to our ACL file. The Protect directive specifies the user ID HMNRSCAUT, which has authority to the ACL file. It turned out that the HTTP server switches the user profile after processing the ACL file. Giving QTMHHTTP read authority to the directory protect solved the problem. This time we got the results we expected.

If you are using ACLs, then your default HTTP server job user profile needs at least read authority to all directories that contain ACLs.

This concludes scenario 6.

4.21 Troubleshooting - HTTP service trace

There is an undocumented facility in the HTTP server that the developers created for debugging purposes. It allows you to have the server print a very detailed trace of what it is doing and why. We found it very useful when our configurations were not giving us the results we expected.

Because it is undocumented you must take it as it comes and cannot expect support for it. Nevertheless we found it a very useful tool.

You can turn on the HTTP service trace when you start an HTTP server. To do this add ’-v’ or ’-vv’ or ’-mtv’ after the server instance name. For example:

```
STRTCPSVR *HTTP HTTPSVR(PROTECT '-vv').
```

The options are case sensitive and have the following meaning:

-v Verbose

-vv Very verbose

-mtv Much too verbose

We generally used '-vv'. Following is an example of output from the service trace using '-vv'.

```
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+
....1....+.
0940595443 00000019 HTParse. HTSimplify.. nothing to do!
0940595443 00000019 HTMPool. MemPool..... creating a new 4240-byte pool.
0940595443 00000019 HTServer About....... to call preexit for "/protect/protected.html".
0940595443 00000019 HTRuleDB Using local address 9.24.104.163.
0940595443 00000019 HTRuleDB Protect..... matched "/protect/protected.html" -> "/protect/protected.html"
0940595443 00000019 HTRuleDB Protection.. setup as defined in config file
.......................... [22/Oct/1999:12:30:42 +0000, 0940595442] 00002201
0940595443 00000019 HTRuleDB Pass........ matched "/protect/protected.html" ->
"/http/protect/protected.html"
0940595443 00000019 HTRuleDB Passing..... "/http/protect/protected.html"
0940595443 00000019 HTMulti. Multi....... for path "/http/protect/protected.html".
0940595443 00000019 HTAccess HTStat...... succeeded on file "/http/protect/protected.html" --> will cache
it.
0940595443 00000019 HTFile.c Searching... for suffix 1: ".html"
0940595443 00000019 HTMulti. Multi...... File quality of 0.10000 acceptable for file
"/http/protect/protected.html"
0940595443 00000019 HTAAServ HTMulti..... gave us a file.
0940595443 00000019 HTAAServ Content-Length 903
0940595443 00000019 HTAAServ Last-Mod.... Fri, 15 Oct 1999 12:20:38 GMT
0940595443 00000019 HTFile.c Searching... for suffix 1: ".html"
0940595443 00000019 HTAAServ AuthCheck... Translated path: "/http/protect/protected.html" (method: GET)
0940595443 00000019 HTAAServ Forbidden... a valid client certificate required
```

Figure 73. HTTP service trace output

You should not always turn on the trace options, because in a production environment the trace files get really big. Again, the trace is intended for debugging purposes of developers and therefore is not easy to read. However, in the case of problems you will probably find helpful information that makes it easier to isolate and solve problems.

We used the trace function to investigate a problem, going to the bottom of the trace, and working back. Generally we had to go back several pages before getting to the relevant part of the trace.

- You can see the incoming URL.
- You can see the protection directives it matches and does not match.
- You can see the routing directives it matches and how the URL gets modified.
- You can see any error messages that occur such as `Not authorized`, `User profile disabled`, and so on.
- You can see the contents of certificates used for SSL client authentication.
- You can see much, much more.

Chapter 5. Digital Certificate Manager for AS/400

This chapter explains the AS/400 Digital Certificate Manager (DCM). It shows how to manage digital certificates for your network. It also explains how to set up and operate a private (also referred to as local) Certificate Authority (CA), how to manage server certificates, and how to issue and manage client certificates using DCM.

To make this chapter as generic as possible we added the name *your.system.name* to the Hosts file of the PC. In most of the scenarios shown in this chapter this name represents the AS/400 host name. In your case you have to replace it with the host name or IP address of your AS/400 system.

5.1 Overview of DCM on the AS/400

DCM was first introduced in OS/400 V4R2 when the Secured Socket Layer (SSL) protocol became available on the AS/400 system. The Digital Certificate Manager must be installed when you want to use the SSL protocol to establish secured communications. For example, each server application on the AS/400 system that communicates over SSL needs a server certificate assigned to it.

DCM is grouped into the following three major tasks:

- Certificate Authority task

  This task allows you to set up your AS/400 system to operate your own local Certificate Authority. Through this task you are able to issue AS/400 server and client certificates. For an environment where you are not accepting certificates from a well-known CA you may consider using the AS/400 system as a CA. However, the CA function of DCM is not intended for operating a CA like a well-known CA. It can be used to operate an intranet CA where, for example, all users still have AS/400 user profiles and you want to migrate the authentication process from user name and password to digital certificates.

  DCM provides a wizard that takes you through all necessary steps to establish a CA.

- System certificate task

  Through the functions provided by the system certificates tasks, you can manage server certificates on the AS/400 system. It allows you to request and receive server certificates, receive CA certificates and to associate server certificates with AS/400 applications. Furthermore, you can define which CA certificates your AS/400 applications trust and which server certificates your applications use for secure communications.

- User certificate task

  These tasks allow AS/400 users to manage their own certificates associated with their AS/400 user profiles. An AS/400 user can register an existing client certificate with its user profile or can delete certificates that are associated with its user profile. If a Certificate Authority is established on the AS/400 system, an AS/400 user can also request a new client certificate from this CA. However, to use these tasks the client user needs an AS/400 user profile.

5.2 Installation prerequisites

This section explains the installation steps of DCM and some important topics you must know before you start to use DCM.

5.2.1 Installation steps

Before you can use any DCM functions, you must prepare the AS/400 system. Following are the steps and information you need to perform to set up the AS/400 system to use the Digital Certificate Manager:

1. License programs needed to run DCM on your AS/400 system.
   - 5769-SS1 option 34 OS/400 - Digital Certificate Manager
   - 5769-DG1 IBM HTTP Server for AS/400
   - Either 5769-AC1, 2, or 3 Crypto Access Provider for AS/400

     These products are subject to U.S. export restrictions. We will discuss this subject in more detail in Appendix A, “Cryptographic product regulations” on page 377.
   - Either 5769-CE1, 2, or 3 Client Encryption (optional)

     If you want to configure Client Access servers to use SSL, these products must be installed. You must select Client Encryption when you install Client Access Express (or during a Selective install of Client Access Express).

     These products are subject to U.S. export restrictions. We will discuss this subject in more detail in Appendix A, “Cryptographic product regulations” on page 377.
2. Start the HTTP server *ADMIN instance.

   Use the command `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)` on an AS/400 command line or use the Client Access Operation Navigator panel to start the server instance. At this step, the *ADMIN instance does not use SSL. You need to enable the *ADMIN server instance for SSL when you:
   - Want to secure all administration tasks provided on the AS/400 Task page.
   - Want to register existing client certificates with AS/400 user profiles over DCM.

   More details on how to enable SSL for the *ADMIN server instance are shown later in this chapter and in Appendix B, “Enabling SSL for the *ADMIN HTTP server instance” on page 379.

Note

If you are familiar with the AS/400 HTTP configuration, you may want to connect securely to the *ADMIN instance and try to put the SSL directive in the *ADMIN instance configuration. *Do not change the *ADMIN server configuration to use SSL at this time.* Even though you can configure it, the HTTP server application is not set to use a certificate at this time, so you cannot connect to the *ADMIN server instance.

3. Prepare an AS/400 user profile.

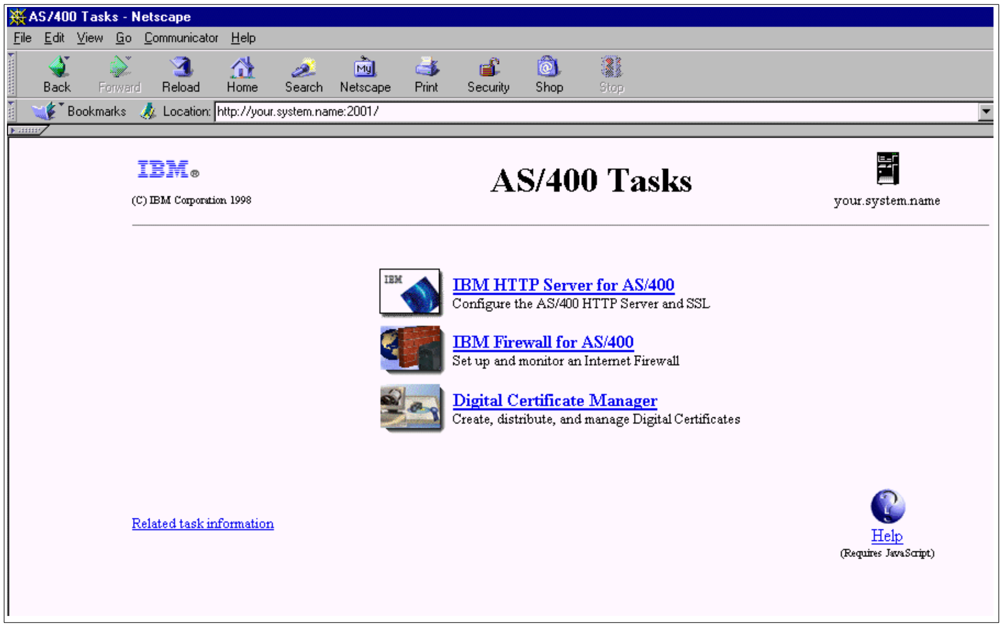
In order to perform all functions provided in DCM, the administrator's user profile must have the special authorities **ALLOBJ* and **SECADM*. Ordinary users only see the User certificate tasks in the DCM configuration window.

4. Start the Web browser.

   The Web browser must supports frames and JavaScript.

5. Sign on to the AS/400 Tasks page.

   Enter the URL *http://your_system_name:2001* to go to the AS/400 Tasks page. Port number 2001 is the default number the *ADMIN server listens to for non-SSL sessions. When the userID/password prompt appears enter your AS/400 user profile and password. Remember to use a user profile that has **ALLOBJ* and **SECADM* authority.



AS/400 Tasks

IBM HTTP Server for AS/400
Configure the AS/400 HTTP Server and SSL

IBM Firewall for AS/400
Set up and monitor an Internet Firewall

Digital Certificate Manager
Create, distribute, and manage Digital Certificates

Related task information

Help
(Requires JavaScript)

Figure 74. The AS/400 Tasks page

If you do not see the Digital Certificate Manager on the AS/400 Tasks page you probably have not installed the OS/400 option 34, which is the Digital Certificate Manager.

5.2.2 Key size considerations

When using DCM to create certificate requests, you will be asked to choose a key size for the public and private key used for authentication. The key sizes used for data encryption depend on the installed Cryptographic Access Provider product and the supported key sizes of the communication partner.

More information about key size and export regulations can be found in Appendix A, “Cryptographic product regulations” on page 377.

5.2.3 Certificate store structure and locations

Certificate Authority, server and user certificates and related information are stored in different directories on the AS/400 system. DCM provides a default store location for you.

Certificate Authority store location

DCM uses a fixed store location for the local CA. You cannot change its location. After you create a local CA you will see the following files in a specific directory. These directories must be protected from unauthorized access. The directory and files for the CA objects are:

/QIBM/UserData/ICSS/Cert/CertAuth	Directory
CA.TXT	CA certificate and public key
DEFAULT.KDB	CA certificate and CA private key
DEFAULT.POL	CA policy file
DEFAULT.STH	Stashed password for accessing the local CA KDB.
/QIBM/UserData/ICSS/Cert/Download/CertAuth	Directory containing the CA certificate available for distribution to clients
CA.CACRT	CA certificate in binary format

System certificate store location

You can select two types of locations to store a certificate. OS/400 server applications, such as HTTP and Telnet, can only use certificates stored in the *SYSTEM certificate store. Another selection is OTHER, which enables you to store certificates in any directory on the AS/400 Integrated File System (IFS). The directory and file structure is as follows:

*SYSTEM (default store location)

/QIBM/UserData/ICSS/Cert/Server	Directory
DEFAULT.KDB	System certificate(s), private key(s) and CA certificates
DEFAULT.RDB	Certificate request
DEFAULT.STH	Stashed password for automatic access to a KDB file by the server

OTHER

You can specify another directory such as /your_directory_name to store certificates. Customer applications that are written to use SSL_Init (instead of the newer SSL_Init_App) can make more use of this. System administrators can also make use of this certificate store for certain kinds of backups or testing before moving into their production environment. Some functions, such as exporting certificates from certificate stores created while the system was on a previous release, may also make use of this. Again do not use this if you want to use OS/400 secure applications.

Note

Prior to V4R4, certificates were stored in separate files. They are called key ring files.

5.2.4 Key label name and CA name consideration

DCM uses default values for key labels. Key labels are used for distinguishing each certificate in a particular certificate store.

*DFTSVR

This is a default system certificate key label name in a KDB file. A key label name must be unique in a KDB file.

*CERTAUTH(n)

This is the name DCM gives to the CA when it is created. (n) is the number of times you have created a CA on your system. Every time you renew your CA or delete and create a CA, the number increases.

5.3 Starting the Digital Certificate Manager

This section explains how to get into DCM and gives an overview of the available functions.

From a browser enter the URL `http://your.system.name:2001` to get to the AS/400 Tasks page on your browser. You will normally be prompted for an AS/400 user profile and password, unless the server's default configuration is intentionally changed. The options displayed on the AS/400 Tasks page as shown in Figure 75 depend on the installed license programs.

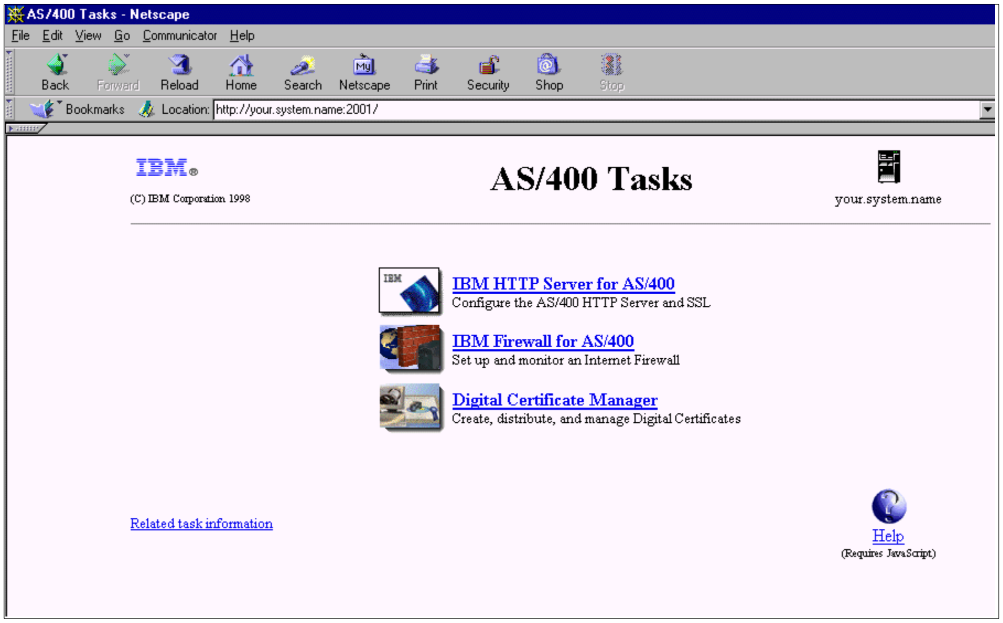
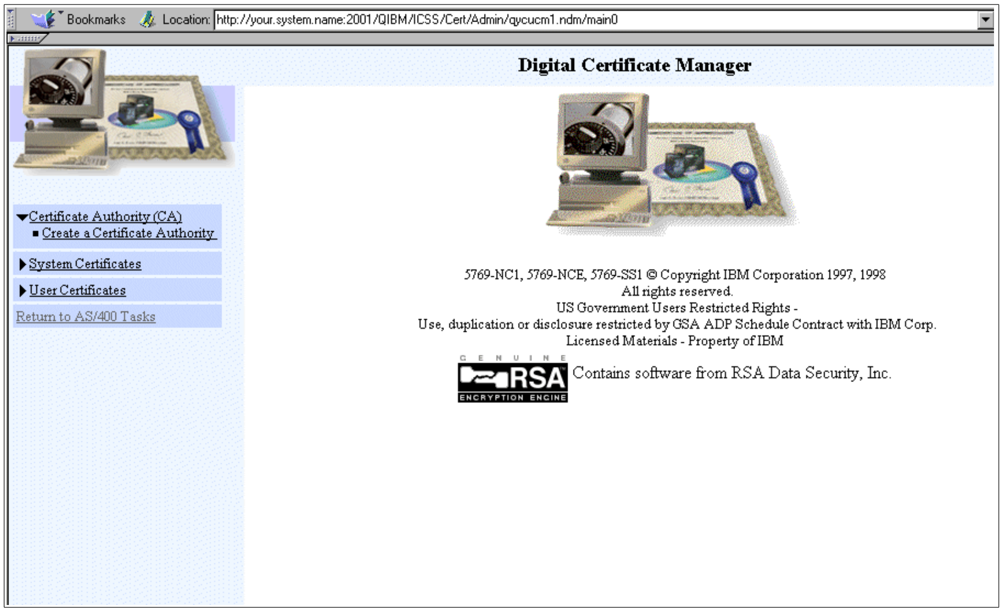

AS/400 Tasks - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://your.system.name:2001/
IBM
(C) IBM Corporation 1998
AS/400 Tasks
your.system.name
IBM HTTP Server for AS/400
Configure the AS/400 HTTP Server and SSL
IBM Firewall for AS/400
Set up and monitor an Internet Firewall
Digital Certificate Manager
Create, distribute, and manage Digital Certificates
Related task information
Help
(Requires JavaScript)

Figure 75. AS/400 Tasks page

Click **Digital Certificate Manager** to start DCM.

By default all option menus on the DCM page are collapsed. When signing on with a user profile that does not have *ALLOBJ and *SECADM authorities, you see only the User Certificate task and if a CA is set up, also the Certificate Authority task.

Expanding the Certificate Authority (CA) menu shows the available options. If there is no CA created yet and you signed on with a user profile with *ALLOBJ and *SECADM authorities, only the Create Certificate Authority option is available as shown in Figure 76. Selecting this option starts a wizard that guides you through the necessary steps to create a local CA.

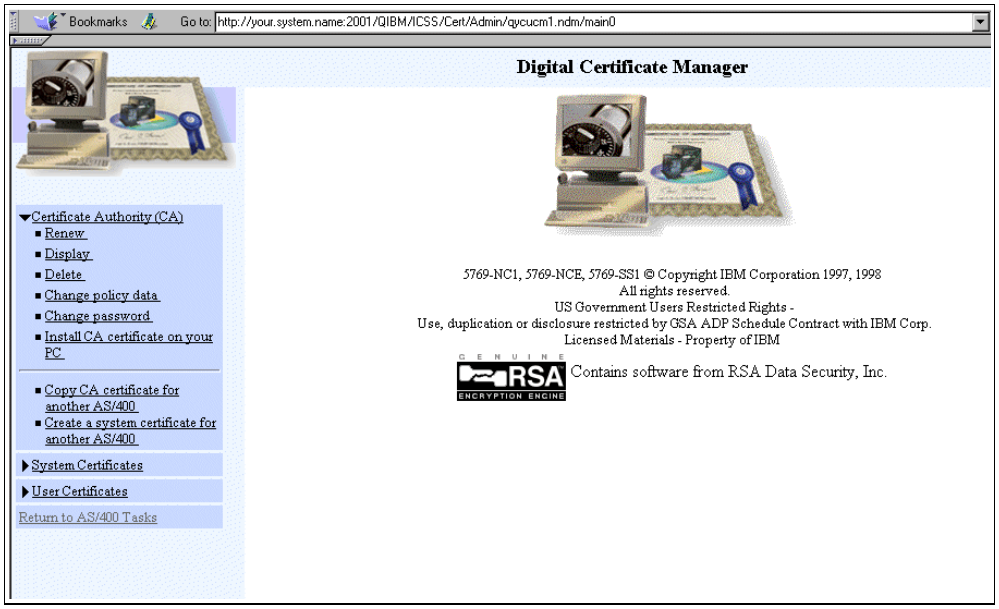

Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Digital Certificate Manager
▼Certificate Authority (CA)
■ Create a Certificate Authority
▶System Certificates
▶User Certificates
Return to AS/400 Tasks

5769-NC1, 5769-NCE, 5769-SS1 © Copyright IBM Corporation 1997, 1998
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

GENUINE RSA ENCRYPTION ENGINE Contains software from RSA Data Security, Inc.

Figure 76. Certificate Authority tasks when no CA exists

If there is already a Certificate Authority created on this system, the set of available options change as shown in Figure 77.



http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager

Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks

5769-NC1, 5769-NCE, 5769-SS1 © Copyright IBM Corporation 1997, 1998
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

Contains software from RSA Data Security, Inc.

Figure 77. Certificate Authority tasks when a CA exists

1. Certificate Authority tasks

   Renew

   > If you want to change some contents of the CA, for example the organization name, unit name, and so forth, you can renew a local CA certificate. Of course, this task should be avoided in a production environment. If you perform this task, existing certificates issued by this CA that are already distributed to PCs or other systems must be replaced. The other reason to renew the CA certificate is when the certificate expires. For more details about managing and renewing certificates refer to Chapter 1, “Introduction to digital certificates” on page 3.

   Display

   > This option allows you to display information about the private (local) CA in the default certificate store.

   Delete

   > This option allows you to delete a local CA certificate and the corresponding default CA certificate store.

   Change policy data

   > Allows you to change the policy to which a local CA refers when issuing server certificates and user certificates. If you want to issue user certificates, you must select the appropriate policy option and specify the validity period.

   Change password

   > The certificate store is protected by a password that is set when creating the CA. Through this option you can change the CA certificate store password and set the password expiration date.

   Install CA certificate on your PC

There are two methods to receive or install a local CA certificate from DCM:

Receive Certificate

Selecting this link triggers the browser to present a dialog window. Follow the directions given to automatically download the CA certificate into your browser's database.

Copy and Paste Certificate

This task shows the CA certificate in base64-encoded ASCII text form on the DCM page. You can copy and paste it into an editor, such as Notepad, and save it. The file containing the certificate can then be distributed to, for example, other PCs or a network drive. There are some applications, such as the IBM Key Management utility of Personal Communications and Client Access, that require the CA certificate in this form.

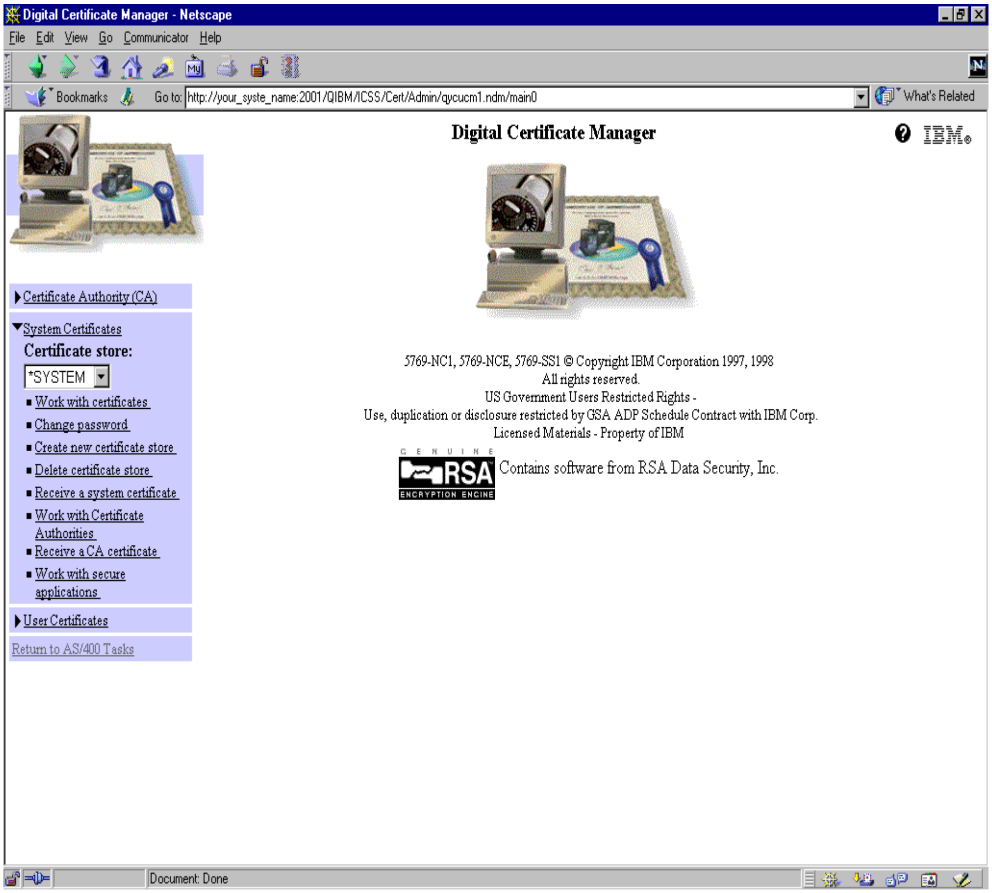
Copy CA certificate for another AS/400

DCM creates a file containing the CA certificate. This file can then be transferred to another AS/400 and imported to a certificate store.

Create a system certificate for another AS/400

DCM creates a system certificate and certificate store files for another AS/400 system. Once the files are created, they need to be transferred in binary format to the target AS/400 system.

Expanding the System Certificate task shows the following options.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_syste_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
Digital Certificate Manager
IBM
GENUINE RSA ENCRYPTION ENGINE
Document: Done

5769-NC1, 5769-NCE, 5769-SS1 © Copyright IBM Corporation 1997, 1998
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

Contains software from RSA Data Security, Inc.

Figure 78. System Certificate task

2. System Certificate tasks

   You can select between the *SYSTEM and user certificate stores. System certificates for all AS/400 standard applications are in the *SYSTEM certificate store. Each certificate store is protected by a password. The user is prompted for this password when expanding the System Certificates tasks for a particular certificate store.

   The options on this menu allow you to manage server certificates that are stored in your AS/400 system.

   Work with certificates

   You can view, delete, renew, export, or set a certificate as a default. You can also import or create a certificate and add it to the current certificate store.

   Change password

   This option allows you to change the password for the current system certificate store. Note that the passwords for the system certificate store and the CA certificate store are not necessarily the same, because these are different stores.

   Create new certificate store

   Selecting this option brings up a series of configuration windows to create a new server certificate store. If you already completed all steps to successfully create a CA on this AS/400 system, the system certificate store was already created at this time.

Delete certificate store

This option allows you to delete the current system certificate store. If you delete a certificate store, you cannot undo the deletion. If you delete the *SYSTEM certificate store, your system will not be able to use SSL for secure communications anymore. Once a system certificate store is deleted you have to create a new store again. If you delete the *SYSTEM certificate store, you have to again assign certificates to applications and import CA certificates from CAs that are not shipped with the OS/400.

It is always advisable to save all related files in case somebody deletes the certificate store by accident.

Receive a system certificate

Use this option when you want to add a system certificate that was issued by a well-known CA to the system certificate store. You can only receive certificates for which the certificate request was created on this system.

Work with Certificate Authorities

You can designate a CA as a trusted root, remove a CA's trusted root status, view information for a CA certificate, and delete a CA certificate. Even though this function may show a CA as trusted in the certificate store, a secure application by default trusts only the CA that signed the system certificate that the application uses for secure connections. Therefore, you must use the Work with Secure Applications task to mark other CAs as trusted by the secure application if desired.

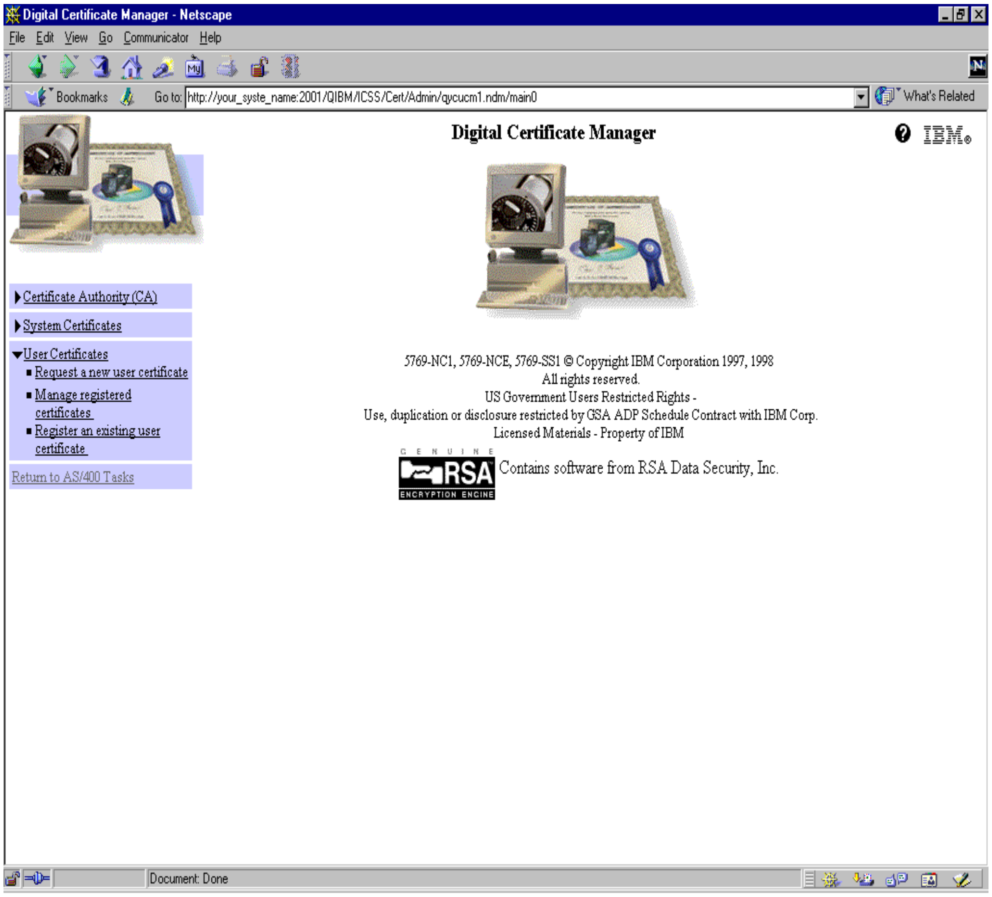
Receive a CA certificate

This option allows you to add a new CA certificate into the current certificate store and designate the CA as a trusted root. This can be either an Internet CA certificate or a local CA certificate that you create using DCM on another AS/400 system.

Work with Secure Applications

This option is available for the *SYSTEM certificate store only. For each secure application, you can view certificate information, work with system certificates that the application uses, or work with CA certificates that the application trusts.

Expanding the User Certificate menu shows the following options.



Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_syste_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related

Digital Certificate Manager

- Certificate Authority (CA)
- System Certificates
- User Certificates
  - Request a new user certificate
  - Manage registered certificates
  - Register an existing user certificate
- Return to AS/400 Tasks

5769-NC1, 5769-NCE, 5769-SS1 © Copyright IBM Corporation 1997, 1998
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

Contains software from RSA Data Security, Inc.

Figure 79. User Certificate task

3. User Certificate tasks

   Request a new user certificate

   This page allows you to request a user certificate from the local CA that is set up on this AS/400 system. This option is not available when there is no Certificate Authority created on this system. Each individual user who wants to request a certificate has to sign on to the AS/400 Tasks page with its user profile and request a certificate through this option.

   Manage registered certificates

   This page allows you to view or delete user certificates for other users, if your user profile has *SECADM and *ALLOBJ special authorities. If your user profile does not have these authorities, you can view or delete your own certificates only.

   Register an existing user certificate

   This page allows you to associate a certificate with a user profile. The certificate may be from an Internet CA or from any local or intranet CA, but the issuing CA must be trusted by the server, and the certificate must not already be associated with a user profile on this system. Note that this function requires the use of SSL, so if the server is not yet configured for SSL, attempts to use this function will give error messages.

5.4 Setting up a local Certificate Authority

This section explains how to configure a local CA on your system.

DCM guides you through a series of steps to set up your own CA. An overview of these steps is shown in Figure 80. These steps allow you to create certificates and set up secure applications.

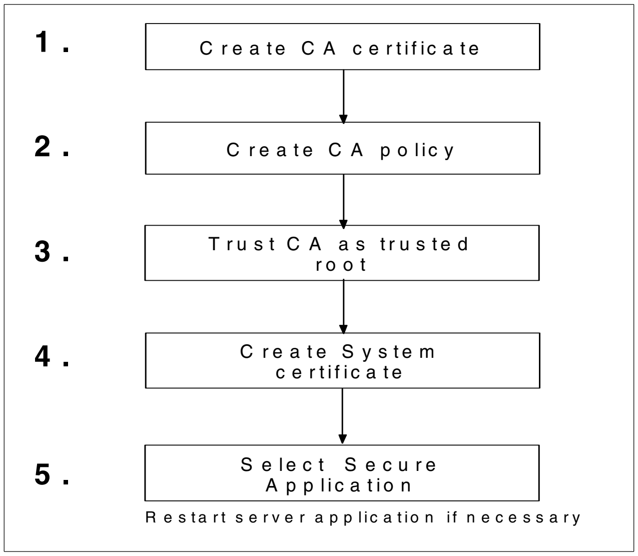

1.
Create CA certificate
2.
Create CA policy
3.
Trust CA as trusted root
4.
Create System certificate
5.
Select Secure Application
Restart server application if necessary

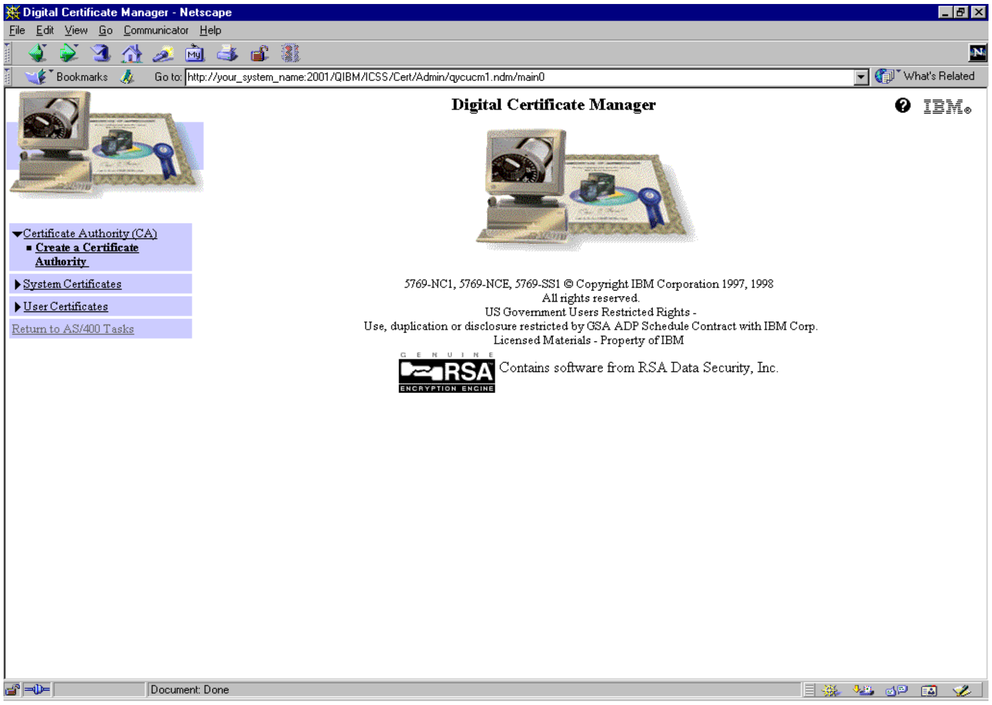
Figure 80. Steps performed when setting up a CA through DCM

5.4.1 Create CA certificate

Perform the following steps to create the Certificate Authority certificate, which is later used to sign certificates issued by this CA. The CA certificate of a local CA must be made available to all entities communicating with server applications running on servers that use certificates issued by this CA. For users that have an AS/400 user profile on the system where the CA resides, they are able to signon to the AS/400 Tasks page and receive the certificate. For all other users the CA certificate must be publicly available through a Web server or a public directory.

1. On the DCM main page, click **Certificate Authority** on the left pane of the window.

   The task menu is expanded and shows all the available options. If the system has not set up its own CA yet, you will only see the Create a Certificate Authority option as shown in Figure 81. DCM automatically determines what kind of options are available for a user, based on the user's system authorities.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

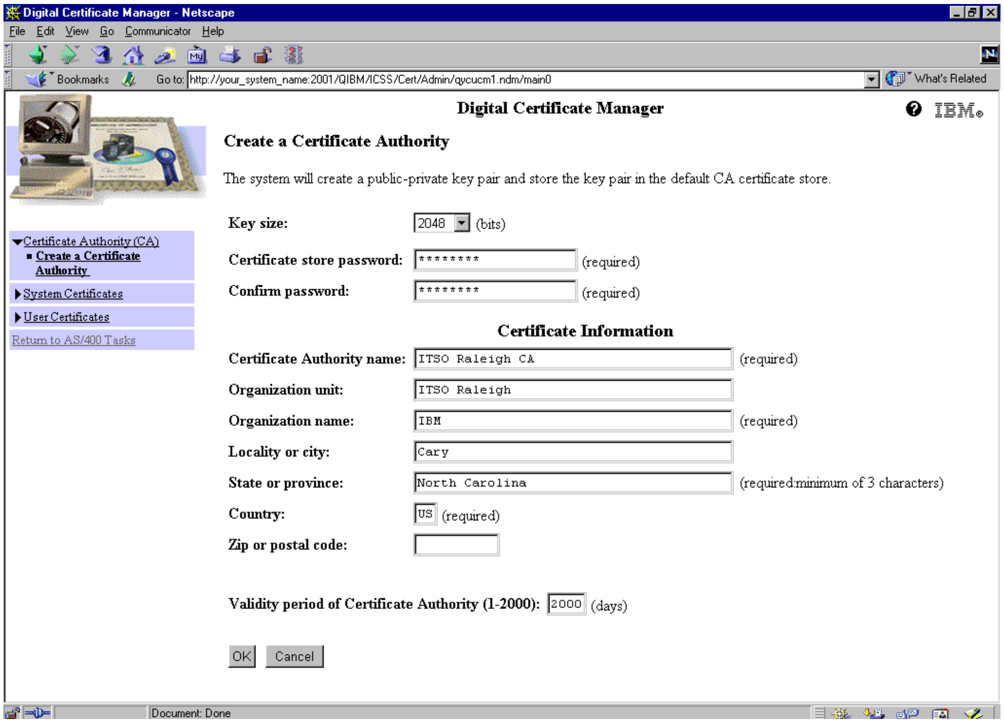
5769-NC1, 5769-NCE, 5769-SS1 © Copyright IBM Corporation 1997, 1998
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

Contains software from RSA Data Security, Inc.

Figure 81. Certificate Authority task page

This is the first page when you create a local CA.

2. Click **Create a Certificate Authority**. The input form for the CA certificate is displayed.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
OK
Cancel
Document: Done

Digital Certificate Manager

Create a Certificate Authority

The system will create a public-private key pair and store the key pair in the default CA certificate store.

Key size: 2048 (bits)

Certificate store password: ******** (required)

Confirm password: ******** (required)

Certificate Information

Certificate Authority name: ITSO Raleigh CA (required)

Organization unit: ITSO Raleigh

Organization name: IBM (required)

Locality or city: Cary

State or province: North Carolina (required:minimum of 3 characters)

Country: US (required)

Zip or postal code:

Validity period of Certificate Authority (1-2000): 2000 (days)

Figure 82. Create certificate authority form

Complete this page by entering each input value as follows:

Key size

Your choices are 2048, 1024, or 512 bits if you are using the Cryptographic Access Provider product 5769-AC3. Depending on the installed version of this product (AC3, AC2, or AC1), you see different values available for the key sizes. The selection made here determines what key size will be used to create the public and private key pair for this CA certificate. A larger key size is more resistant to cracking. However, a larger key size will cause slower performance of your IBM HTTP Web server when using secure connections. From the security point of view, always try to use the largest key size as possible. You have to balance between your security requirements and the server performance.

Certificate store password

This is used to protect the certificate store from unauthorized access. You must choose your password phrase and remember it. Your password is case sensitive. It is stored in the stashed password file (STH file).

Confirm password

Re-enter your password.

Certificate Authority name

Type the name to describe the CA. Use a simple and clear name. Once you issue the CA in a production environment, changing the name is an involved task.

Organization unit

Type a name of this certificate issuer's unit, for example a department name.

Organization name

Type your company name or organizational section.

Locality or city

Type the CA location name.

State or province

Type the name of the CA issuer's state or province. This name must be a minimum of three characters in length.

Country

Type a two-letter symbol for your country (for example, US for United States, DE for Germany, NZ for New Zealand, JP for Japan).

Zip or postal code

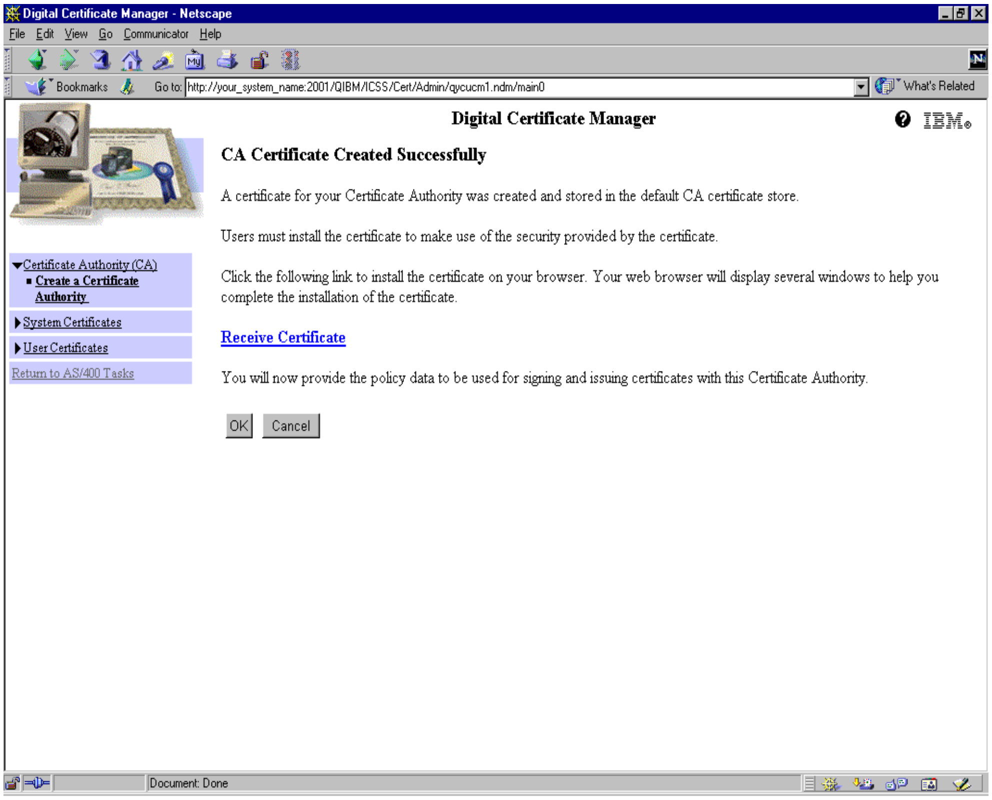
Enter a zip code. Note that this is an optional field. Most of the well-known CAs do not support the zip code in their distinguished name. Therefore, it is best to leave the field blank. Be aware that Netscape Browser 4.01 to 4.61 have an acknowledged problem performing client authentication when the zip code field is filled. If you want to use client authentication with this browser, leave this field blank. The problem is fixed with Netscape Communicator 4.7.

Validity period of Certificate Authority (1-2000)

Type the number of days for which the CA certificate is valid. We recommend you set this field to the largest number possible. The default is 1095 days (3 years).

3. Click **OK** at the bottom of the page.

DCM creates the Certificate Authority and generates public/private keys and the CA's certificate. The created objects and information are then stored into the directories and files as shown in 5.2.3, "Certificate store structure and locations" on page 110. After the objects are created, a completion message appears as shown in the following figure.



Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

CA Certificate Created Successfully

A certificate for your Certificate Authority was created and stored in the default CA certificate store.

Users must install the certificate to make use of the security provided by the certificate.

Click the following link to install the certificate on your browser. Your web browser will display several windows to help you complete the installation of the certificate.

Receive Certificate

You will now provide the policy data to be used for signing and issuing certificates with this Certificate Authority.

OK Cancel

Figure 83. CA Certificate created successfully

From this page you can download the CA certificate to your browser. This selection is an optional task. The Install CA certificate on your PC task allows you to download a local CA certificate at a later time.

4. Click **OK,** and the Certificate Authority Policy Data page is displayed.

5.4.2 Create CA policy

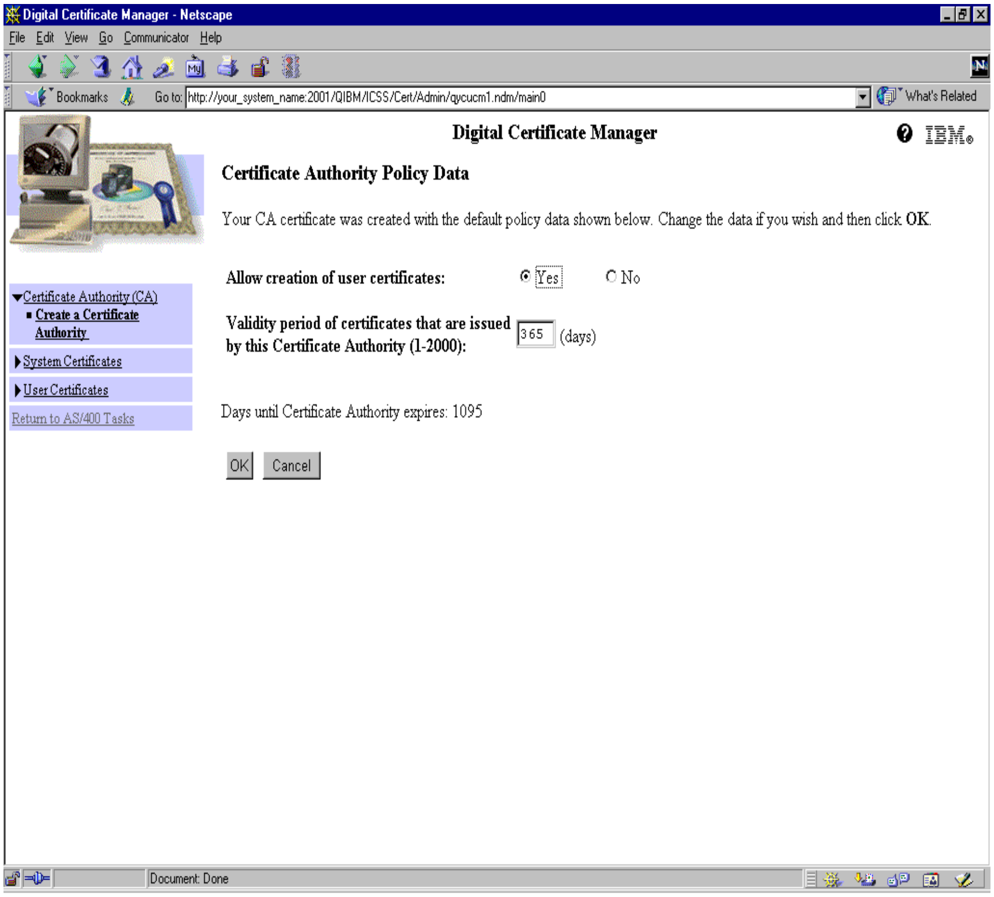
On this page, you must select the local CA policy settings. This policy is used when DCM creates a system certificate and a user certificate.

Allow creation of user certificates

This field specifies if this Certificate Authority allows a user that has an AS/400 user profile on the system where the CA resides to request a user certificate. If you specify No, the CA can only issue server certificates.

Validity period of certificates

The validity period is used when the CA issues system or user certificates. It defines the validity period of a certificate issued by this CA. This value must be less than or equal to the validity period specified for the CA certificate.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
IBM
Document: Done

Digital Certificate Manager

Certificate Authority Policy Data

Your CA certificate was created with the default policy data shown below. Change the data if you wish and then click OK.

Allow creation of user certificates: ● Yes ○ No

Validity period of certificates that are issued by this Certificate Authority (1-2000): 365 (days)

Days until Certificate Authority expires: 1095

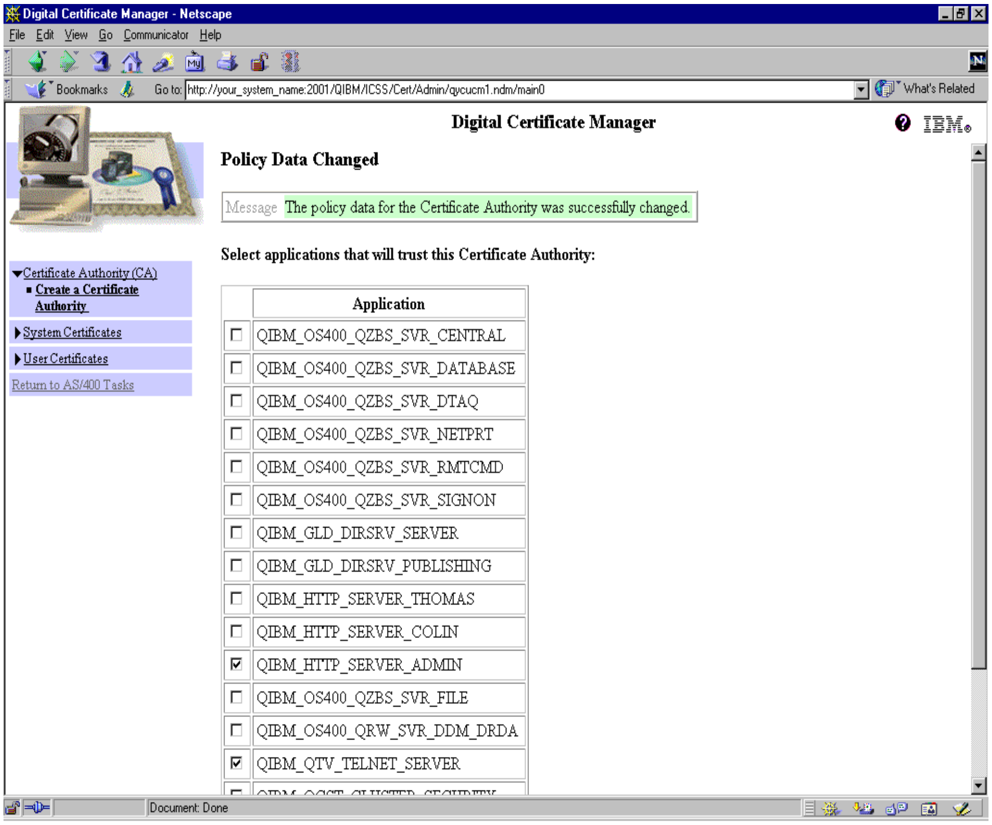
OK Cancel

Figure 84. Certificate Authority Policy Data window

1. Click **OK.** DCM creates a policy file in the default certificate store location. The next window appears showing the completion message of the previous step.

   If applications have been registered with Digital Certificate Manager, you can select the applications that should trust your intranet Certificate Authority when you create it. These are the applications registered for certificate use and trust certificates that are issued by your intranet CA. For example, if the application ID QIBM_HTTP_SERVER_ADMIN, which is the ADMIN server instance, should accept client certificates issued by the intranet CA, you must check the application ID on this page.

5.4.3 Applications trusting certificates issued by the intranet CA


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM.
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

Policy Data Changed

Message The policy data for the Certificate Authority was successfully changed.

Select applications that will trust this Certificate Authority:

	Application
□	QIBM_OS400_QZBS_SVR_CENTRAL
□	QIBM_OS400_QZBS_SVR_DATABASE
□	QIBM_OS400_QZBS_SVR_DTAQ
□	QIBM_OS400_QZBS_SVR_NETPRT
□	QIBM_OS400_QZBS_SVR_RMTCMD
□	QIBM_OS400_QZBS_SVR_SIGNON
□	QIBM_GLD_DIRSRV_SERVER
□	QIBM_GLD_DIRSRV_PUBLISHING
□	QIBM_HTTP_SERVER_THOMAS
□	QIBM_HTTP_SERVER_COLIN
☑	QIBM_HTTP_SERVER_ADMIN
□	QIBM_OS400_QZBS_SVR_FILE
□	QIBM_OS400_QRW_SVR_DDM_DRDA
☑	QIBM_QTV_TELNET_SERVER

Figure 85. Policy Data Changed window

1. Select all the applications that should trust certificates issued by this CA.

   Table 3 shows all IBM-supplied secure application names:

Table 3. IBM-supplied secure application names

Application Name	Corresponding Application
QIBM_HTTP_SERVER_ADMIN	HTTP server Admin instance
QIBM_HTTP_SERVER_CONFIG	HTTP server Default instance
QIBM_QTV_TELNET_SERVER	OS/400 TCP/IP Telnet Server
QIBM_OS400_QZBS_SVR_CENTRAL	OS/400 TCP Central Server
QIBM_OS400_QZBS_SVR_DATABASE	OS/400 TCP Database Server
QIBM_OS400_QZBS_SVR_DTAQ	OS/400 TCP Data Queue Server
QIBM_OS400_QZBS_SVR_NETPRT	OS/400 TCP Network Print Server
QIBM_OS400_QZBS_SVR_RMTCMD	OS/400 TCP Remote Command Server
QIBM_OS400_QZBS_SVR_SIGNON	OS/400 Signon Server
QIBM_OS400_QZBS_SVR_FILE	OS/400 TCP File Server
QIBM_GLD_DIRSRV_SERVER	Directory Service (LDAP) server
QIBM_GLD_DIRSRV_PUBLISHING	Directory Service (LDAP) publishing

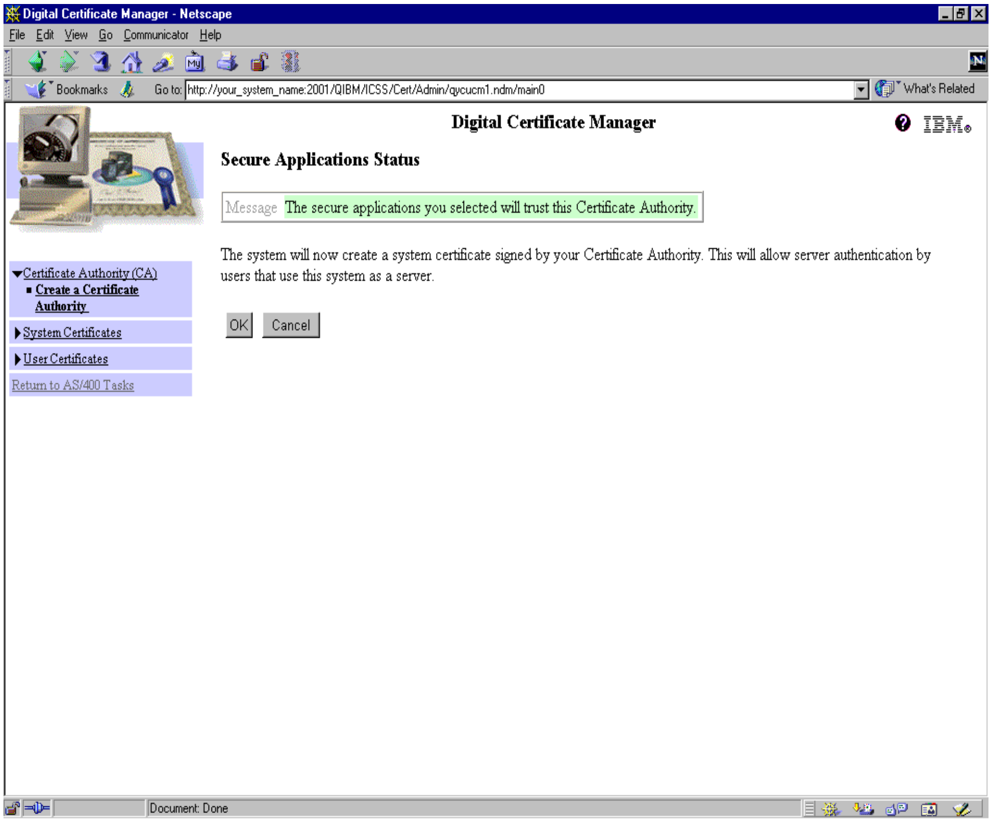
Application Name	Corresponding Application
QIBM_OS400_QRW_SVR_DDM_DRDA	OS/400 DDM/DRDA Server-TCP/IP
QIBM_QCST_CLUSTER_SECURITY	OS/400 Cluster Security
QIBM_OS400_QYPS_MGTCTRL_SVR	OS/400 Management Central server

Note

Currently, client authentication is available for the HTTP server only. You can select other secure applications, but they do not use this. In the future, secure application code will be changed and each secure application can be selected separately.

2. Click **OK**.

   The Secure Applications Status window as shown in Figure 86 confirms that the applications that you selected now trust the CA.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM.
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
OK
Cancel
Document: Done

Secure Applications Status

Message The secure applications you selected will trust this Certificate Authority.

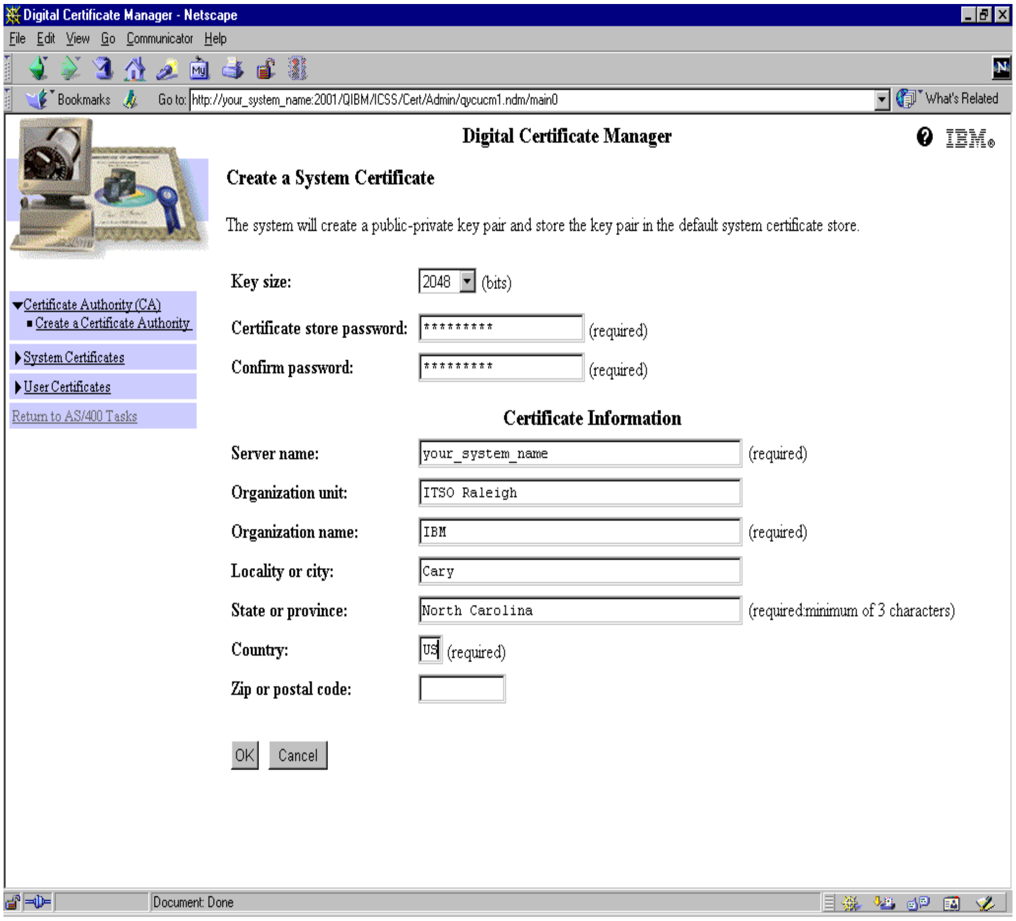
The system will now create a system certificate signed by your Certificate Authority. This will allow server authentication by users that use this system as a server.

Figure 86. Secure Application Status window

3. Click **OK**. The Create System Certificate window is displayed.

5.4.4 Create system certificate

To finish the process of creating an intranet Certificate Authority (CA), you must use the new CA to create a system certificate. The Create a System Certificate form displays after you select the applications that trust the new CA. If no registered applications are available for you to select, the Create a System Certificate page displays after you set the policy data for your CA.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
IBM
OK
Cancel
Document: Done

Digital Certificate Manager

Create a System Certificate

The system will create a public-private key pair and store the key pair in the default system certificate store.

Key size: 2048 (bits)

Certificate store password: ********* (required)

Confirm password: ********* (required)

Certificate Information

Server name: your_system_name (required)

Organization unit: ITSO Raleigh

Organization name: IBM (required)

Locality or city: Cary

State or province: North Carolina (required:minimum of 3 characters)

Country: US (required)

Zip or postal code:

Figure 87. Create a System Certificate window

This form is similar to the Create Certificate Authority page.

1. Fill in all required parameters.

   Key size

   Select a key size to use for the public and private keys for the certificate. The larger the key, the more secure the encryption it provides. But a larger key also decreases the server performance.Your choices are 2048, 1024, or 512 bits if you are using the Cryptographic Access Provider product 5769-AC3. Depending on the installed version of this product (AC3, AC2, or AC1) you see different values available for the key sizes.

   Certificate store password / Confirm password

   This password is used to protect the system certificate store from unauthorized access. You must choose your password phrase and remember it. Your password is case sensitive. This is stored in the stashed password file (STH file).

Warning

You must be sure that you can remember the password that you set, or that you write it down and store it in a secure place. If you forget the password, you cannot reset it or recover it and you will lose access to your certificate store files.

Server name

Enter a name to describe your system certificate. We recommend that you use the TCP/IP host name of the server that is used in browser URL requests.

Note

If you use a different name from the name used to access your server through a browser, the users get a message every time the server presents the certificate. For example, the Netscape browser checks if the DNS name specified in the URL and the server name specified in the certificate are the same. If not, the user gets a message and has to confirm to proceed.

Organization unit

Type the name of this certificate holder's unit.

Organization name

Type your company name or organizational section.

Locality or city

Type the location name of this certificate holder.

State or province

Type a name for this certificate holder's state or province. This name must be a minimum of three characters in length.

Country

Type a two-letter symbol for your country, for example, DE for Germany, US for United States, NZ for New Zealand, and so on.

Zip or postal code

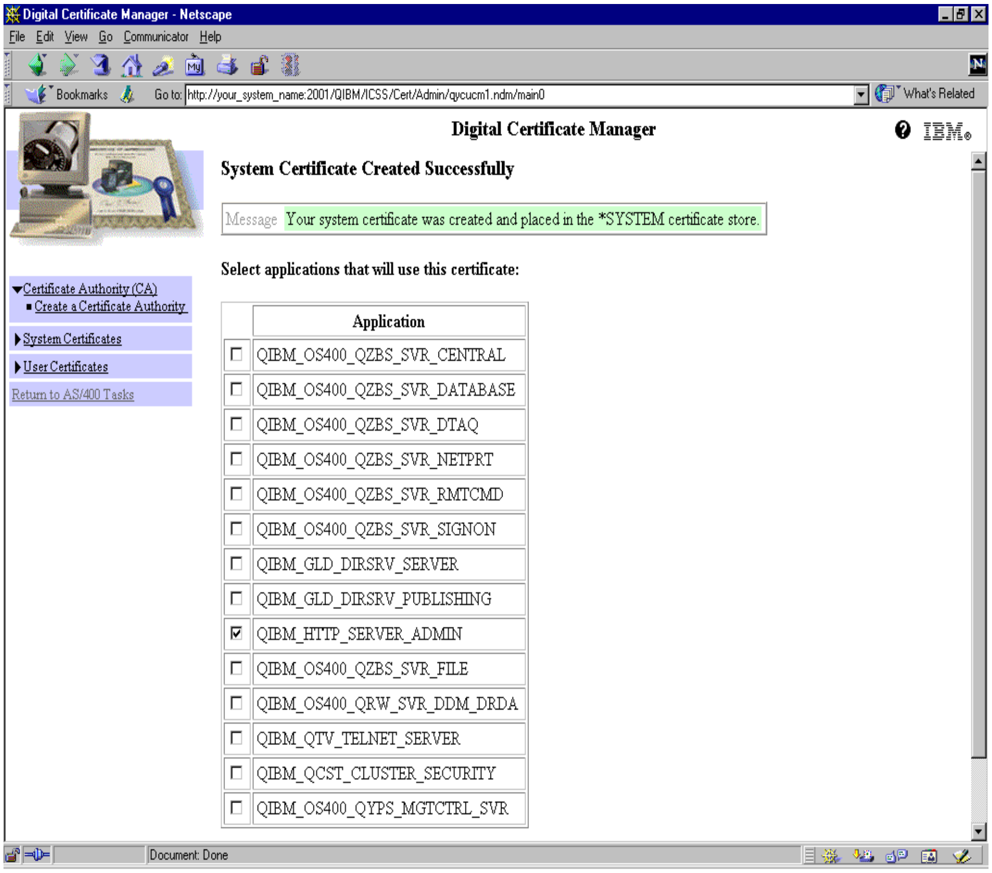
Enter a zip code. This field is optional and should be left blank, because most well-known CAs do not support the zip code in their distinguished name. Note also that Netscape Browser 4.01 to 4.61 (on Windows platforms) have an acknowledged problem performing client authentication when the zip code field is filled. If you want to use client authentication with these browser versions, leave this field blank. The problem is fixed with Netscape Communicator 4.7.

2. Click **OK** at the bottom of the page.

   DCM uses the input to create a system certificate and a system certificate store. This task may take a couple of minutes, depending on the AS/400 model.

5.4.5 Select secure application

The following page allows you to select which applications should use this certificate for secure communications, if applications have been registered with DCM.



Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

System Certificate Created Successfully

Message Your system certificate was created and placed in the *SYSTEM certificate store.

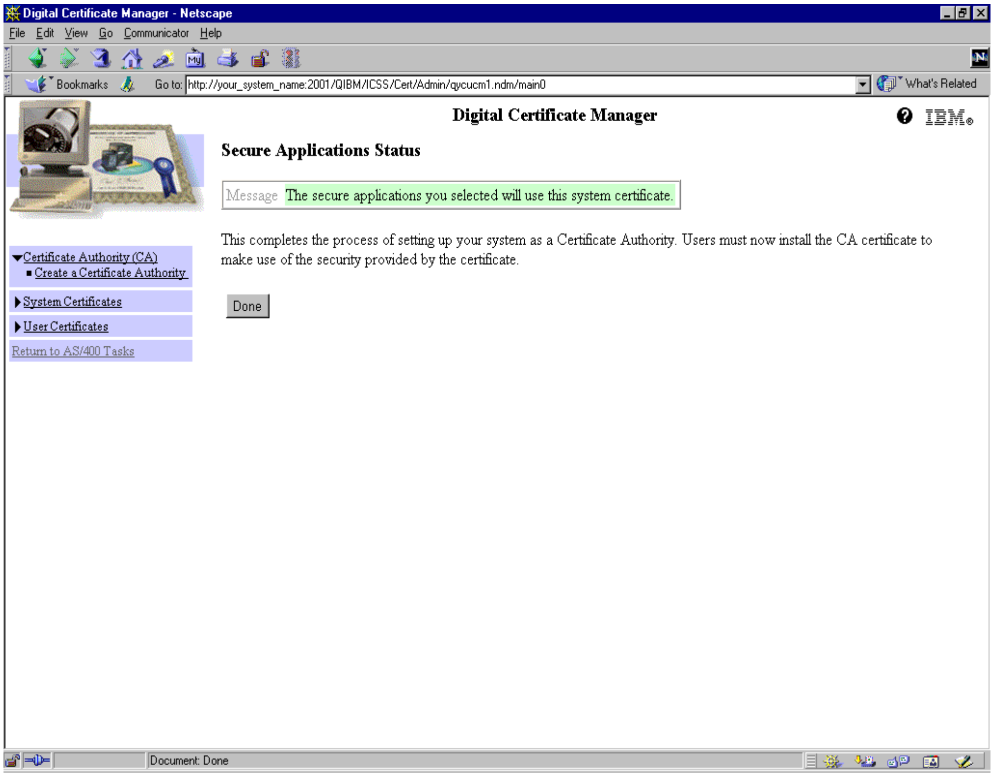
Select applications that will use this certificate:

	Application
□	QIBM_OS400_QZBS_SVR_CENTRAL
□	QIBM_OS400_QZBS_SVR_DATABASE
□	QIBM_OS400_QZBS_SVR_DTAQ
□	QIBM_OS400_QZBS_SVR_NETPRT
□	QIBM_OS400_QZBS_SVR_RMTCMD
□	QIBM_OS400_QZBS_SVR_SIGNON
□	QIBM_GLD_DIRSRV_SERVER
□	QIBM_GLD_DIRSRV_PUBLISHING
☑	QIBM_HTTP_SERVER_ADMIN
□	QIBM_OS400_QZBS_SVR_FILE
□	QIBM_OS400_QRW_SVR_DDM_DRDA
□	QIBM_QTV_TELNET_SERVER
□	QIBM_QCST_CLUSTER_SECURITY
□	QIBM_OS400_QYPS_MGTCTRL_SVR

Figure 88. System Certificate Created Successfully window

1. Select which applications in the list should use the new certificate for SSL communications, and click the **OK** button. The Secure Applications Status page as shown in Figure 89 confirms that the selected applications are set to use the new certificate.

   Remember to distribute the CA certificate to all clients that are communicating with applications that have this server certificate assigned to it. A more common way is to allow users to access a Web page from which they can receive the CA certificate into their browsers. Users that have an AS/400 user profile can connect to DCM and receive the CA certificate through the Install CA certificate on your PC task.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
Create a Certificate Authority
System Certificates
User Certificates
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

Secure Applications Status

Message The secure applications you selected will use this system certificate.

This completes the process of setting up your system as a Certificate Authority. Users must now install the CA certificate to make use of the security provided by the certificate.

Done

Figure 89. Secure Applications Status window

2. Click **Done** to finish the process of creating the CA. The DCM main page is displayed.

When you now click **Certificate Authority** to expand it, you see all the available options when a CA is set up on this AS/400 system, as shown in Figure 77 on page 113.

Now you are ready to use the local CA certificate and the system certificate issued by the local CA in secured TCP/IP applications. Before you actually can establish an SSL connection to such a server, you must configure the server for SSL, and if necessary end the server and restart it. After the server is restarted it listens on a different port for SSL connection requests.

Refer to Chapter 6, “Enabling SSL on AS/400 standard server applications” on page 187 to see how to configure standard TCP/IP server applications for SSL.

5.5 Managing a Certificate Authority

This section describes how to manage an existing local Certificate Authority with DCM. After creating a local CA certificate, you can use the following management tasks:

- Copy the CA certificate for another AS/400 system.
- Install a CA certificate on a PC.
- Delete a CA certificate.
- Renew a CA certificate.

- Change a CA certificate store password.
- Change CA policy data.

5.5.1 Copy CA certificate for another AS/400 system

Once your CA is set up and working, you can issue system certificates for other AS/400 systems. These certificates are stored in a system certificate store that is explicitly created for the target system and has to be transferred to that system.

The new system certificate can be moved to the target AS/400 system in different ways depending on what certificate stores already exist on the target system. If the target AS/400 system does not have a certificate store or the certificate store that exists with the same path and file name on the target system does not have any needed certificates and can be replaced, then the entire certificate store (which includes a copy of the local CA certificate that issued it) should be moved to the correct path and file name. For this scenario, the Copy CA certificate task would not be needed. If the target AS/400 system already has an existing certificate store that cannot be replaced, you would also have to transfer the CA certificate to that system as described here.

The following figure depicts the process of how CA certificates are exported, transferred, and installed.

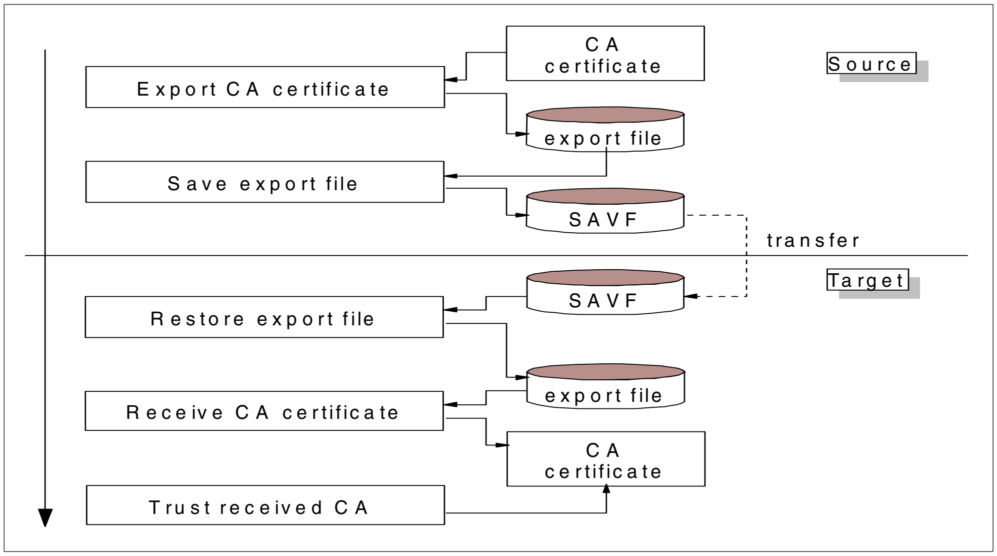
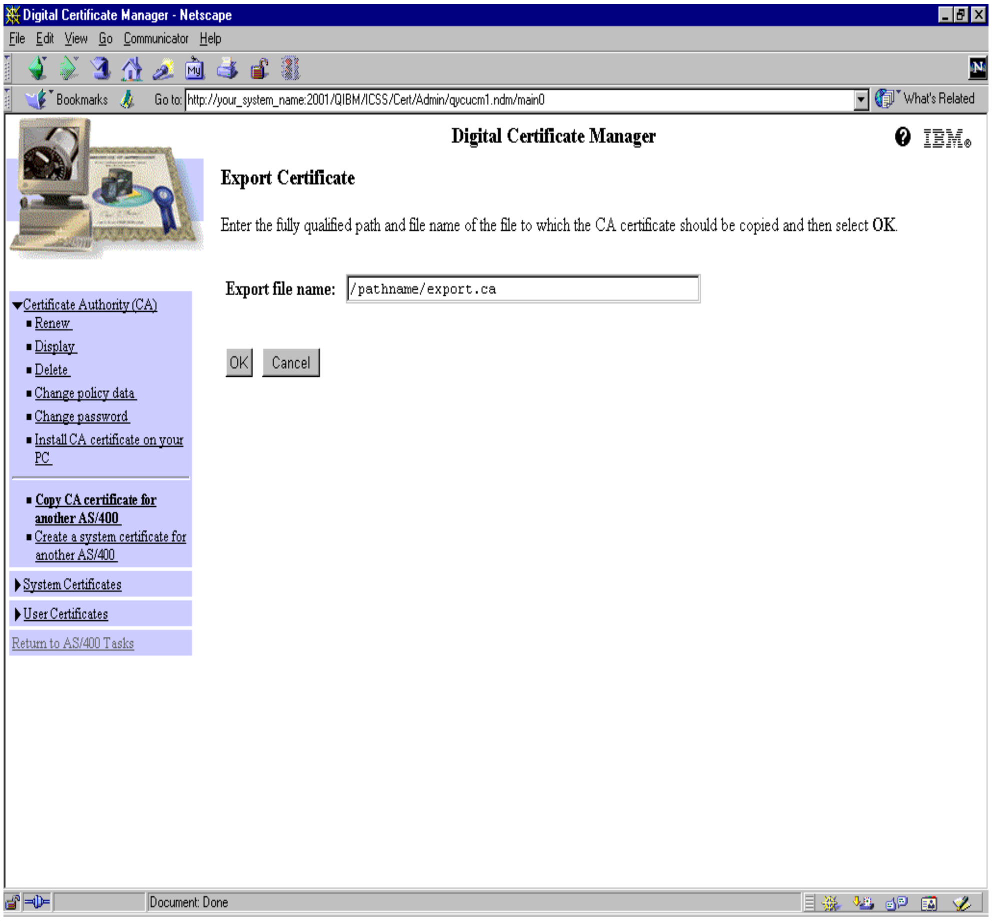


Figure 90. Copy steps overview

5.5.1.1 Export CA certificate

In the first step you have to export the CA certificate into a file within the Integrated File System (IFS). Perform the following steps to export the CA certificate:

1. Click **Copy CA certificate for another AS/400** in the Certificate Authority menu. The Export Certificate page is displayed.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
What's Related
IBM
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
OK
Cancel
Document: Done

Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager

Export Certificate

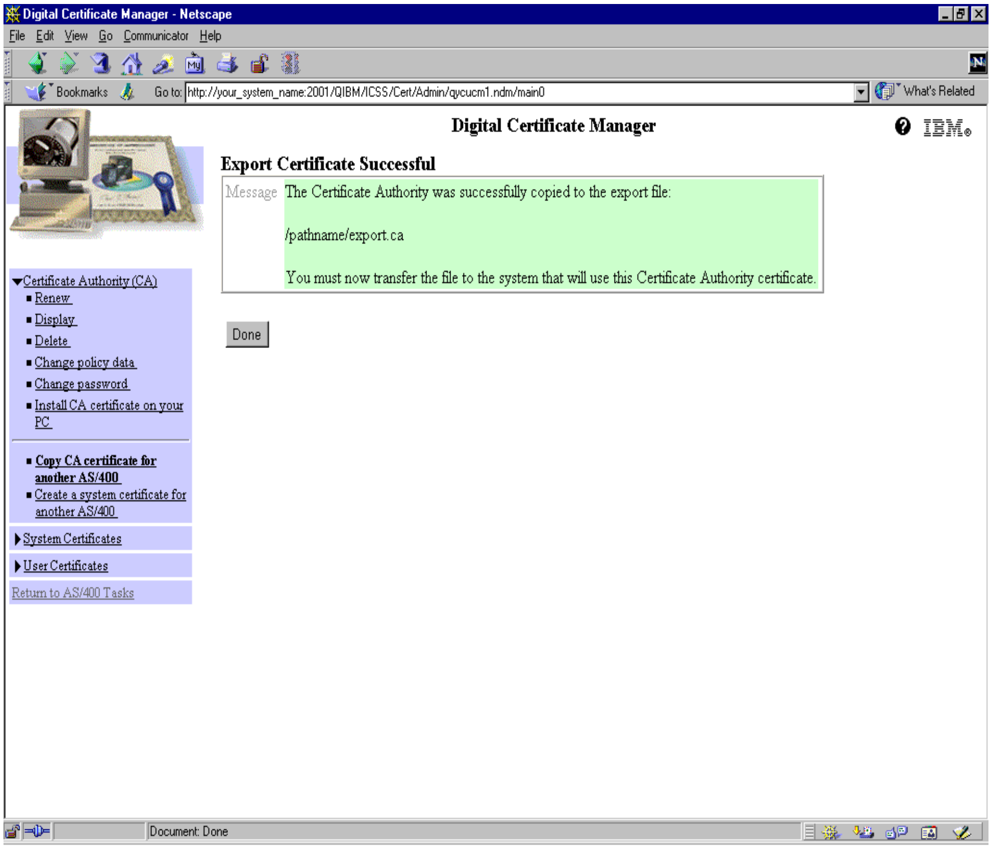
Enter the fully qualified path and file name of the file to which the CA certificate should be copied and then select OK.

Export file name: /pathname/export.ca

Figure 91. Export Certificate window

2. Enter the fully qualified path name and file name. Do not use the file name extension `.KDB`. If you specify a path and file name for an existing file, you will get an error message because DCM does not allow you to overwrite existing files.
3. Click **OK**.

   DCM puts the CA certificate into the export file you specified. The completion message page is shown in Figure 92.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
Done
Document: Done

Export Certificate Successful

Message The Certificate Authority was successfully copied to the export file:

/pathname/export.ca

You must now transfer the file to the system that will use this Certificate Authority certificate.

Figure 92. Export Certificate Successful window

4. Click **Done**, and you will return to the DCM main page.

Now we have an export file on the source machine.

5.5.1.2 Transfer the CA certificate

Note that the following instructions only describe a summary of steps and not the details because basic OS/400 knowledge is presumed. To move this export file from the source to the target system, follow these instructions:

1. Create a save file (SAVF).
2. Save the export file from the IFS using the `SAV` command into the SAVF.
3. Transfer the SAVF to the target system.
4. Restore the export file to the IFS using the `RST` command.

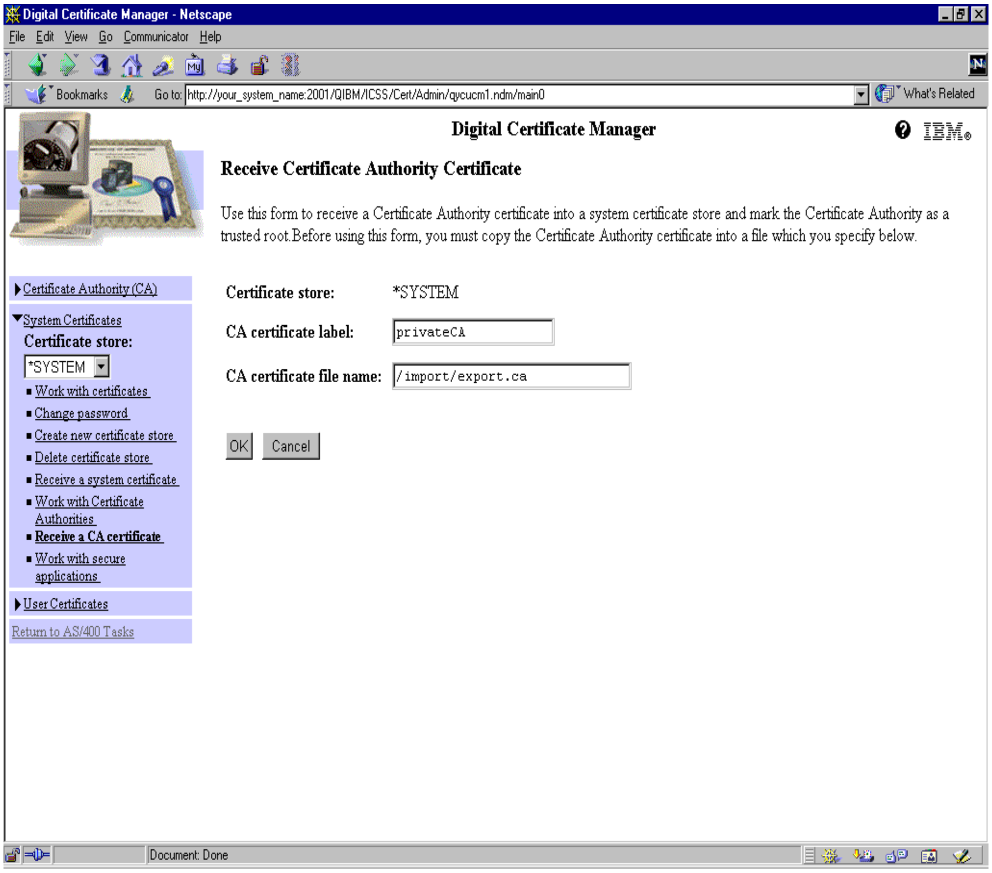
Tip

We recommend the approach described here to transfer the CA certificate using a save file. If you use FTP to transfer the export file directly, this can cause the error `Base64 encode error` when receiving the CA certificate on the target system. This error occurs when you use the wrong format when FTPing the file. So, using the savefile approach is a safer way to do it.

5.5.1.3 Receive a CA certificate

Once the save file that contains the CA certificate is transferred to the target AS/400 system and restored to the IFS, you have to receive it through the appropriate function in DCM. Perform the following steps to receive the CA certificate:

1. Sign on to DCM.
2. Click the **System certificate** task to expand its menu.
3. Select the certificate store ***SYSTEM** or **OTHER** that you want to receive the CA certificate in.
4. Click the **Receive a CA certificate** link. The Receive a CA certificate page is displayed.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
OK
Cancel
Document: Done

Digital Certificate Manager

Receive Certificate Authority Certificate

Use this form to receive a Certificate Authority certificate into a system certificate store and mark the Certificate Authority as a trusted root.Before using this form, you must copy the Certificate Authority certificate into a file which you specify below.

Certificate store: *SYSTEM

CA certificate label: privateCA

CA certificate file name: /import/export.ca

Figure 93. Receive CA Certificate window

5. Fill out the required parameters.

   CA certificate label

   The CA certificate label identifies a CA certificate within a certificate store. This name must be unique within a single certificate store and therefore cannot already exist.

   CA certificate file name

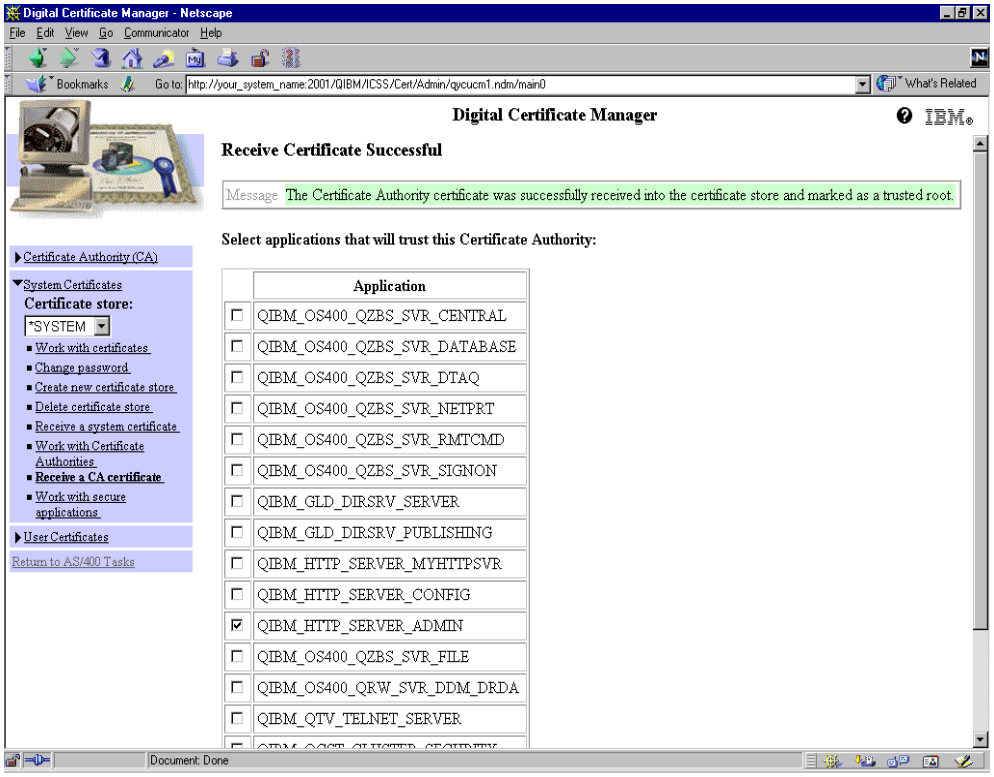
   Specify the fully qualified path and file name of the file in the IFS that contains the CA certificate that you want to receive.

6. Click **OK**.

DCM receives the CA certificate from the copied file you specified and stores the CA certificate in the certificate store you selected. From now on you can identify the CA certificate by the name given in the Receive CA Certificate window. Since this is an arbitrary name, you should use a naming convention for CA certificate labels, particularly when using the CA certificate on multiple systems.

The completion message page is displayed as shown in Figure 94.

When the CA certificate is received into the *SYSTEM certificate store, DCM automatically displays a list with all applications that are registered for certificate use.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM.
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

Receive Certificate Successful

Message The Certificate Authority certificate was successfully received into the certificate store and marked as a trusted root.

Select applications that will trust this Certificate Authority:

	Application
□	QIBM_OS400_QZBS_SVR_CENTRAL
□	QIBM_OS400_QZBS_SVR_DATABASE
□	QIBM_OS400_QZBS_SVR_DTAQ
□	QIBM_OS400_QZBS_SVR_NETPRT
□	QIBM_OS400_QZBS_SVR_RMTCMD
□	QIBM_OS400_QZBS_SVR_SIGNON
□	QIBM_GLD_DIRSRV_SERVER
□	QIBM_GLD_DIRSRV_PUBLISHING
□	QIBM_HTTP_SERVER_MYHTTPSVR
□	QIBM_HTTP_SERVER_CONFIG
☑	QIBM_HTTP_SERVER_ADMIN
□	QIBM_OS400_QZBS_SVR_FILE
□	QIBM_OS400_QRW_SVR_DDM_DRDA
□	QIBM_QTV_TELNET_SERVER

Figure 94. Receive Certificate Successfully window

7. Select which application(s) in the list should trust certificates that are signed by the received CA certificate.
8. Click **OK**.

   The Secure Applications Status window is displayed to indicate that the selected applications will trust the new Certificate Authority. If you select **Other** as the certificate store, this window displays a confirmation message only.
9. Click **OK**, and you will return to the DCM main window.

By clicking the **Work with CA certificate** option of DCM, you can view all Certificate Authorities that are stored on the AS/400 system in a specific certificate store.

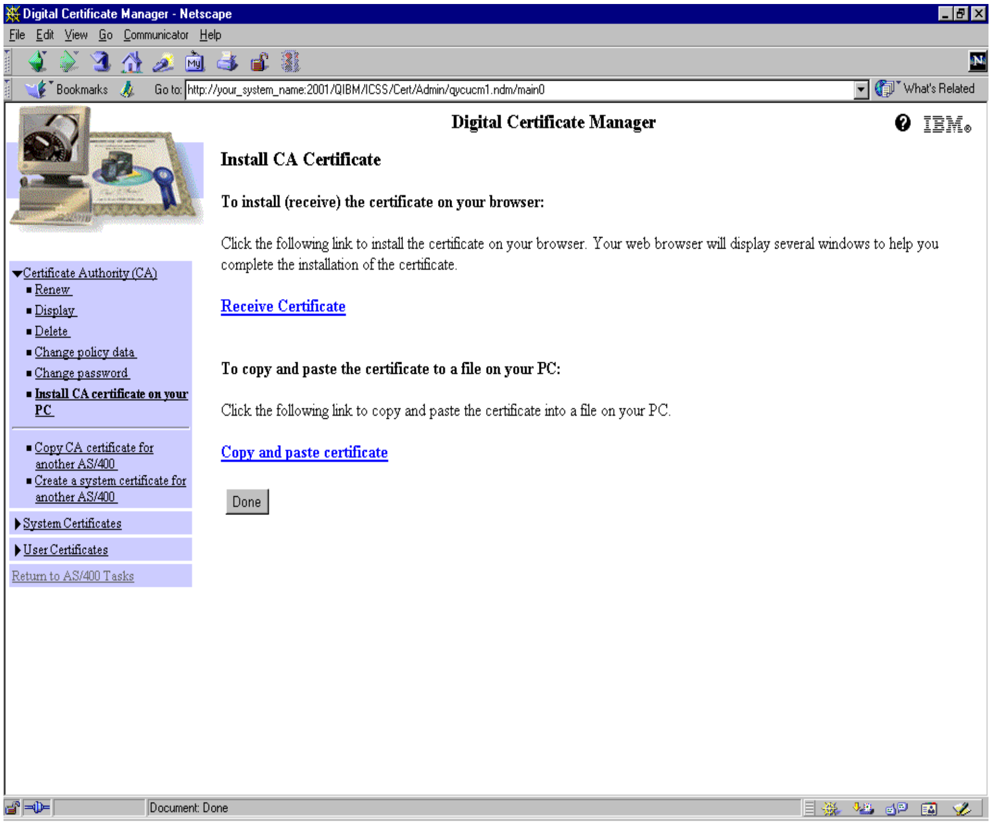
5.5.2 Install CA certificate on your PC (copy and paste)

Each client that communicates with an AS/400 application that uses a system certificate issued by an intranet CA needs to have its CA certificate. There are some applications, such as the Netscape browser, that have built-in functions to directly receive a CA certificate into their database. Other applications, such as eNetwork Personal Communications, have their own management utilities, for example, the IBM Key Management utility, to receive CA certificates. In this case the CA certificate is received through the copy and paste function. The Install CA certificate on your PC task of DCM allows both methods:

- Trigger the client to receive the CA certificate automatically.
- Using the copy and paste approach.

The following steps describe the copy and paste method:

1. Select the **Install CA certificate on your PC** link in the Certificate Authority task menu.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM.
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

Install CA Certificate

To install (receive) the certificate on your browser:

Click the following link to install the certificate on your browser. Your web browser will display several windows to help you complete the installation of the certificate.

Receive Certificate

To copy and paste the certificate to a file on your PC:

Click the following link to copy and paste the certificate into a file on your PC.

Copy and paste certificate

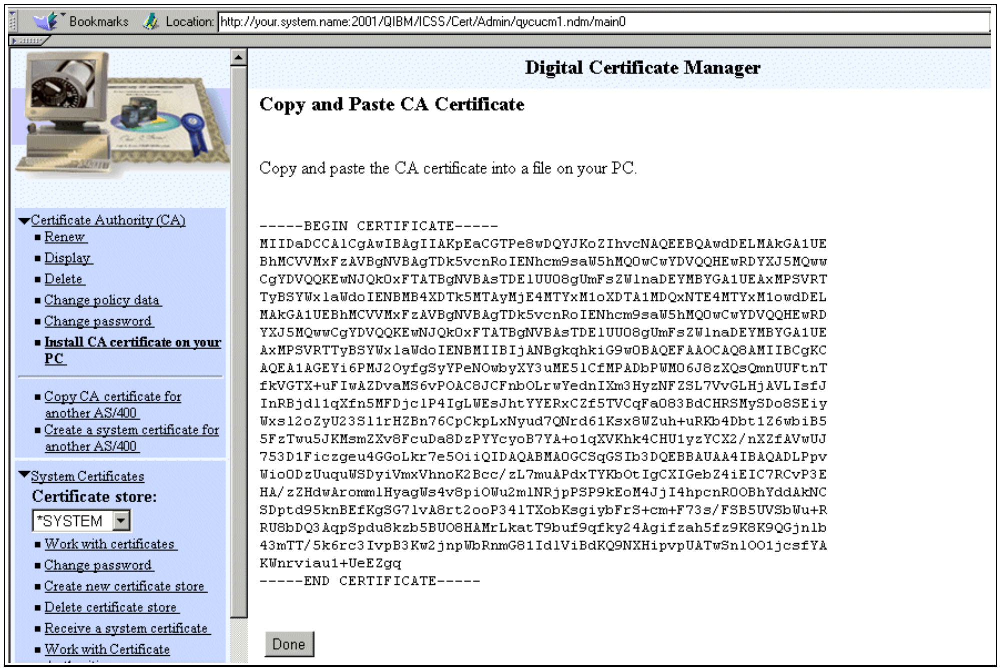
Done

Figure 95. Install CA Certificate window

Note that you have to click the **Receive Certificate** link when installing the CA certificate in the browser.

2. Click **Copy and Paste certificate**.

   DCM displays the CA certificate in base64-encoded ASCII text format as shown in Figure 96 on page 135.


Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Digital Certificate Manager
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate
Done

Copy and Paste CA Certificate

Copy and paste the CA certificate into a file on your PC.

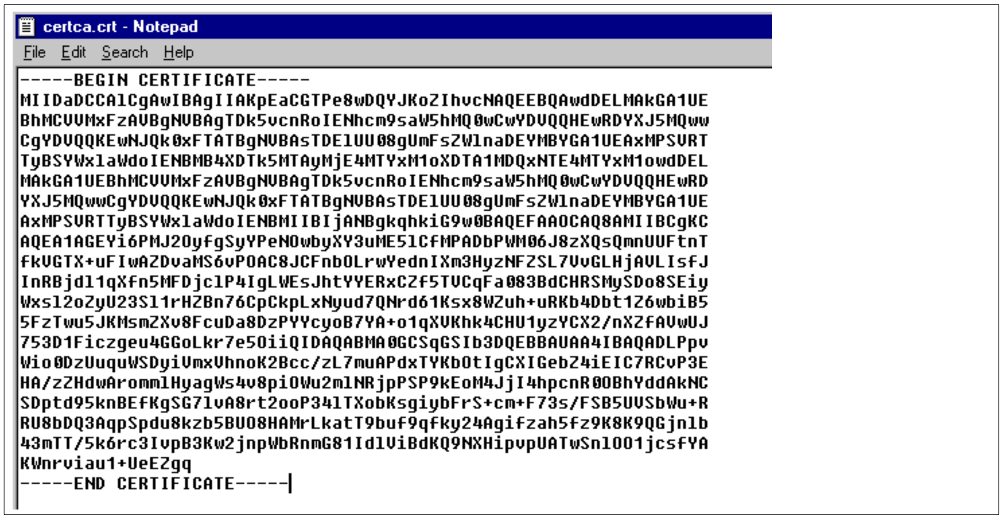
```
-----BEGIN CERTIFICATE-----
MIIDaDCCAlCgAwIBAgIIAKpEaCGTPe8wDQYJKoZIhvcNAQEEBQAwdDELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMQ0wCwYDVQQHEwRDYXJ5MQww
CgYDVQQKEwNJQk0xFTATBgNVBAsTDE1UU08gUmFsZWlnaDEYMBYGA1UEAxMPSVRT
TyBSYWxlaWdoIENBMB4XDTk5MTAyMjE4MTYxM1oXDTA1MDQxNTE4MTYxM1owdDEL
MAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMQ0wCwYDVQQHEwRD
YXJ5MQwwCgYDVQQKEwNJQk0xFTATBgNVBAsTDE1UU08gUmFsZWlnaDEYMBYGA1UE
AxMPSVRTTyBSYWxlaWdoIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA1AGEYi6PMJ2OyfgSyYPeNOwbyXY3uME5lCfMPADbPWM06J8zXQsQmnUUFtnT
fkVGTX+uFIwAZDvaMS6vPOAC8JCFnbOLrwYednIXm3HyzNFZSL7VvGLHjAVLIsfJ
InRBjdl1qXfn5MFDjclP4IgLWEsJhtYYERxCZf5TVCqFa083BdCHRSMySDo8SEiy
Wxsl2oZyU23Sl1rHZBn76CpCkpLxNyud7QNrd61Ksx8WZuh+uRKb4Dbt1Z6wbiB5
5FzTwu5JKMsmZXv8FcuDa8DzPYYcyoB7YA+o1qXVKhk4CHU1yzYCX2/nXZfAVwUJ
753D1Ficzgeu4GGoLkr7e5OiiQIDAQABMA0GCSqGSIb3DQEBBAUAA4IBAQADLPpv
Wio0DzUuquWSDyiVmxVhnoK2Bcc/zL7muAPdxTYKbOtIgCXIGebZ4iEIC7RCvP3E
HA/zZHdwArommlHyagWs4v8piOWu2mlNRjpPSP9kEoM4JjI4hpcnR0OBhYddAkNC
SDptd95knBEfKgSG7lvA8rt2ooP34lTXobKsgiybFrS+cm+F73s/FSB5UVSbWu+R
RU8bDQ3AqpSpdu8kzb5BUO8HAMrLkatT9buf9qfky24Agifzah5fz9K8K9QGjnlb
43mTT/5k6rc3IvpB3Kw2jnpWbRnmG81IdlViBdKQ9NXHipvpUATwSnlOO1jcsfYA
KWnrviau1+UeEZgq
-----END CERTIFICATE-----
```

Figure 96. Copy and Paste CA Certificate window

3. Select the certificate data displayed on the Copy and Paste CA Certificate window.

   Be sure to include `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` as shown in Figure 96.

4. Once the area is selected, press Ctrl+C to copy the certificate data into the clipboard.
5. Start a text editor. We used Notepad.
6. Use Ctrl+V to paste the certificate into the editor window.



```
-----BEGIN CERTIFICATE-----
MIIDaDCCAlCgAwIBAgIIAKpEaCGTPe8wDQYJKoZIhvcNAQEEBQAwdDELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMQ0wCwYDVQQHEwRDYXJ5MQww
CgYDVQQKEwNJQk0xFTATBgNVBAsTDE1UU08gUmFsZWlnaDEYMBYGA1UEAxMPSVRT
TyBSYWxlaWdoIENBMB4XDTk5MTAyMjE4MTYxM1oXDTA1MDQxNTE4MTYxM1owdDEL
MAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMQ0wCwYDVQQHEwRD
YXJ5MQwwCgYDVQQKEwNJQk0xFTATBgNVBAsTDE1UU08gUmFsZWlnaDEYMBYGA1UE
AxMPSVRTTyBSYWxlaWdoIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA1AGEYi6PMJ2OyfgSyYPeNOwbyXY3uME5lCfMPADbPWM06J8zXQsQmnUUFtnT
fkVGTX+uFIwAZDvaMS6vPOAC8JCFnbOLrwYednIXm3HyzNFZSL7VvGLHjAVLIsfJ
InRBjdl1qXfn5MFDjclP4IgLWEsJhtYYERxCZf5TVCqFa083BdCHRSMySDo8SEiy
Wxsl2oZyU23Sl1rHZBn76CpCkpLxNyud7QNrd61Ksx8WZuh+uRKb4Dbt1Z6wbiB5
5FzTwu5JKMsmZXv8FcuDa8DzPYYcyoB7YA+o1qXVKhk4CHU1yzYCX2/nXZfAVwUJ
753D1Ficzgeu4GGoLkr7e5OiiQIDAQABMA0GCSqGSIb3DQEBBAUAA4IBAQADLPpv
Wio0DzUuquWSDyiVmxVhnoK2Bcc/zL7muAPdxTYKbOtIgCXIGebZ4iEIC7RCvP3E
HA/zZHdwArommlHyagWs4v8piOWu2mlNRjpPSP9kEoM4JjI4hpcnR0OBhYddAkNC
SDptd95knBEfKgSG7lvA8rt2ooP34lTXobKsgiybFrS+cm+F73s/FSB5UVSbWu+R
RU8bDQ3AqpSpdu8kzb5BUO8HAMrLkatT9buf9qfky24Agifzah5fz9K8K9QGjnlb
43mTT/5k6rc3IvpB3Kw2jnpWbRnmG81IdlViBdKQ9NXHipvpUATwSnlOO1jcsfYA
KWnrviau1+UeEZgq
-----END CERTIFICATE-----
```

Figure 97. Paste CA certificate into browser

Make sure you also have the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` part included.

7. Save this as a TEXT file.

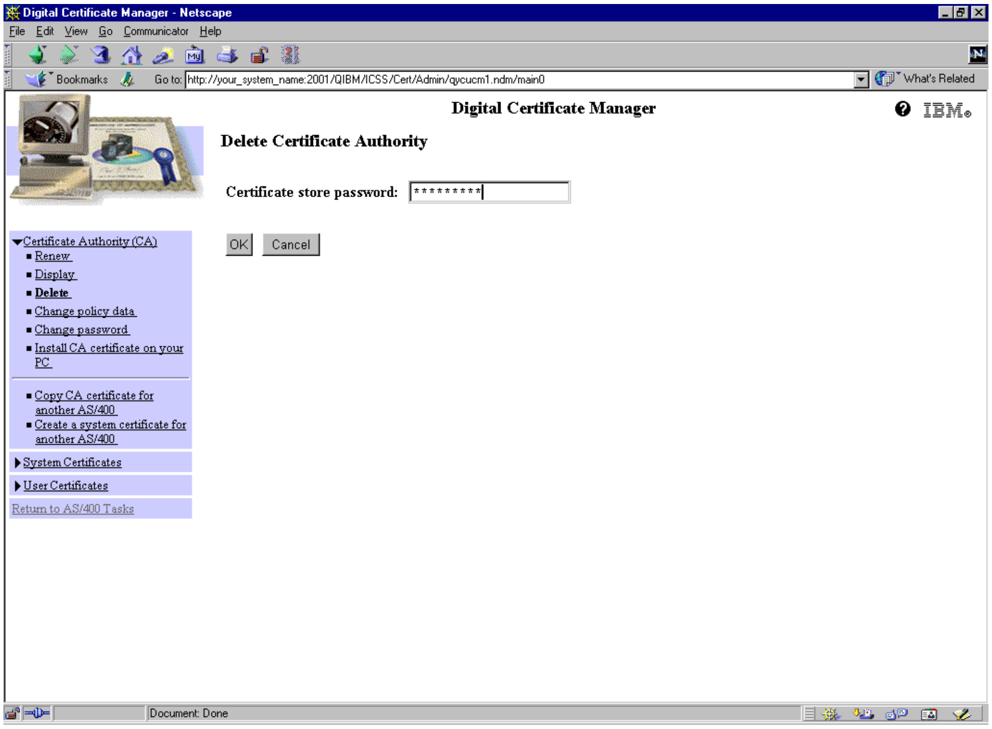
   The file now contains the CA certificate and may be used by various key management utilities to import the CA certificate. An example of importing a CA certificate is shown in 6.5, “Enabling SSL for IBM eNetwork Personal Communications” on page 231.

5.5.3 Delete CA

This section explains how to delete a local CA. This task cannot be undone. Once you delete the CA, you must create a local CA again, performing the same activities as the first time it was created.

To delete a local CA, follow these steps:

1. Click the **Delete** option in the Certificate Authority menu.



Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
What's Related
IBM
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
OK
Cancel
Document: Done

Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager

Delete Certificate Authority

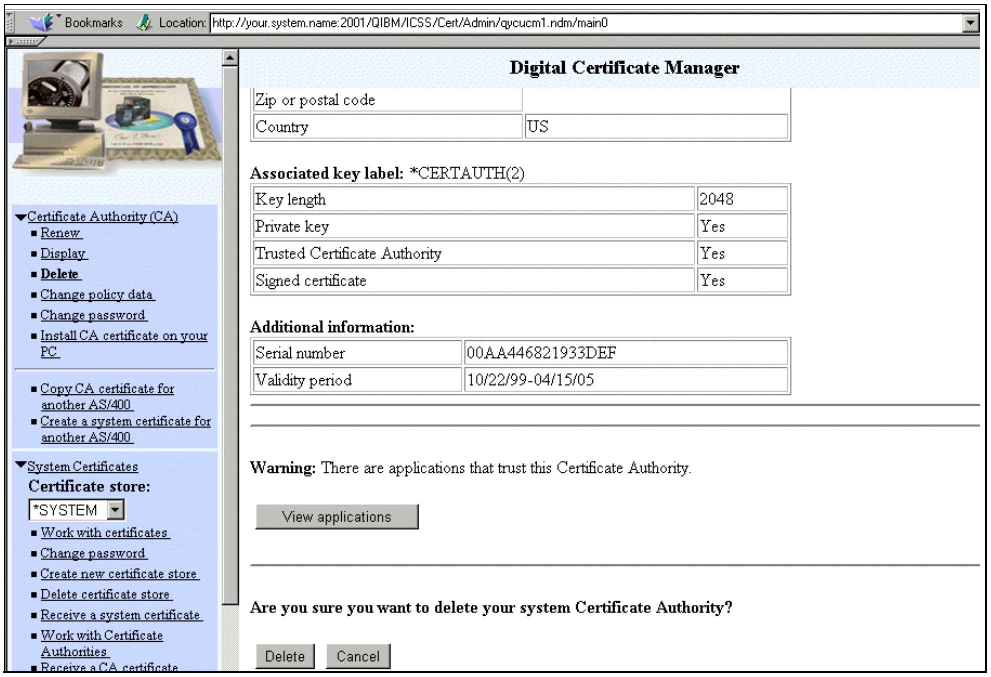
Certificate store password: *********

Figure 98. Delete Certificate Authority window

2. Enter the CA certificate store password. The password is case sensitive.

3. Click **OK**.

   DCM shows you the CA certificate information that is stored in the current working certificate store.


Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
View applications
Delete
Cancel

Digital Certificate Manager

Zip or postal code	
Country	US

Associated key label: *CERTAUTH(2)

Key length	2048
Private key	Yes
Trusted Certificate Authority	Yes
Signed certificate	Yes

Additional information:

Serial number	00AA446821933DEF
Validity period	10/22/99-04/15/05

Warning: There are applications that trust this Certificate Authority.

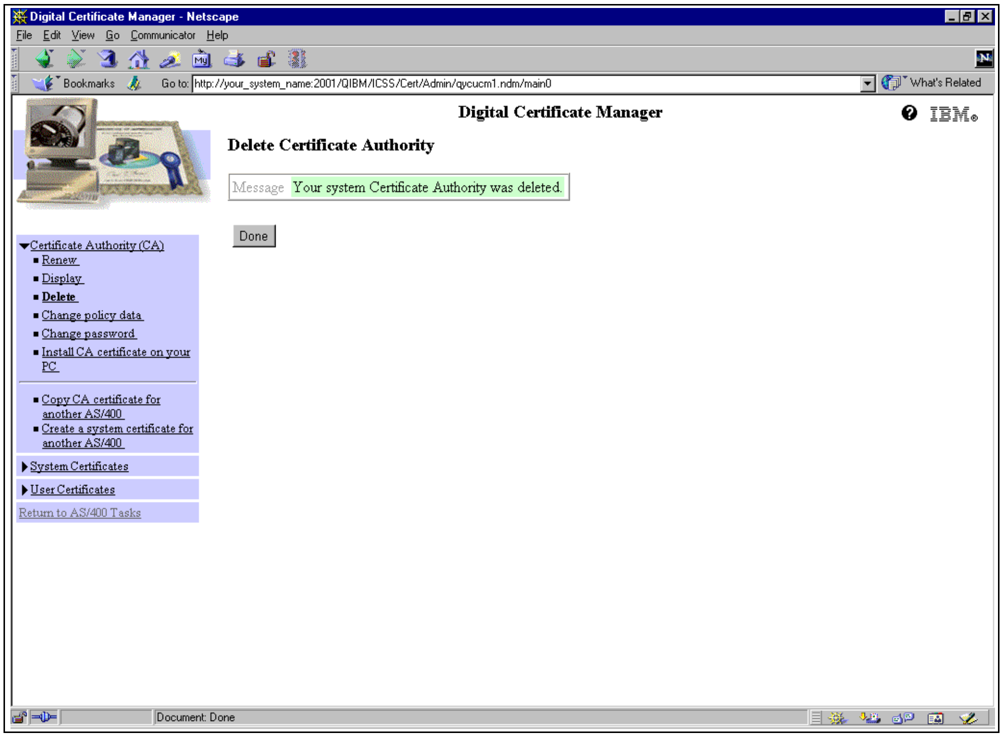
Are you sure you want to delete your system Certificate Authority?

Figure 99. Delete Certificate Authority (confirmation)

If there are still applications that trust the CA as a trusted root, DCM displays a warning message as shown in Figure 99.

4. Click **Delete** to confirm.

   DCM deletes all of the local CA files except for the CA policy file (kdb, ca.txt, sth, and ca.cacrt). Note that copies of the local CA certificate that are contained in other certificate stores (for example, *SYSTEM) are not deleted from those stores. There is no way to undo this task. After the deletion is finished, a completion message is displayed.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
Done
Document: Done

Delete Certificate Authority

Message Your system Certificate Authority was deleted.

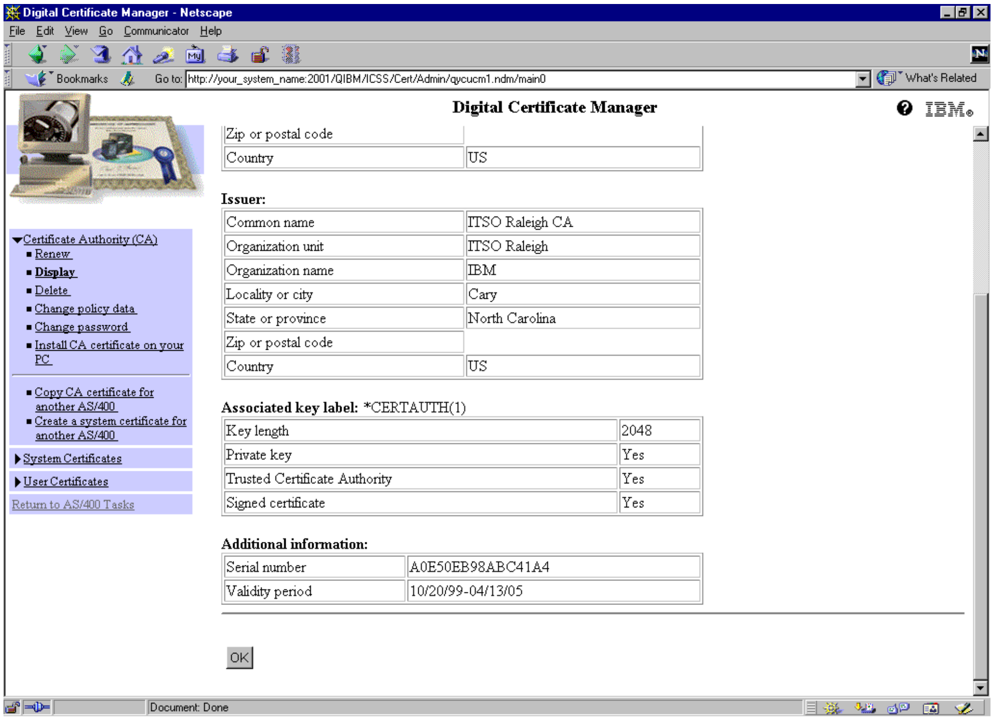
Figure 100. Delete Certificate Authority (successfully)

5.5.4 Renew CA

Use the Renew a Certificate Authority form to renew your current Certificate Authority (CA) certificate. Reasons for renewing the CA certificate might be that the certificate will expire soon or some attribute data need to be changed. When you access the form, the fields contain any previous information that you associated with the certificate. You can change any of this information as part of renewing your CA certificate.The renew task updates certificate information and the number at the end of the label is incremented by one, for example CERTAUTH(1) becomes CERTAUTH(2).

Before you renew the CA certificate, you should check the current CA certificate status.

1. To display the current CA certificate information, click **Display** in the Certificate Authority menu.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
OK
Document: Done

Zip or postal code	
Country	US

Issuer:

Common name	ITSO Raleigh CA
Organization unit	ITSO Raleigh
Organization name	IBM
Locality or city	Cary
State or province	North Carolina
Zip or postal code	
Country	US

Associated key label: *CERTAUTH(1)

Key length	2048
Private key	Yes
Trusted Certificate Authority	Yes
Signed certificate	Yes

Additional information:

Serial number	A0E50EB98ABC41A4
Validity period	10/20/99-04/13/05

Figure 101. Display CA (before renewal)

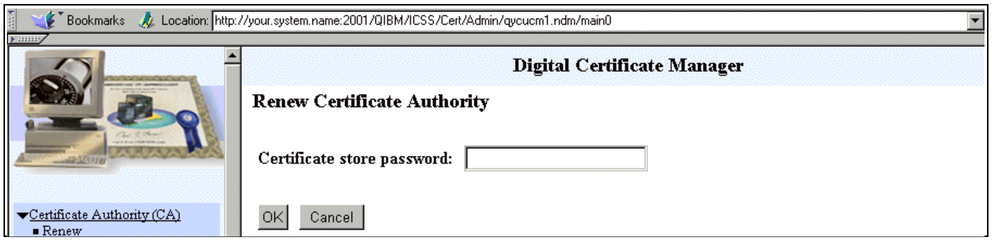
This window contains the current CA certificate contents. You may want to record the serial number and validity period for later use. For example, when you distribute the new CA certificate, you may want to inform clients about the obsolete CA certificate. Since the CA certificate attributes can still be the same, clients need the serial number to uniquely identify the proper CA certificate to be removed.

2. Click **OK**, and you will return to the DCM main window.

To renew the CA certificate perform the following steps:

3. Within DCM, click **Renew** in the Certificate Authority menu.

   The password prompt for the CA certificate store is displayed as shown in Figure 102.


Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Digital Certificate Manager
Certificate Authority (CA)
Renew
OK
Cancel

Renew Certificate Authority

Certificate store password:

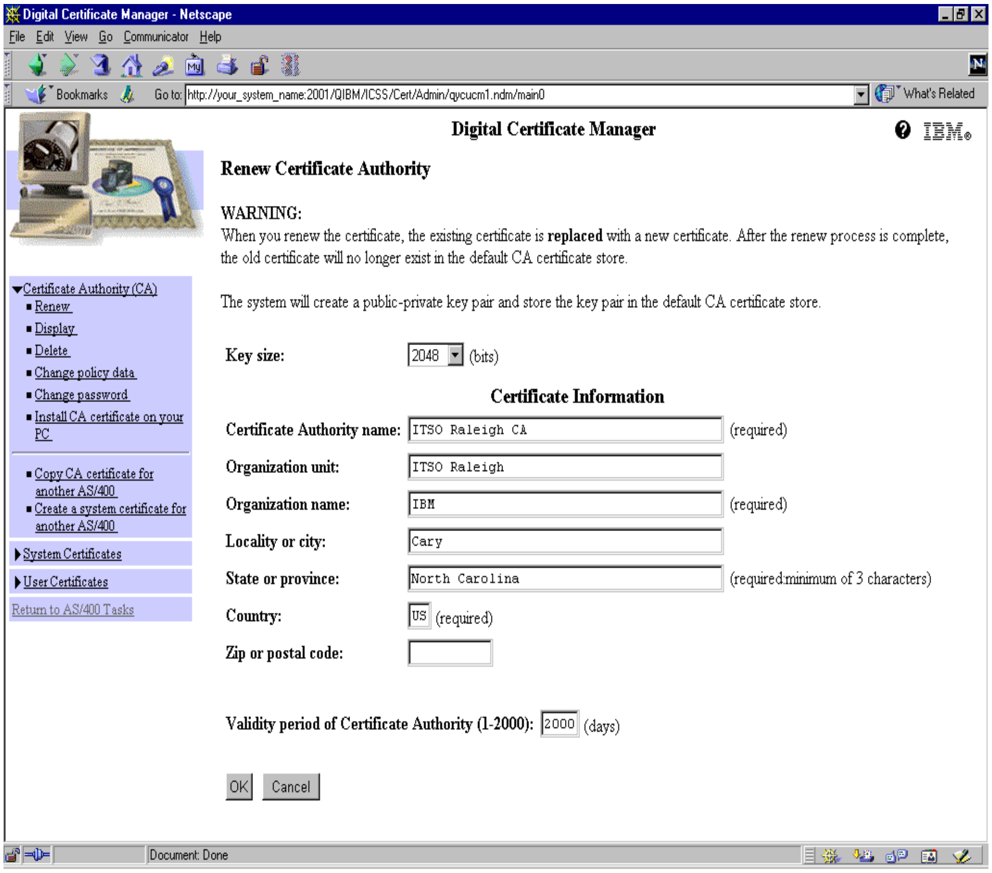
Figure 102. Renew CA - password prompt

4. Enter the password for the CA certificate store, not the system certificate store.

   The password is case sensitive.

5. Click **OK**.

DCM retrieves the current CA certificate information. The Renew CA form as shown in Figure 103 is displayed.



Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

Renew Certificate Authority

WARNING:
When you renew the certificate, the existing certificate is **replaced** with a new certificate. After the renew process is complete, the old certificate will no longer exist in the default CA certificate store.

The system will create a public-private key pair and store the key pair in the default CA certificate store.

Key size: 2048 (bits)

Certificate Information

Certificate Authority name:	ITSO Raleigh CA	(required)
Organization unit:	ITSO Raleigh	
Organization name:	IBM	(required)
Locality or city:	Cary	
State or province:	North Carolina	(required:minimum of 3 characters)
Country:	US	(required)
Zip or postal code:		

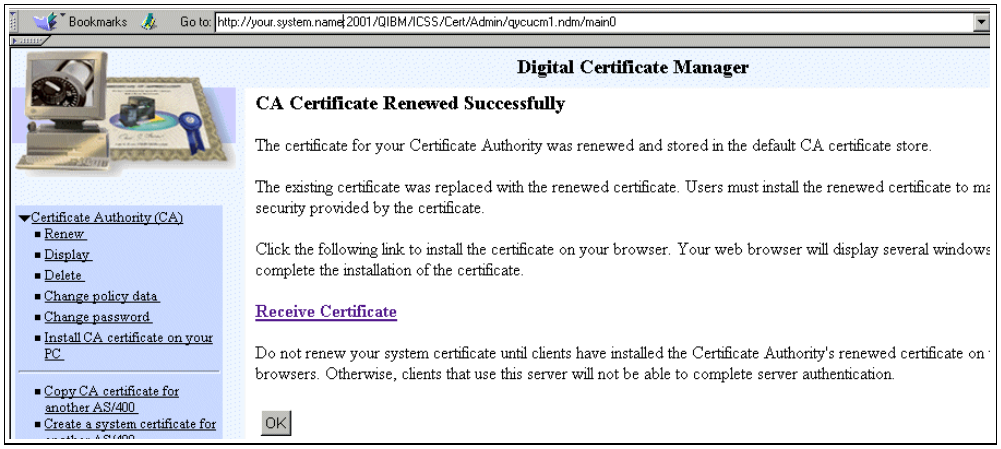
Validity period of Certificate Authority (1-2000): 2000 (days)

OK Cancel

Figure 103. Renew CA certificate form

6. Accept the current settings or make the desired changes.
7. Click **OK** to complete the renew task.

   DCM changes the CA certificate information directly. No backup is saved and you cannot undo this task. Note that the actual old CA is gone, meaning the old CA cannot issue certificates anymore, but there will still be a copy of that old CA in certificate stores that were used by the old CA, such as *SYSTEM. This copy is not useful for issuing certificates, since it is a copy without the private key, and so on, but it is still useful for verifying trust status during SSL requests, so there is a reason for not automatically deleting it from *SYSTEM. After the renewal task completes, the completion message is displayed as shown in Figure 104 on page 141.


Bookmarks
Go to: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
OK

Digital Certificate Manager

CA Certificate Renewed Successfully

The certificate for your Certificate Authority was renewed and stored in the default CA certificate store.

The existing certificate was replaced with the renewed certificate. Users must install the renewed certificate to ma security provided by the certificate.

Click the following link to install the certificate on your browser. Your web browser will display several windows complete the installation of the certificate.

Receive Certificate

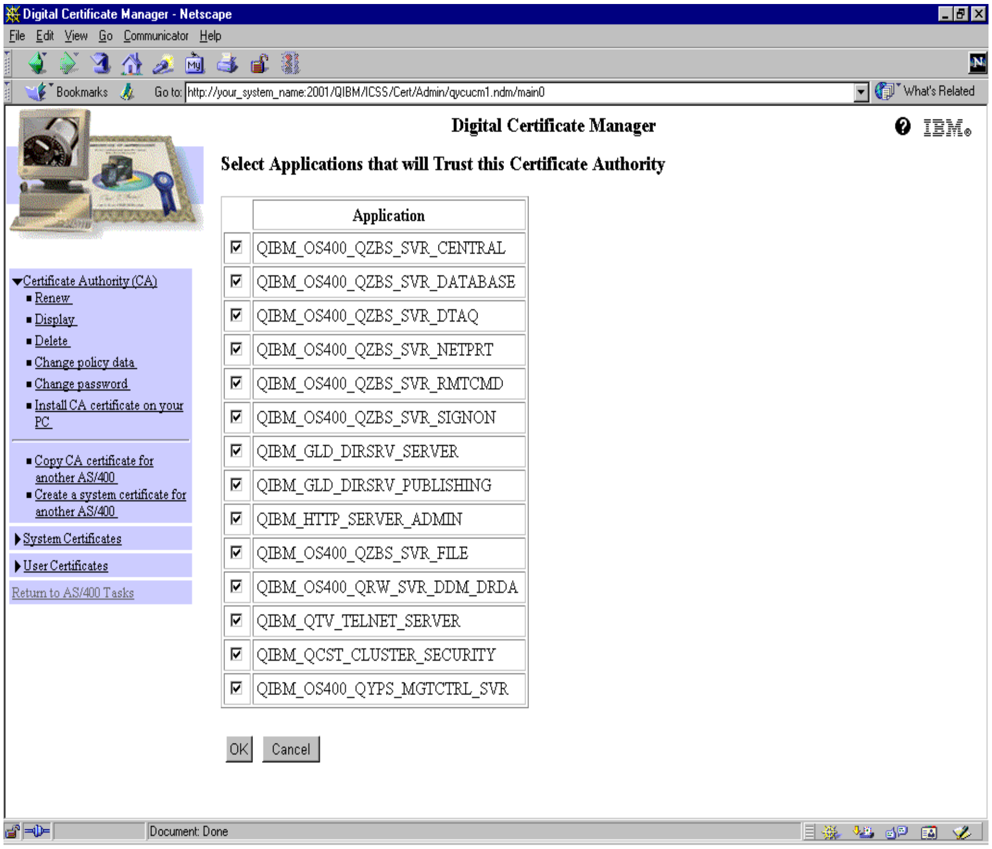
Do not renew your system certificate until clients have installed the Certificate Authority's renewed certificate on browsers. Otherwise, clients that use this server will not be able to complete server authentication.

Figure 104. CA Certificate Renewed Successfully window

8. Click **Receive Certificate** to install the new CA certificate in your browser. The browser displays a series of windows that guide you through the installation process of the new CA certificate. Note that this is an optional task.

   All entities communicating with applications that use certificates issued by this CA need to install the new CA certificate.

9. Click **OK**.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM.
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
OK
Cancel
Document: Done

Digital Certificate Manager

Select Applications that will Trust this Certificate Authority

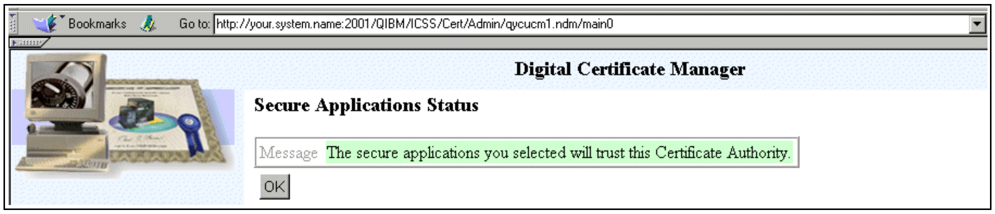
	Application
☑	QIBM_OS400_QZBS_SVR_CENTRAL
☑	QIBM_OS400_QZBS_SVR_DATABASE
☑	QIBM_OS400_QZBS_SVR_DTAQ
☑	QIBM_OS400_QZBS_SVR_NETPRT
☑	QIBM_OS400_QZBS_SVR_RMTCMD
☑	QIBM_OS400_QZBS_SVR_SIGNON
☑	QIBM_GLD_DIRSRV_SERVER
☑	QIBM_GLD_DIRSRV_PUBLISHING
☑	QIBM_HTTP_SERVER_ADMIN
☑	QIBM_OS400_QZBS_SVR_FILE
☑	QIBM_OS400_QRW_SVR_DDM_DRDA
☑	QIBM_QTV_TELNET_SERVER
☑	QIBM_QCST_CLUSTER_SECURITY
☑	QIBM_OS400_QYPS_MGTCTRL_SVR

Figure 105. Renew CA certificate - application selection

On the page shown in Figure 105 are listed all applications listed that are registered for certificate use. Select the applications that you want to trust the new CA. Even though the old CA certificate has been trusted by the secure applications, this setting is not reflected to the renewed CA.

10.Check the box for the application name that you want to trust and click **OK**.

Then completion message is displayed (Figure 106).


Bookmarks
Go to: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
OK

Digital Certificate Manager

Secure Applications Status

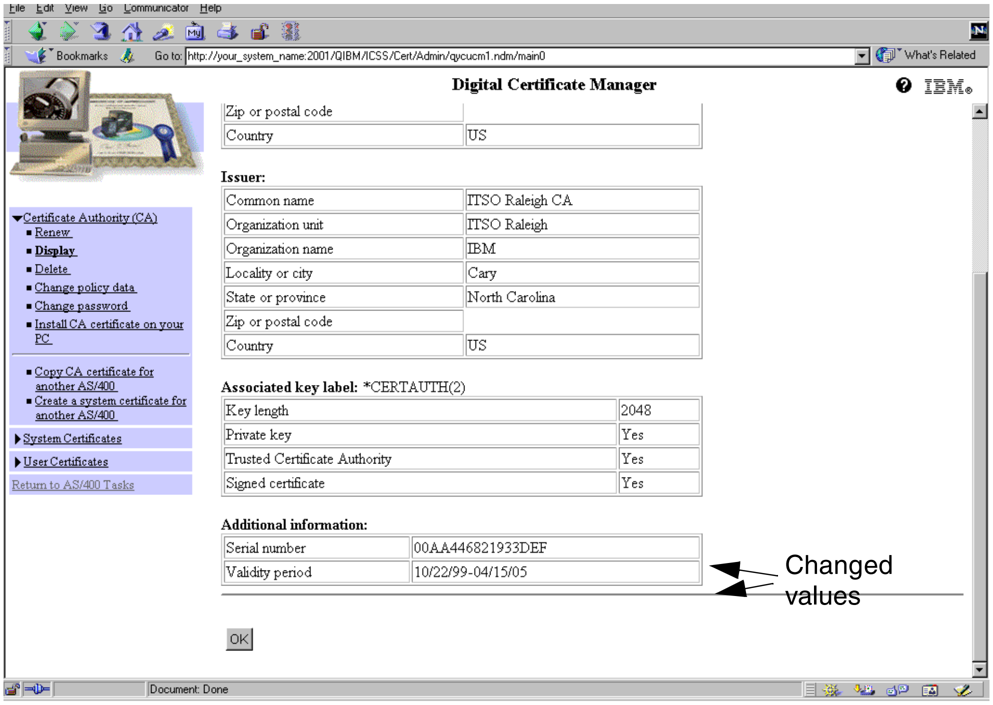
Message	The secure applications you selected will trust this Certificate Authority.

Figure 106. Renew completion message

11.To go back to the DCM main window, click the **OK** button.

The following step is optional and shows that even if the attribute data were not changed for the CA certificate, the serial number has changed. Since the serial number is a part of a certificate, it explains why the CA certificate has to be distributed to all client entities.

12.Click **Display** on the Certificate Authority menu in DCM.


File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM.
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
OK
Document: Done

Digital Certificate Manager

Zip or postal code	
Country	US

Issuer:

Common name	ITSO Raleigh CA
Organization unit	ITSO Raleigh
Organization name	IBM
Locality or city	Cary
State or province	North Carolina
Zip or postal code	
Country	US

Associated key label: *CERTAUTH(2)

Key length	2048
Private key	Yes
Trusted Certificate Authority	Yes
Signed certificate	Yes

Additional information:

Serial number	00AA446821933DEF
Validity period	10/22/99-04/15/05

Changed values

Figure 107. Display CA - after renewal

Check that the values are changed, especially the serial number and validity period. If not, you must do this task again.

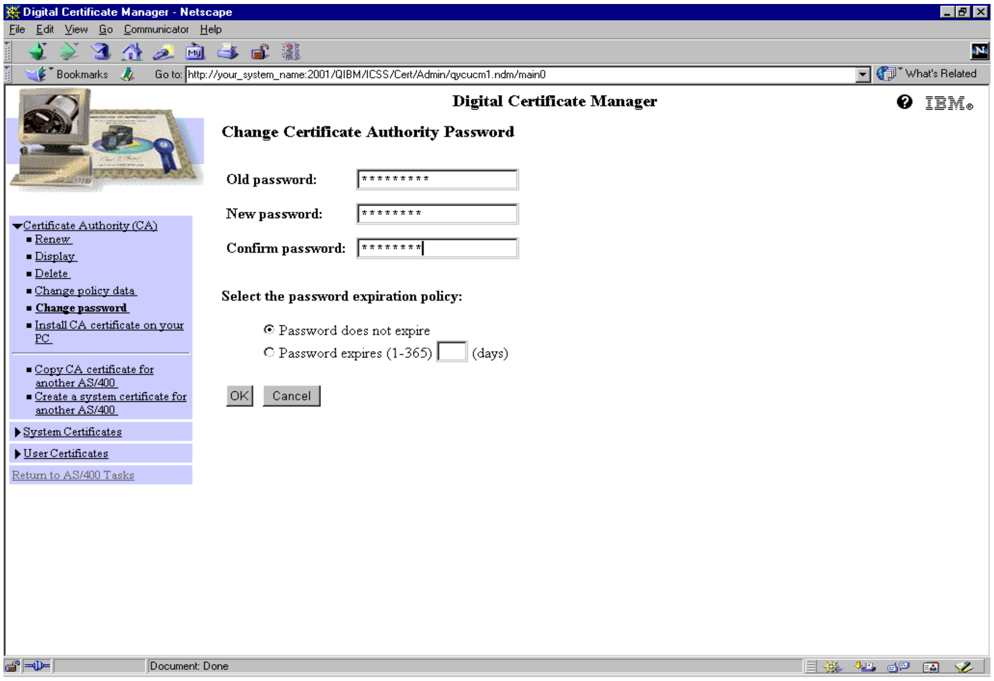
5.5.5 Change CA password

From a security point of view, it is wise to change the CA store password on a regular basis. For additional security after your HTTP Server is set up as a secure application, you can switch to use the secure connection. This means using https and the secure port instead of http and the non-secure port. This additional security can be used when changing the password and for all other transactions. The security concern of access to the IFS directory that holds the CA can also be checked outside of DCM, for example by using an AS/400 command prompt to see that the /qibm/userdata/icss/cert/certauth/ directory is still *PUBLIC *EXCLUDE as it was when DCM created it.

From the Change Certificate Store Password window, you can change the password for the local system certificate store. From this window you can also set the password expiration policy for the certificate store.

Perform the following steps to change the CA certificate store password:

1. Click **Change Password** in the Certificate Authority menu in DCM.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
OK
Cancel
Document: Done

Digital Certificate Manager

Change Certificate Authority Password

Old password: *********

New password: ********

Confirm password: ********

Select the password expiration policy:

● Password does not expire

○ Password expires (1-365) [ ] (days)

Figure 108. Change CA Password form

2. Enter the values for the old and new password.

   Old password

      Enter the current CA certificate store password.

   New password

      Type a CA certificate store password that you want to change.

   Confirm password

      Re-type a new password for verification.

> **Be careful**
>
> You must be sure that you can remember the password that you set, or that you write it down and store it in a secure place. If you forget the password, you cannot reset it or recover it, and you will lose access to your certificate store.

Select the password expiration policy

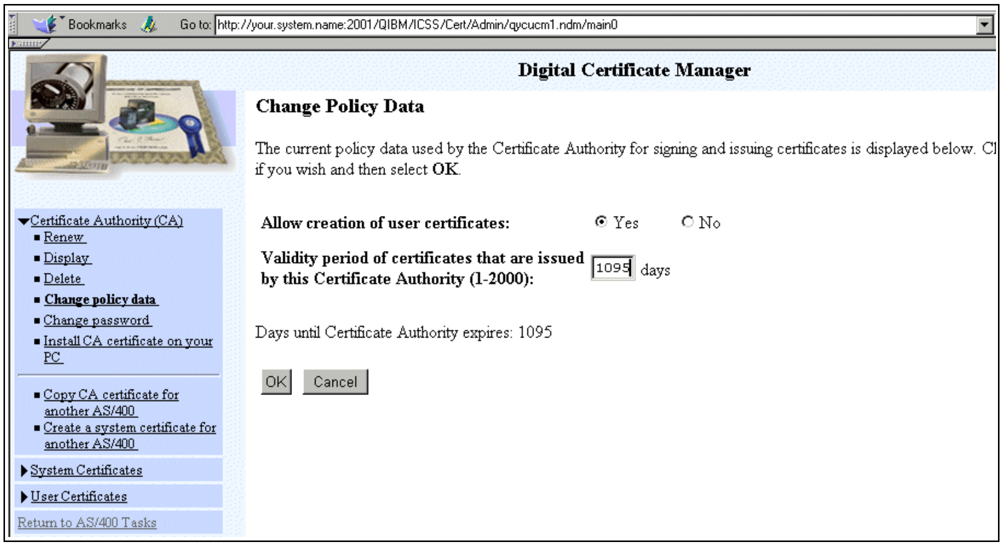
If you want the password to expire after a specific period, select the **Password expires** option and enter in the number of days for which the new password is valid.

3. Click **OK** to apply the changes. A completion message is displayed to indicate the successful password change.

5.5.6 Change CA policy data

This task allows you to change the CA policy rules regarding the validity period of issued certificates. In addition, you can specify whether the CA can issue and sign user certificates. Follow these steps to change the CA's policy data:

1. Click **Change policy data** from the Certificate Authority menu.


Bookmarks
Go to: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
OK
Cancel

Digital Certificate Manager

Change Policy Data

The current policy data used by the Certificate Authority for signing and issuing certificates is displayed below. Cl if you wish and then select OK.

Allow creation of user certificates: ● Yes ○ No

Validity period of certificates that are issued by this Certificate Authority (1-2000): 1095 days

Days until Certificate Authority expires: 1095

Figure 109. Change Policy form

In this window, you can change the following selections.

Allow creation of user certificate

Select **Yes** if you want to enable the CA to issue and sign user certificates.

Note that the intranet CA cannot issue certificates on behalf of another person. Each person has to signon to the AS/400 Tasks page with his or her own user to request a user certificate from this CA.

No is the default.

Validity period

This value is used when a system or user certificate is created. Specify the number of days certificates issued by this CA will be valid. Existing certificate's validity periods are not affected by this change.

2. Click **OK**.

   DCM updates the information in the certificate policy file and confirms the change in a completion message.

5.6 Obtaining a system certificate

This section explains how to obtain a system certificate. The previous section has shown how to issue a CA and system certificate for a system that acts as a local or intranet Certificate Authority. In this section you see how a system certificate is obtained from:

- An AS/400 system running an intranet CA
- A well-known Internet CA

The way a system certificate is obtained is different whether you are requesting it from an intranet CA running on an AS/400 system or a well-known CA. There are other intranet CA software products that may have different requirements for issuing certificates. However, this section covers the most commonly used ways of obtaining a system certificate.

5.6.1 Obtaining a certificate from an AS/400 intranet CA

The first approach shows how a system certificate is requested, issued, and installed. The basic tasks to be performed to obtain a system certificate from an intranet CA on an AS/400 system are:

1. The administrator of the target AS/400 system has to contact the intranet CA administrator and request a system certificate.
2. The intranet CA administrator creates and issues the system certificate on the intranet CA system (source).
3. The new certificate is transferred to the target system.
4. The system certificate is installed on the target system.

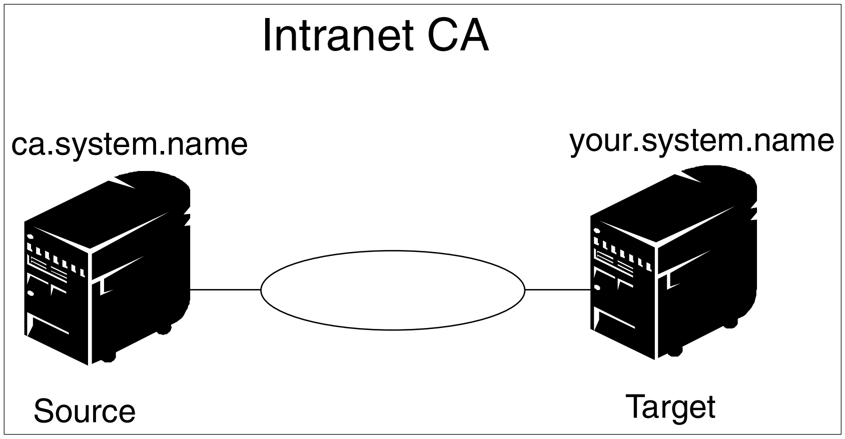
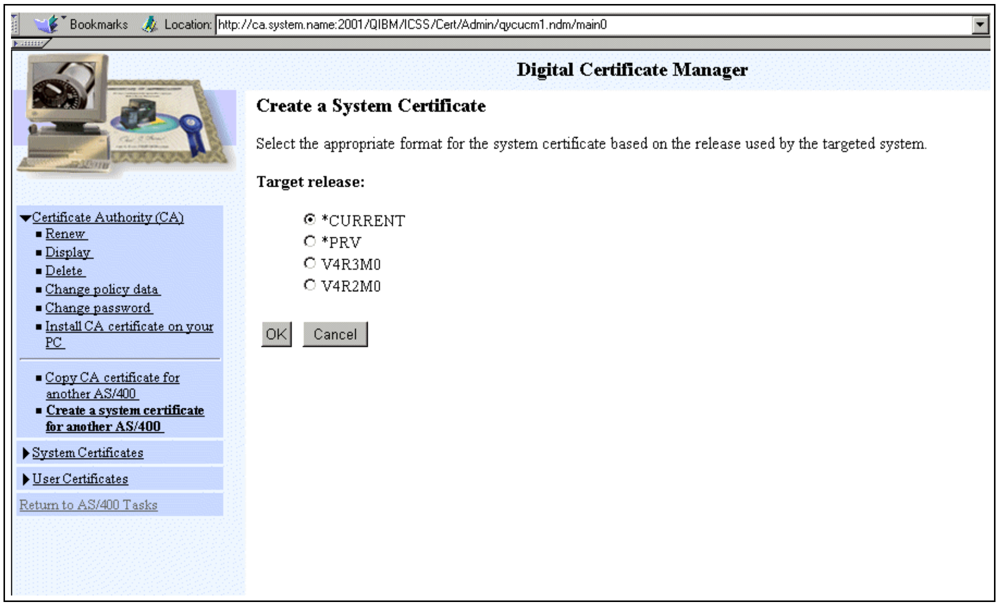


Figure 110. Network view - Intranet CA

5.6.1.1 Create a system certificate on the source AS/400 system

Once the intranet CA administrator has received the request to issue a system certificate for the target AS/400 system, the following steps are performed to create and issue the system certificate on the source AS/400 system:

1. Expand the **Certificate Authority** menu in DCM on the source system.
2. Click **Create a system certificate for another AS/400**.



Location: http://ca.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager

Create a System Certificate

Select the appropriate format for the system certificate based on the release used by the targeted system.

Target release:

● *CURRENT
○ *PRV
○ V4R3M0
○ V4R2M0

Bookmarks
Location:
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks
OK
Cancel

Figure 111. Create a System Certificate for another AS/400

On the first of a series of configuration windows, you can select the target release of the AS/400 system for which the system certificate is requested. The format that you select must be compatible with the version of DCM on the target system.

Target release

*CURRENT

This means to create a system certificate for an AS/400 system that has the same release level installed as the intranet CA system.

*PRV

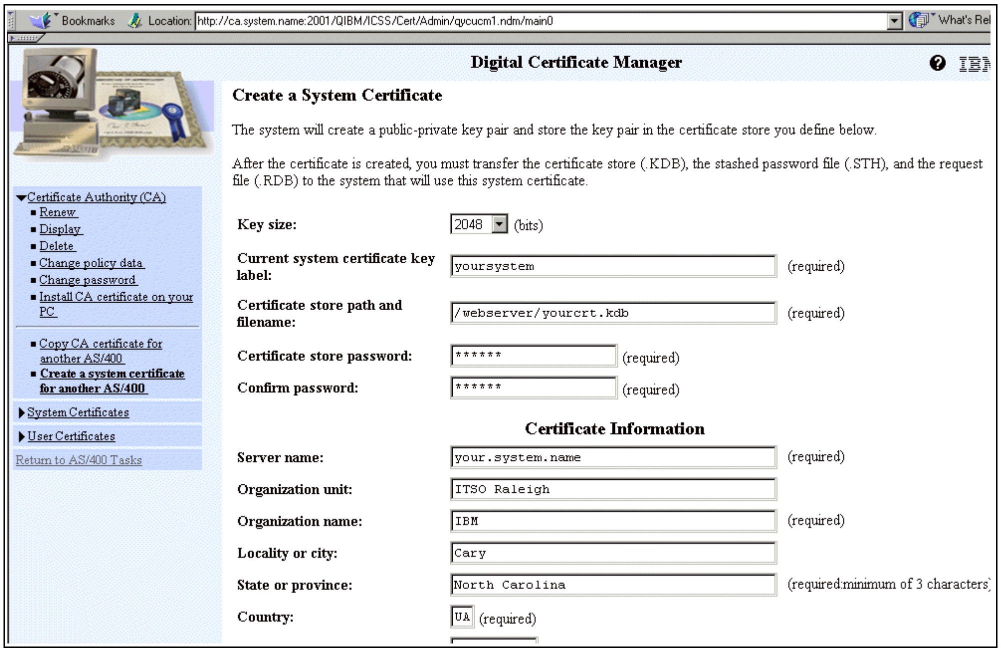
Select this format if DCM on the other system is one release level behind this instance of DCM.

V4R3M0

V4R2M0

3. Click **OK**.

Depending on the release level chosen, the following page is displayed differently. For a V4R4 system, the certificate configuration page is displayed as shown in Figure 112 on page 147.


Bookmarks
Location: http://ca.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Rel
IBM
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
User Certificates
Return to AS/400 Tasks

Digital Certificate Manager

Create a System Certificate

The system will create a public-private key pair and store the key pair in the certificate store you define below.

After the certificate is created, you must transfer the certificate store (.KDB), the stashed password file (.STH), and the request file (.RDB) to the system that will use this system certificate.

Key size:	2048 (bits)	
Current system certificate key label:	yoursystem	(required)
Certificate store path and filename:	/webserver/yourcrt.kdb	(required)
Certificate store password:	******	(required)
Confirm password:	******	(required)

Certificate Information

Server name:	your.system.name	(required)
Organization unit:	ITSO Raleigh	
Organization name:	IBM	(required)
Locality or city:	Cary	
State or province:	North Carolina	(required:minimum of 3 characters)
Country:	UA (required)	

Figure 112. Create a System Certificate for another AS/400 input form

Fill in the required parameters:

Key size

Your choices are 2048, 1024, or 512 bits. The value specifies the key length of the public and private key used for the new certificate. Always use the largest number size you can select. Remember, the larger the key size the higher the workload for the server. The displayed values depend on which cryptographic product (5769-AC1, 2 or 3) is installed.

Current system certificate key label

Accept the default key label or type a name to identify the system certificate private key. Note that certificate (key) labels in a certificate store must be unique. Therefore, you should plan ahead regarding the use of the certificate being created here and where that certificate will be stored. For example, if the default label of *DFTSVR is used and then you try to add this certificate to a different certificate store that already has a certificate with a label of *DFTSVR, you will not be able to add this certificate to that store because the labels are not unique (a duplicate key label error will occur). There is no function in DCM to change a certificate label. If you have a duplicate key problem, the only choice is to create a new certificate with a different label.

Certificate Store path and filename

Enter the fully qualified path and file name that you want to use for the new certificate. For example: `/webserver/cert/targetsys.kdb`. As usual, use reasonable security practices to protect the directory you are about to select from access by those who do not have a need to get at these files. For example, having the file and directory owned by QSYS and authority settings *PUBLIC *EXCLUDE and *QSYS *RWX are good choices.

Tips

For a target release of V4R4M0, use KDB as the file extension.

Prior to V4R4M0, use KYR as the file extension.

You must type a file extension in your file name. DCM does not add file extensions automatically. If you forget it, the creation process will fail.

Certificate store password

This password is used to protect the certificate store from unauthorized access. You must choose your password phrase and remember it. The password is case sensitive and is stored in a stashed password file (STH file).

Confirm password

Re-enter your password.

Server name

Enter a name to describe your system certificate. We recommend that you use the TCP/IP host name of the target AS/400 system that is used in browser URL requests.

Note

If you use a different name from the name used to access your server through a browser, the users get a message every time the server presents the certificate. For example, the Netscape browser checks if the DNS name specified in the URL and the server name specified in the certificate are the same. If not, the user gets a message and has to confirm to proceed.

Organization unit

Type the name of this certificate holder's unit.

Organization name

Type your company name or organizational section.

Locality or city

Type the location name of this certificate holder.

State or province

Type a name for this certificate holder's state or province. This name must be a minimum of three characters in length.

Country

Type a two-letter symbol for your country (for example, US for United States, DE for Germany, NZ for New Zealand, JP for Japan).

Zip or postal code

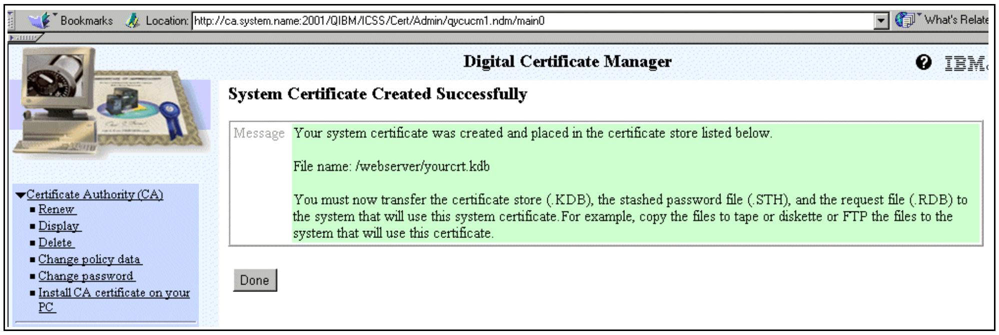
Enter a zip code. Note that this is an optional field. Most of the well-known CAs do not support the zip code in their distinguished name. Therefore, it is best to leave the field blank. Be aware that Netscape Browser 4.01 to 4.61 on a Windows platform have an acknowledged problem performing client authentication when the zip code field is filled. If you want to use client authentication with these browser versions, leave this field blank. The problem is fixed with Netscape Communicator 4.7.

While some CAs verify the fields that are entered, DCM does not verify everything about every field. Correct information should be entered to avoid problems, for example when the certificate would be signed by a CA that does verify and validate the fields. The fields in the certificate that are not verified/validated should not be used by the server as an access check. If this server function is used, more care must be used in determining which CAs validate which fields and therefore which CAs should be marked as trusted for the application.

4. To complete this task, click **OK**.

   DCM generates the private and public key pair and creates the system certificate for the target AS/400 system. Then DCM creates the certificate store file and stores the new certificate in it.

> **Note**
>
> Note that the private and public key pair is generated on the intranet CA AS/400 system. Usually private and public keys are generated on the system that requests the certificate, in this case, `your.system.name`.


Bookmarks
Location: http://ca.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Relate
Digital Certificate Manager
IBM
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Done

System Certificate Created Successfully

Message Your system certificate was created and placed in the certificate store listed below.

File name: /webserver/yourcrt.kdb

You must now transfer the certificate store (.KDB), the stashed password file (.STH), and the request file (.RDB) to the system that will use this system certificate.For example, copy the files to tape or diskette or FTP the files to the system that will use this certificate.

Figure 113. System certificate created successfully

5. Click **Done**.

   The system certificate is now stored in the specified directory (/webserver) and must be transferred to the target AS/400 system. Use reasonable security practices to protect this directory from access by those who do not have a need to get at these files. For example, having the file and directory owned by QSYS and authority settings *PUBLIC *EXCLUDE and *QSYS *RWX are good choices.

5.6.1.2 Transfer the system certificate to the target AS/400 system

After the certificate is created, it has to be transferred to the target system. There are several methods to transfer a certificate from the intranet CA system to the target AS/400 system.

1. Transfer directly the key database (KDB), stashed password file (STH) and certificate request file (RDB) to the target system. This can be done by either

copying the files on a PC that has both directories mapped or by saving and restoring the files using the `SAV` and `RST` commands.

When using these methods you have to ensure that nobody intercepts these files while they are being transferred. Note that transferring or copying the files will override an existing certificate store on the target AS/400 system.

Note

Do not send these files directly using FTP. FTP creates new files on the target system. Certificate store files must have the same creation date and attributes. If you want to use FTP for sending, use an archive program that saves the files into an archive and send this archive to the target AS/400 system.

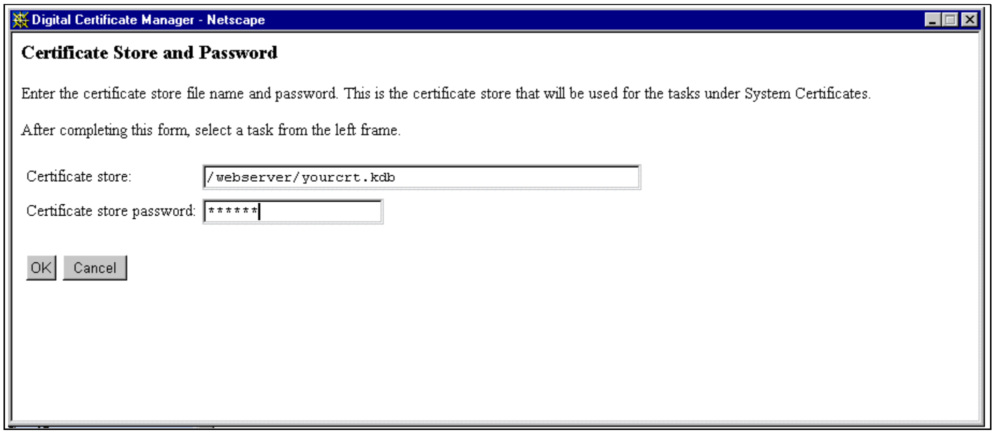
2. Use Export/Import function of DCM

   This is the recommended way to transfer system certificates and must be used if the target system already has a certificate store in place.

5.6.1.3 Export task on the source AS/400 system

The following steps describe the second approach to export the certificate:

1. Click **System Certificate** to expand the menu.
2. Select **Other** for the certificate store under System Certificates. The certificate store path and password must be entered as shown in Figure 114.



Certificate Store and Password

Enter the certificate store file name and password. This is the certificate store that will be used for the tasks under System Certificates.

After completing this form, select a task from the left frame.

Certificate store: /webserver/yourcrt.kdb

Certificate store password: ******

Figure 114. Certificate Store and Password (Other)

Certificate store

Enter the fully qualified path and filename of the certificate store files created in 5.6.1.1, “Create a system certificate on the source AS/400 system” on page 146.

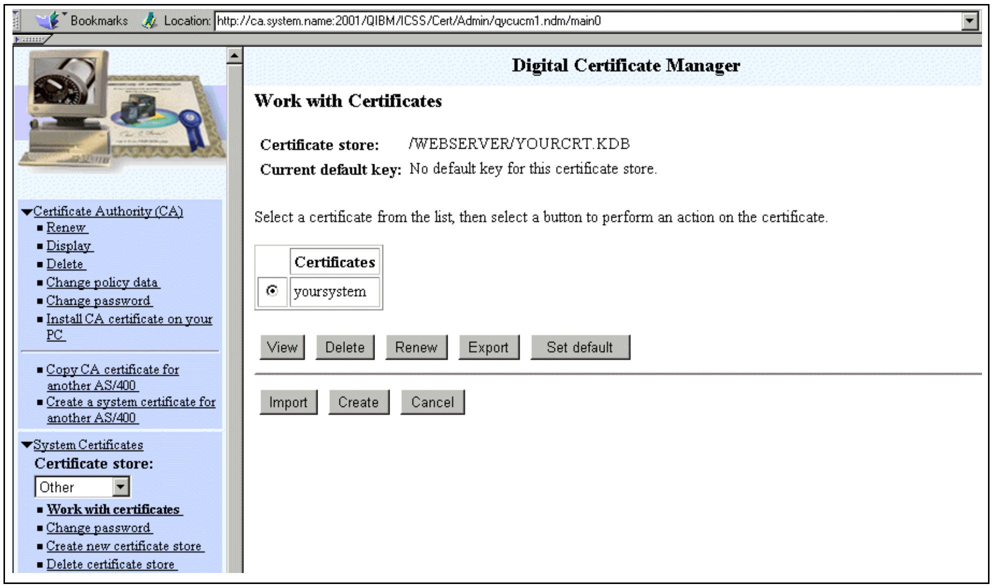
Password

Enter the password specified when you created the certificate store.

3. Fill in the parameter and click **OK**.

   Now DCM refers to the Other certificate store location.

4. Click **Work with certificate** under System Certificates in DCM.


Bookmarks
Location: http://ca.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
Certificate store:
Other
Work with certificates
Change password
Create new certificate store
Delete certificate store
View
Delete
Renew
Export
Set default
Import
Create
Cancel

Digital Certificate Manager

Work with Certificates

Certificate store: /WEBSERVER/YOURCRT.KDB

Current default key: No default key for this certificate store.

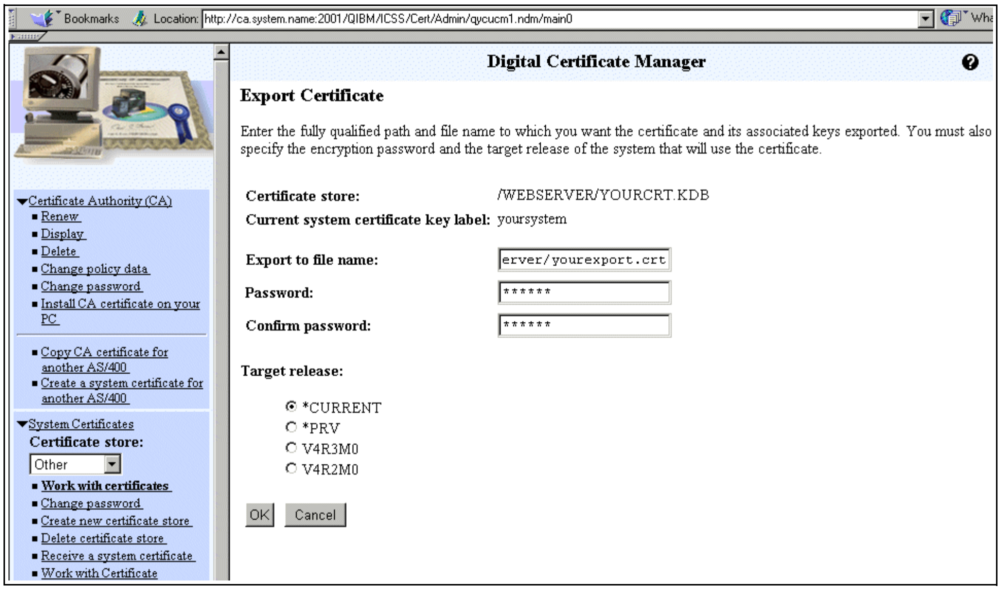
Select a certificate from the list, then select a button to perform an action on the certificate.

	Certificates
●	yoursystem

Figure 115. Work with certificate (Other)

Confirm that you have selected the correct certificate store by checking the **Certificate store** shown on this page.

5. Click **Export**.


Bookmarks
Location: http://ca.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Wha
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
Certificate store:
Other
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate
OK
Cancel

Digital Certificate Manager

Export Certificate

Enter the fully qualified path and file name to which you want the certificate and its associated keys exported. You must also specify the encryption password and the target release of the system that will use the certificate.

Certificate store: /WEBSERVER/YOURCRT.KDB

Current system certificate key label: yoursystem

Export to file name: erver/yourexport.crt

Password: ******

Confirm password: ******

Target release:

● *CURRENT
○ *PRV
○ V4R3M0
○ V4R2M0

Figure 116. Export certificate

Export file name

Type the fully qualified path and export file name. Use reasonable security practices to protect the file, directory and the password that you specify for users who do not have a need to access the file.

Also remember to enter a "/" as the first character in the path.

Note

Because DCM has no default path name, the export process fails if no path is specified on this parameter. The error message that appears is:

```
An error occurred while opening files to write.
```

Password

Enter a password to protect the export file. The password is not related to the certificate store password and is used during import of the certificate on the target AS/400 system. The password is case sensitive.

Confirm password

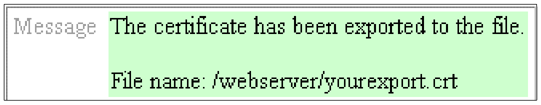
Re-type password.

Target release

Choose the release of the AS/400 system where the exported certificate will be installed. In this case it is the target system `your.system.name`.

6. Enter the parameter as shown in Figure 116 on page 151.
7. Click **OK** to create the export file.

   DCM confirms with a completion message the successful creation of the export file.



Message The certificate has been exported to the file.

File name: /webserver/yourexport.crt

Figure 117. Export certificate confirmation message

The export file can now be transferred in binary mode to the target AS/400 system.

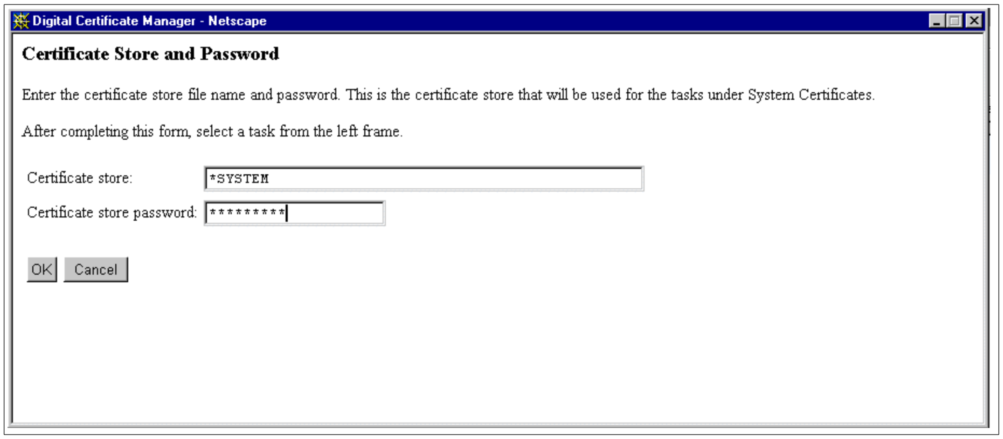
5.6.1.4 Importing the certificate on the target AS/400 system

In this scenario, we signed on to the target AS/400 system, created a new directory and transferred the export file using FTP with the following subcommands:

```
bin
nam 1
get /webserver/yourexport.crt /barlen/yourexport.crt
```

You can also save and restore the file using the `SAV` and `RST` command. After the export file is transferred to a directory in the IFS, perform the following steps to import the certificate into the certificate store on the target AS/400 system:

1. Sign on to DCM on target AS/400 system.
2. Click **System Certificate** to expand its menu.
3. Enter the password for the *SYSTEM certificate store when prompted.



Digital Certificate Manager - Netscape

Certificate Store and Password

Enter the certificate store file name and password. This is the certificate store that will be used for the tasks under System Certificates.

After completing this form, select a task from the left frame.

Certificate store: *SYSTEM

Certificate store password: *********

Figure 118. Certificate store and password

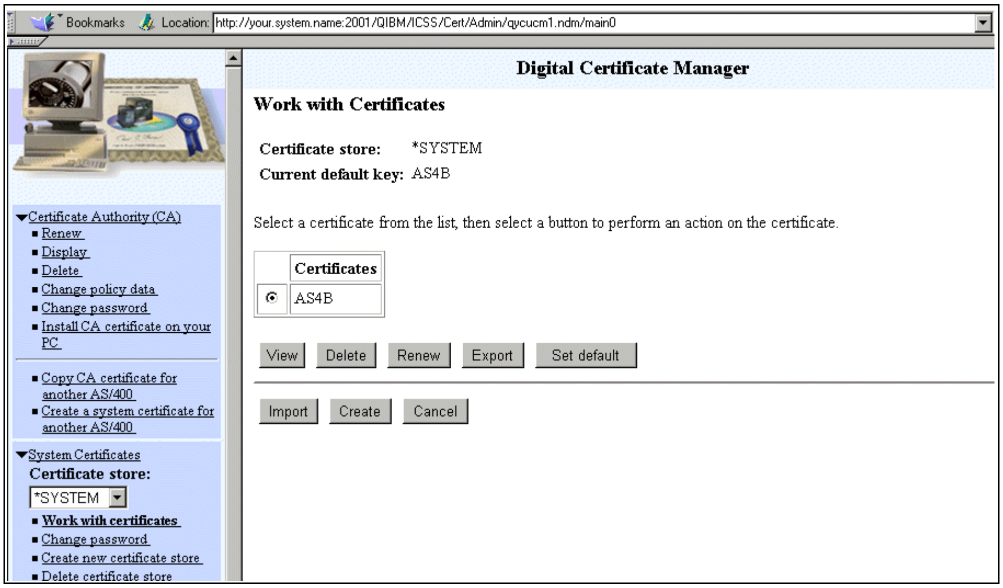
Certificate store

In this case, leave the default as *SYSTEM, which refers to the default certificate store location (see 5.2.3, “Certificate store structure and locations” on page 110).

Certificate store password

Enter the certificate store password. The password is case sensitive.

4. Click **OK**.
5. Click **Work with certificate** to display the installed certificates in the system certificate store.



Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager

Work with Certificates

Certificate store: *SYSTEM

Current default key: AS4B

Select a certificate from the list, then select a button to perform an action on the certificate.

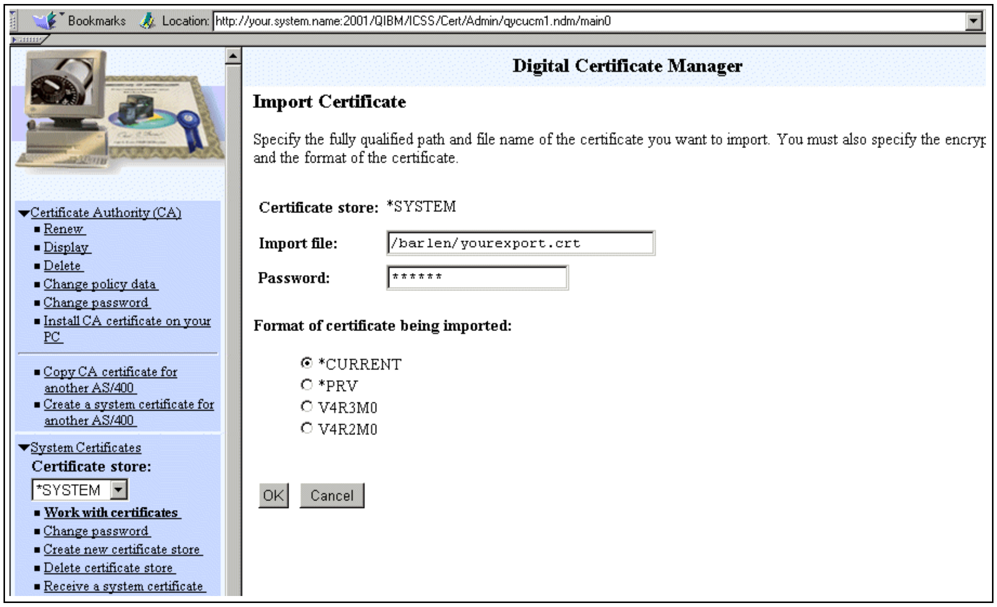
	Certificates
●	AS4B

Figure 119. Work with certificate - Target system

Verify that the *SYSTEM certificate store is displayed.

6. Click **Import**.

DCM shows the Import Certificate window.



Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager

Import Certificate

Specify the fully qualified path and file name of the certificate you want to import. You must also specify the encryp and the format of the certificate.

Certificate store: *SYSTEM

Import file: /barlen/yourexport.crt

Password: ******

Format of certificate being imported:

- ● *CURRENT
- ○ *PRV
- ○ V4R3M0
- ○ V4R2M0

Bookmarks
OK
Cancel
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate

Figure 120. Import certificate on target system

Import file

Enter the fully qualified path and the export file name as shown in Figure 120. Remember to enter the path name; otherwise, DCM fails to import the certificate.

Password

Enter the password to access the export file that is being imported. Use the same password that you used when you created the export file. The password is case sensitive.

Version of certificate being imported

Select the version that you specified when you exported the certificate.

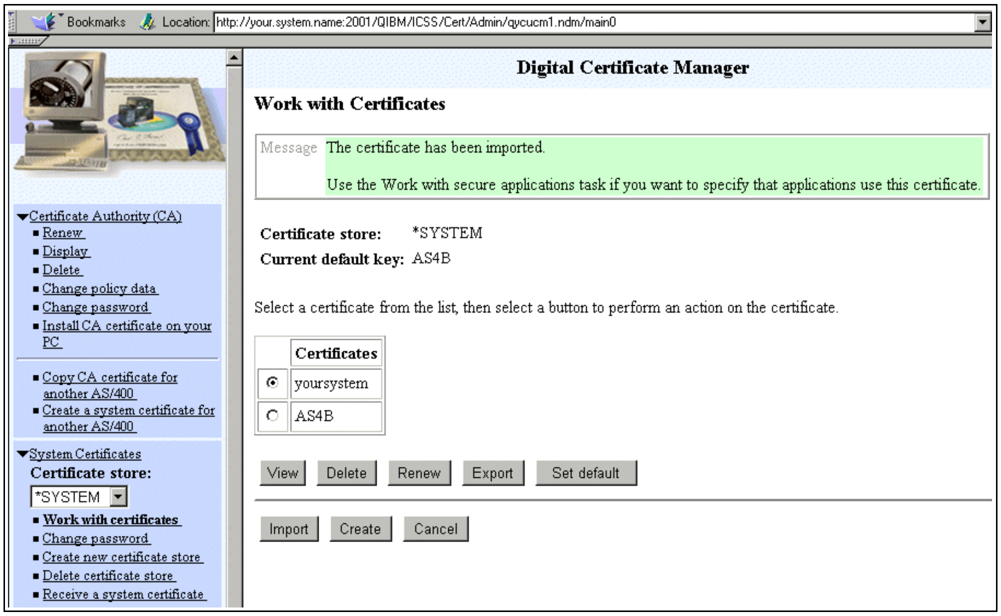
7. Click **OK**.

DCM unlocks the export file using the password you entered and imports the certificate into the system certificate store.

Note

If the key label of the certificate to be imported already exists in the certificate store, the process will fail.

After the certificate is imported, a completion message is displayed and the new certificate is listed in the certificate store as shown in Figure 121.


Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
View
Delete
Renew
Export
Set default
Import
Create
Cancel

Digital Certificate Manager

Work with Certificates

Message The certificate has been imported.

Use the Work with secure applications task if you want to specify that applications use this certificate.

Certificate store: *SYSTEM
Current default key: AS4B

Select a certificate from the list, then select a button to perform an action on the certificate.

	Certificates
●	yoursystem
○	AS4B

Figure 121. Successfully imported certificate on target AS/400 system

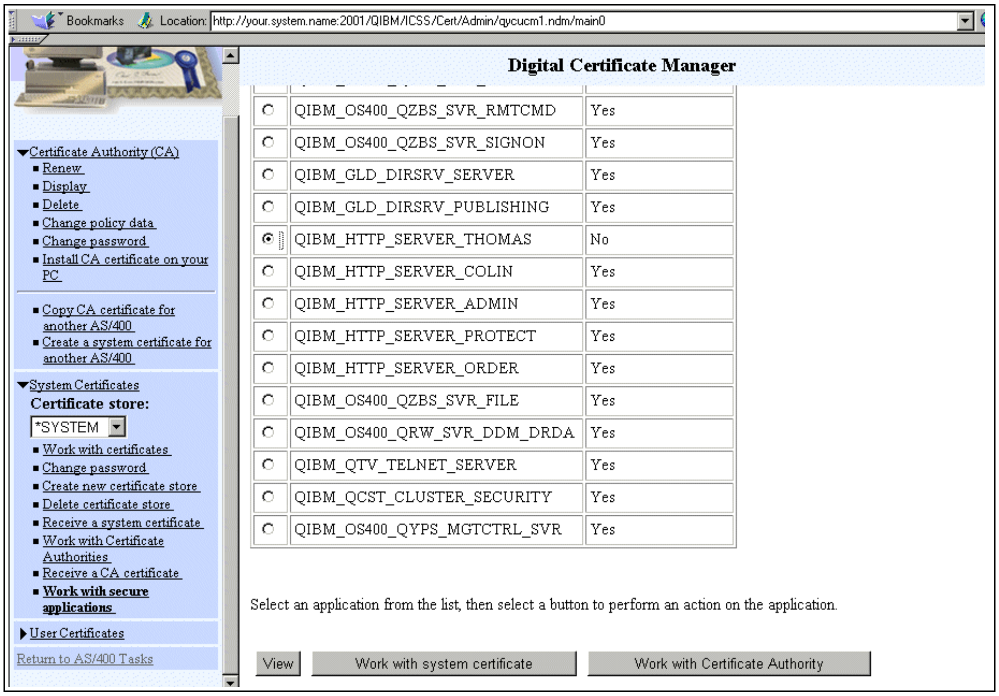
After the certificate is imported into the system certificate store, it needs to be associated with applications that should use the new certificate.

5.6.1.5 Associate the certificate with a secure application

At this time, the imported system certificate is not associated with any secure application on the target AS/400 system. In order for the certificate to be used, it has to be associated with applications as shown in the following steps:

1. Click **Work with secure applications** under System Certificates in DCM.

   The Work with Secure Application window is displayed as shown in Figure 122.


Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Digital Certificate Manager
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Work with system certificate
Work with Certificate Authority

Certificate store: *SYSTEM

○	QIBM_OS400_QZBS_SVR_RMTCMD	Yes
○	QIBM_OS400_QZBS_SVR_SIGNON	Yes
○	QIBM_GLD_DIRSRV_SERVER	Yes
○	QIBM_GLD_DIRSRV_PUBLISHING	Yes
●	QIBM_HTTP_SERVER_THOMAS	No
○	QIBM_HTTP_SERVER_COLIN	Yes
○	QIBM_HTTP_SERVER_ADMIN	Yes
○	QIBM_HTTP_SERVER_PROTECT	Yes
○	QIBM_HTTP_SERVER_ORDER	Yes
○	QIBM_OS400_QZBS_SVR_FILE	Yes
○	QIBM_OS400_QRW_SVR_DDM_DRDA	Yes
○	QIBM_QTV_TELNET_SERVER	Yes
○	QIBM_QCST_CLUSTER_SECURITY	Yes
○	QIBM_OS400_QYPS_MGTCTRL_SVR	Yes

Select an application from the list, then select a button to perform an action on the application.

Figure 122. Work with Secure Applications window

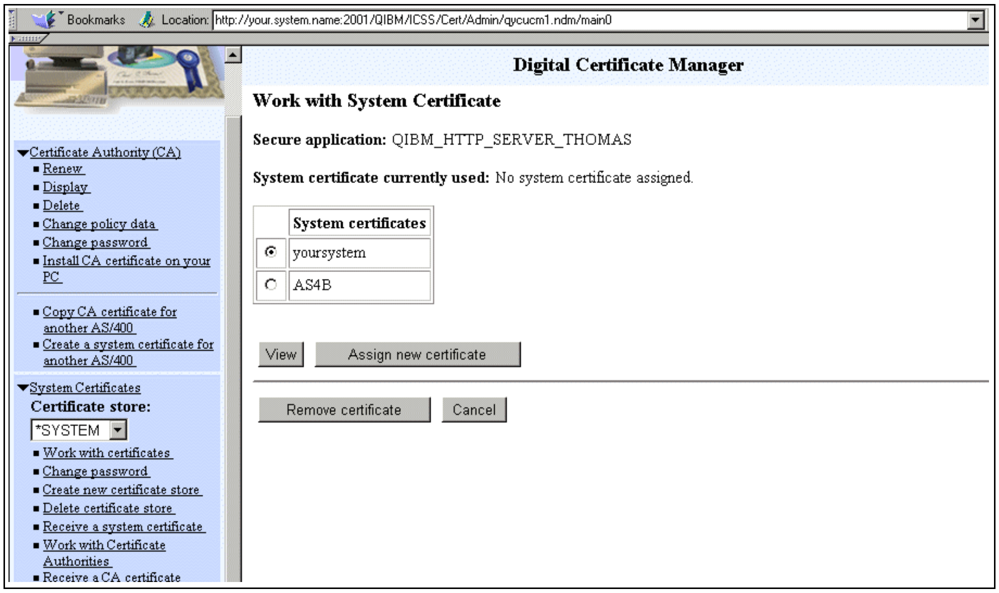
To secure application traffic using the SSL protocol, a system certificate must be associated with that application. In the Work with Secure Applications window all applications that are currently registered for certificate use are displayed. Many IBM applications that are configured for SSL are also automatically registered for certificate use. But it is important to use the intended interfaces to configure those applications, in order to get the application registered in DCM. If, for example, you create an HTTP server instance by copying the directives into a new member, this new server instance is not being registered in DCM. You have to use the HTTP Configuration and Administration utility to configure an HTTP server instance.

User-written applications must be registered by using certificate APIs.

2. Mark the application that should use the new certificate and click the **Work with system certificate** button.

   For the meaning of each application name, refer to Table 3 on page 123.

For example, if you want to associate the certificate with the HTTP server instance THOMAS, select **QIBM_HTTP_SERVER_THOMAS** and click **Work with system certificate**. DCM displays the secure application status as shown in Figure 123 on page 157.


Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
View
Assign new certificate
Remove certificate
Cancel

Digital Certificate Manager

Work with System Certificate

Secure application: QIBM_HTTP_SERVER_THOMAS

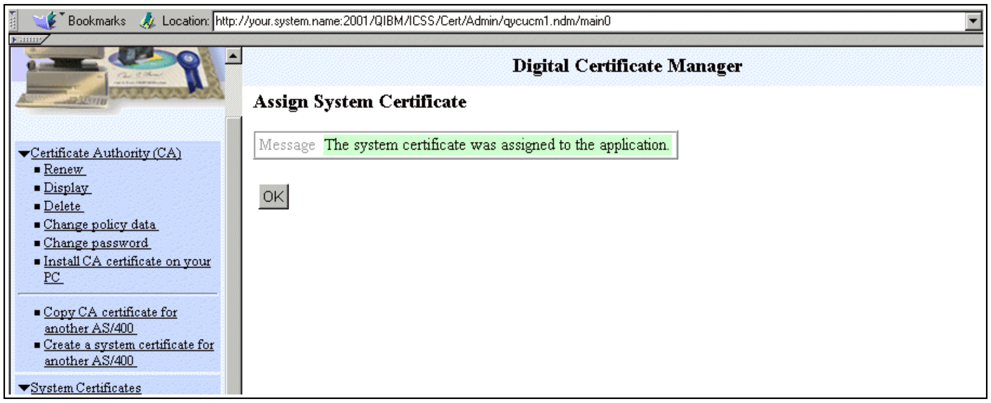
System certificate currently used: No system certificate assigned.

	System certificates
●	yoursystem
○	AS4B

Figure 123. Assign certificate

3. Select the certificate to be assigned and click **Assign a new certificate**.

   DCM associates the certificate with the application and displays a confirmation message.


Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
OK

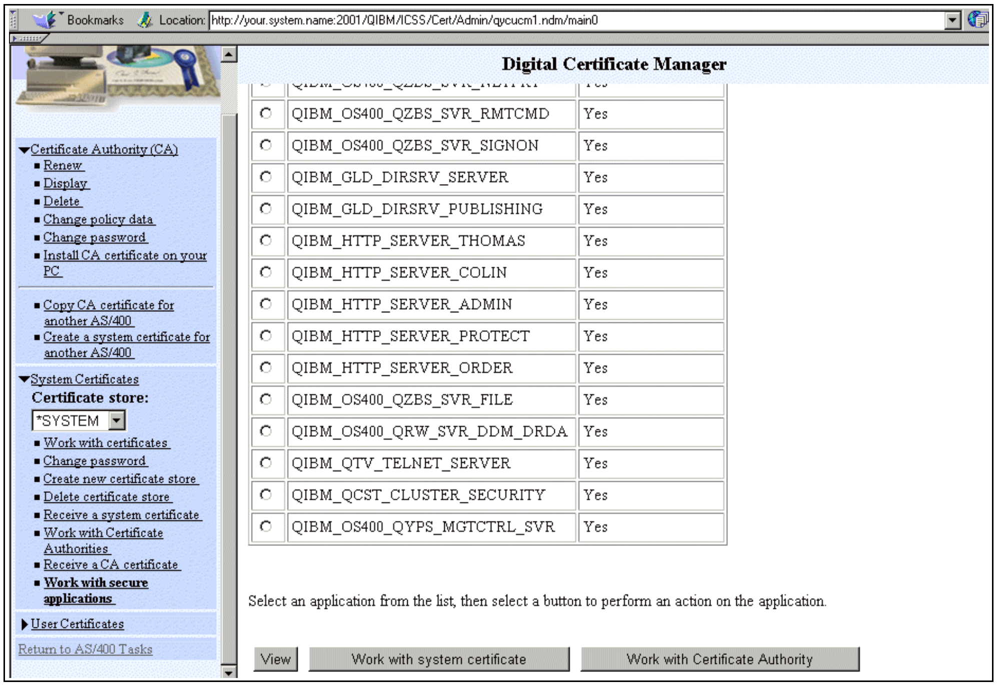
Digital Certificate Manager

Assign System Certificate

Message The system certificate was assigned to the application.

Figure 124. Assign system certificate - confirmation

4. Click **OK**. The Work with Secure Applications window is displayed again showing that a certificates is now associated with the `QIBM_HTTP_SERVER_THOMAS` application.



Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Work with system certificate
Work with Certificate Authority

Digital Certificate Manager

○	QIBM_OS400_QZBS_SVR_RMTCMD	Yes
○	QIBM_OS400_QZBS_SVR_SIGNON	Yes
○	QIBM_GLD_DIRSRV_SERVER	Yes
○	QIBM_GLD_DIRSRV_PUBLISHING	Yes
○	QIBM_HTTP_SERVER_THOMAS	Yes
○	QIBM_HTTP_SERVER_COLIN	Yes
○	QIBM_HTTP_SERVER_ADMIN	Yes
○	QIBM_HTTP_SERVER_PROTECT	Yes
○	QIBM_HTTP_SERVER_ORDER	Yes
○	QIBM_OS400_QZBS_SVR_FILE	Yes
○	QIBM_OS400_QRW_SVR_DDM_DRDA	Yes
○	QIBM_QTV_TELNET_SERVER	Yes
○	QIBM_QCST_CLUSTER_SECURITY	Yes
○	QIBM_OS400_QYPS_MGTCTRL_SVR	Yes

Select an application from the list, then select a button to perform an action on the application.

Figure 125. Work with secure application - after assigning certificate

The certificate is now associated with the secure application. After a new certificate is assigned to an application or an assignment has changed, the application needs to be restarted to reflect the changes.

5.6.2 Obtaining a server certificate from a well-known CA

This section shows how to request and receive a server certificate from a well-known CA. Using a system certificate (also referred to as a server certificate) that has been issued by a well-known CA is the typical scenario when making an application available to the Internet. When using such a certificate, you do not have to worry about distributing and maintaining a local CAs certificate. But from the security point of view you and the users have to fully trust the issuing CA. Refer to Chapter 1, “Introduction to digital certificates” on page 3 for more information about digital certificates and Certificate Authorities.

The process of obtaining a server certificate from a well-known CA is different from obtaining a certificate from an intranet or local CA. Unlike the approach of using a local CA, the certificate request for a well-known CA is created on the AS/400 system requesting the certificate. This includes the generation of the private and public key pair.

The following steps take you through the process of obtaining a server certificate from a well-known CA:

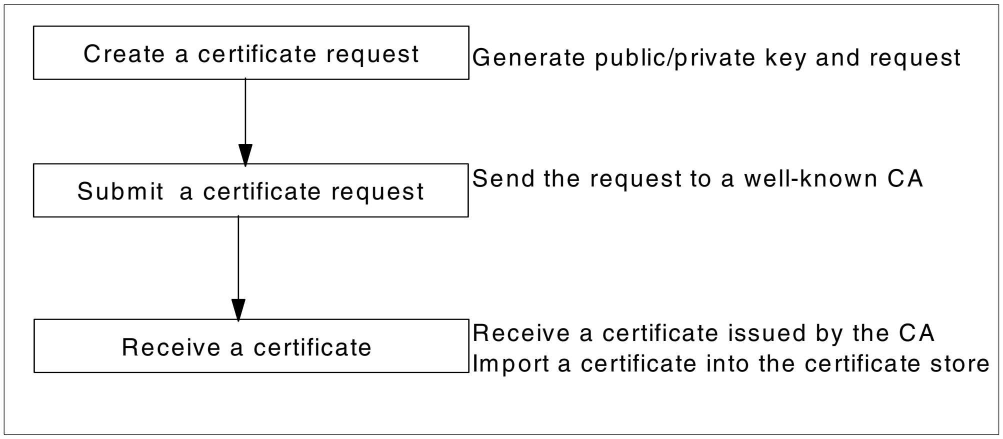

Create a certificate request
Generate public/private key and request
Submit a certificate request
Send the request to a well-known CA
Receive a certificate
Receive a certificate issued by the CA
Import a certificate into the certificate store

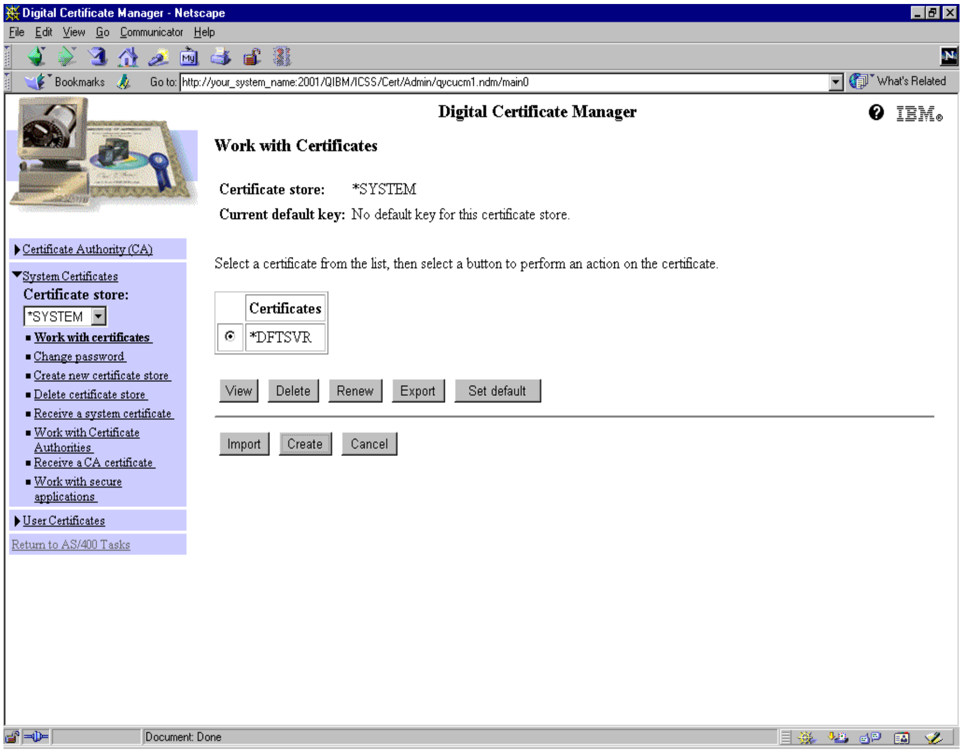
Figure 126. Obtaining a server certificate from a well-known CA overview

5.6.2.1 Create a system certificate request

The first task when obtaining a system certificate is to create the certificate request using DCM.

1. Start DCM and click **System Certificates**. Enter the system certificate store password when prompted.

2. To create a system certificate request, click **Work with Certificates** under System Certificates in DCM. The Work with Certificate window is displayed.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Delete
Renew
Export
Set default
Import
Create
Cancel
Document: Done
IBM.

Digital Certificate Manager

Work with Certificates

Certificate store: *SYSTEM
Current default key: No default key for this certificate store.

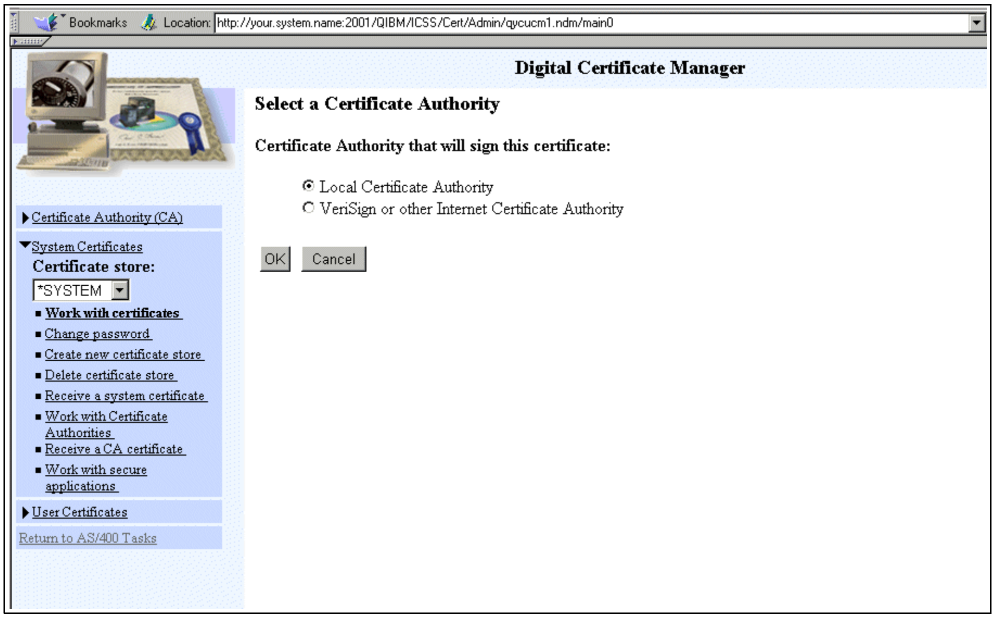
Select a certificate from the list, then select a button to perform an action on the certificate.

	Certificates
●	*DFTSVR

Figure 127. Work with certificates

Confirm that you are working with the correct certificate store. In this case it is the *SYSTEM certificate store containing the *DFTSVR key label.

3. Click **Create** to start the certificate request process.


Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
System Certificates
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
OK
Cancel

Digital Certificate Manager

Select a Certificate Authority

Certificate Authority that will sign this certificate:

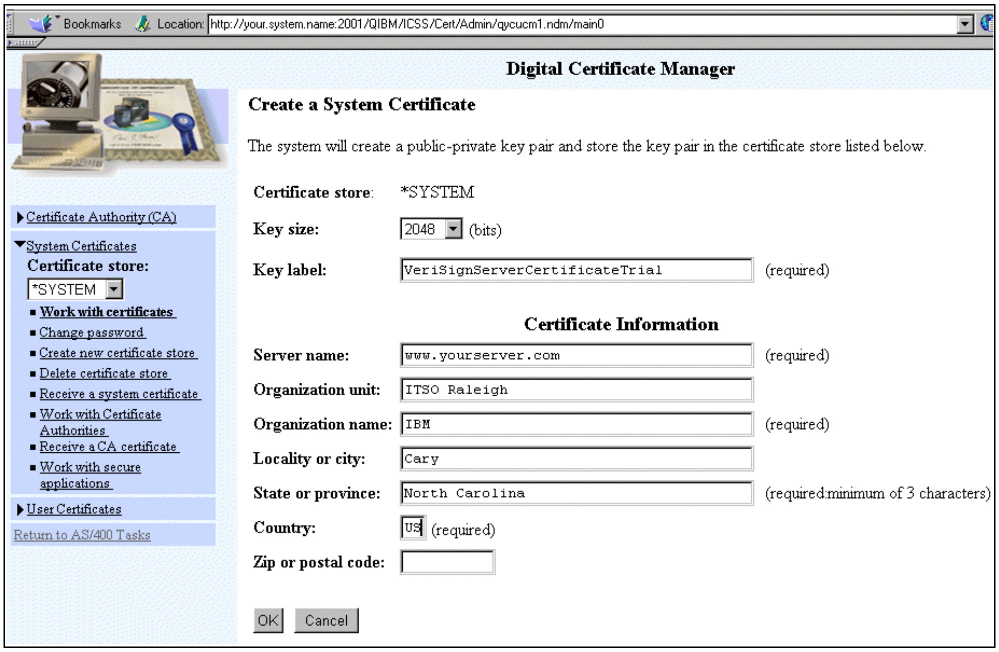
● Local Certificate Authority
○ VeriSign or other Internet Certificate Authority

Certificate store: *SYSTEM

Figure 128. Select a Certificate Authority

4. Select **VeriSign or other Internet Certificate Authority**. If there is no local CA setup on this system, the Local Certificate Authority option does not appear.

5. Click **OK**. The Create a System Certificate window is displayed.


Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
System Certificates
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
OK
Cancel

Digital Certificate Manager

Create a System Certificate

The system will create a public-private key pair and store the key pair in the certificate store listed below.

Certificate store:	*SYSTEM	
Key size:	2048 (bits)	
Key label:	VeriSignServerCertificateTrial	(required)

Certificate Information

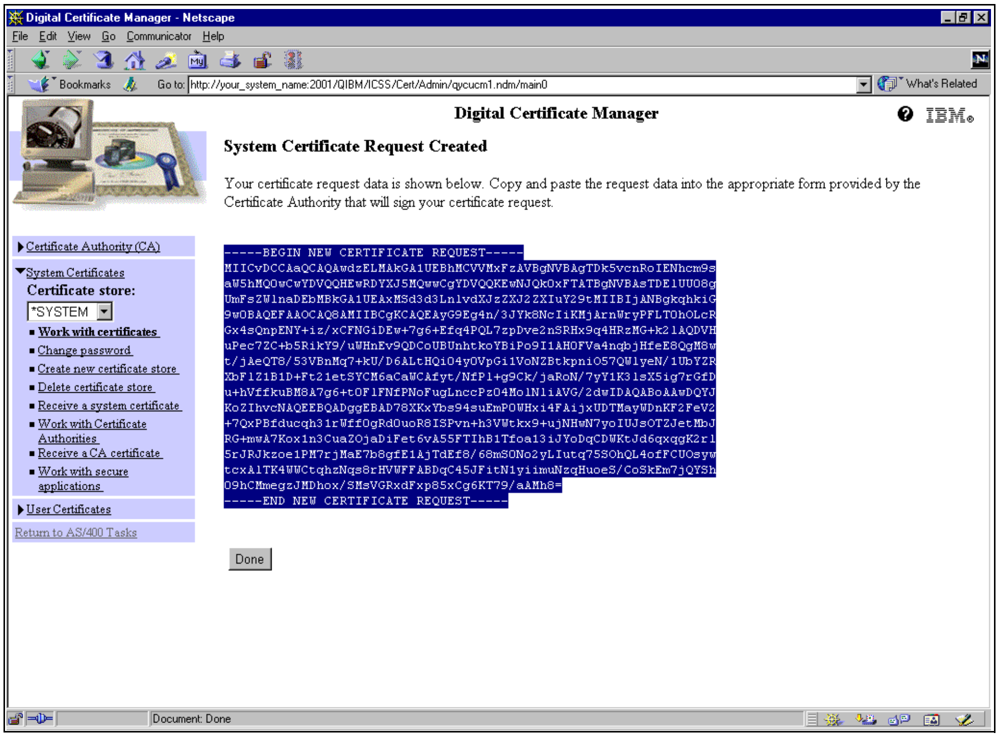
Server name:	www.yourserver.com	(required)
Organization unit:	ITSO Raleigh	
Organization name:	IBM	(required)
Locality or city:	Cary	
State or province:	North Carolina	(required:minimum of 3 characters)
Country:	US	(required)
Zip or postal code:		

Figure 129. Create a system certificate for a well-known CA

Fill in this form. Refer to 5.6.1.1, “Create a system certificate on the source AS/400 system” on page 146 for details on the required parameters.

6. Click **OK**.

DCM generates the private and public key. The public key and the certificate information are combined in the certificate request. The private key is kept in the certificate store. After the certificate request is created, DCM displays the request data in base64-encoded ASCII text format as shown in Figure 130.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM.
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
Done
Document: Done

Digital Certificate Manager

System Certificate Request Created

Your certificate request data is shown below. Copy and paste the request data into the appropriate form provided by the Certificate Authority that will sign your certificate request.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9s
aW5hMQ0wCwYDVQQHEwRDYXJ5MQwwCgYDVQQKEwNJQk0xFTATBgNVBAsTDE1UUO8g
UmFsZWlnaDEbMBkGA1UEAxMSd3d3LnlvdXJzZXJ2ZXIuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyG9Eg4n/3JYk8NcIiKMjArnWryPFLTOhOLcR
Gx4sQnpENY+iz/xCFNGiDEw+7g6+Efq4PQL7zpDve2nSRHx9q4HRzMG+k2lAQDVH
uPec7ZC+b5RikY9/uWHnEv9QDCoUBUnhtkoYBiPo9I1AHOFVa4nqbjHfeE8QgM8w
t/jAeQT8/53VBnMq7+kU/D6ALtHQiO4yOVpGi1VoNZBtkpniO57QWlyeN/1UbYZR
XbFlZ1B1D+Ft21etSYCM6aCaWCAfyt/NfPl+g9Ck/jaRoN/7yY1K3lsX5ig7rGfD
u+hVffkuBM8A7g6+tOFlFNfPNoFugLnccPzO4MolNliAVG/2dwIDAQABoAAwDQYJ
KoZIhvcNAQEEBQADggEBAD78XKxYbs94suEmPOWHxi4FAijxUDTMayWDnKF2FeV2
+7QxPBfducqh31rWffOgRdOuoR8ISPvn+h3VWtkx9+ujNHwN7yoIUJsOTZJetMbJ
RG+mwA7Kox1n3CuaZOjaDiFet6vA55FTIhB1Tfoa13iJYoDqCDWKtJd6qxqgK2rl
5rJRJkzoe1PM7rjMaE7b8gfE1AjTdEf8/68mSONo2yLIutq75SOhQL4ofFCUOsyw
tcxAlTK4WWCtqhzNqs8rHVWFFABDqC45JFitN1yiimuNzqHuoeS/CoSkEm7jQYSh
O9hCMmegzJMDhox/SMsVGRxdFxp85xCg6KT79/aAMh8=
-----END NEW CERTIFICATE REQUEST-----
```

Figure 130. System certificate request created

7. Copy the certificate request to the clipboard.

   Make sure you select the area that includes “`-----BEGIN NEW CERTIFICATE REQUEST-----`” through the area that ends with “`-----END NEW CERTIFICATE REQUEST-----`”

The certificate request data is prepared for requesting the certificate from the CA.

Since some CAs charge a considerable amount of money for the certificates that they issue (or that they re-issue), it may be wise to save the certificate store files in their present state before the CA has returned the signed certificate for you to receive. That way, if you are delayed several days and in the meantime you mistakenly delete the certificate store or some other unforseen problem arises, you will be able to use the backup.

5.6.2.2 Submitting a certificate request to a well-known CA

Of course at this stage you have already decided from which CA the certificate will be requested. Depending on the Certification Practice Statement of the CA and the required certificate class, the issuing process may take from a couple of hours up to a few days.

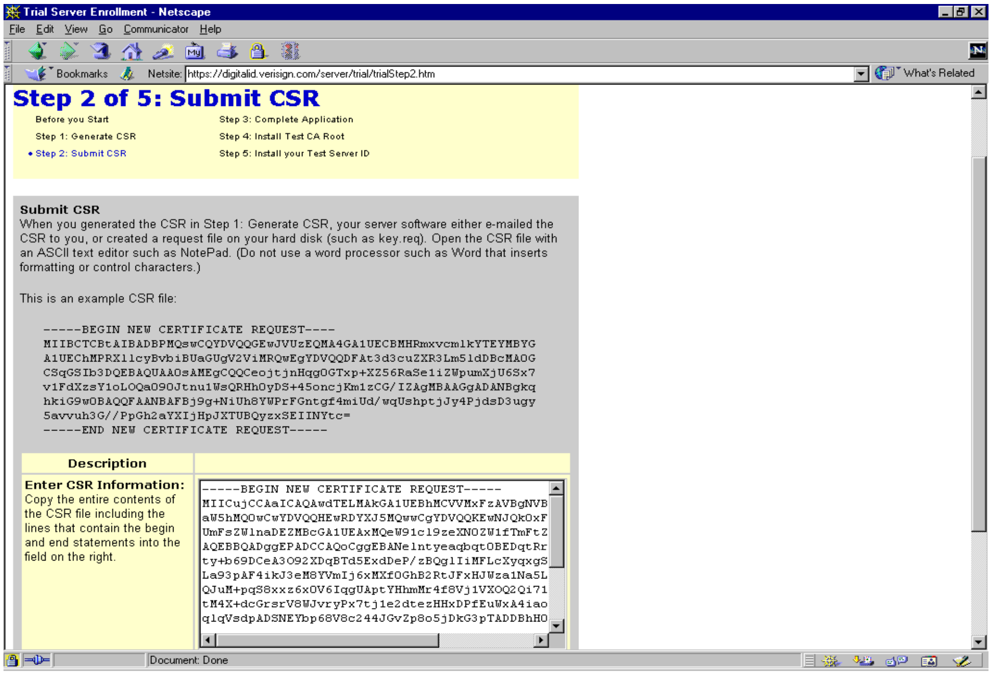
The way to submit a request depends on the CA. You may have to send the request data via e-mail to the CA or submit the request online over the Internet.

In this case, the certificate request is submitted online over the Internet choosing VeriSign as the well-known CA. For demonstration purposes a trial certificate is requested.

The following steps outline the major tasks involved in requesting a certificate over the Interne :

1. To request a certificate from VeriSign, enter the URL `www.verisign.com` and follow the directions given on this Web site.

   After you provided the necessary information requested by the CA, you will get a form to paste in the certificate request data from the clipboard.



Trial Server Enrollment - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: https://digitalid.verisign.com/server/trial/trialStep2.htm
What's Related

Step 2 of 5: Submit CSR

Before you Start
Step 1: Generate CSR
• Step 2: Submit CSR
Step 3: Complete Application
Step 4: Install Test CA Root
Step 5: Install your Test Server ID

Submit CSR
When you generated the CSR in Step 1: Generate CSR, your server software either e-mailed the CSR to you, or created a request file on your hard disk (such as key.req). Open the CSR file with an ASCII text editor such as NotePad. (Do not use a word processor such as Word that inserts formatting or control characters.)

This is an example CSR file:

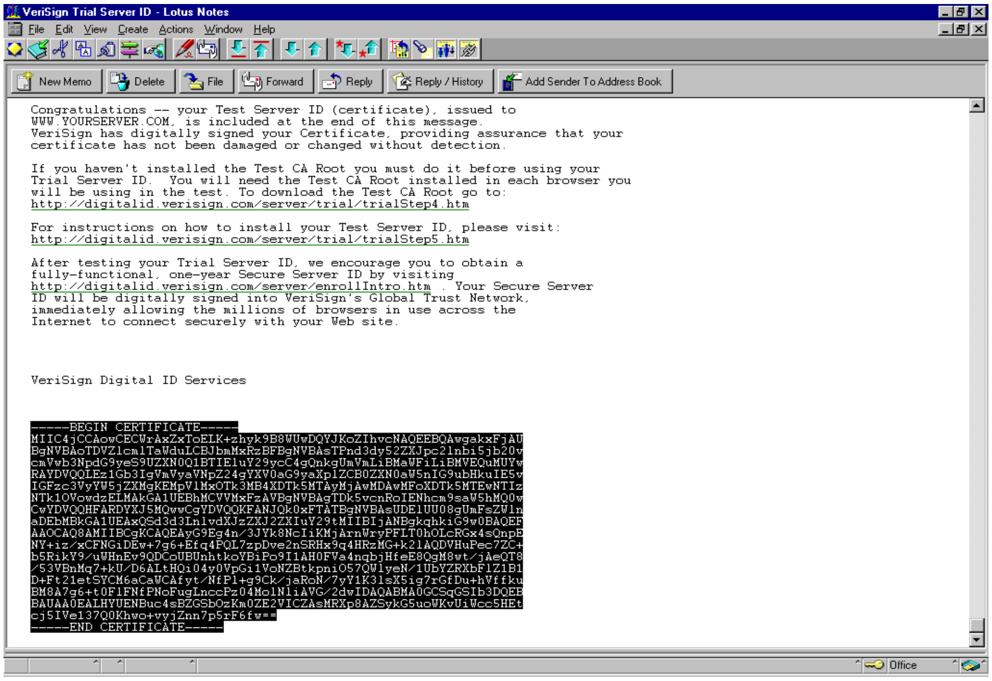
```
-----BEGIN NEW CERTIFICATE REQUEST----
MIIBCTCBtAIBADBPMQswCQYDVQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTEYMBYG
A1UEChMPRXllcyBvbiBUaGUgV2ViMRQwEgYDVQQDFAt3d3cuZXR3Lm5ldDBcMA0G
CSqGSIb3DQEBAQUAA0sAMEgCQQCeojtjnHqg0GTxp+XZ56RaSe1iZWpumXjU6Sx7
v1FdXzsY1oLOQa090Jtnu1WsQRHh0yDS+45oncjKm1zCG/IZAgMBAAGgADANBgkq
hkiG9w0BAQQFAANBAFBj9g+NiUh8YWPrFGntgf4miUd/wqUshptjJy4PjdsD3ugy
5avvuh3G//PpGh2aYXIjHpJXTUBQyzxSEIINYtc=
-----END NEW CERTIFICATE REQUEST-----
```

Description	
Enter CSR Information: Copy the entire contents of the CSR file including the lines that contain the begin and end statements into the field on the right.	-----BEGIN NEW CERTIFICATE REQUEST----- MIICujCCAaICAQAwdTELMAkGA1UEBhMCVVMxFzAVBgNVB aW5hMQ0wCwYDVQQHEwRDYXJ5MQwwCgYDVQQKEwNJQk0xF UmFsZWlnaDEZMBcGA1UEAxMQeW91cl9zeXN0ZW1fTmFtZ AQEBBQADggEPADCCAQoCggEBANe1ntyeaqbqt0BEDqtRr ty+b69DCeA3O92XDqBTd5ExdDeP/zBQglIiMFLcXyqxgS La93pAF4ikJ3eM8YVmIj6xMXf0GhB2RtJFxHJWza1Na5L QJuM+pqS8xxz6x0V6IqgUAptYHhmMr4f8Vj1VXOQ2Qi71 tM4X+dcGrsrV8WJvryPx7tj1e2dtezHHxDPfEuWxA4iao qlqVsdpADSNEYbp68V8c244JGvZp8o5jDkG3pTADDBhHO

Figure 131. Submit CSR

2. Paste your certificate request data into this form and complete the instructions given by the CA. At the end of a certificate request, the CA tells the requester how to proceed to obtain the certificate.

   Since this request is for a trial server certificate only, no further checking and approval work is performed by the issuing CA. After a certain time the person who submitted the request receives the certificate through e-mail as shown in Figure 132. Note that the e-mail address was provided during the online request.


VeriSign Trial Server ID - Lotus Notes
File Edit View Create Actions Window Help
New Memo
Delete
File
Forward
Reply
Reply / History
Add Sender To Address Book
Office

```
Congratulations -- your Test Server ID (certificate), issued to
WWW.YOURSERVER.COM, is included at the end of this message.
VeriSign has digitally signed your Certificate, providing assurance that your
certificate has not been damaged or changed without detection.

If you haven't installed the Test CA Root you must do it before using your
Trial Server ID.  You will need the Test CA Root installed in each browser you
will be using in the test. To download the Test CA Root go to:
http://digitalid.verisign.com/server/trial/trialStep4.htm

For instructions on how to install your Test Server ID, please visit:
http://digitalid.verisign.com/server/trial/trialStep5.htm

After testing your Trial Server ID, we encourage you to obtain a
fully-functional, one-year Secure Server ID by visiting
http://digitalid.verisign.com/server/enrollIntro.htm . Your Secure Server
ID will be digitally signed into VeriSign's Global Trust Network,
immediately allowing the millions of browsers in use across the
Internet to connect securely with your Web site.



VeriSign Digital ID Services
```

```
-----BEGIN CERTIFICATE-----
MIIC4jCCAowCECWrAxZxToELK+zhyk9B8WUwDQYJKoZIhvcNAQEEBQAwgakxFjAU
BgNVBAoTDVZlcmlTaWduLCBJbmMxRzBFBgNVBAsTPnd3dy52ZXJpc2lnbi5jb20v
cmVwb3NpdG9yeS9UZXN0Q1BTIEluY29ycC4gQnkgUmVmLiBMaWFiLiBMVEQuMUYw
RAYDVQQLEz1Gb3IgVmVyaVNpZ24gYXV0aG9yaXplZCB0ZXN0aW5nIG9ubHkuIE5v
IGFzc3VyYW5jZXMgKEMpVlMxOTk3MB4XDTk5MTAyMjAwMDAwMFoXDTk5MTEwNTIz
NTk1OVowdzELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMQ0w
CwYDVQQHFARDYXJ5MQwwCgYDVQQKFANJQk0xFTATBgNVBAsUDElUU08gUmFsZWln
aDEbMBkGA1UEAxQSd3d3LnlvdXJzZXJ2ZXIuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAyG9Eg4n/3JYk8NcIiKMjArnWryPFLT0hOLcRGx4sQnpE
NY+iz/xCFNGiDEw+7g6+Efq4PQL7zpDve2nSRHx9q4HRzMG+k2lAQDVHuPec7ZC+
b5RikY9/uWHnEv9QDCoUBUnhtkoYBiPo9I1AH0FVa4nqbjHfeE8QgM8wt/jAeQT8
/53VBnMq7+kU/D6ALtHQi04y0VpGi1VoNZBtkpni057QWlyeN/1UbYZRXbFlZ1B1
D+Ft21etSYCM6aCaWCAfyt/NfPl+g9Ck/jaRoN/7yY1K3lsX5ig7rGfDu+hVffku
BM8A7g6+t0FlFNfPNoFugLnccPz04MolNliAVG/2dwIDAQABMA0GCSqGSIb3DQEB
BAUAA0EALHYUENBuc4sBZGSbOzKm0ZE2VICZAsMRXp8AZSykG5uoWKvUiWcc5HEt
cj5IVe137Q0Khwo+vyjZnn7p5rF6fw==
-----END CERTIFICATE-----
```

Figure 132. System certificate signed by well-known CA

3. Copy and paste the certificate data into a text file on your PC using, for example the Notepad editor. Then transfer the PC file by using FTP or map a directory to your AS/400 to store the file in IFS. If using FTP, the PC file must be transferred in ASCII format. Dragging and dropping the PC file onto a mapped AS/400 drive does not always work properly. Sometimes the file gets corrupted and errors occur when receiving the certificate into the certificate store. So we recommend that you FTP the file.

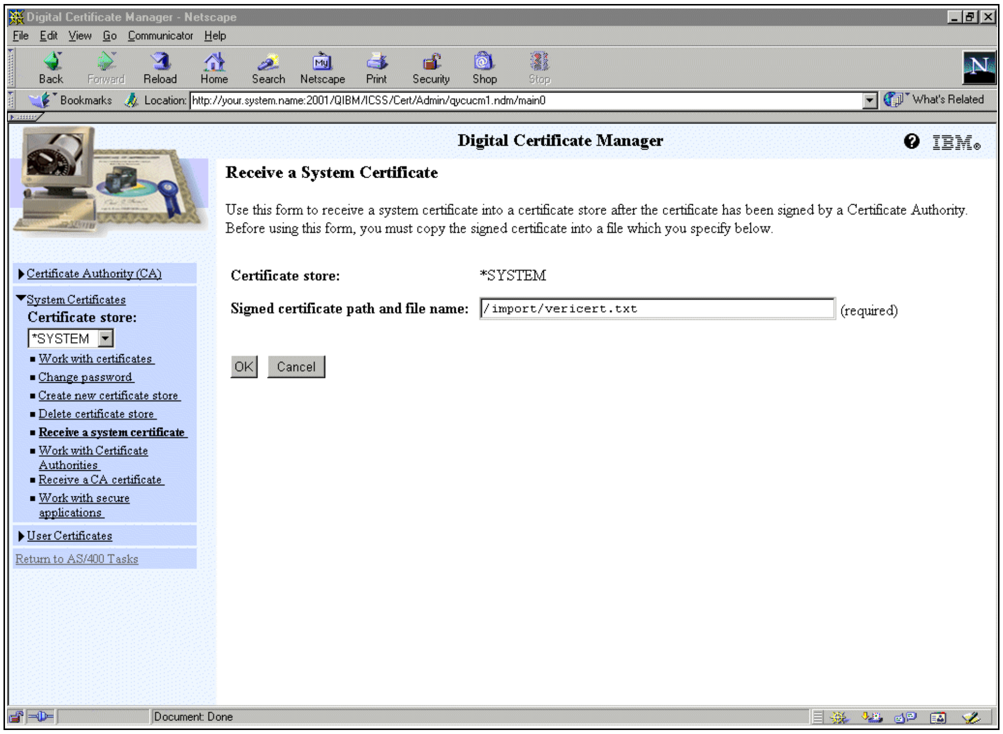
   Note that there are different methods in place for obtaining the certificate data. For example, some CAs send just e-mail containing a certificate identifier and you have to go to a specific URL to obtain the certificate data from there.

   But in all cases you have to copy and paste the certificate data into an ASCII text editor. And this file needs to be transferred to a directory in the IFS on the AS/400 system.

5.6.2.3 Receive a system certificate issued by a well-known CA

Once the file containing the certificate data is stored within an IFS directory, you have to perform the following steps to receive the certificate into the certificate store. Note that the user must receive the signed certificate into the same certificate store where the request was created:

1. Click **Receive system certificate** under System Certificates in DCM.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

Receive a System Certificate

Use this form to receive a system certificate into a certificate store after the certificate has been signed by a Certificate Authority. Before using this form, you must copy the signed certificate into a file which you specify below.

Certificate store: *SYSTEM

Signed certificate path and file name: /import/vericert.txt (required)

OK Cancel

Figure 133. Receive a system certificate from a well-known CA

Enter the fully qualified path and file name of the file containing the new certificate.

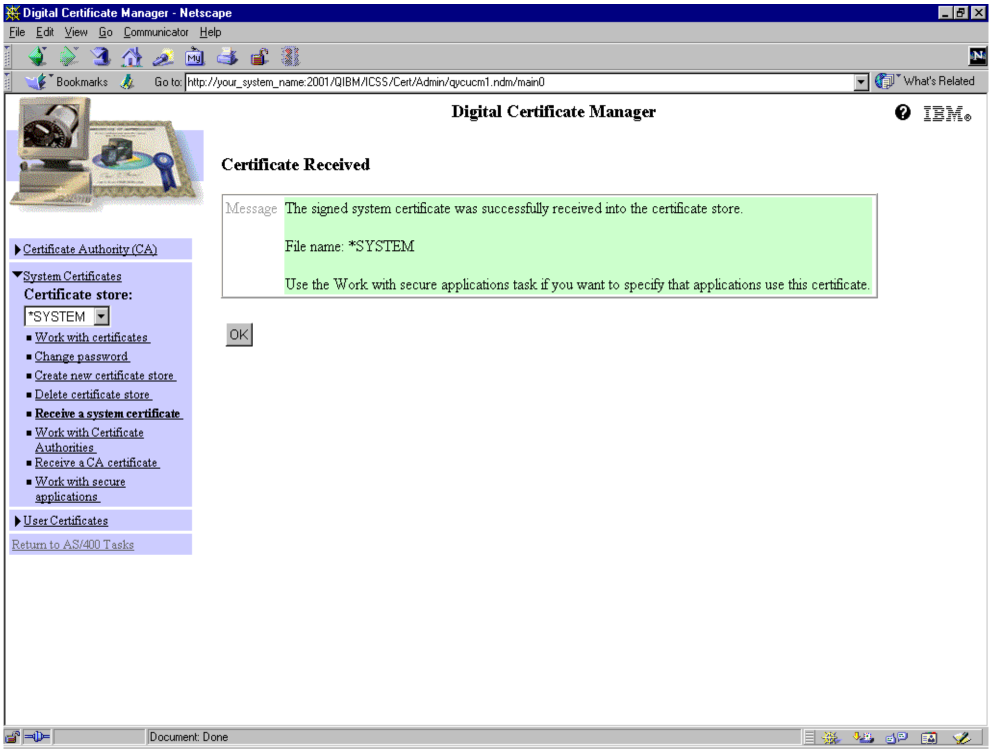
2. Click **OK**.

   DCM retrieves the certificate from the file and puts it in the certificate store that you specified.

Note

Since the private key resides on the AS/400 system where the certificate request was created, you can receive a system certificate only on the same system where the request was created.

DCM confirms the successful installation of the certificate by displaying a completion message as shown in Figure 134.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM.
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
OK
Document: Done

Digital Certificate Manager

Certificate Received

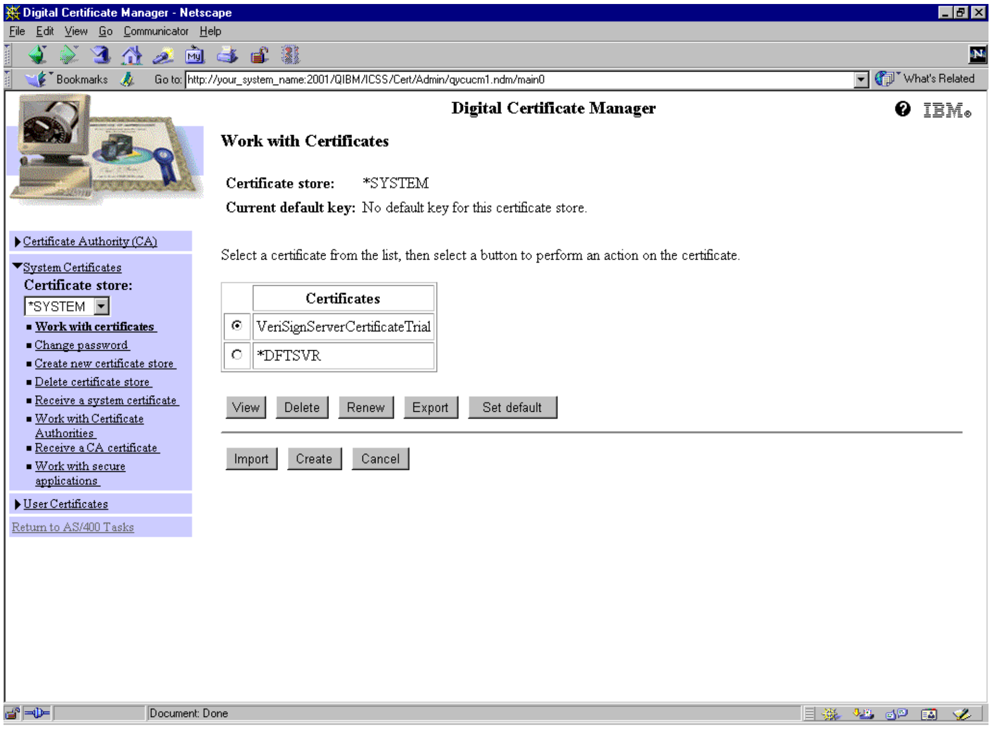
Message: The signed system certificate was successfully received into the certificate store.

File name: *SYSTEM

Use the Work with secure applications task if you want to specify that applications use this certificate.

Figure 134. Certificate received

3. Click **OK** to return to the DCM main page.
4. You can verify that the certificate is stored correctly by clicking **Work with certificates** under System Certificates in DCM.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM.
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Delete
Renew
Export
Set default
Import
Create
Cancel
Document: Done

Digital Certificate Manager

Work with Certificates

Certificate store: *SYSTEM
Current default key: No default key for this certificate store.

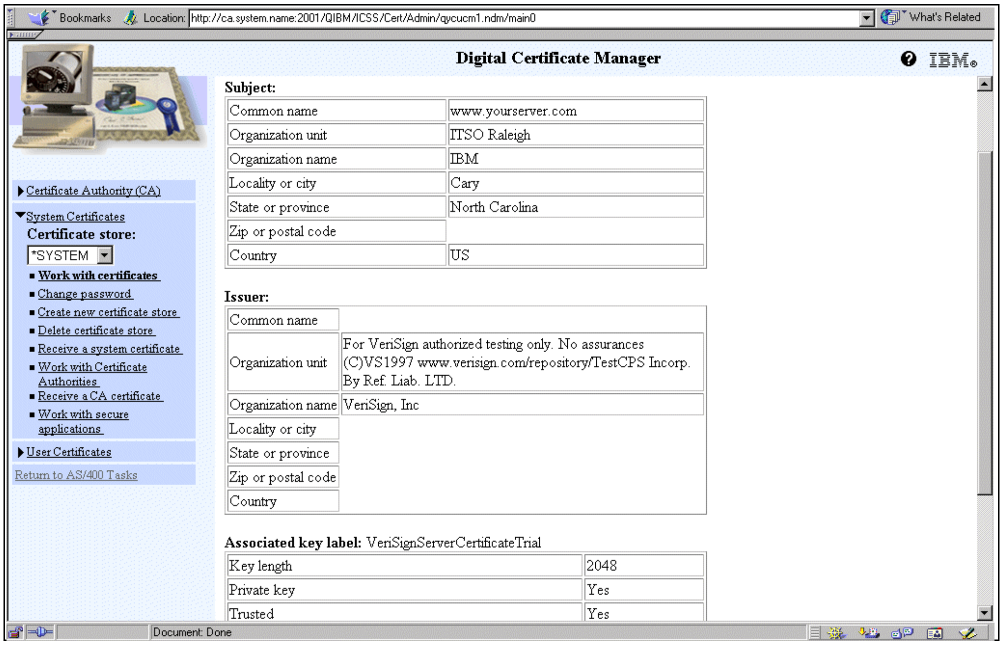
Select a certificate from the list, then select a button to perform an action on the certificate.

	Certificates
●	VeriSignServerCertificateTrial
○	*DFTSVR

Figure 135. Work with certificates (after)

This window shows the new certificate.

5. Select the received certificate name and click **VIEW**.


Bookmarks
Location: http://ca.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
Document: Done

Subject:

Common name	www.yourserver.com
Organization unit	ITSO Raleigh
Organization name	IBM
Locality or city	Cary
State or province	North Carolina
Zip or postal code	
Country	US

Issuer:

Common name	
Organization unit	For VeriSign authorized testing only. No assurances (C)VS1997 www.verisign.com/repository/TestCPS Incorp. By Ref. Liab. LTD.
Organization name	VeriSign, Inc
Locality or city	
State or province	
Zip or postal code	
Country	

Associated key label: VeriSignServerCertificateTrial

Key length	2048
Private key	Yes
Trusted	Yes

Figure 136. System certificate issued by a well-known CA

This window shows the system certificate and issuer's information on the new certificate.

6. Click **OK** to return to the Work with Certificates window.

To use this certificate, you must associate the certificate with a secure application as shown in 5.6.1.5, "Associate the certificate with a secure application" on page 155.

After the certificate is assigned to the applications, the application servers must be restarted to activate the changes.

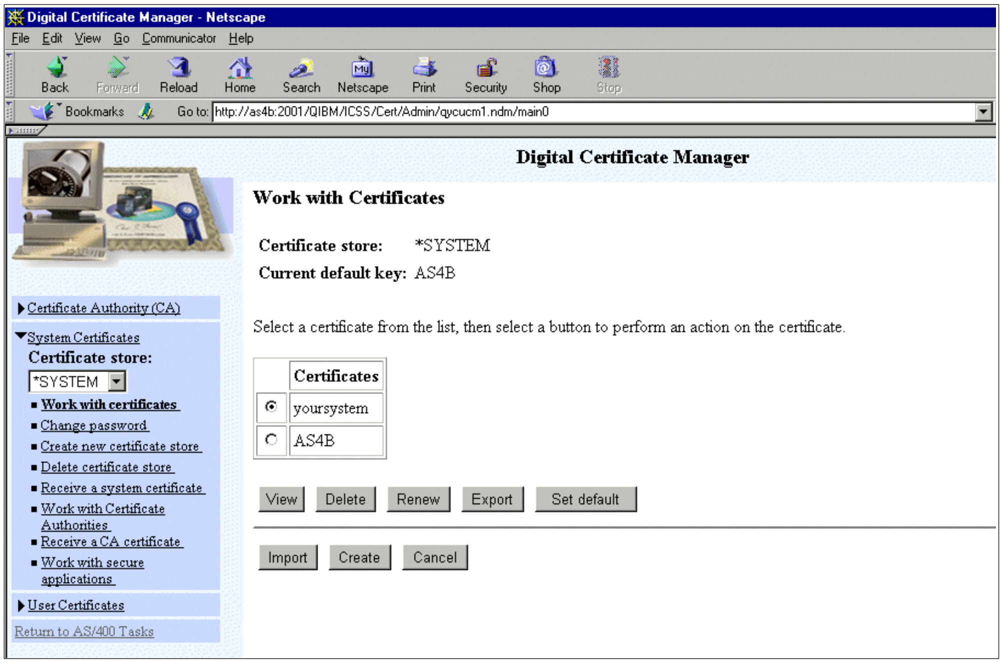
5.7 Managing system certificates

This section describes the rest of the tasks that are available under the System Certificates menu in DCM. For information about obtaining and receiving CA certificates and system certificates refer to 5.6, "Obtaining a system certificate" on page 145.

The System Certificates menu provides tasks to manage certificate stores as well as system certificates and CA certificates.

5.7.1 Work with certificates

To start this task click **Work with certificates** under System Certificates in DCM.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks
Go to: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Delete
Renew
Export
Set default
Import
Create
Cancel

Digital Certificate Manager

Work with Certificates

Certificate store: *SYSTEM

Current default key: AS4B

Select a certificate from the list, then select a button to perform an action on the certificate.

	Certificates
●	yoursystem
○	AS4B

Figure 137. Work with Certificates window

This task provides the following functions:

View This option allows you to view the attributes of installed system certificates.

Delete You can use this option to delete system certificates from a specific certificate store.

Renew You can use this option to request a new certificate before the old one expires or to request a new certificate when certificate attributes need to be changed. When performing this task, a window will be shown that contains the attributes of the current certificate, except the key label. Since key labels are unique for a specific certificate store, you have to enter a new label. The label is not used in the certificate itself. It just defines the name under which the certificate is listed in the certificate store.

Note that renewing a system certificate involves the same steps that need to be performed when creating a certificate request for a new system certificate. Refer to 5.6, “Obtaining a system certificate” on page 145 for more information about the request process.

Export This option is used to export a system certificate. The certificate is stored in a file that is protected by a password. You also have to specify the OS/400 release of the target AS/400 system where the certificate will be imported. This file must be transferred to the other system to be imported. For example, if you have two AS/400 systems, where one is the production and the other one the backup system, you can then install the same system certificate on both systems. So when the production system is down, the backup system can use this certificate to establish SSL connections. An example of how to use the export task is shown in 5.6.2, “Obtaining a server certificate from a well-known CA” on page 158.

Set default Set a certificate as the default certificate for the current system certificate store that is used for SSL.

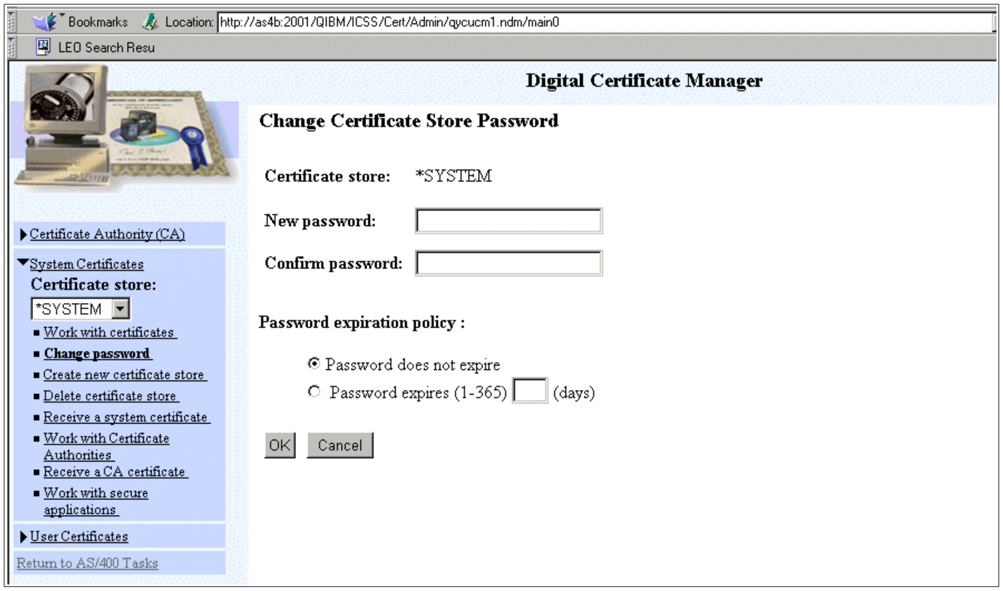
Import Through this option you can import a system certificate that was previously exported on another AS/400 system. The file containing the exported certificate must exist in an IFS directory prior to performing this option. You also have to specify the format under which the certificate was exported (OS/400 release). An example of how to use the export task is shown in 5.6.2, “Obtaining a server certificate from a well-known CA” on page 158.

Create This option allows you to request a new system certificate. Refer to 5.6, “Obtaining a system certificate” on page 145 for more information about the requesting a new certificate.

5.7.2 Change password

The Change Password task allows you to change the access password for a particular certificate store.

To start this task click **Change password** under System Certificates in DCM.



Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager

Change Certificate Store Password

Certificate store: *SYSTEM

New password:

Confirm password:

Password expiration policy :

● Password does not expire

○ Password expires (1-365) (days)

Figure 138. Change Certificate Store Password window

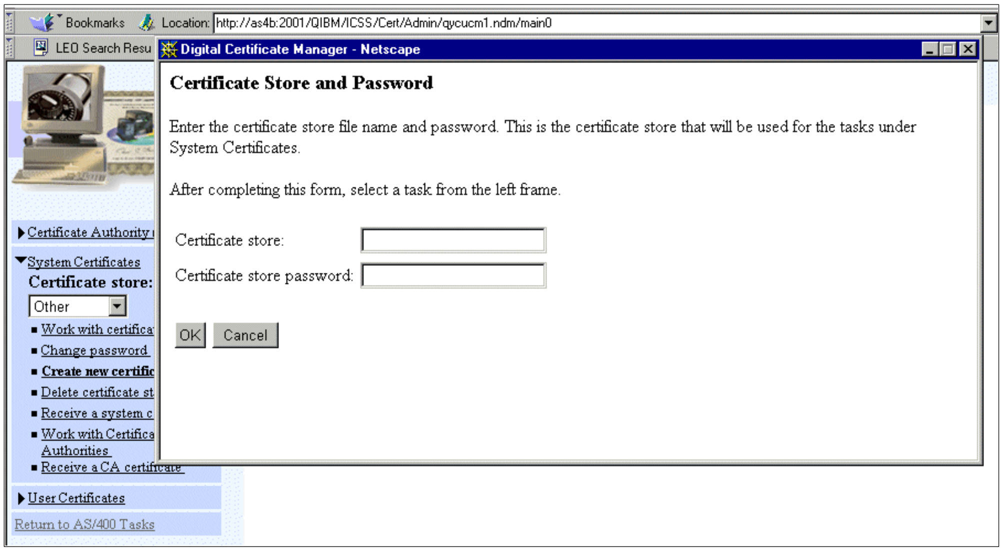
Since you already entered the current certificate store password, you have to enter only the new password. In addition you can specify if the password for this particular certificate store will expire. The default is that the password does not expire.

Change the password in a regular manner. We recommend that you always perform DCM tasks using a secured session. That means that the session traffic, for example, to change the password is protected by SSL.

5.7.3 Create new certificate store

This task allows you to create other certificate stores. The new certificate store must contain a system certificate. The following steps show you how to create other certificate stores.

1. Start DCM and expand **System Certificates**. You will be prompted for the certificate store and password to open. Click **Cancel** on the Certificate Store and Password window. Figure 139 shows the prompt when a user certificate store was used before.



Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager - Netscape

Certificate Store and Password

Enter the certificate store file name and password. This is the certificate store that will be used for the tasks under System Certificates.

After completing this form, select a task from the left frame.

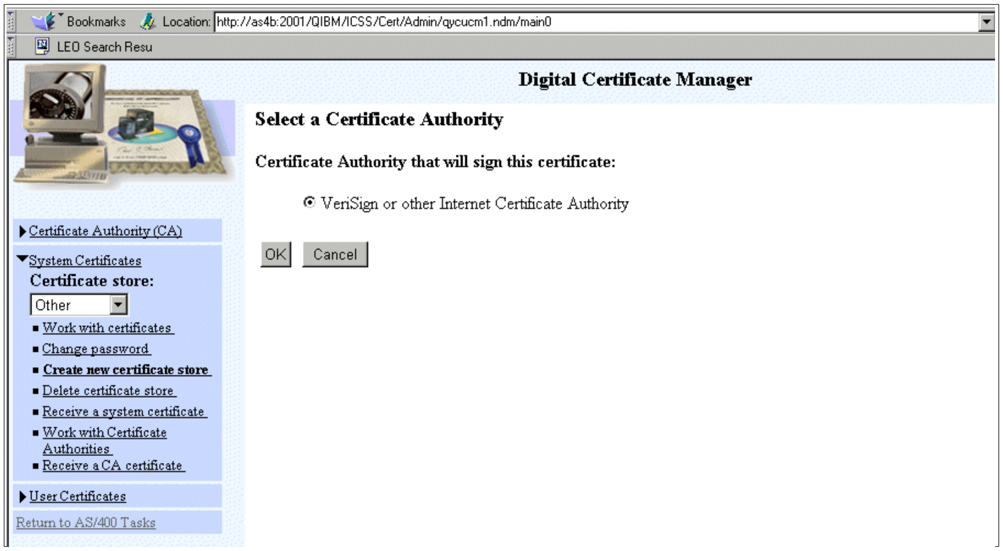
Certificate store:

Certificate store password:

Figure 139. Create a user certificate store - part 1

2. Enter the path and file name of the new certificate store and provide a password. The file name of the certificate store must end with the extension .KDB. Note that this information is not verified yet. Click **OK**.

3. Click **Create new certificate store**.



Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Digital Certificate Manager

Select a Certificate Authority

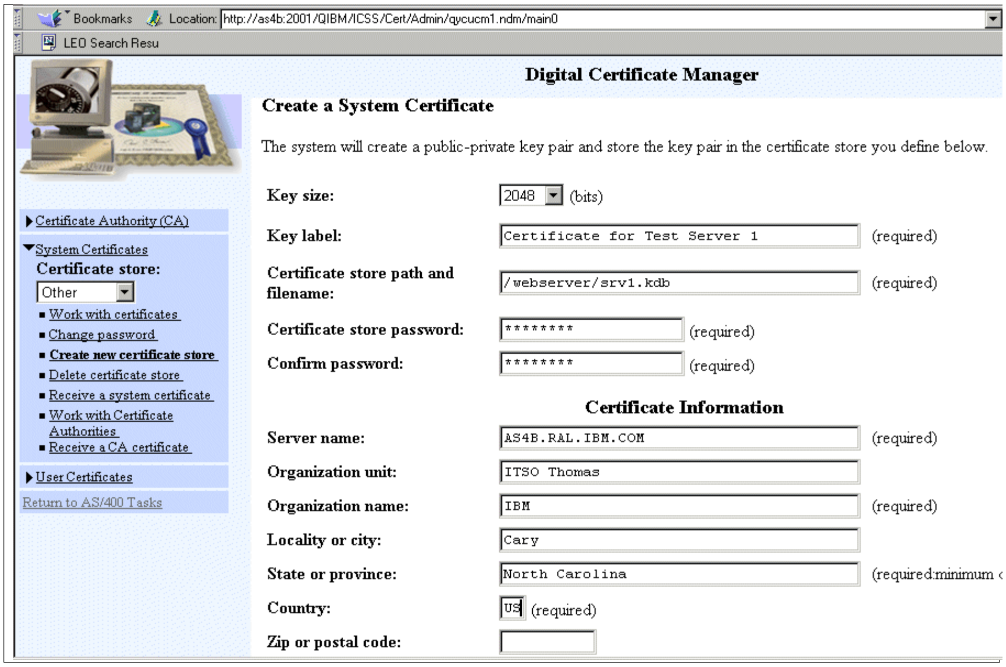
Certificate Authority that will sign this certificate:

● VeriSign or other Internet Certificate Authority

Figure 140. Create a user certificate store - part 2

Select the Certificate Authority that will sign the new system certificate. If there is no local CA set up on this system, the only available option is the well-known CA option. In this case there exists no local CA on this AS/400 system. Therefore, accept the default (VeriSign or other Certificate Authority).

4. Click **OK** to display the input window for the new system certificate.



Digital Certificate Manager

Create a System Certificate

The system will create a public-private key pair and store the key pair in the certificate store you define below.

Key size:	2048 (bits)	
Key label:	Certificate for Test Server 1	(required)
Certificate store path and filename:	/webserver/srv1.kdb	(required)
Certificate store password:	********	(required)
Confirm password:	********	(required)

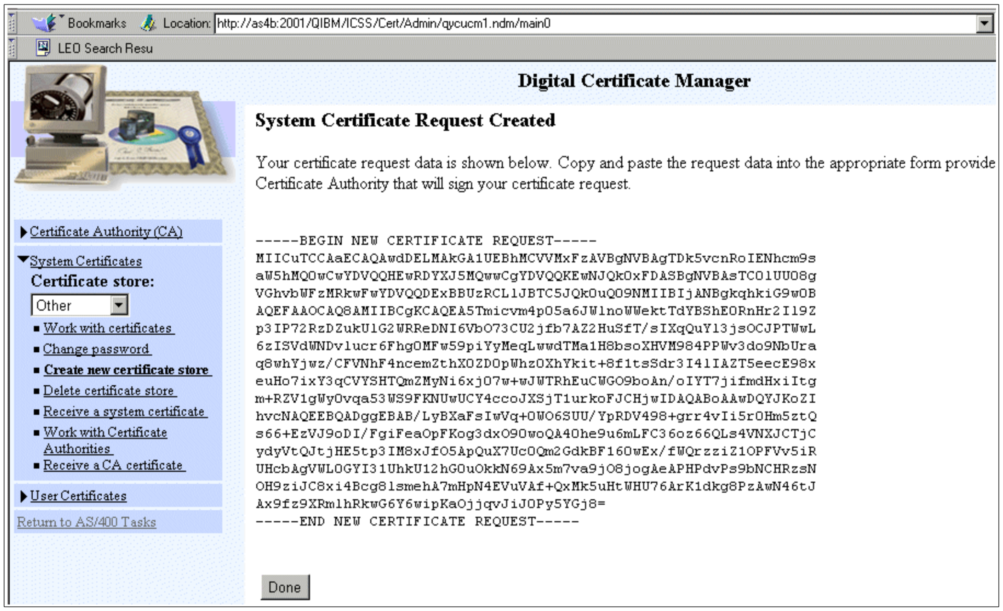
Certificate Information

Server name:	AS4B.RAL.IBM.COM	(required)
Organization unit:	ITSO Thomas	
Organization name:	IBM	(required)
Locality or city:	Cary	
State or province:	North Carolina	(required:minimum
Country:	US	(required)
Zip or postal code:		

Figure 141. Create a user certificate store - part 3

Enter the parameters as shown in Figure 141. Note that you have to re-enter the full path and file name of the new certificate store. For more information about the meaning of the fields on this form, refer to 5.6.2, “Obtaining a server certificate from a well-known CA” on page 158.

5. Click **OK**. DCM creates the private and public key pair and the certificate request data. The certificate request is displayed in base64 ASCII text encoded form.



Digital Certificate Manager

System Certificate Request Created

Your certificate request data is shown below. Copy and paste the request data into the appropriate form provide
Certificate Authority that will sign your certificate request.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICuTCCAaECAQAwdDELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9s
aW5hMQ0wCwYDVQQHEwRDYXJ5MQwwCgYDVQQKEwNJQk0xFDASBgNVBAsTC0lUU08g
VGhvbWFzMRkwFwYDVQQDExBBUzRCLlJBTC5JQk0uQ09NMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA5Tmicvm4p05a6JWlnoWWektTdYBShE0RnHr2Il9Z
p3IP72RzDZukUlG2WRReDNI6VbO73CU2jfb7AZ2HuSfT/sIXqQuYl3jsOCJPTWwL
6zISVdWNDvlucr6Fhg0MFw59piYyMeqLwwdTMa1H8bsoXHVM984PPWv3do9NbUra
q8whYjwz/CFVNhF4ncemZthX0ZD0pWhz0XhYkit+8f1tsSdr3I4lIAZT5eecE98x
euHo7ixY3qCVYSHTQmZMyNi6xj07w+wJWTRhEuCWGO9boAn/oIYT7jifmdHxiItg
m+RZV1gWy0vqa53WS9FKNUwUCY4ccoJXSjT1urkoFJCHjwIDAQABoAAwDQYJKoZI
hvcNAQEEBQADggEBAB/LyBXaFsIwVq+0WO6SUU/YpRDV498+grr4vIi5r0Hm5ztQ
s66+EzVJ9oDI/FgiFeaOpFKog3dx090woQA40he9u6mLFC36oz66QLs4VNXJCTjC
ydyVtQJtjHE5tp3IM8xJfO5ApQuX7Uc0Qm2GdkBF160wEx/fWQrzziZ1OPFVv5iR
UHcbAgVWL0GYI31UhkU12hG0uOkkN69Ax5m7va9jO8jogAeAPHPdvPs9bNCHRzsN
OH9ziJC8xi4Bcg8lsmehA7mHpN4EVuVAf+QxMk5uHtWHU76ArK1dkg8PzAwN46tJ
Ax9fz9XRmlhRkwG6Y6wipKaOjjqvJiJOPy5YGj8=
-----END NEW CERTIFICATE REQUEST-----
```

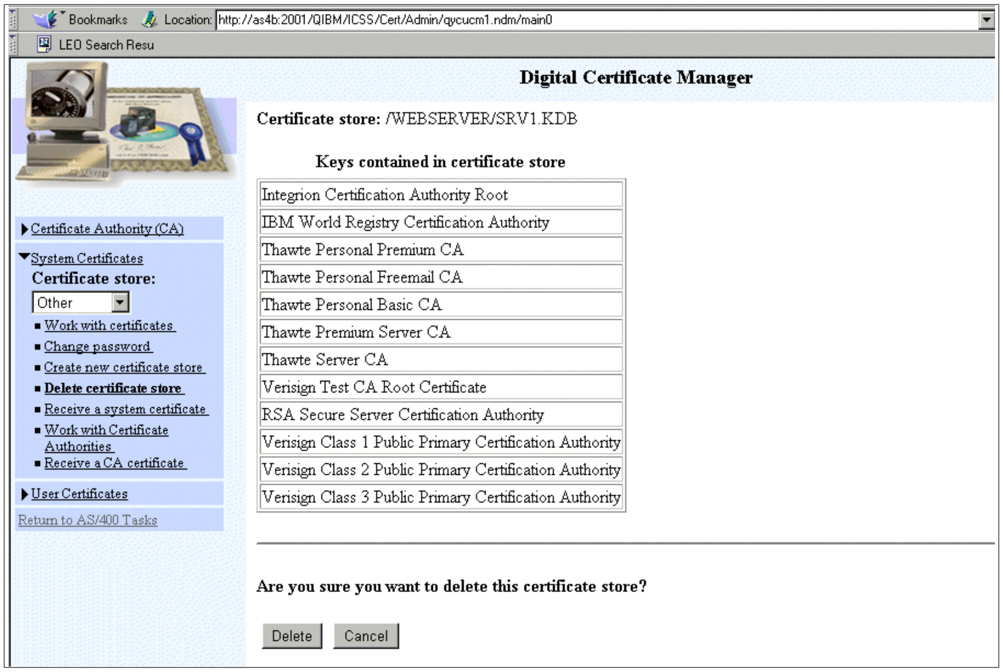
Figure 142. Create a user certificate store - part 4

Follow the instructions of the CA of your choice for obtaining a system certificate. You may either copy and paste the certificate request data into a Web form or send it via e-mail.

6. Click **Done** to complete the creation process. Once you get the signed certificate from the CA, receive it into the new certificate store as described in 5.6.2, “Obtaining a server certificate from a well-known CA” on page 158.

5.7.4 Delete certificate store

To delete a certificate store, click **Delete certificate store** under System Certificates in DCM.



Digital Certificate Manager

Certificate store: /WEBSERVER/SRV1.KDB

Keys contained in certificate store

Integrion Certification Authority Root
IBM World Registry Certification Authority
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
Verisign Test CA Root Certificate
RSA Secure Server Certification Authority
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority

Are you sure you want to delete this certificate store?

Figure 143. Delete a Certificate Store

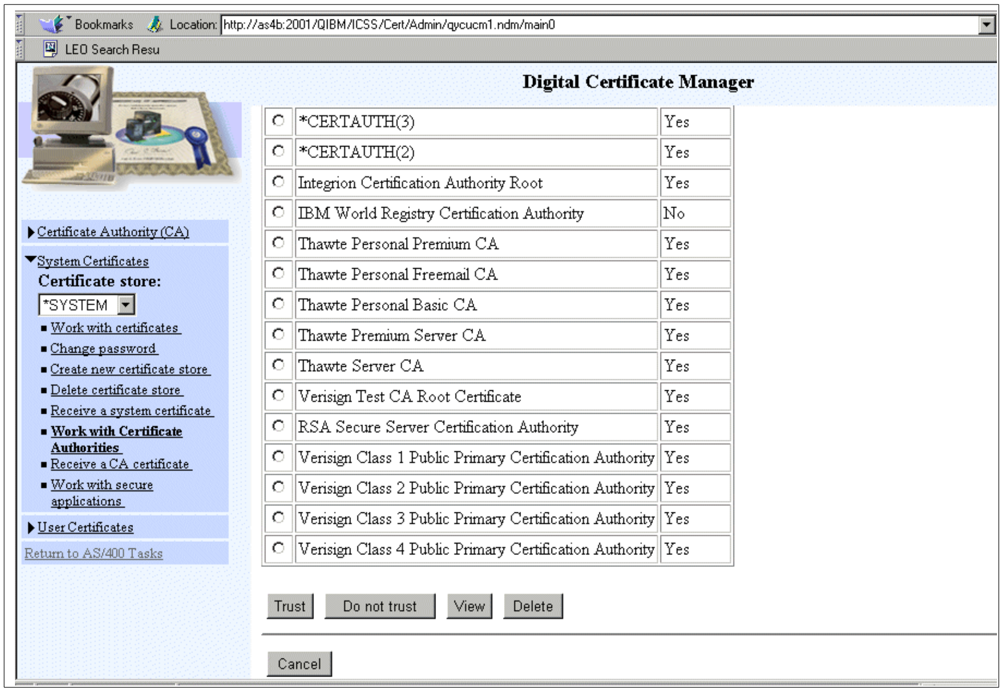
You can delete the *SYSTEM or user certificate stores. If there are still applications that use the certificate store, an additional button (View applications) will be displayed to check which applications are using that particular certificate store.

Click **Delete** to delete the certificate store. A message is shown to confirm that the certificate store was successfully deleted.

5.7.5 Work with Certificate Authorities

Through this task you can manage the CA certificates that are stored in a particular certificate store. A basic set of well-known CA certificates are shipped with the system. Intranet CA certificates and CA certificates from other Internet CAs must be installed manually. If you set up a local CA on this AS/400 system, the CA certificate is automatically stored in the certificate store.

To start this task click **Work with Certificate Authorities** in the System Certificates menu in DCM.


Bookmarks
Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
LEO Search Resu
Digital Certificate Manager
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
Trust
Do not trust
View
Delete
Cancel

○	*CERTAUTH(3)	Yes
○	*CERTAUTH(2)	Yes
○	Integrion Certification Authority Root	Yes
○	IBM World Registry Certification Authority	No
○	Thawte Personal Premium CA	Yes
○	Thawte Personal Freemail CA	Yes
○	Thawte Personal Basic CA	Yes
○	Thawte Premium Server CA	Yes
○	Thawte Server CA	Yes
○	Verisign Test CA Root Certificate	Yes
○	RSA Secure Server Certification Authority	Yes
○	Verisign Class 1 Public Primary Certification Authority	Yes
○	Verisign Class 2 Public Primary Certification Authority	Yes
○	Verisign Class 3 Public Primary Certification Authority	Yes
○	Verisign Class 4 Public Primary Certification Authority	Yes

Figure 144. Work with Certificate Authorities

All registered CAs are listed along with whether it is marked as trusted or not. For each CA listed, you have the following options:

- Trust

  You can mark each individual CA as trusted. That means your server is accepting only certificates that are signed by a trusted CA.

- Do not trust

  This option allows you to change the status of a trusted CA to not trusted.

- View

  This option displays the CA certificate details. For example, it shows the CA common name, the serial number, and more details.

- Delete

  You can delete CA certificates from the list of installed CA certificates for this particular certificate store.

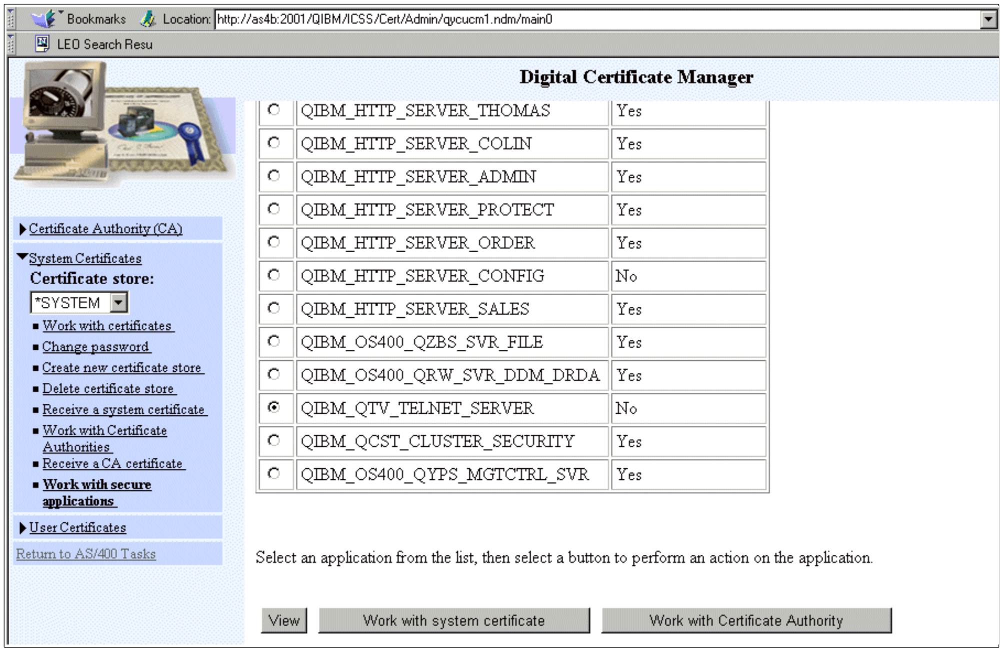
5.7.6 Work with secure applications

This task provides functions to assign system certificates to applications. These applications must be registered in DCM prior to assigning a certificate. All AS/400 standard applications are automatically registered as secure applications in DCM. Some of these applications are not shown in the list of secured applications unless they are enabled for SSL. In addition, you can define which CAs each application trusts.

Note that the Work with secure applications task appears in the System Certificates task list only if you are working in the *SYSTEM certificate store.

The following steps take you through the process of associating a system certificate to an application.

1. Click **Work with secure applications** under System Certificates in DCM.


Bookmarks
Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
LEO Search Resu
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Work with system certificate
Work with Certificate Authority

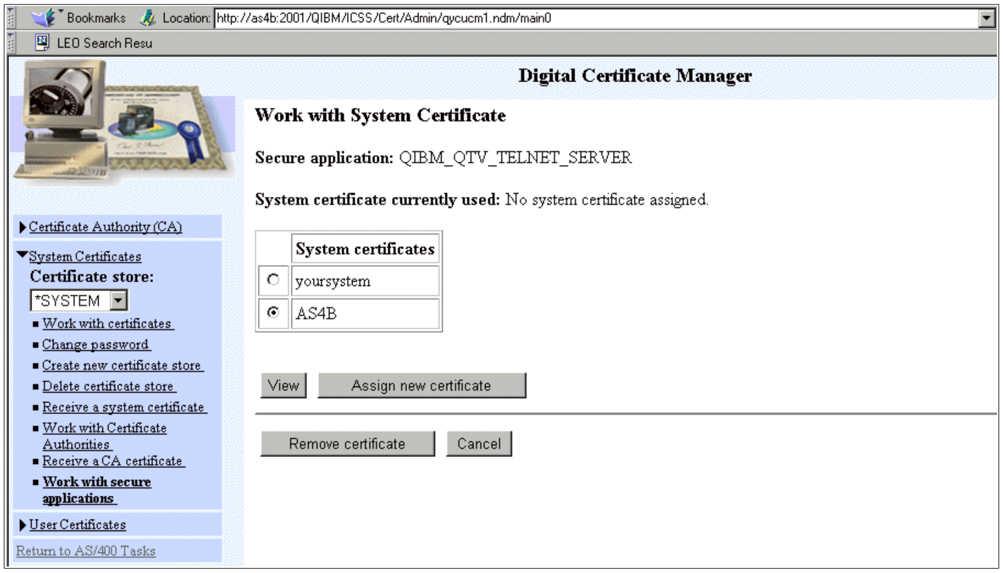
Digital Certificate Manager

○	QIBM_HTTP_SERVER_THOMAS	Yes
○	QIBM_HTTP_SERVER_COLIN	Yes
○	QIBM_HTTP_SERVER_ADMIN	Yes
○	QIBM_HTTP_SERVER_PROTECT	Yes
○	QIBM_HTTP_SERVER_ORDER	Yes
○	QIBM_HTTP_SERVER_CONFIG	No
○	QIBM_HTTP_SERVER_SALES	Yes
○	QIBM_OS400_QZBS_SVR_FILE	Yes
○	QIBM_OS400_QRW_SVR_DDM_DRDA	Yes
●	QIBM_QTV_TELNET_SERVER	No
○	QIBM_QCST_CLUSTER_SECURITY	Yes
○	QIBM_OS400_QYPS_MGTCTRL_SVR	Yes

Select an application from the list, then select a button to perform an action on the application.

Figure 145. Work with Secure Applications window

2. Select the application you want to assign a certificate to and click **Work with system certificate**.



Digital Certificate Manager

Work with System Certificate

Secure application: QIBM_QTV_TELNET_SERVER

System certificate currently used: No system certificate assigned.

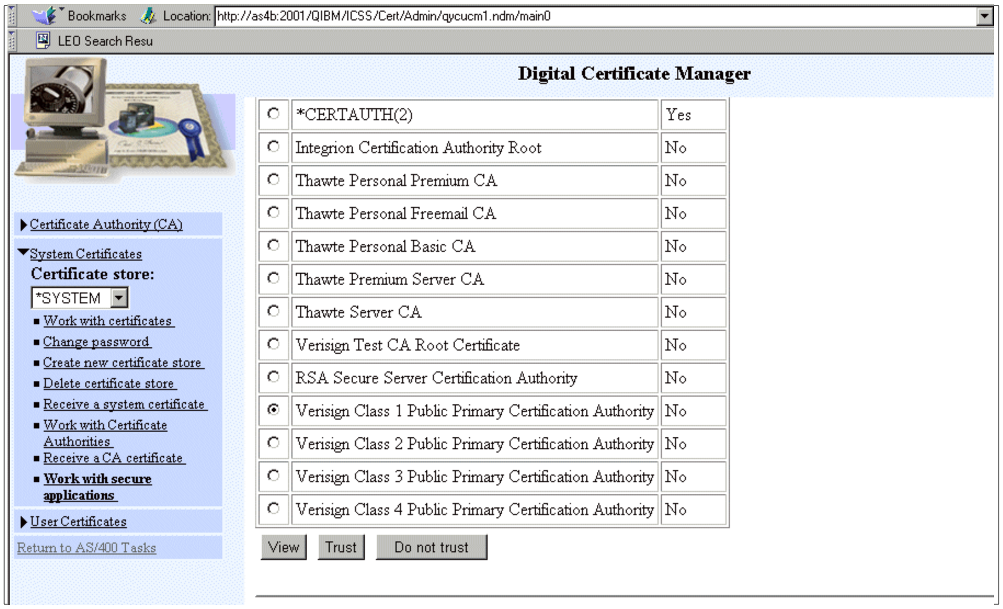
	System certificates
○	yoursystem
●	AS4B

Figure 146. Work with System Certificate window

All available system certificates in the current certificate store are displayed. Note that no certificate is currently assigned to the application.

3. Select the desired certificate and click **Assign new certificate**.

4. A confirmation is displayed. Click **OK** to return to the list of secure applications.
5. Select the application from step 2 and click **Work with Certificate Authority**.


Bookmarks
Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
LEO Search Resu
Digital Certificate Manager
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Trust
Do not trust

○	*CERTAUTH(2)	Yes
○	Integrion Certification Authority Root	No
○	Thawte Personal Premium CA	No
○	Thawte Personal Freemail CA	No
○	Thawte Personal Basic CA	No
○	Thawte Premium Server CA	No
○	Thawte Server CA	No
○	Verisign Test CA Root Certificate	No
○	RSA Secure Server Certification Authority	No
●	Verisign Class 1 Public Primary Certification Authority	No
○	Verisign Class 2 Public Primary Certification Authority	No
○	Verisign Class 3 Public Primary Certification Authority	No
○	Verisign Class 4 Public Primary Certification Authority	No

Figure 147. Work with Certificate Authority window

The CA *CERTAUTH(2) that signed the system certificate AS4B which is associated with this application is automatically marked as trusted. If you are using applications that are not performing client authentication with certificates, you do not need to mark more CAs as trusted. If the application is performing client authentication using client certificates you need to trust all CAs that issued client certificates accepted by this application.

6. Select the CA and click **Trust**. The CA will be marked as trusted and the list of CAs is shown again. Repeat this step until all desired CAs are marked as trusted and click **Cancel** to return to the list of secure applications.

5.8 Working with user certificates in DCM

The Digital Certificate Manager offers three major functions for managing user certificates. The available options in the User Certificates menu depend on the authorities of the user profile and the existence of a local CA on this AS/400 system.

Request a new user certificate

This option allows a client user who has an AS/400 user profile to request a user certificate to be issued by the local CA. The option is available only if a local CA is configured on this AS/400 system.

Manage registered certificates

A client user can manage its own user certificates. If the user profile that signs on to DCM has *SECADM and *ALLOBJ authorities, the user can also manage certificates registered to other user profiles.

Register an existing user certificate

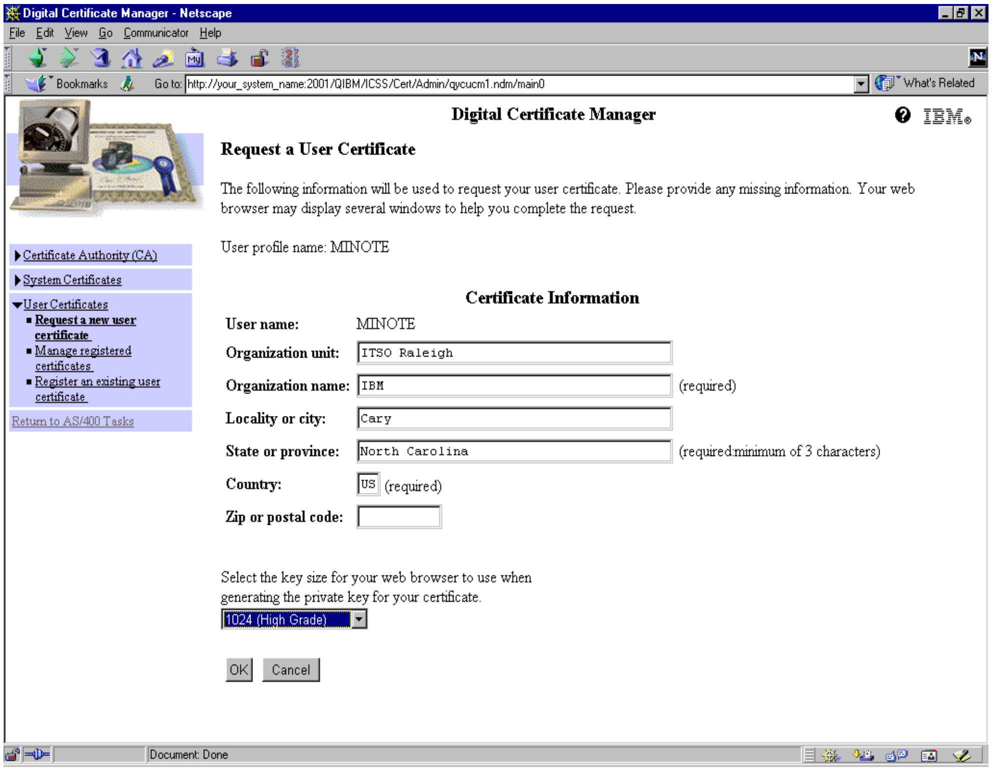
This option allows a client user who has an AS/400 user profile to register a certificate that was already issued by a local CA or a well-known CA with its user profile.

This section explains how these functions are used.

5.8.1 Request a user certificate

Only users that have an AS/400 user profile can request a user certificate that will be issued by the local CA. No user can request a user certificate on behalf of another user. Each user who requests a user certificate has to sign on to DCM with its own user profile. To request a user certificate, perform the following steps:

1. Sign on to DCM and click **User certificate**.
2. Click **Request a new user certificate**.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
System Certificates
User Certificates
Request a new user certificate
Manage registered certificates
Register an existing user certificate
Return to AS/400 Tasks
IBM
OK
Cancel
Document: Done

Digital Certificate Manager

Request a User Certificate

The following information will be used to request your user certificate. Please provide any missing information. Your web browser may display several windows to help you complete the request.

User profile name: MINOTE

Certificate Information

User name:	MINOTE	
Organization unit:	ITSO Raleigh	
Organization name:	IBM	(required)
Locality or city:	Cary	
State or province:	North Carolina	(required:minimum of 3 characters)
Country:	US	(required)
Zip or postal code:		

Select the key size for your web browser to use when generating the private key for your certificate.
1024 (High Grade)

Figure 148. Request a User certificate form

The Common name, also referred to as User name, on the request form is automatically filled in with the AS/400 user profile name. This field cannot be altered. The rest of the certificate attributes need to be filled in by the user.

3. Fill in the fields.

   Organization unit

      Type the name of this certificate holder’s unit.

   Organization name

      Type your company name or organizational section.

   Locality or city

Type the location name of this certificate holder.

State or province

Type a name for this certificate holder's state or province. This name must be a minimum of three characters in length.

Country

Type a two-letter symbol for your country, for example, DE for Germany, US for United States, NZ for New Zealand.

Zip or postal code

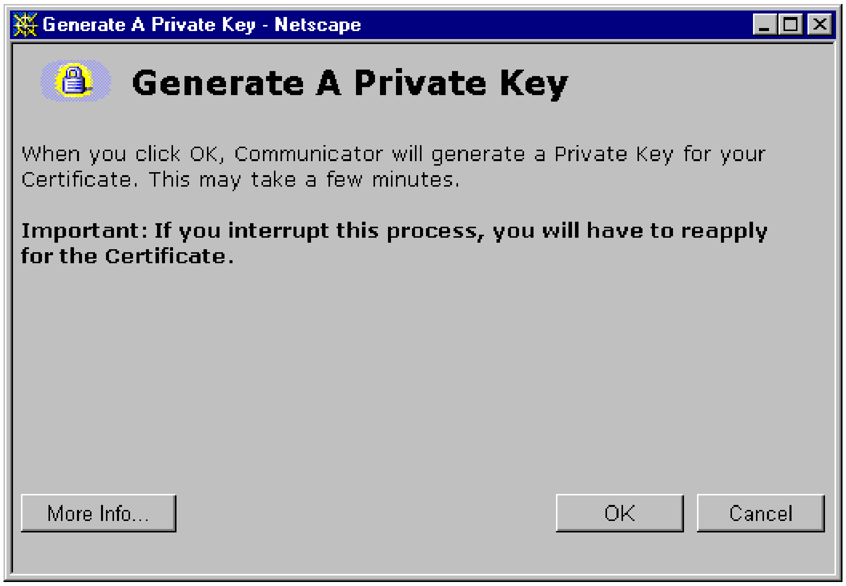
Enter a zip code. This is an optional field. Most of the well-known CAs do not support the zip code in their distinguished name. Therefore, it is best to leave the field blank. Note that Netscape Browser 4.01 to 4.61on Windows platforms have an acknowledged problem performing client authentication when the zip code field is filled. If you want to use client authentication with these browser versions, leave this field blank. The problem is fixed with Netscape Communicator 4.7.

Key size

The available key sizes are different from the sizes when requesting a system certificate. They also depend on the installed browser version, because the available values are determined by the Web browser and not the AS/400 system.

4. Click **OK** to submit the request.

   At this time DCM evokes the browser's key generation module, which generates the private and public key within the Web browser. Netscape, for example, asks the user to confirm the generation of the keys as shown in Figure 136.



Generate A Private Key

When you click OK, Communicator will generate a Private Key for your Certificate. This may take a few minutes.

Important: If you interrupt this process, you will have to reapply for the Certificate.

Figure 149. Generate a private key

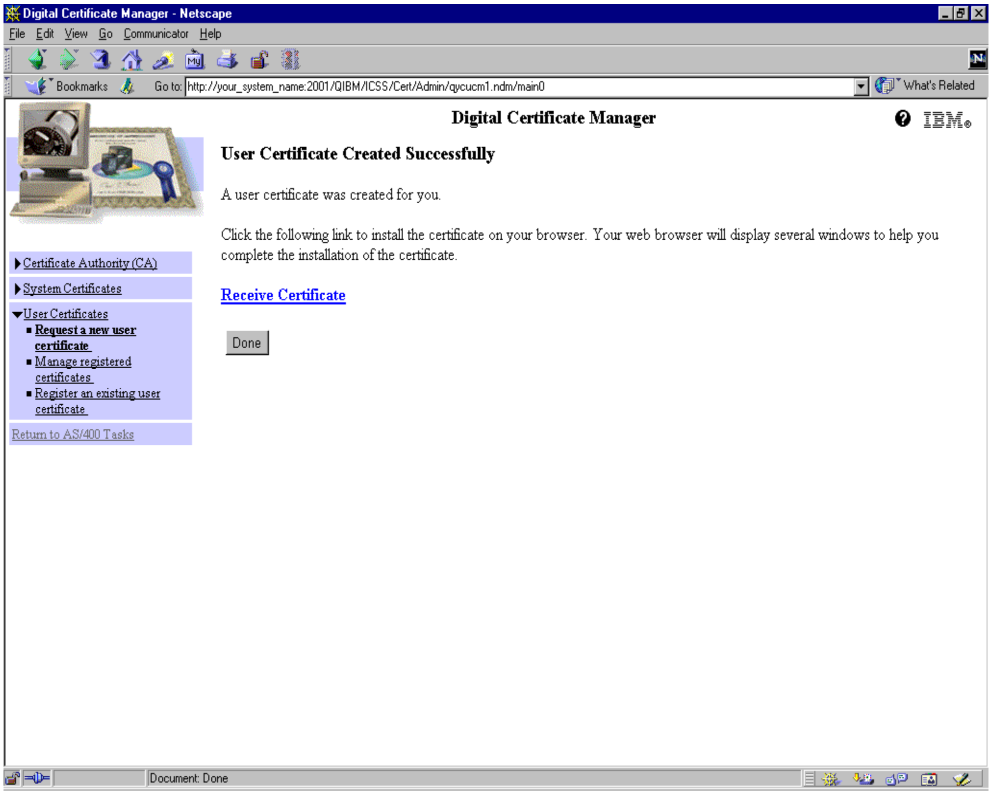
5. Click **OK**.

The browser now generates the private and public keys and puts the public key along with the certificate information into a certificate requestm which itself is passed to DCM. DCM then creates the user certificate and stores it in the system default directory:

Directory `/QIBM/UserData/ICSS/Cert/Download/Client`

File name `xxxx.USRCRT` where xxxx is the AS/400 user profile name

After the certificate is created and stored in the proper directory, a page is shown confirming the successful creation of the certificate. It also provides a link to receive the new certificate into the browser.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM
Certificate Authority (CA)
System Certificates
User Certificates
Request a new user certificate
Manage registered certificates
Register an existing user certificate
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

User Certificate Created Successfully

A user certificate was created for you.

Click the following link to install the certificate on your browser. Your web browser will display several windows to help you complete the installation of the certificate.

Receive Certificate

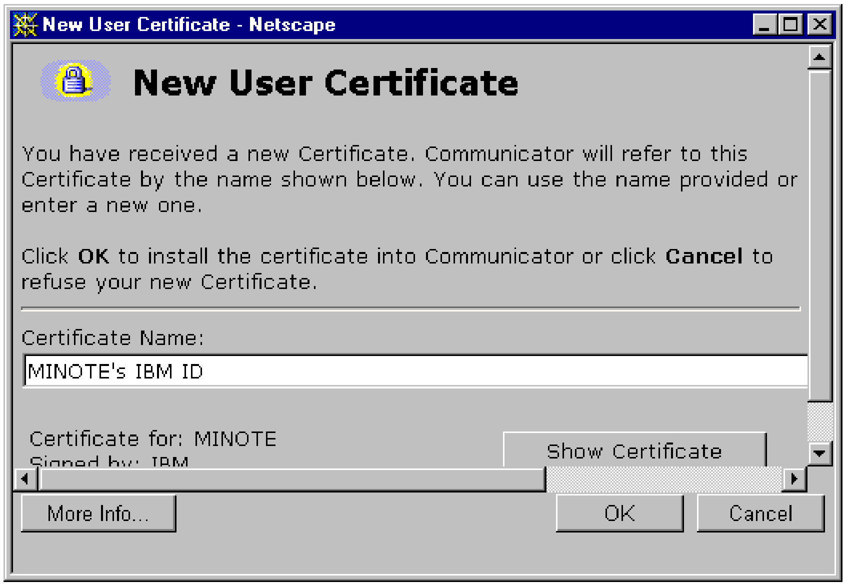
Done

Figure 150. User certificate created successfully

Receiving the user certificate into the browser also varies depending on the type of browser. When using Internet Explorer, a Receive Certificate link is not shown. Instead, an Install button is displayed for installing the certificate into the browser.

6. Click **Receive certificate** to receive the new certificate.

   DCM sends the user certificate to the browser. The browser then presents a window to confirm the installation of a new certificate as shown in Figure 151.



New User Certificate

You have received a new Certificate. Communicator will refer to this Certificate by the name shown below. You can use the name provided or enter a new one.

Click **OK** to install the certificate into Communicator or click **Cancel** to refuse your new Certificate.

Certificate Name:

MINOTE's IBM ID

Certificate for: MINOTE

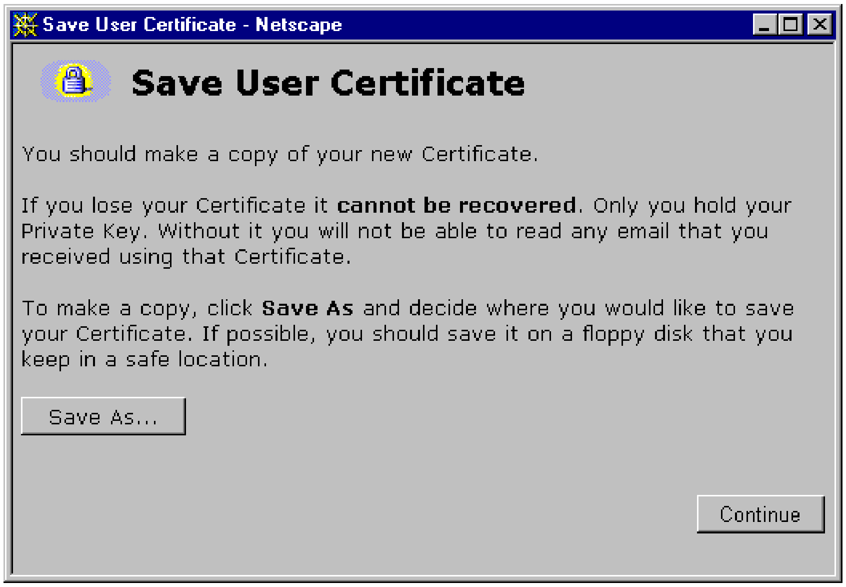
Signed by: IBM

Figure 151. New user certificate

Note that Internet Explorer does not have this window.

7. Click **OK** to confirm.

   The browser stores the user certificate into the certificate database. When the certificate is received, the browser asks the user to save the new certificate and also explains why this action should be taken.



Save User Certificate

You should make a copy of your new Certificate.

If you lose your Certificate it **cannot be recovered**. Only you hold your Private Key. Without it you will not be able to read any email that you received using that Certificate.

To make a copy, click **Save As** and decide where you would like to save your Certificate. If possible, you should save it on a floppy disk that you keep in a safe location.

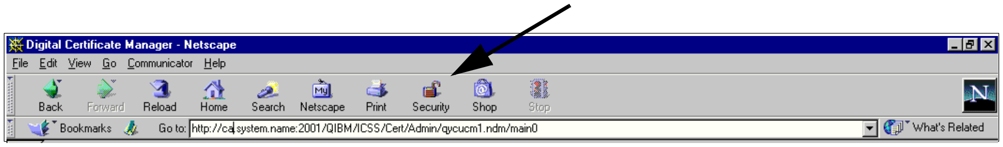
Figure 152. Save user certificate

We also recommend that you save the new certificate in a file and keep that file in a secure place, because the private key is only stored in the certificate database. If the certificate database gets corrupted or you forget the certificate database access password, you cannot use this certificate anymore. Even if you have the certificate stored on the AS/400 system, it does not contain the private key. But when saving the certificate into a file, the private key is also saved.

8. Click **Continue** to return to DCM.

The following steps are optional and can be used to verify that the new certificate is correctly stored in the browser's certificate database. The example in this section shows how to verify the certificate in Netscape Communicator 4.7.

9. In the Netscape browser navigation bar click the **Security** padlock.

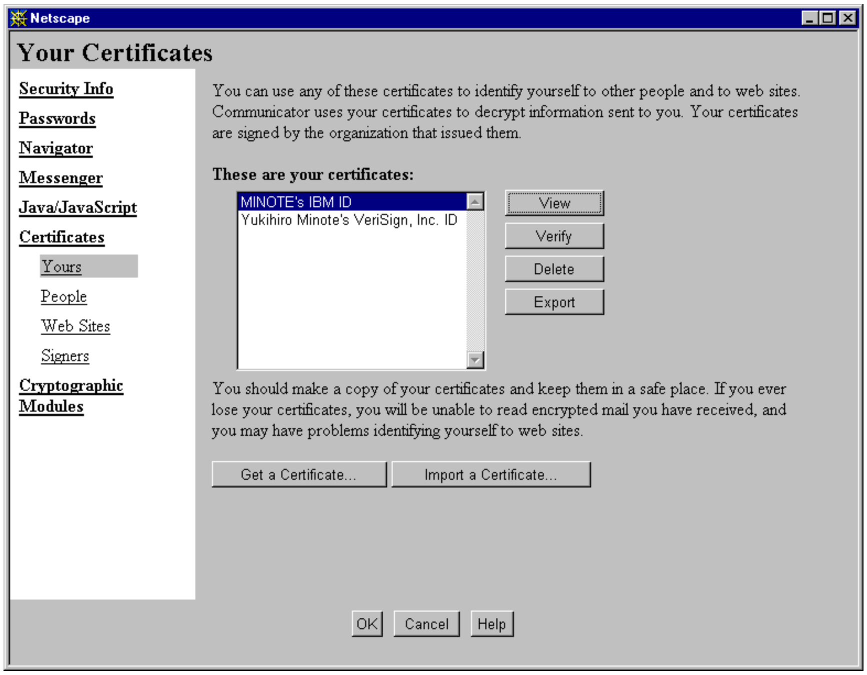


http://ca system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

Figure 153. Netscape browser navigation bar

The Security Info page is shown.

10.Click **Certificates->Yours** to list all user certificates in the browser certificate database. If the installation process completed successfully, the new user certificate is now displayed in the list of installed certificate.



Your Certificates

You can use any of these certificates to identify yourself to other people and to web sites. Communicator uses your certificates to decrypt information sent to you. Your certificates are signed by the organization that issued them.

These are your certificates:

MINOTE's IBM ID
Yukihiro Minote's VeriSign, Inc. ID

You should make a copy of your certificates and keep them in a safe place. If you ever lose your certificates, you will be unable to read encrypted mail you have received, and you may have problems identifying yourself to web sites.

Figure 154. Your certificates

In a local CA environment remember to install also the local CA certificate on the browser as shown in 5.5.2, "Install CA certificate on your PC (copy and paste)" on page 134.

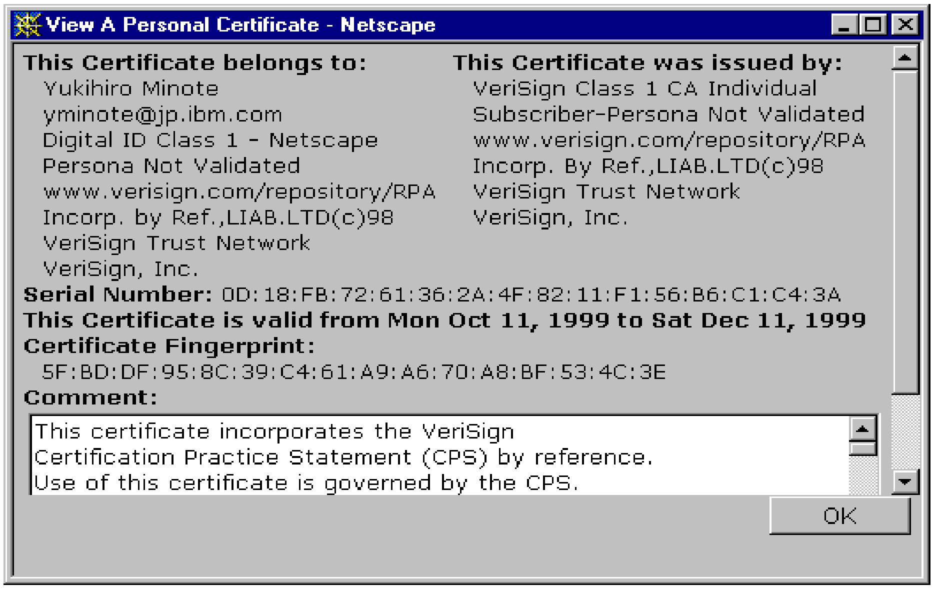
5.8.2 Register an existing user certificate

The process described in this section can be used to associate an existing user certificate with an AS/400 user profile. The user certificate might have been issued by a local CA installed on another system or by a well-known CA. Note that user certificates issued by a local CA on the same AS/400 system are automatically associated with the requesting user profile.

This section does not show you how to obtain a user certificate. The ways of obtaining a user certificate depend on the issuing CA. You always have to follow the instructions given by the individual CA to obtain a user certificate. However, Appendix C, “Obtaining a digital certificate” on page 387 shows an example of obtaining a user certificate using VeriSign as the CA.

Registering or associating a user certificate with an AS/400 user profile allows you to leverage the AS/400 object authorities for controlling access.

It is assumed that the following user certificate issued by a well-known CA is already installed in the Web browser. Using the Security option of the Netscape browser navigation bar, the attributes of the existing user certificate are displayed as shown in Figure 155.



This Certificate belongs to:
Yukihiro Minote
yminote@jp.ibm.com
Digital ID Class 1 - Netscape
Persona Not Validated
www.verisign.com/repository/RPA
Incorp. by Ref.,LIAB.LTD(c)98
VeriSign Trust Network
VeriSign, Inc.

This Certificate was issued by:
VeriSign Class 1 CA Individual
Subscriber-Persona Not Validated
www.verisign.com/repository/RPA
Incorp. By Ref.,LIAB.LTD(c)98
VeriSign Trust Network
VeriSign, Inc.

Serial Number: 0D:18:FB:72:61:36:2A:4F:82:11:F1:56:B6:C1:C4:3A
This Certificate is valid from Mon Oct 11, 1999 to Sat Dec 11, 1999
Certificate Fingerprint:
5F:BD:DF:95:8C:39:C4:61:A9:A6:70:A8:BF:53:4C:3E
Comment:
This certificate incorporates the VeriSign
Certification Practice Statement (CPS) by reference.
Use of this certificate is governed by the CPS.

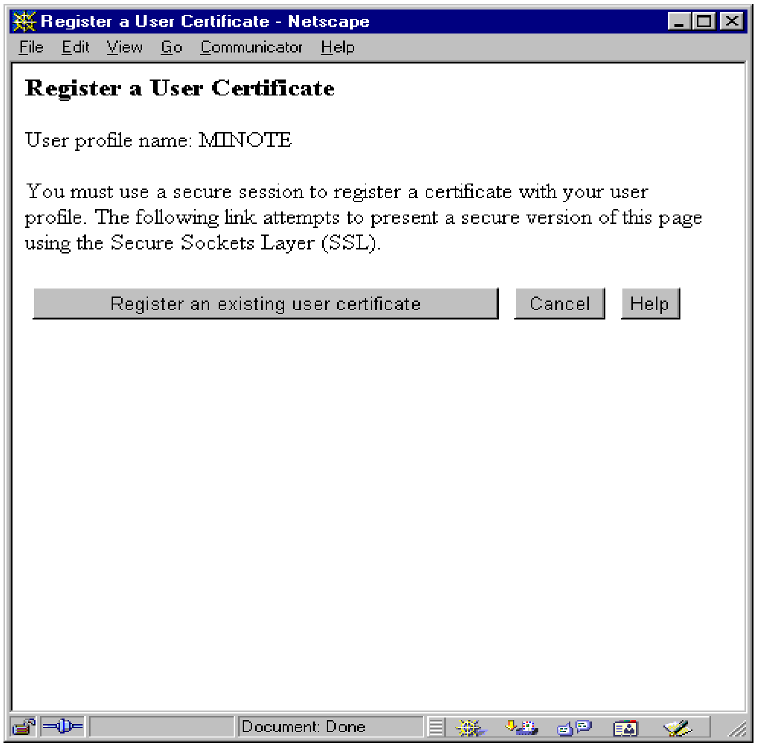
Figure 155. VeriSign user certificate

To register an existing user certificate with DCM, perform the following steps:

1. Sign on to DCM on the AS/400 system you want to register the user certificate. Use the user profile you want to associate the certificate with.
2. Click **User certificate** in DCM.
3. Click **Register a user certificate**.

   DCM uses an SSL connection to register user certificates. The *ADMIN HTTP server instance must be configured for SSL. The steps to enable SSL for the *ADMIN server are shown in Appendix B, “Enabling SSL for the *ADMIN HTTP server instance” on page 379.

   If the user signed on without using an SSL connection, an additional window is displayed (s shown in Figure 156) to switch to an SSL connection.


Register a User Certificate - Netscape
File Edit View Go Communicator Help

Register a User Certificate

User profile name: MINOTE

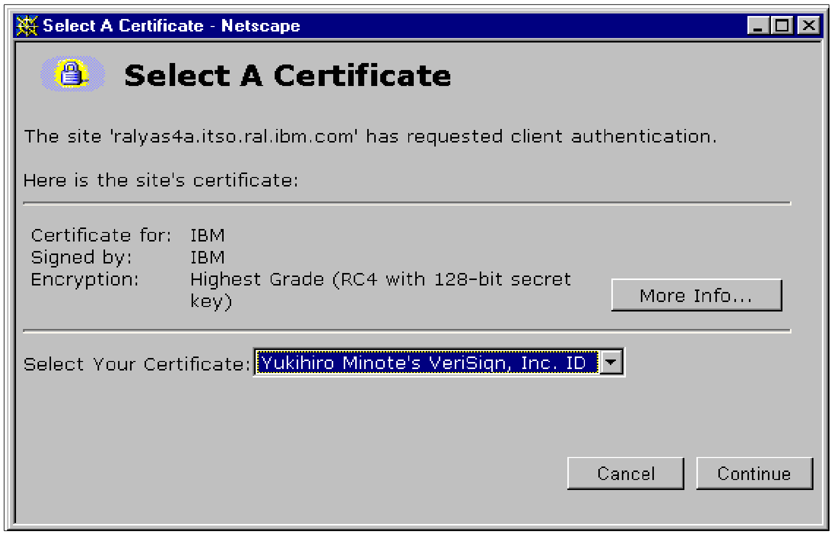
You must use a secure session to register a certificate with your user profile. The following link attempts to present a secure version of this page using the Secure Sockets Layer (SSL).

Register an existing user certificate
Cancel
Help
Document: Done

Figure 156. Register a user certificate - step 1

4. Click **Register an existing user certificate**.

   If you have multiple user certificates stored in your browser's certificate database, you will get a prompt to select the appropriate user certificate as shown in Figure 157.



Select A Certificate

The site 'ralyas4a.itso.ral.ibm.com' has requested client authentication.

Here is the site's certificate:

Certificate for: IBM
Signed by: IBM
Encryption: Highest Grade (RC4 with 128-bit secret key)

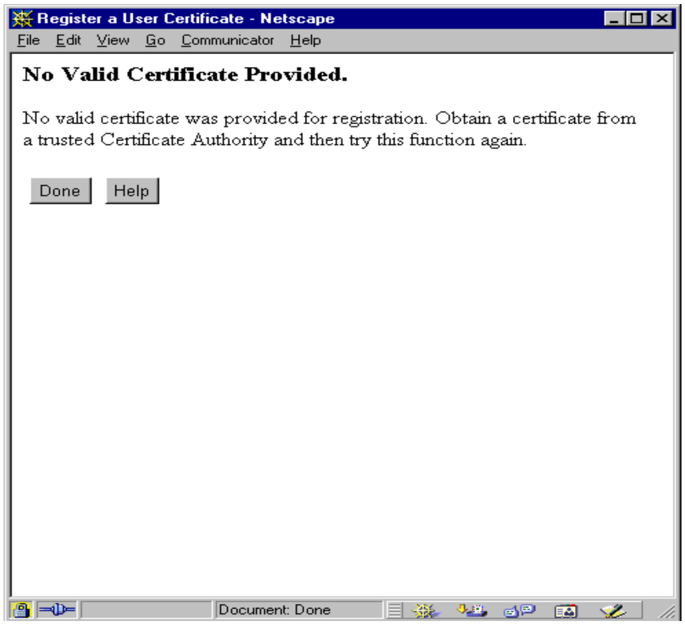
Select Your Certificate: Yukihiro Minote's VeriSign, Inc. ID

Figure 157. Netscape browser certificate selection window

If the certificate selection window does not appear and instead the `No Valid Certificate Provided` message is displayed as shown in Figure 158, an error occurred. Check that you have valid user certificates stored in the browser certificate database. If the error still occurs, the problem is probably caused by a configuration error in the *ADMIN server configuration.

Note

In order to register user certificates with AS/400 user profiles, the *ADMIN server instance must be correctly configured. The server directive `SSLClientAuth` must be set to `On`.Otherwise you get the message as shown in Figure 158. The directive can be configured through the HTTP Configuration and Administration utility setting SSL client authentication to Optional or by changing the directive in the HTTP configuration to `SSLClientAuth On`. Do not set the SSL client authentication to Required. The registration process would also fail.


Register a User Certificate - Netscape
File Edit View Go Communicator Help
Done
Help
Document: Done

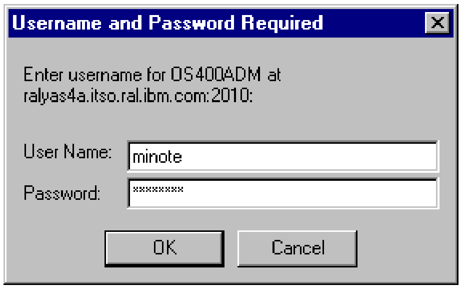
No Valid Certificate Provided.

No valid certificate was provided for registration. Obtain a certificate from a trusted Certificate Authority and then try this function again.

Figure 158. No valid certificate provided

5. Select a user certificate which you want to register.
6. Click **Continue**.

   DCM starts an SSL session to receive the user certificate securely. The HTTP server prompts you again for the user and password of the AS/400 user profile.



Enter username for OS400ADM at ralyas4a.itso.ral.ibm.com:2010:

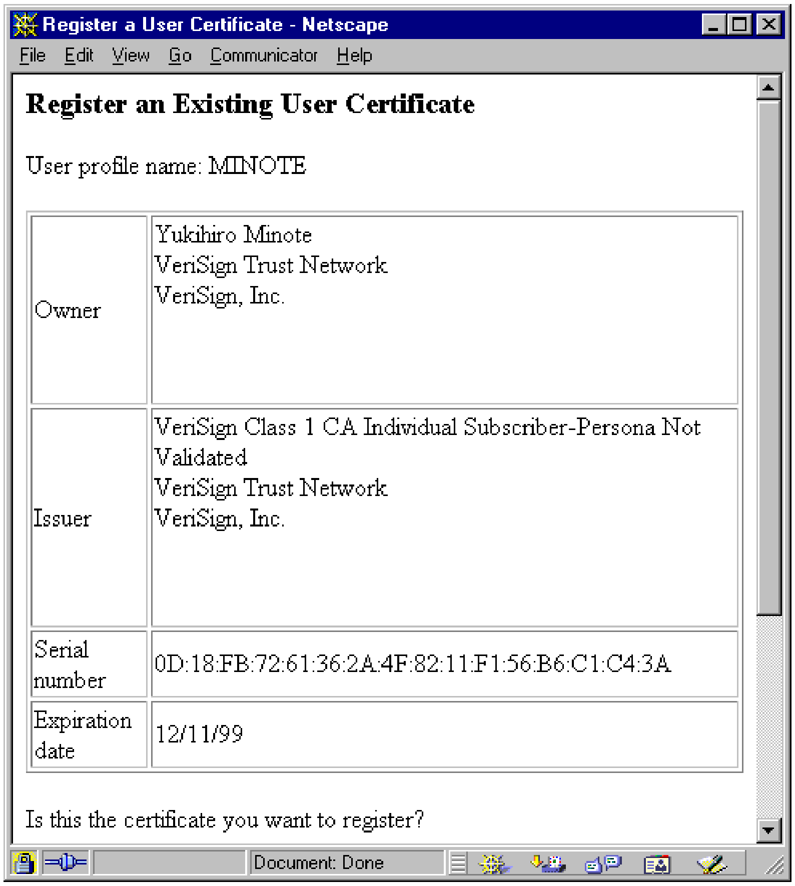
User Name: minote

Password: ********

Figure 159. User profile and password for the secure session

7. Enter the user profile name and password.

   The SSL connection is established between the browser and DCM. The user certificate is being sent to DCM. The user then verifies that the user certificate is the certificate intended for registration.



Register a User Certificate - Netscape
File Edit View Go Communicator Help
Document: Done

Register an Existing User Certificate

User profile name: MINOTE

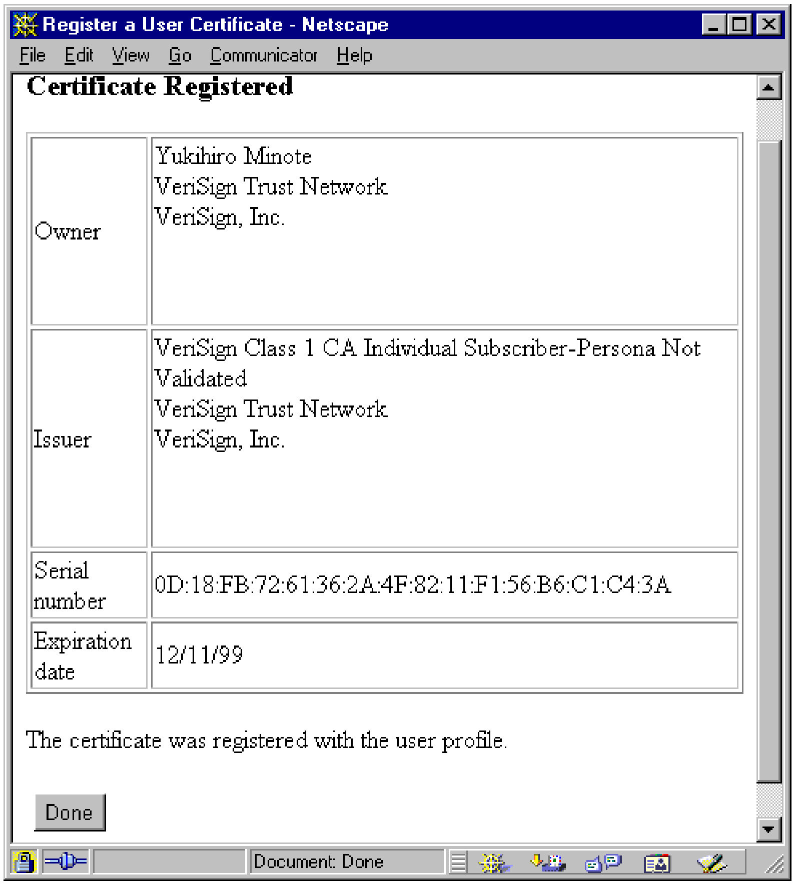
Owner	Yukihiro Minote VeriSign Trust Network VeriSign, Inc.
Issuer	VeriSign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Trust Network VeriSign, Inc.
Serial number	0D:18:FB:72:61:36:2A:4F:82:11:F1:56:B6:C1:C4:3A
Expiration date	12/11/99

Is this the certificate you want to register?

Figure 160. Register an existing user certificate

8. Click **OK**.

   DCM associates the received user certificate with the user profile. After that, a completion message is displayed as shown in Figure 161.



Register a User Certificate - Netscape
File Edit View Go Communicator Help
Document: Done

Certificate Registered

Owner	Yukihiro Minote VeriSign Trust Network VeriSign, Inc.
Issuer	VeriSign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Trust Network VeriSign, Inc.
Serial number	0D:18:FB:72:61:36:2A:4F:82:11:F1:56:B6:C1:C4:3A
Expiration date	12/11/99

The certificate was registered with the user profile.

Done

Figure 161. Certificate registered

9. Click **Done** to return to the DCM main window.

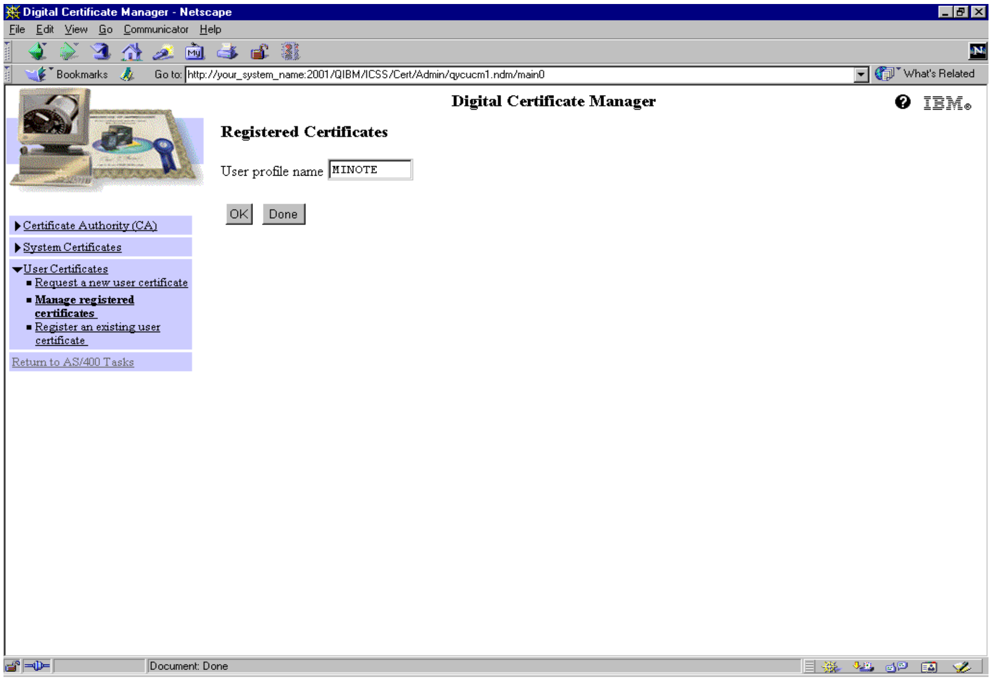
Now the user certificate has been associated with the AS/400 user profile.

5.8.3 Manage registered certificates

DCM also allows you to manage registered user certificates. You can view and delete a user certificate that is associated with an AS/400 user profile. To do this, follow these steps:

1. In the DCM main window, click **User certificate** to expand its menu.
2. Click **Manage registered certificates**.

   If the user who is currently signed on to DCM has *ALLOBJ and *SECADM special authorities, the user profile selection window is displayed as shown in Figure 162. The user profile name of the current user profile is shown in this window. If the signed-on user profile does not have the special authorities mentioned above, the Registered Certificates window is displayed as shown in Figure 163. Note that ordinary users, without *ALLOBJ and *SECADM authorities, can only manage user certificates associated with their own user profile.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
System Certificates
User Certificates
Request a new user certificate
Manage registered certificates
Register an existing user certificate
Return to AS/400 Tasks
OK
Done
Document: Done

Digital Certificate Manager

Registered Certificates

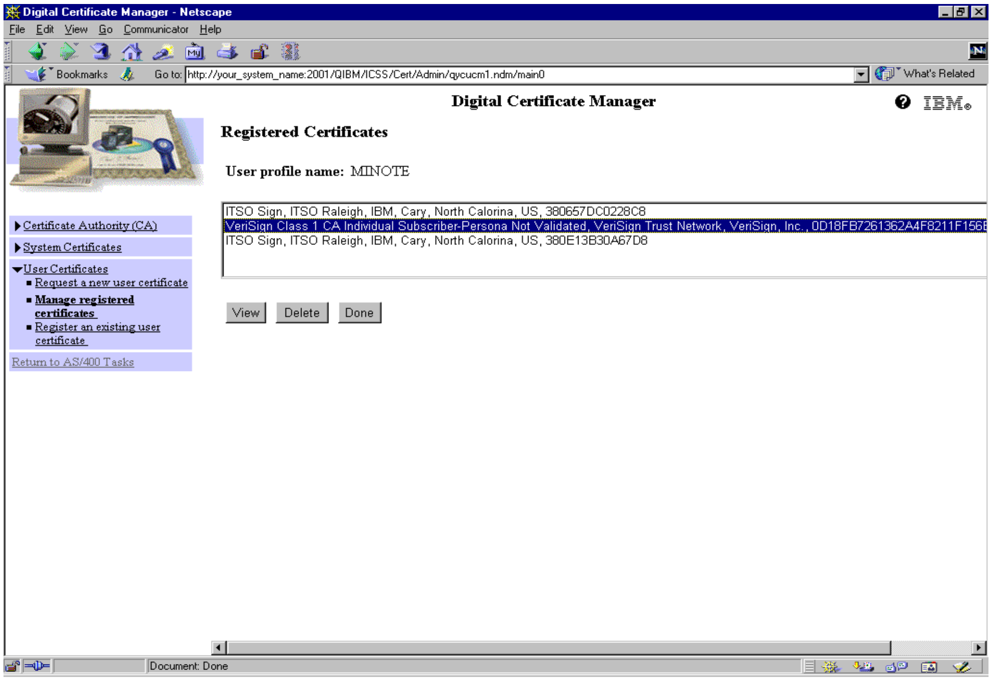
User profile name: MINOTE

Figure 162. Registered certificate - user selection

3. Enter a user profile name you want to manage.

4. Click **OK**.

   DCM displays all user certificates that are associated with the given user profile.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
System Certificates
User Certificates
Request a new user certificate
Manage registered certificates
Register an existing user certificate
Return to AS/400 Tasks
View
Delete
Done
Document: Done

Digital Certificate Manager

Registered Certificates

User profile name: MINOTE

ITSO Sign, ITSO Raleigh, IBM, Cary, North Calorina, US, 380657DC0228C8
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated, VeriSign Trust Network, VeriSign, Inc., 0D18FB7261362A4F8211F156
ITSO Sign, ITSO Raleigh, IBM, Cary, North Calorina, US, 380E13B30A67D8

Figure 163. Registered certificate list

From this window you can view the certificate attributes of the selected certificate or remove the certificate from the given user profile.

Chapter 6. Enabling SSL on AS/400 standard server applications

On the AS/400 system there are many TCP/IP server applications available that are able to communicate over SSL. This chapter provides detailed information on how to set up the AS/400 system and the appropriate clients to use SSL for encrypting the data between the server and the client. Although certificates can be used to authenticate a communication partner, most of the TCP/IP servers do not support client authentication yet. At the time this redbook was written, there was only the HTTP Server for AS/400 that supported client authentication using digital certificates. However, a client can always authenticate the server using its server certificate.

The server applications covered in this chapter are:

- IBM HTTP Server for AS/400
- IBM AS/400 Client Access Express
- Management Central
- Lightweight Directory Access Protocol (LDAP)
- IBM eNetwork Personal Communications
- IBM SecureWay Host On-Demand
- Java applications using the AS/400 Toolbox for Java
- Distributed Relational Database Architecture (DRDA)
- Distributed Data Management (DDM)

6.1 Using certificates with HTTP Server for AS/400

The IBM HTTP Server for AS/400 supports digital certificates for server and client authentication. Various configuration settings in the HTTP server directives allow the system administrator to control access to the HTTP server in general or just a single part of it. Since the HTTP server provides a huge variety of security functions and settings, a separate chapter is devoted to cover only those topics. Refer to Chapter 4, “Securing the HTTP Server for AS/400” on page 35 for details on how to secure the HTTP server.

6.2 Enabling SSL for IBM AS/400 Client Access Express

All IBM AS/400 Client Access Express functions can communicate over SSL, except the Messaging Application Program Interface (MAPI). IBM AS/400 Client Access Express applications that can communicate over SSL are:

- Operations Navigator
- PC5250 emulation
- Data Transfer
- ODBC

You can also use the IBM AS/400 Client Access Express application programming interfaces (APIs) to create your applications that can use SSL. The following table is a summary of the IBM-supplied secure TCP/IP host server application names and port numbers. Once you enable those servers to use SSL, the host servers will listen to an additional port number for SSL connections. To assure which secure servers are up and running, you can check the status of the following port numbers.

Table 4. IBM-supplied secure TCP/IP host server application name and port numbers

Application Name	Corresponding Application	Port	Service name
QIBM_OS400_QZBS_SVR_CENTRAL	Central Server	9470	as-central-s
QIBM_OS400_QZBS_SVR_DATABASE	Database Server	9471	as-database-s
QIBM_OS400_QZBS_SVR_DTAQ	Data Queue Server	9472	as-dtaq-s
QIBM_OS400_QZBS_SVR_NETPRT	Network Print Server	9474	as-netprt-s
QIBM_OS400_QZBS_SVR_RMTCMD	Remote Command Server	9475	as-rmtcmd-s
QIBM_OS400_QZBS_SVR_SIGNON	Signon Server	9476	as-signon-s
QIBM_OS400_QZBS_SVR_FILE	File Server	9473	as-file-s

In order to use SSL with IBM AS/400 Client Access Express, the CA certificate of the Certificate Authority that issued the server certificate used by the host servers must be stored on the client PC. All CA certificates, whether they are issued by a private CA or a well-known CA are stored in the *Key Database* file. This file is protected by a password, which is stored into a stashed key (STH) file. The default file names and locations are as follows:

Key database file name	cwbssldf.kdb
Stashed Key file name	cwbssldf.sth
Stored directory	\Program Files\IBM\Client Access\ (IBM AS/400 Client Access Express install directory)

The CA certificates from the following well-known Internet Certificate Authorities are already built into the IBM AS/400 Client Access Express key database and are registered as trusted roots. Using a certificate from one of these well-known CAs simplifies setting up your IBM AS/400 Client Access Express clients to use SSL:

- Integrion Certification Authority Root
- IBM World Registry Certification Authority
- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA

- RSA secure server CA (also obtained from VeriSign)
- Verisign class 4 public primary CA
- Verisign class 3 public primary CA
- Verisign class 2 public primary CA
- Verisign class 1 public primary CA

6.2.0.1 Implementation tasks overview

To use IBM AS/400 Client Access Express with the Secured Socket Layer (SSL) protocol, you must perform the following tasks:

1. Be sure to have all required license programs installed.
2. Obtain a server certificate and its CA certificate.

   Refer to Chapter 5, “Digital Certificate Manager for AS/400” on page 107 for detailed information on obtaining a server certificate.
3. Set up the IBM AS/400 Client Access Express host servers on the AS/400 system to use SSL.
4. Set up the IBM AS/400 Client Access Express client software on the PC.

6.2.1 Objective

The objective of this section is to show how to configure the IBM AS/400 Client Access Express to use the SSL protocol for secured communication.

6.2.2 Prerequisites

Before you can enable SSL for IBM AS/400 Client Access Express and its associated applications, including Operations Navigator, Data Transfer, PC5250, and OBDC, you must have installed the required license programs and set up digital certificates on your AS/400.

AS/400 license programs

- Digital Certificate Manager (DCM), option 34 of OS/400 (5769-SS1)
- TCP/IP Connectivity Utilities for AS/400 (5769-TC1)
- IBM HTTP server for AS/400 (5769-DG1)
- One of the IBM Cryptographic Access Provider products:

  5769-AC1 (40-bit)

  5769-AC2 (56-bit)

  5769-AC3 (128-bit)
- At least one of the AS/400 products:

  5769-CE1 (40-bit)

  5769-CE2 (56-bit)

  5769-CE3 (128-bit)

Note

If you want to use the 5250 emulation that is shipped with the IBM eNetwork Personal Communications (PCOM) product, you do not need to install a client encryption product. PCOM has its own built-in encryption code.

Server certificate

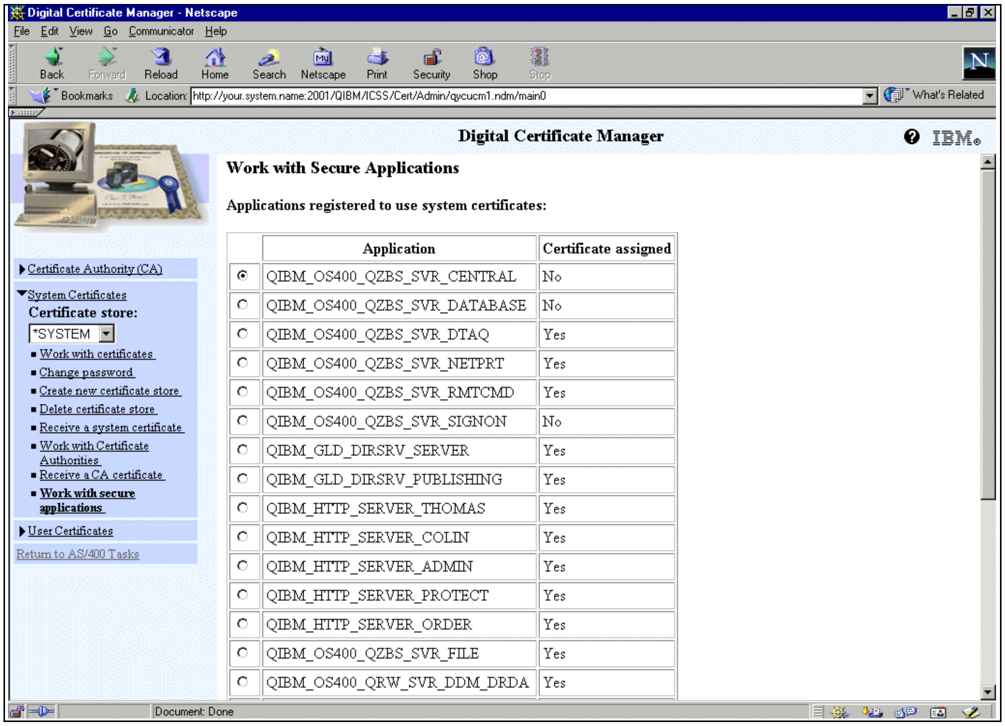
Obtain a server certificate that will be assigned to the TCP/IP host servers. This could be a certificate issued by a private or intranet CA or by a well-known CA.

6.2.3 Configuring the AS/400 system

We assume that a server certificate was already issued and received on the AS/400 system. Also the CA certificate of the CA that issued the server certificate is stored in the AS/400 certificate store. Detailed information for obtaining and receiving certificates is available in Chapter 5, “Digital Certificate Manager for AS/400” on page 107.

To assign the server certificate with the TCP/IP host servers, perform the following steps:

1. Start DCM and expand **System Certificate**. Remember to sign on with a user profile that has *SECADM and *ALLOBJ special authorities.
2. Click **Work with secure applications**.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
IBM
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
Document: Done

Digital Certificate Manager

Work with Secure Applications

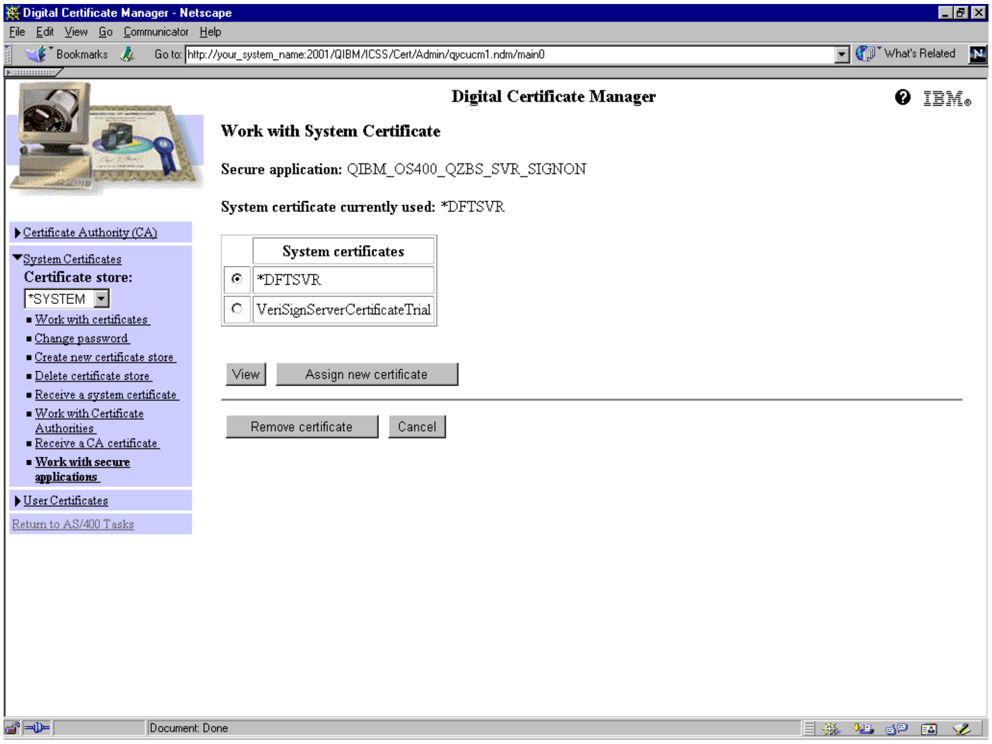
Applications registered to use system certificates:

	Application	Certificate assigned
●	QIBM_OS400_QZBS_SVR_CENTRAL	No
○	QIBM_OS400_QZBS_SVR_DATABASE	No
○	QIBM_OS400_QZBS_SVR_DTAQ	Yes
○	QIBM_OS400_QZBS_SVR_NETPRT	Yes
○	QIBM_OS400_QZBS_SVR_RMTCMD	Yes
○	QIBM_OS400_QZBS_SVR_SIGNON	No
○	QIBM_GLD_DIRSRV_SERVER	Yes
○	QIBM_GLD_DIRSRV_PUBLISHING	Yes
○	QIBM_HTTP_SERVER_THOMAS	Yes
○	QIBM_HTTP_SERVER_COLIN	Yes
○	QIBM_HTTP_SERVER_ADMIN	Yes
○	QIBM_HTTP_SERVER_PROTECT	Yes
○	QIBM_HTTP_SERVER_ORDER	Yes
○	QIBM_OS400_QZBS_SVR_FILE	Yes
○	QIBM_OS400_QRW_SVR_DDM_DRDA	Yes

Figure 164. Work with Secure Applications window

3. Select the secure application server name for which you want to assign the certificate and click **Work with system certificate.**

You must at least associate the QIBM_OS400_QZBS_SVR_SIGNON application ID with the certificate.



Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://your_system_name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Assign new certificate
Remove certificate
Cancel
Document: Done

Work with System Certificate

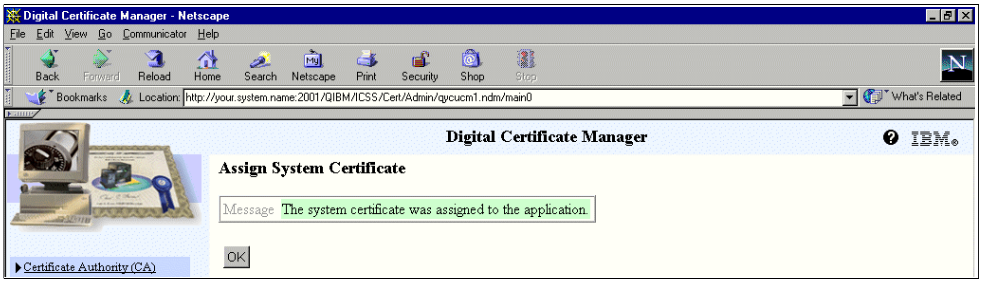
Secure application: QIBM_OS400_QZBS_SVR_SIGNON

System certificate currently used: *DFTSVR

	System certificates
●	*DFTSVR
○	VeriSignServerCertificateTrial

Figure 165. Work with System Certificate window

4. Select the appropriate server certificate and click **Assign new certificate**. The completion message is displayed.



Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Shop
Stop
Bookmarks
Location: http://your.system.name:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
Certificate Authority (CA)
OK

Assign System Certificate

Message The system certificate was assigned to the application.

Figure 166. Assign system certificate completion message

You need to enable one or more additional TCP/IP host servers. It depends on what IBM AS/400 Client Access Express application you want to use SSL with (refer to Table 4 on page 188). Repeat the previous steps to assign a certificate to each host server application.

5. Restart the host servers.

To reflect these changes to the TCP/IP host server applications, you must restart these server jobs on your AS/400 system. Use the following commands:

To stop: `ENDHOSTSVR SERVER(*ALL)`

To start: `STRHOSTSVR SERVER(*ALL) RQDPCL(*TCP)`

6.2.4 Configuring the PC

By default, the Data transfer, ODBC, and PC5250 application included in the Client Access Express refer to the Operations Navigator security settings when they establish the connection to the AS/400 system. For example, when the Operations Navigator is already set to use SSL and a PC5250 session is established, it also uses, by default, SSL for this connection. If you want to configure one of these applications explicitly to use or not to use SSL, you can specify this on the property settings of each application.

It is a two-step process to activate SSL for IBM AS/400 Client Access Express on the PC. The first step is to configure IBM AS/400 Client Access Express for SSL. The second step is optional and allows you to enable or disable SSL for individual IBM AS/400 Client Access Express applications, such as PC5250 emulation.

6.2.4.1 Configuring Client Access Express for SSL

Perform the following steps to enable IBM AS/400 Client Access Express for SSL:

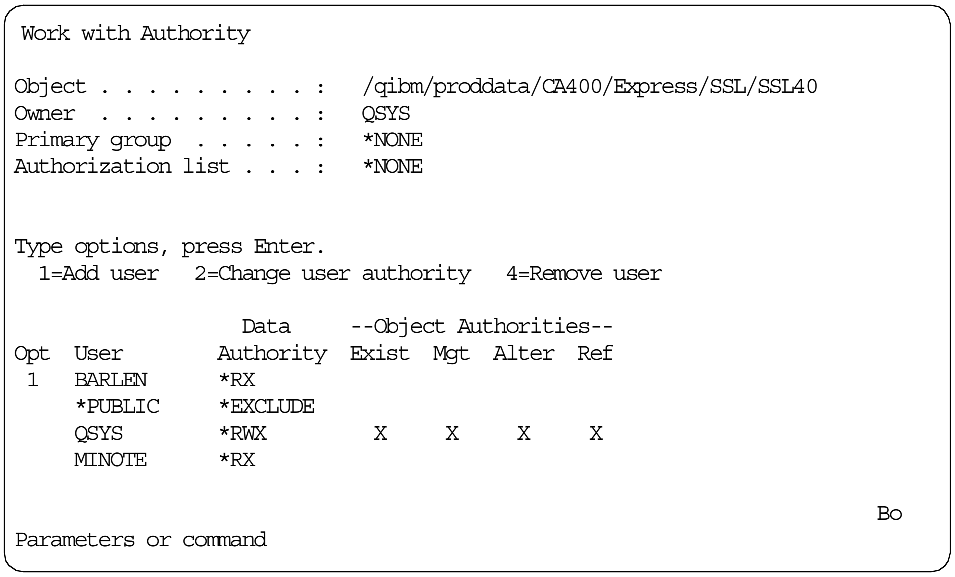
1. Authorize the appropriate user profile to the Client Encryption products.

   Because of export regulations for products that contain encryption technology, the Client Encryption products are installed with data authority set to *PUBLIC *EXCLUDE. So you must authorize the appropriate user profile to the Client Encryption products. To meet the requirements for export regulations, authorize users only to those products they are allowed to use in their country. For example, if your AS/400 system is located in the United States and you have users in different countries, you can install multiple Client Encryption products on that system. But authorize American users only to the 128-bit encryption product and French users to the 40-bit encryption product. You can change the authority in one of the following two ways:

   a. Through the AS/400 command prompt by using the following command:

      ```
      WRKAUT OBJ('/QIBM/ProdData/CA400/EXPRESS/SSL/SSL40')
      ```

      where SSL40 stands for the Client Encryption product CE1 (40-bit). Replace the number with the corresponding encryption level of the installed product, for example SSL56 for CE2 and SSL128 for the CE3 product.



```
 Work with Authority

Object . . . . . . . . . :   /qibm/proddata/CA400/Express/SSL/SSL40
Owner  . . . . . . . . . :   QSYS
Primary group  . . . . . :   *NONE
Authorization list . . . :   *NONE


Type options, press Enter.
  1=Add user   2=Change user authority   4=Remove user

                     Data     --Object Authorities--
Opt  User        Authority  Exist  Mgt  Alter  Ref
 1   BARLEN      *RX
     *PUBLIC     *EXCLUDE
     QSYS        *RWX         X     X     X     X
     MINOTE      *RX

                                                                        Bo
Parameters or command
```

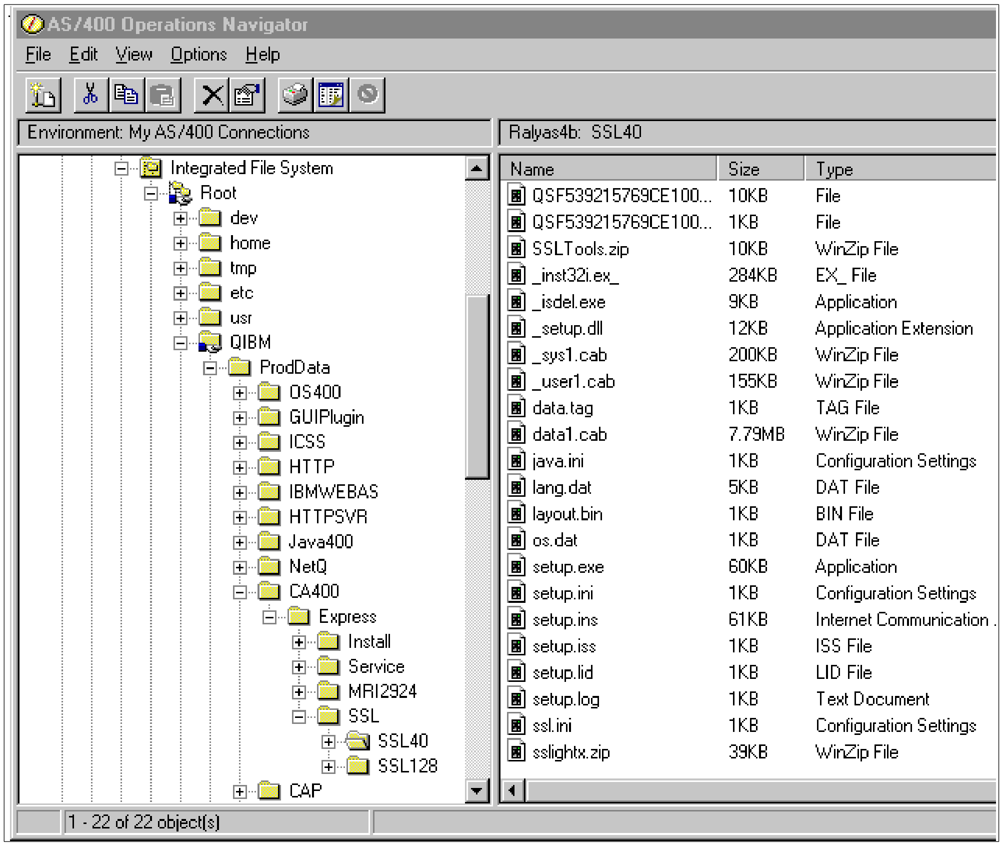
You have the choice of giving Read and Execute (*RX) authority to *PUBLIC, to groups or individual users.

b. If IBM AS/400 Client Access Express is already installed on a PC, you can also grant the permissions through the Operations Navigator by performing the following steps:

   1. Start the Operations Navigator.

   2. Expand your AS/400 system icon and select the **File system**.

   3. Expand the **Integrated File System** -> **Root** -> **QIBM** -> **ProdData** -> **CA400** ->**Express** -> **SSL.** The Client Encryption product’s directory is shown in Figure 167.

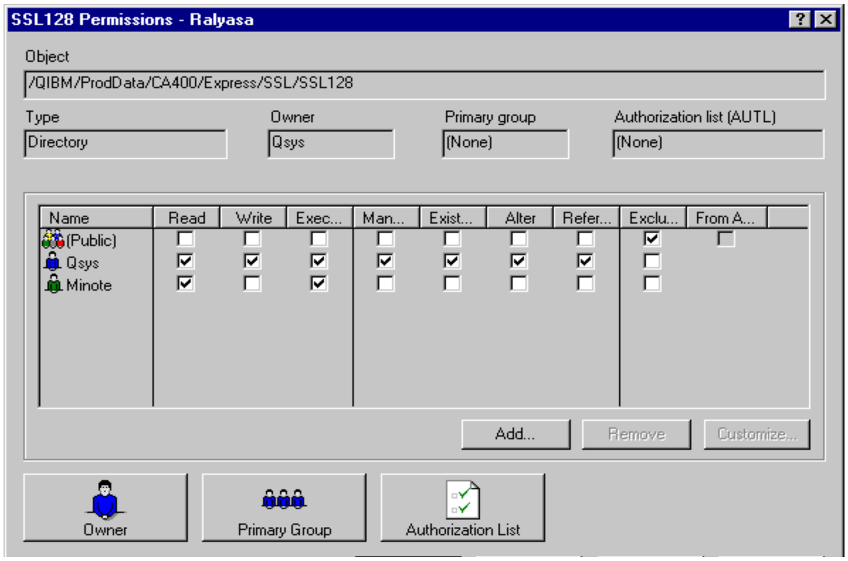


Name	Size	Type
QSF539215769CE100...	10KB	File
QSF539215769CE100...	1KB	File
SSLTools.zip	10KB	WinZip File
inst32i.ex	284KB	EX_ File
_isdel.exe	9KB	Application
_setup.dll	12KB	Application Extension
_sys1.cab	200KB	WinZip File
_user1.cab	155KB	WinZip File
data.tag	1KB	TAG File
data1.cab	7.79MB	WinZip File
java.ini	1KB	Configuration Settings
lang.dat	5KB	DAT File
layout.bin	1KB	BIN File
os.dat	1KB	DAT File
setup.exe	60KB	Application
setup.ini	1KB	Configuration Settings
setup.ins	61KB	Internet Communication .
setup.iss	1KB	ISS File
setup.lid	1KB	LID File
setup.log	1KB	Text Document
ssl.ini	1KB	Configuration Settings
sslightx.zip	39KB	WinZip File

1 - 22 of 22 object(s)

Figure 167. Operations Navigator

   4. Right-click the **SSL*num*** (where *num* is the bit key length (40, 56 or 128) of the Client Encryption product) and select **Permissions.** Operations Navigator then displays the current permission settings for that directory as shown in Figure 168.



SSL128 Permissions - Ralyasa

Object: /QIBM/ProdData/CA400/Express/SSL/SSL128

Type: Directory

Owner: Qsys

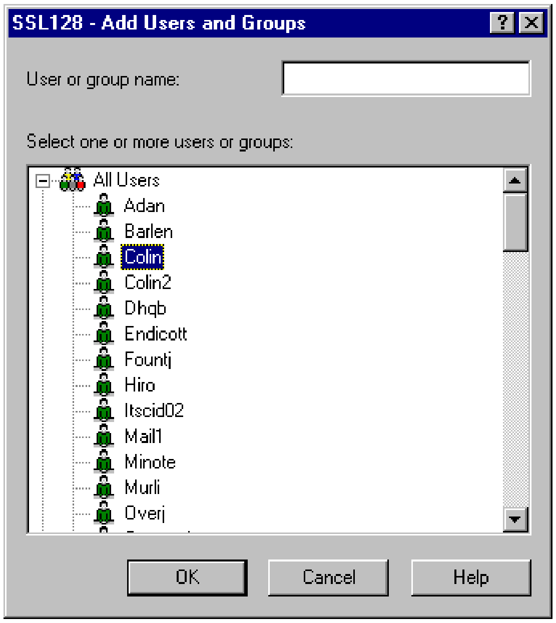
Primary group: (None)

Authorization list (AUTL): (None)

Name	Read	Write	Exec...	Man...	Exist...	Alter	Refer...	Exclu...	From A...
(Public)	☐	☐	☐	☐	☐	☐	☐	☑	☐
Qsys	☑	☑	☑	☑	☑	☑	☑	☐	
Minote	☑	☐	☑	☐	☐	☐	☐	☐	

Figure 168. Permission display window

5. Click the **Add** button to add a new user.



SSL128 - Add Users and Groups

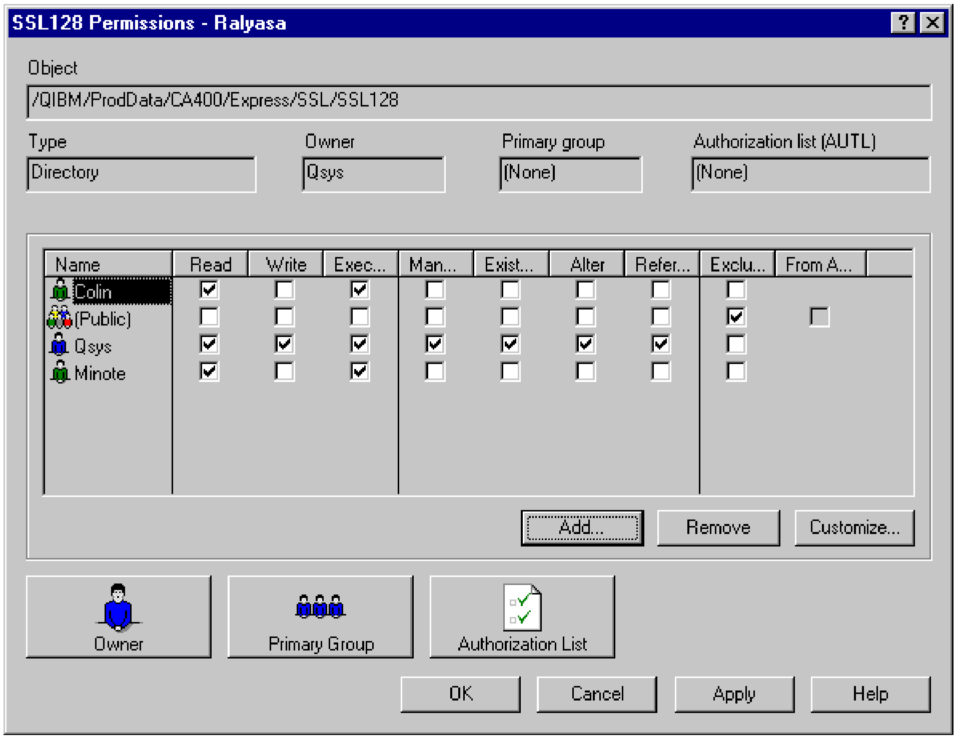
User or group name:

Select one or more users or groups:

- All Users
  - Adan
  - Barlen
  - Colin
  - Colin2
  - Dhqb
  - Endicott
  - Fountj
  - Hiro
  - Itscid02
  - Mail1
  - Minote
  - Murli
  - Overj

Figure 169. User ID selection window

6. Click the **All Users** icon to expand and select the user name you want to grant permission. Then click **OK**.



Object: /QIBM/ProdData/CA400/Express/SSL/SSL128

Type: Directory

Owner: Qsys

Primary group: (None)

Authorization list (AUTL): (None)

Name	Read	Write	Exec...	Man...	Exist...	Alter	Refer...	Exclu...	From A...
Colin	☑	□	☑	□	□	□	□	□	
(Public)	□	□	□	□	□	□	□	☑	□
Qsys	☑	☑	☑	☑	☑	☑	☑	□	
Minote	☑	□	☑	□	□	□	□	□	

Figure 170. Permission display window

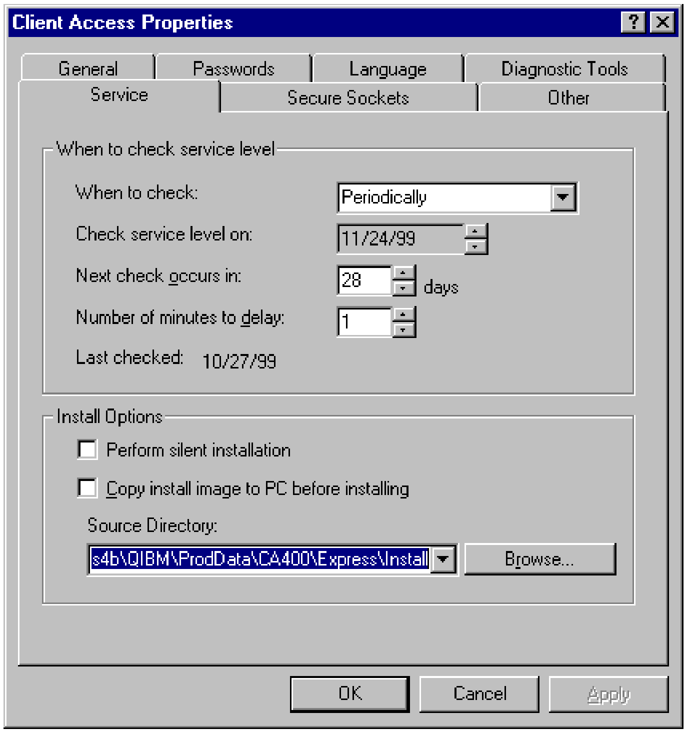
7. Click **OK**. The Operations Navigator applies Read and Execute authority to the user, and you will return to the Operations Navigator main window.

Now the specified user can access the Client Encryption product. The next step is the installation of the SSL component from this directory.

2. Install the SSL component of Client Access Express.

   If you have installed the Client Access Express from a CD-ROM or installation image files that are placed on a network drive, you must change the source directory to use the IFS directory to install the SSL component. Detailed steps follow:

   1. Open the **Client Access Properties** icon.



When to check service level

When to check: Periodically

Check service level on: 11/24/99

Next check occurs in: 28 days

Number of minutes to delay: 1

Last checked: 10/27/99

Install Options

☐ Perform silent installation

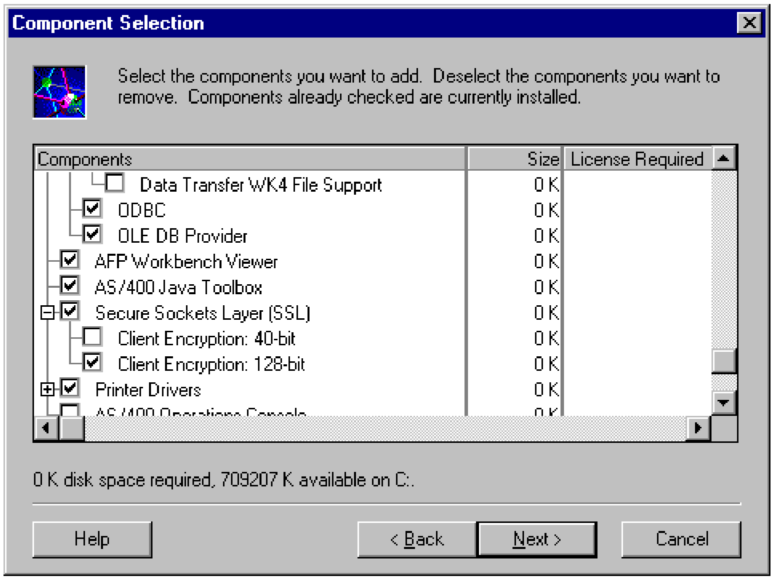
☐ Copy install image to PC before installing

Source Directory: s4b\QIBM\ProdData\CA400\Express\Install

Figure 171. Client Access Properties window

2. Select the **Service** tab and change the **Source directory** parameter to `\\your_system_name\QIBM\ProdData\CA400\Express\Install` (where *your_system_name* is the AS/400 Netserver's name).
3. Click **OK**. From now on the installation source drive refers to the AS/400 IFS directory.
4. Click the **Selective Setup** icon in the IBM AS/400 Client Access Express window.

   The Selective Setup program launches. After you answer some questions in the installation wizard, the component selection window is displayed as shown in Figure 172.



Select the components you want to add. Deselect the components you want to remove. Components already checked are currently installed.

Components	Size	License Required
□ Data Transfer WK4 File Support	0 K	
☑ ODBC	0 K	
☑ OLE DB Provider	0 K	
☑ AFP Workbench Viewer	0 K	
☑ AS/400 Java Toolbox	0 K	
☑ Secure Sockets Layer (SSL)	0 K	
□ Client Encryption: 40-bit	0 K	
☑ Client Encryption: 128-bit	0 K	
☑ Printer Drivers	0 K	
□ AS/400 Operations Console	0 K	

0 K disk space required, 709207 K available on C:.

Figure 172. Component Selection window

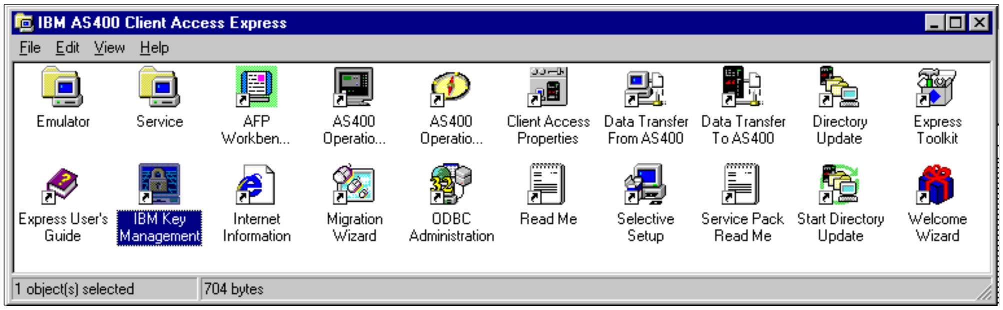
5. Select the desired Client Encryption product to be installed on the PC by checking the appropriate box and click **Next**.

Note

Only the Client Encryption products that are installed on the AS/400 system are shown in this window.

6. Proceed with the following steps. After the Selective Setup program has finished, you must restart the Operations Navigator.

   You will see the new IBM Key Management icon on the IBM AS/400 IBM AS/400 Client Access Express window as shown in Figure 173.



1 object(s) selected | 704 bytes

Figure 173. The IBM AS/400 Client Access window

3. Add a CA certificate to the Client Access Express key database.

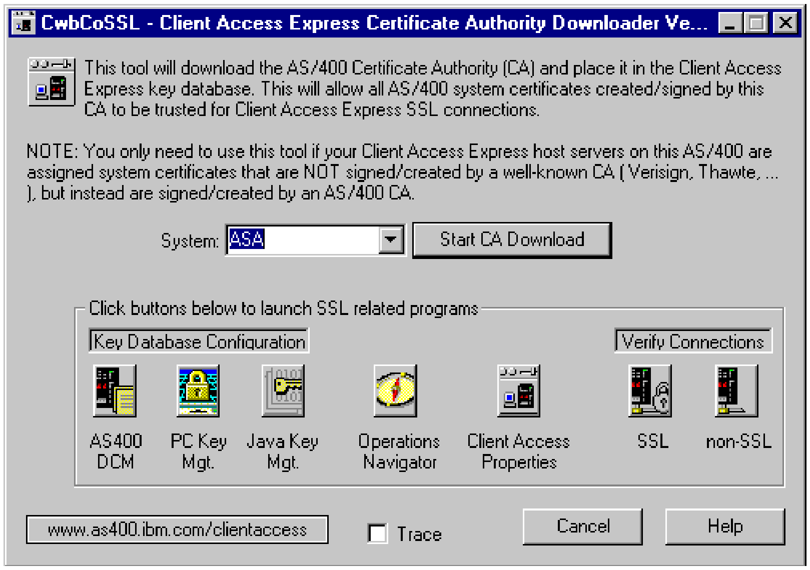
   There are two methods available to install the CA certificate on your PC.

   The first method is using a utility program that is available from the IBM AS/400 Client Access Express Web site at the following URL:

   `http://www.as400.ibm.com/clientaccess/cwbcossz.htm`

This tool automates the download of an AS/400 CA certificate to the PC and Java key database for the IBM AS/400 Client Access Express SSL support. You have to use this tool only when the TCP/IP host servers are using server certificates issued by an AS/400 CA and not from well-known CAs.

1. After the tool is downloaded to the PC, launch the program `cwbcossl.exe`.



CwbCoSSL - Client Access Express Certificate Authority Downloader Ve...

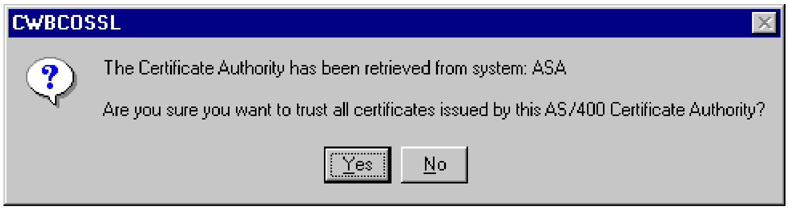
This tool will download the AS/400 Certificate Authority (CA) and place it in the Client Access Express key database. This will allow all AS/400 system certificates created/signed by this CA to be trusted for Client Access Express SSL connections.

NOTE: You only need to use this tool if your Client Access Express host servers on this AS/400 are assigned system certificates that are NOT signed/created by a well-known CA (Verisign, Thawte, ...), but instead are signed/created by an AS/400 CA.

System: ASA

Figure 174. The CwbCoSSL utility

2. Select the AS/400 system you want to download the CA certificate from and click **Start CA Download**.



CWBCOSSL

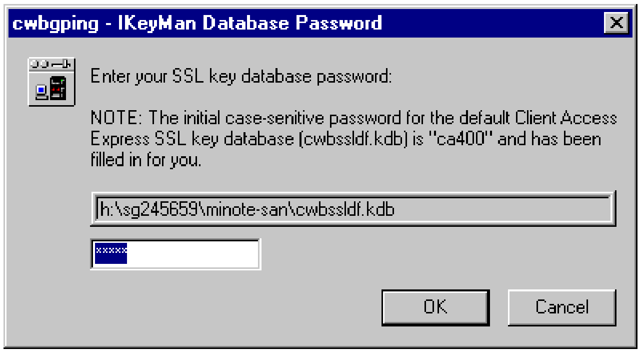
The Certificate Authority has been retrieved from system: ASA

Are you sure you want to trust all certificates issued by this AS/400 Certificate Authority?

Figure 175. Trust the private CA confirmation window

3. Click **Yes**.

   You must trust this downloaded CA as a trusted root.



cwbgping - IKeyMan Database Password

Enter your SSL key database password:

NOTE: The initial case-senitive password for the default Client Access Express SSL key database (cwbssldf.kdb) is "ca400" and has been filled in for you.

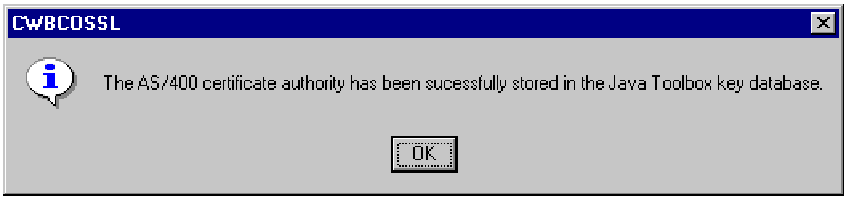
h:\sg245659\minote-san\cwbssldf.kdb

*****

Figure 176. Key Database access confirmation window

4. Click **OK**.

   The utility program opens the key database file on your PC and stores the CA certificate in it. The downloaded CA certificate is stored as a trusted root. After that, the utility stores the CA certificate in the AS/400 Toolbox for Java key database. The completion message window is displayed.



CWBCOSSL

The AS/400 certificate authority has been sucessfully stored in the Java Toolbox key database.

Figure 177. Successfully completion message from the utility program.

5. Click **OK**.

If you do not want to use the utility program or do not have it, you can use the copy and paste method to install the CA certificate into the PC key database. You can create in DCM a binary-text format certificate and save it into a PC text file. For a detailed description of how to perform this task with DCM, refer to 5.5.2, “Install CA certificate on your PC (copy and paste)” on page 134. The steps described here suppose that you already have the CA certificate in binary-text format stored in a file. To import this file into the Client Access Express key database, follow these steps:

1. Start the IBM Key Management program from the Client Access folder or by clicking **Start->Programs->IBM AS400 IBM AS/400 Client Access Express->IBM Key Management**.

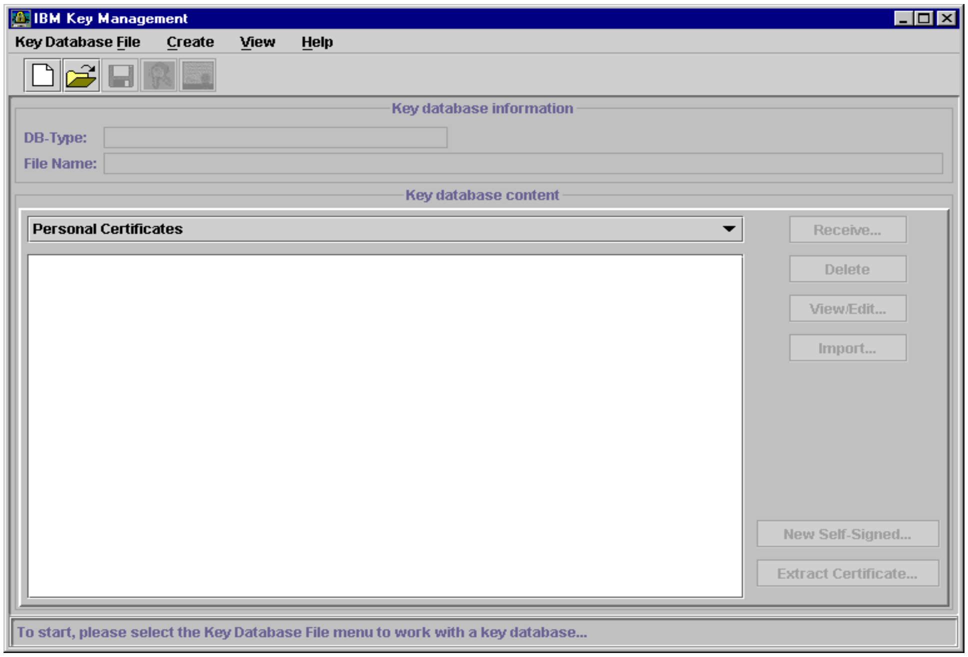
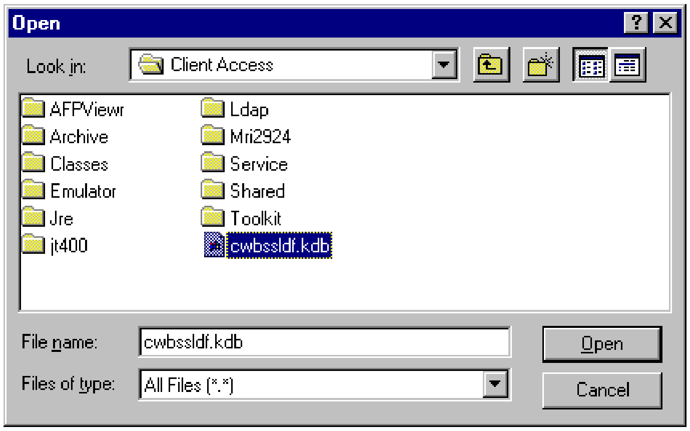


Figure 178. IBM Key Management window

2. Click **Key Database File**->**Open**.



File name: cwbssldf.kdb

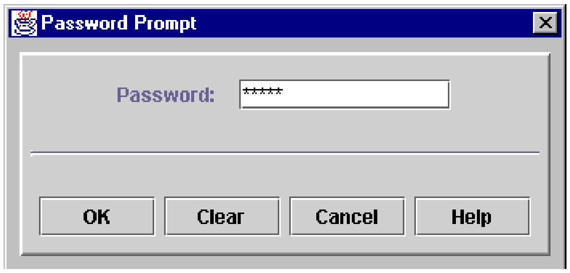
Files of type: All Files (*.*)

Figure 179. Open a default key database file

3. Find the key database file: cwbssldf.kdb and open it.

Note

The key database shown in Figure 179 is the default key database that is, by default stored in the root directory for IBM AS/400 Client Access Express. The default root directory is c:\Program Files\IBM\Client Access\. If you have chosen to use a different key database, select it from the appropriate directory.



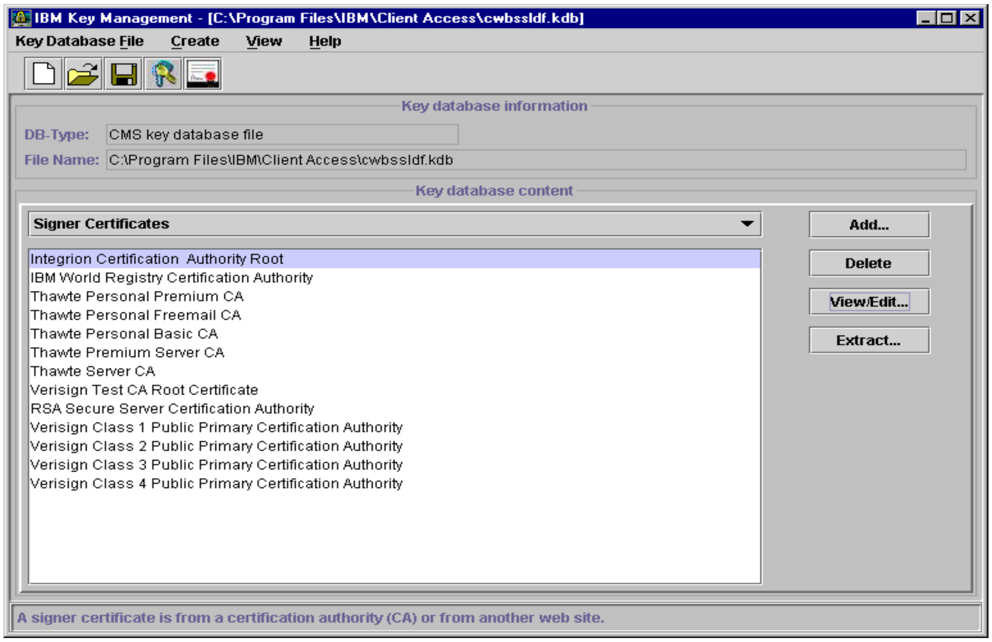
Password: *****

Figure 180. Password prompt

4. Enter the password and click **OK**.

   By default, the password is `ca400`. The password is case sensitive.

   A list of the currently installed CA certificates is displayed.



DB-Type: CMS key database file

File Name: C:\Program Files\IBM\Client Access\cwbssldf.kdb

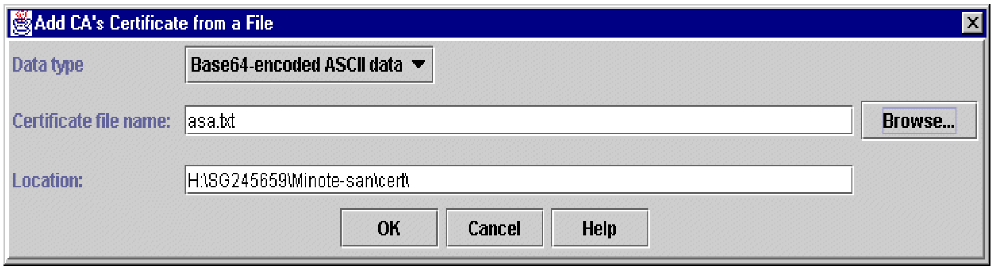
Signer Certificates

Integrion Certification Authority Root
IBM World Registry Certification Authority
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
Verisign Test CA Root Certificate
RSA Secure Server Certification Authority
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority
Verisign Class 4 Public Primary Certification Authority

A signer certificate is from a certification authority (CA) or from another web site.

Figure 181. IBM Key Management program main window

5. Click **Add**.



Data type: Base64-encoded ASCII data

Certificate file name: asa.txt

Location: H:\SG245659\Minote-san\cert\

Figure 182. ADD CA's Certificate from a File window

6. Type the path name and the file name of the file that contains the CA certificate to be imported and click **OK**. The CA certificate can be one of a private CA or a well-known CA. In this scenario it is a private CA

certificate that was previously copied into an ASCII PC file through DCM.

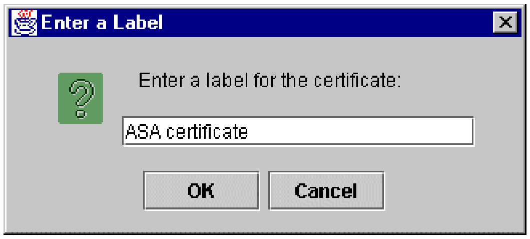
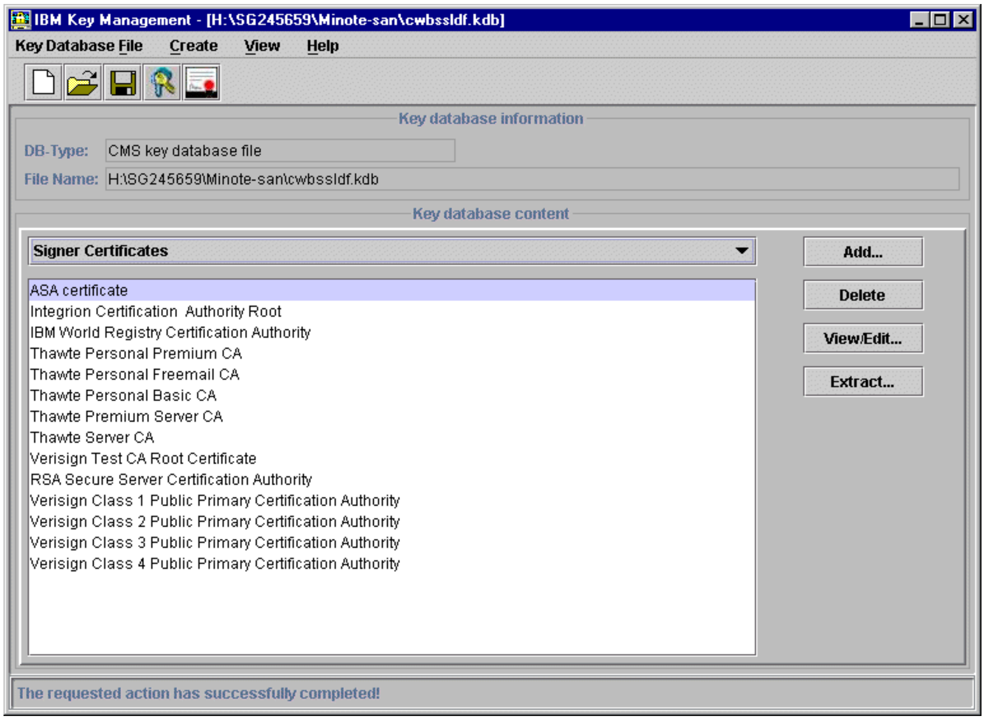


Figure 183. Enter a label

7. Enter a label for the CA certificate and click **OK**.

   The certificate is stored as a trusted root in the key database file. The label specified here is the name that is shown in the list of trusted root CAs.



DB-Type: CMS key database file

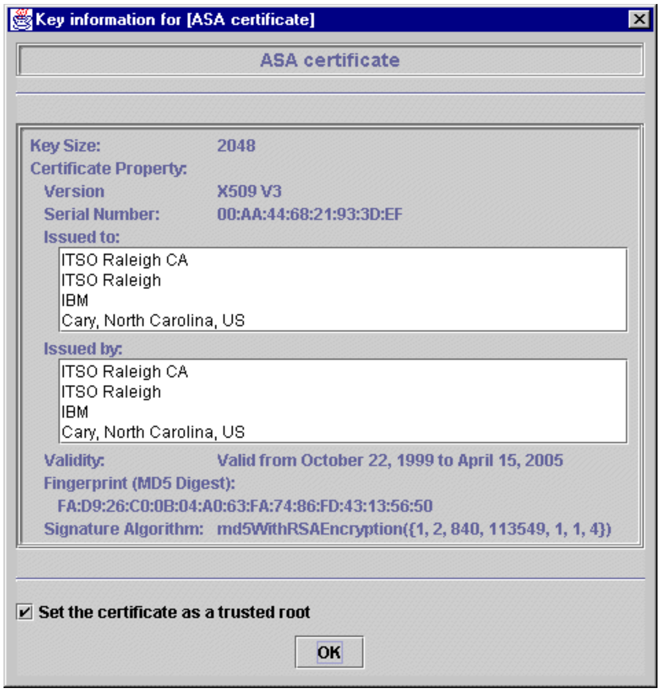
File Name: H:\SG245659\Minote-san\cwbssldf.kdb

ASA certificate
Integrion Certification Authority Root
IBM World Registry Certification Authority
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
Verisign Test CA Root Certificate
RSA Secure Server Certification Authority
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority
Verisign Class 4 Public Primary Certification Authority

The requested action has successfully completed!

Figure 184. IBM Key Management main window

8. Click **View/Edit** to confirm the imported certificate’s content.



Key information for [ASA certificate]

ASA certificate

Key Size: 2048

Certificate Property:

Version X509 V3

Serial Number: 00:AA:44:68:21:93:3D:EF

Issued to:

ITSO Raleigh CA
ITSO Raleigh
IBM
Cary, North Carolina, US

Issued by:

ITSO Raleigh CA
ITSO Raleigh
IBM
Cary, North Carolina, US

Validity: Valid from October 22, 1999 to April 15, 2005

Fingerprint (MD5 Digest):

FA:D9:26:C0:0B:04:A0:63:FA:74:86:FD:43:13:56:50

Signature Algorithm: md5WithRSAEncryption({1, 2, 840, 113549, 1, 1, 4})

☑ Set the certificate as a trusted root

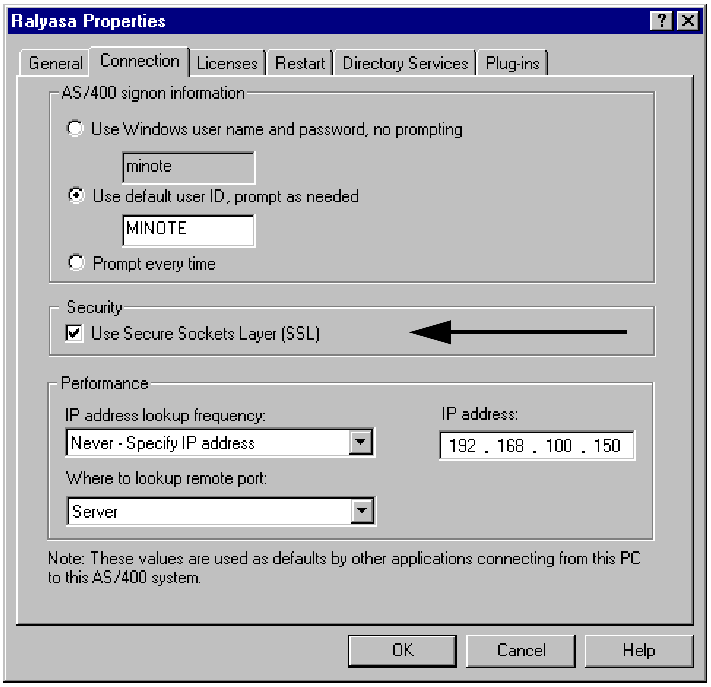
Figure 185. Key information window

IBM AS/400 Client Access Express is now able to communicate with server applications that are using certificates issued by the listed CAs. The next step is to configure each function, such as Operations Navigator, ODBC, and so forth, to use SSL.

6.2.4.2 Configuring Operations Navigator for SSL

The following steps describe how to configure the Operations Navigator for SSL.

1. Start Operations Navigator.
2. Right-click the **AS/400 connection** icon from the available AS/400 connections and select **Properties**.
3. Select the **Connection** tab.



AS/400 signon information

○ Use Windows user name and password, no prompting

minote

● Use default user ID, prompt as needed

MINOTE

○ Prompt every time

Security

☑ Use Secure Sockets Layer (SSL)

Performance

IP address lookup frequency: Never - Specify IP address

IP address: 192 . 168 . 100 . 150

Where to lookup remote port: Server

Note: These values are used as defaults by other applications connecting from this PC to this AS/400 system.

Figure 186. Connection property window

4. Check **Use Secure Socket Layer (SSL)** and click **OK**.

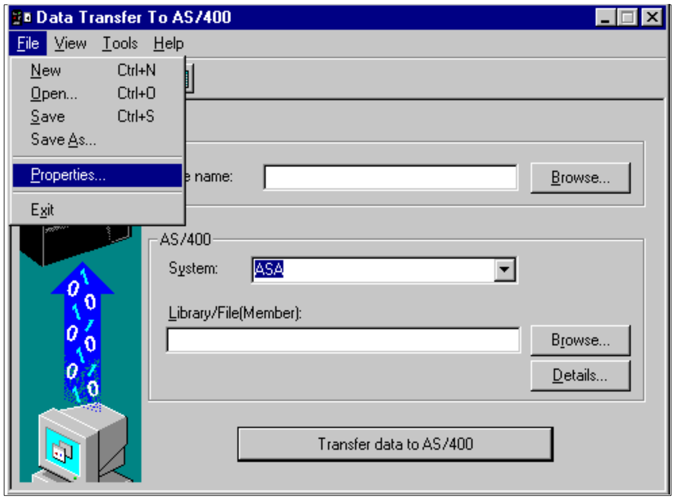
   This means that SSL is used only for this particular AS/400 connection and not for the entire Client Access Express.

5. Restart the Operations Navigator to activate the change.

6.2.4.3 Configuring data transfer for SSL

The Data Transfer application uses by default the security settings of the Operations Navigator. Through the following steps you can override the default.

1. Open the appropriate data transfer session.
2. Click **File -> Properties**.



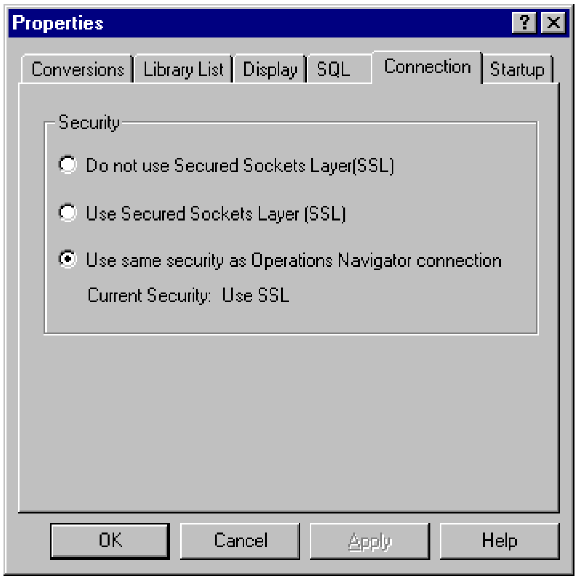
AS/400

System: ASA

Library/File(Member):

Figure 187. IBM AS/400 Client Access Express Data Transfer window

3. Select the **Connection** tab.



○ Do not use Secured Sockets Layer(SSL)

○ Use Secured Sockets Layer (SSL)

● Use same security as Operations Navigator connection

Current Security: Use SSL

Figure 188. Data Transfer's property window

The properties window shows the current SSL setting of the appropriate AS/400 connection.

4. Choose the appropriate security setting and click **OK**.

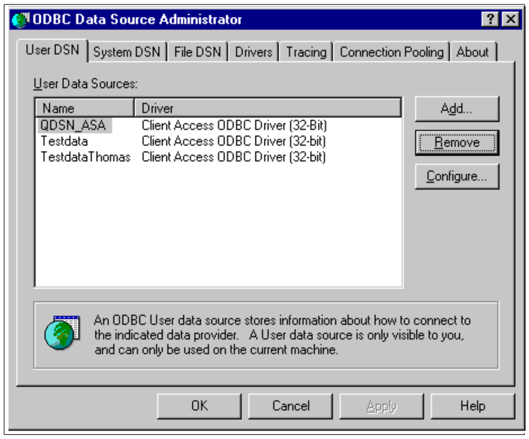
   If you want explicitly to configure the application to use SSL, you must select **Use Secured Socket Layer (SSL).** This means this session always uses SSL, and does not depend on the Operations Navigator setting.

5. Restart the data transfer session to activate the changes.

6.2.4.4 Configuring ODBC for SSL

ODBC uses by default the security settings of the Operations Navigator. Through the following steps you can override the default.

1. Open ODBC Administration in the IBM AS/400 Client Access Express window.
2. Select the **User DSN** tab.



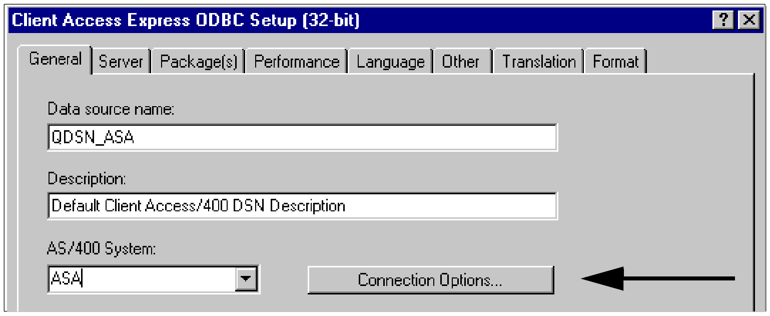
User Data Sources:

Name	Driver
QDSN_ASA	Client Access ODBC Driver (32-Bit)
Testdata	Client Access ODBC Driver (32-bit)
TestdataThomas	Client Access ODBC Driver (32-bit)

An ODBC User data source stores information about how to connect to the indicated data provider. A User data source is only visible to you, and can only be used on the current machine.

Figure 189. IBM AS/400 Client Access Express - ODBC

3. Double-click **User Data Source** for your AS/400 system.



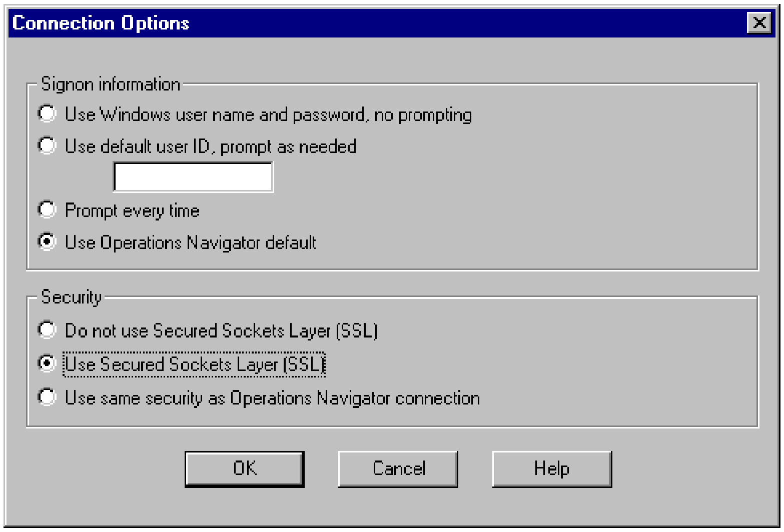
Data source name: QDSN_ASA

Description: Default Client Access/400 DSN Description

AS/400 System: ASA

Figure 190. IBM AS/400 Client Access Express - ODBC User Data Source

4. Click the **Connection Options** button.



Signon information

○ Use Windows user name and password, no prompting

○ Use default user ID, prompt as needed

○ Prompt every time

● Use Operations Navigator default

Security

○ Do not use Secured Sockets Layer (SSL)

● Use Secured Sockets Layer (SSL)

○ Use same security as Operations Navigator connection

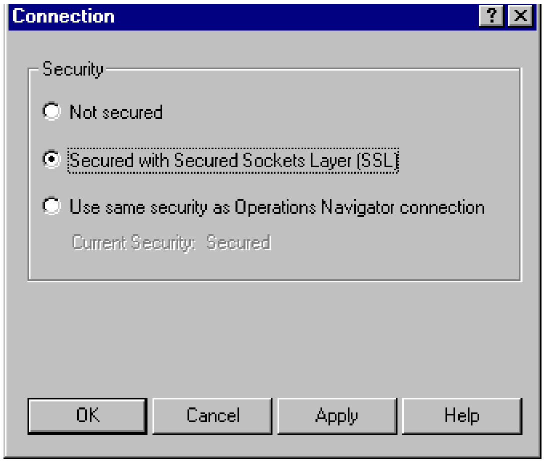
Figure 191. ODBC Connection Options window

5. Choose the appropriate security setting and click **OK**. Click **OK** again to return to the ODBC Administration window.

6.2.4.5 Configuring 5250 emulation for SSL

The 5250 emulation uses by default the security settings of the Operations Navigator. Through the following steps you can override the default.

1. Open the appropriate PC5250 session.
2. Open the **Communication** menu and select **Configure**.
3. Click **Properties**.



Security

○ Not secured

● Secured with Secured Sockets Layer (SSL)

○ Use same security as Operations Navigator connection

Current Security: Secured

Figure 192. PC5250 Connection window

4. Choose the appropriate security setting and click **OK**.

> **Note**
>
> For each 5250 session destination, the Telnet server of the appropriate AS/400 system needs to be configured for SSL. That also means that you may have to install additional CA certificates into the key database on the PC. This depends on whether the server certificates used on the destination AS/400 system are issued by other private CAs or unlisted well-known CAs.

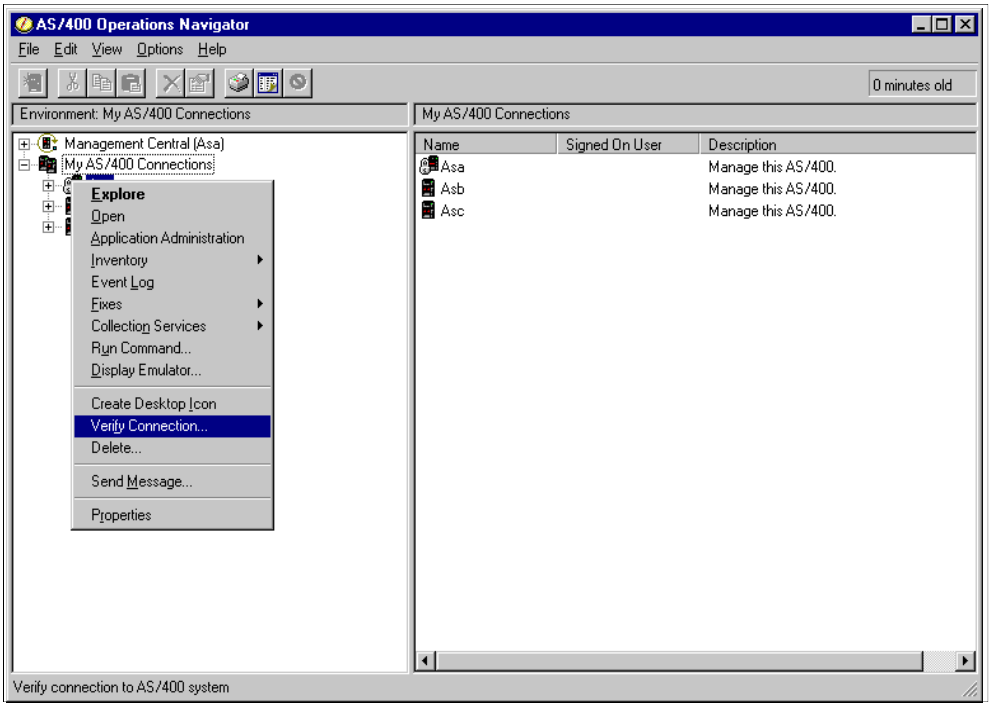
6.2.5 Verifying a SSL connection

After IBM AS/400 Client Access Express finally is configured for SSL and all the required license programs are installed, you can test the SSL connection. For some applications of IBM AS/400 Client Access Express it is sufficient to check that TCP/IP is listening for the correct port number.

6.2.5.1 Testing Operations Navigator for SSL

The following steps show how you can verify that Operations Navigator is communicating over SSL with the AS/400 host servers.

1. Start the Operations Navigator on the PC.

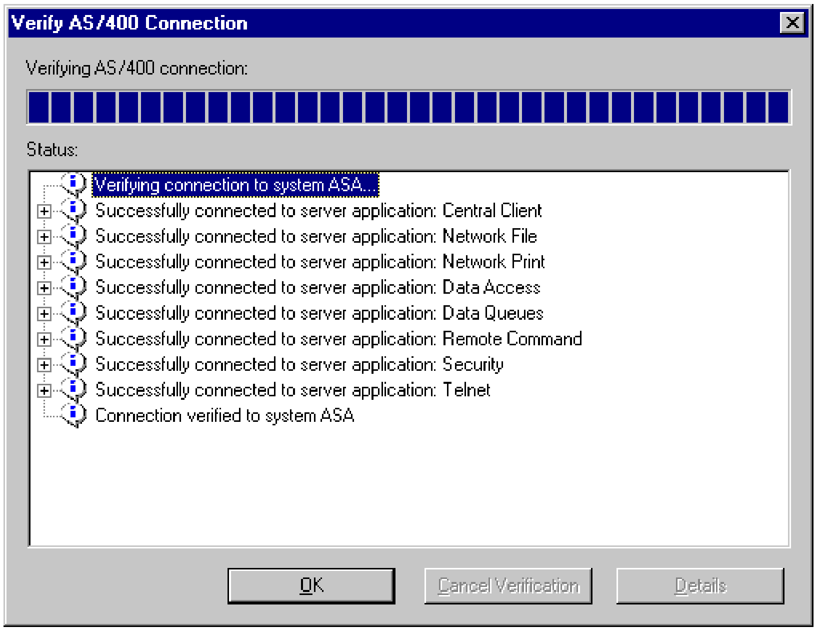


Name	Signed On User	Description
Asa		Manage this AS/400.
Asb		Manage this AS/400.
Asc		Manage this AS/400.

Verify connection to AS/400 system

Figure 193. Verify connection

2. Right-click the **AS/400 Connection** configured for SSL and select **Verify Connection**.

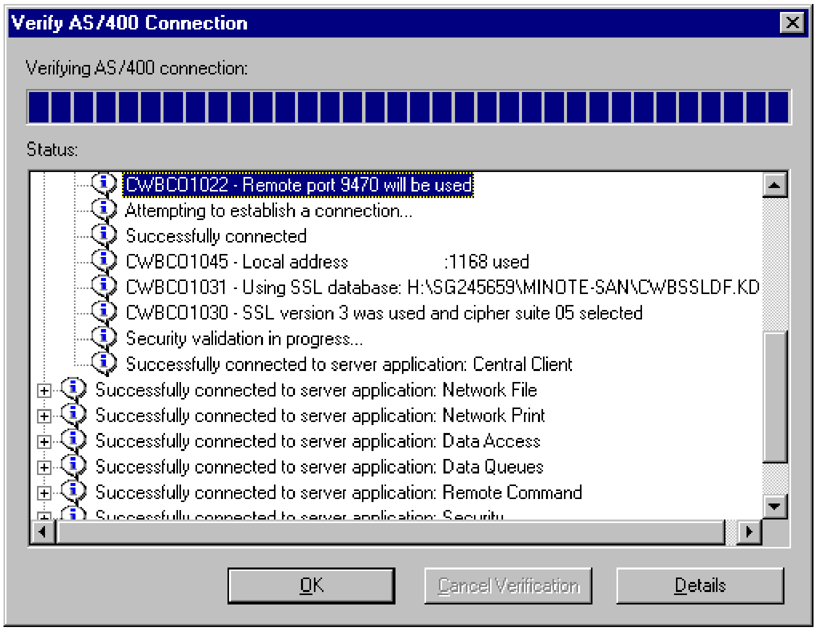


Verifying connection to system ASA...
Successfully connected to server application: Central Client
Successfully connected to server application: Network File
Successfully connected to server application: Network Print
Successfully connected to server application: Data Access
Successfully connected to server application: Data Queues
Successfully connected to server application: Remote Command
Successfully connected to server application: Security
Successfully connected to server application: Telnet
Connection verified to system ASA

Figure 194. Verify AS/400 connection results

3. The Verify AS/400 Connection window is displayed, and automatically verifies the various server connections using the SSL ports of the host servers.

4. Expand the verify result message line. The detailed messages are displayed.



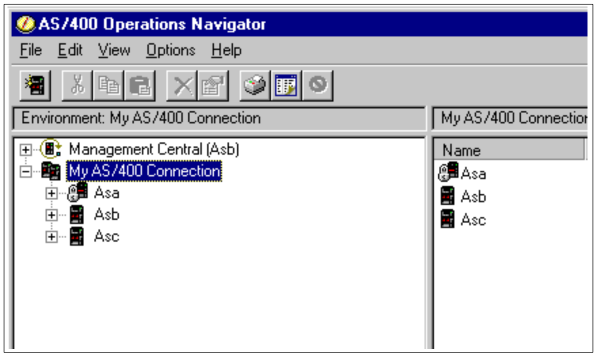
CWBCO1022 - Remote port 9470 will be used
Attempting to establish a connection...
Successfully connected
CWBCO1045 - Local address :1168 used
CWBCO1031 - Using SSL database: H:\SG245659\MINOTE-SAN\CWBSSLDF.KD
CWBCO1030 - SSL version 3 was used and cipher suite 05 selected
Security validation in progress...
Successfully connected to server application: Central Client
Successfully connected to server application: Network File
Successfully connected to server application: Network Print
Successfully connected to server application: Data Access
Successfully connected to server application: Data Queues
Successfully connected to server application: Remote Command
Successfully connected to server application: Security

Figure 195. Verify AS/400 Connection status detail

5. Be sure that all host servers, except the Port Mapper, are using SSL. Refer to Table 4 on page 188 for the port numbers used by the AS/400 host servers for SSL connections.

6. Click **OK** to close the Verify Connection window.

7. Check the padlock icon that represents your AS/400.



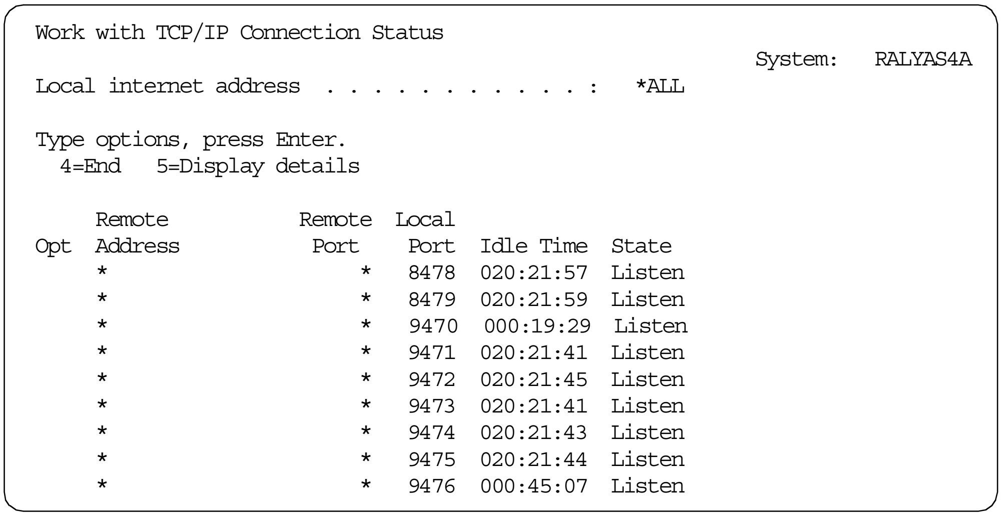
AS/400 Operations Navigator
File Edit View Options Help
Environment: My AS/400 Connection
My AS/400 Connectior
Management Central (Asb)
My AS/400 Connection
Asa
Asb
Asc
Name
Asa
Asb
Asc

Figure 196. AS/400 connection icon with padlock symbol

AS/400 connections configured for SSL have a padlock icon, indicating that this is a secured connection.

8. Another way to check that the AS/400 host servers are configured for SSL is to check the port number they are listening to.

   Use the command `NETSTAT OPTION(*CNN)` on your AS/400 command prompt.



```
Work with TCP/IP Connection Status
                                                            System:   RALYAS4A
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote          Remote  Local
Opt  Address          Port    Port  Idle Time  State
     *                    *   8478  020:21:57  Listen
     *                    *   8479  020:21:59  Listen
     *                    *   9470   000:19:29  Listen
     *                    *   9471  020:21:41  Listen
     *                    *   9472  020:21:45  Listen
     *                    *   9473  020:21:41  Listen
     *                    *   9474  020:21:43  Listen
     *                    *   9475  020:21:44  Listen
     *                    *   9476  000:45:07  Listen
```

Figure 197. Work with TCP/IP Connection Status.

Make sure that the port numbers from 9470 to 9476 are in the status `Listen`. Refer to Table 4 on page 188 for the list of port numbers and associated host servers.

6.2.5.2 Testing file transfer for SSL

Perform the following steps to verify that the application is configured for SSL and that it is using SSL for the communication between the client and the server.

1. Use the AS/400 command `NETSTAT *CNN` to check that port number 9471 is in Listen state. The IBM AS/400 Client Access Express file transfer function is using port 9471 for secured communication.
2. Perform a file transfer and check with the AS/400 command `NETSTAT *CNN` that the session from the client IP address is using a connection for local port 9471.

6.2.5.3 Testing ODBC for SSL

Perform the following steps to verify that the application is configured for SSL and that it is using SSL for the communication between the client and the server.

1. Use the AS/400 command `NETSTAT *CNN` to check that port number 9471 is in Listen state. The IBM AS/400 Client Access Express ODBC function is also using port 9471 for secured communication.
2. Use ODBC to access data on the AS/400 system and check with the AS/400 command `NETSTAT *CNN` that the session from the client IP address is using a connection for local port 9471.

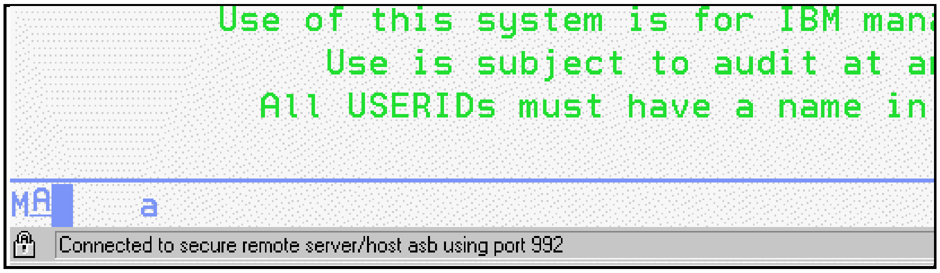
6.2.5.4 Testing 5250 emulation for SSL

Perform the following steps to verify that the application is configured for SSL and that it is using SSL for the communication between the client and the server.

1. Use the AS/400 command `NETSTAT *CNN` to check that port number 992 is in Listen state. The 5250 Telnet server is using port 992 for secured communication.

2. Start a 5250 emulator session and check with the AS/400 command `NETSTAT *CNN` that the session from the client IP address is using a connection for local port 992.

   In addition a secured Telnet session can also be verified by looking at the status bar of the emulator window. A padlock and an appropriate message in the status bar indicate that the connection is protected using the SSL protocol.



```
Use of this system is for IBM mana
     Use is subject to audit at a
  All USERIDs must have a name in
MA      a
Connected to secure remote server/host asb using port 992
```

Figure 198. PC5250 using an SSL connection

6.3 Enabling SSL for Management Central

Management Central with SSL support is available only on AS/400 systems that have installed OS/400 V4R4 or higher. This section provide the steps necessary to enable SSL for Management Central. However, detailed information about SSL support for Management Central can be found in *Management Central: A Smart Way to Manage AS/400 Systems*, SG24-5407.

Management Central can use two authentication levels:

- Server authentication

  This allows the Management Central system (SSL client) to authenticate the server certificate.

- Client and server authentication

  This allows the central system and the endpoint system to authenticate each other's certificates for CA authenticity. However, the Operations Navigator does not support client and server authentication using SSL. This authentication is used between the central AS/400 system and the endpoint AS/400 system that is managed by the central system.

There are two environment variables that Management Central refers to when establishing a SSL connection. They are:

QYPS_SSL

QYPS_AUTH_LEVEL

The Management Central server refers to these variables when they establish a connection between peer systems. Table 5 lists the possible values and port numbers.

Table 5. Environment variable and port number

Connection	QYPS_SSL	QYPS_AUTH_LEVEL	Port number	Service name
No SSL	0	0	5555	as-mgtctrl
Server authentication	1	1	5566	as-mgtctrl-ss
Client and server authentication	1	2	5577	as-mgtctrl-cs

6.3.1 Implementation tasks overview

The following list summarizes the various steps that need to be performed to enable SSL for Management Central communications.

1. Make sure that you have all of the required products installed.

   Refer to 6.3.3, "Prerequisites" on page 212 for the list of license programs.

2. Prepare a CA certificate and server certificate.

   Refer to Chapter 5, "Digital Certificate Manager for AS/400" on page 107.

3. Set up the Client Access Express servers and the Management Central server on your central and endpoint AS/400 systems to use SSL.
4. Set up IBM AS/400 Client Access Express and Management Central on each of your client PCs you want to use for Management Central tasks.

6.3.2 Objective

The objective of this section is to show how to configure Management Central to use SSL. The authentication type is server authentication. Figure 199 shows an overview of the environment discussed in this section.

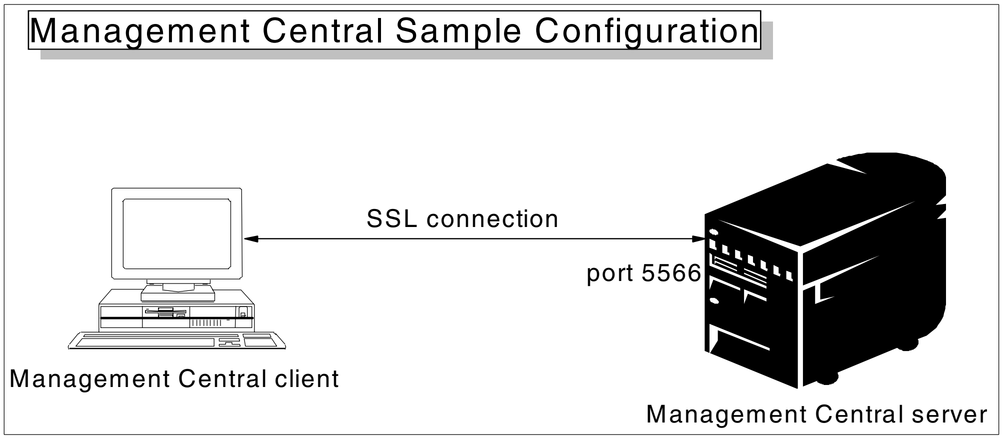

Management Central Sample Configuration
SSL connection
port 5566
Management Central client
Management Central server

Figure 199. Management Central sample configuration

6.3.3 Prerequisites

The following AS/400 license programs must be installed for this scenario:

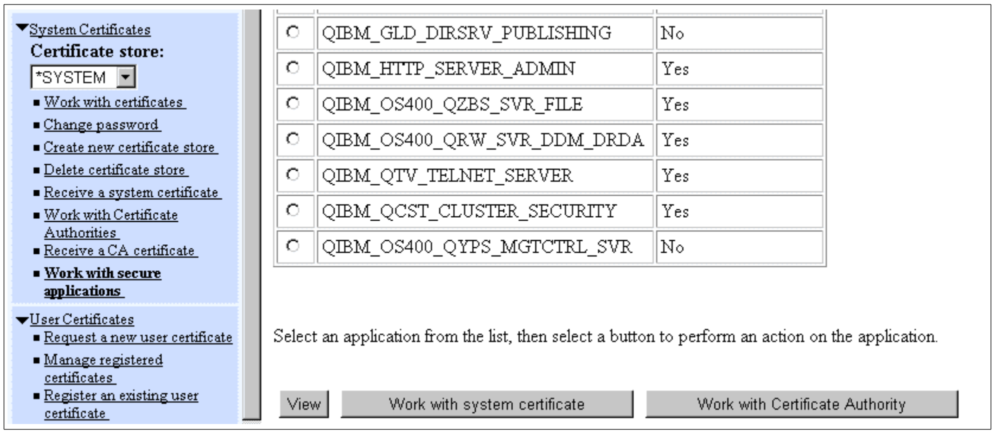
- 5769-SS1 option 34 OS/400 - Digital Certificate Manager
- 5769-DG1 IBM HTTP Server for AS/400

- Either 5769-AC1,2,3 Crypto Access Provider for AS/400
- 5769-XE1 Client Access/400 Express for Windows
- 5769-TC1 TCP/IP Connectivity Utilities for AS/400

6.3.4 Configuring the AS/400 system

You must associate a server certificate with the Management Central application ID. All AS/400 systems that are participating in the Management Central network and that have V4R4 or higher installed, must have a server certificate assigned to the Management Central server. This includes the central and the endpoint systems. Perform the following steps:

1. Start DCM.
2. Click **System Certificates**.
3. Enter the *SYSTEM certificate store and its password.
4. Click **Work with secure applications**.

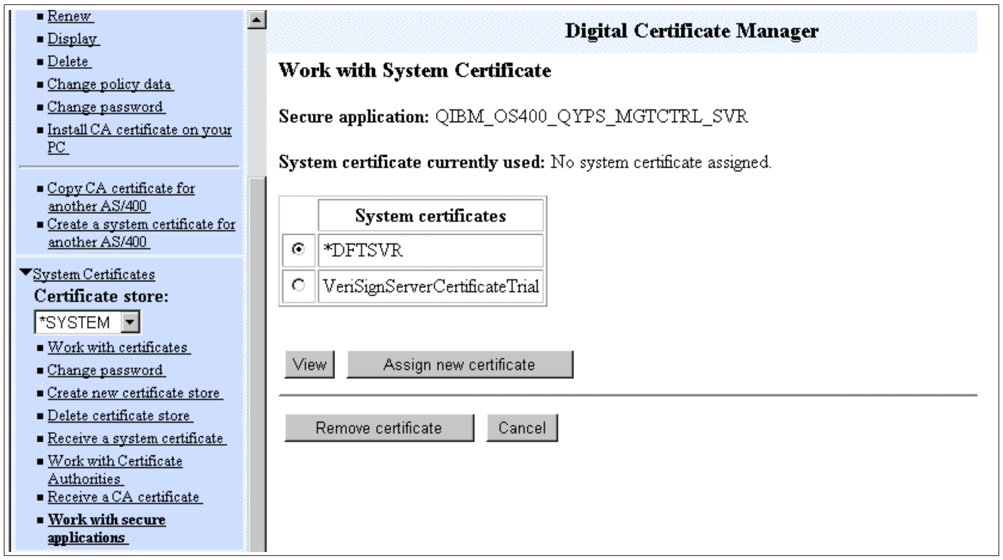

System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Request a new user certificate
Manage registered certificates
Register an existing user certificate
View
Work with system certificate
Work with Certificate Authority

○	QIBM_GLD_DIRSRV_PUBLISHING	No
○	QIBM_HTTP_SERVER_ADMIN	Yes
○	QIBM_OS400_QZBS_SVR_FILE	Yes
○	QIBM_OS400_QRW_SVR_DDM_DRDA	Yes
○	QIBM_QTV_TELNET_SERVER	Yes
○	QIBM_QCST_CLUSTER_SECURITY	Yes
○	QIBM_OS400_QYPS_MGTCTRL_SVR	No

Select an application from the list, then select a button to perform an action on the application.

Figure 200. Work with secure applications

5. Select the application ID **QIBM_OS400_QYPS_MGTCTRL_SVR.**
6. Click **Work with system certificate**.


Renew
Display
Delete
Change policy data
Change password
Install CA certificate on your PC
Copy CA certificate for another AS/400
Create a system certificate for another AS/400
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
View
Assign new certificate
Remove certificate
Cancel

Digital Certificate Manager

Work with System Certificate

Secure application: QIBM_OS400_QYPS_MGTCTRL_SVR

System certificate currently used: No system certificate assigned.

	System certificates
●	*DFTSVR
○	VeriSignServerCertificateTrial

Figure 201. Work with System Certificate window

7. Select the certificate from the list that you want Management Central to use to establish SSL connections between AS/400 systems.

8. Click **Assign new certificate**.

9. DCM displays a confirmation message. Click **OK**.

10. Restart the Management Central server.

    You have to restart the Management Central server application to activate the changes by using the following commands:

    To stop: `ENDTCPSVR SERVER(*MGTC)`

    To start: `STRTCPSVR SERVER(*MGTC)`

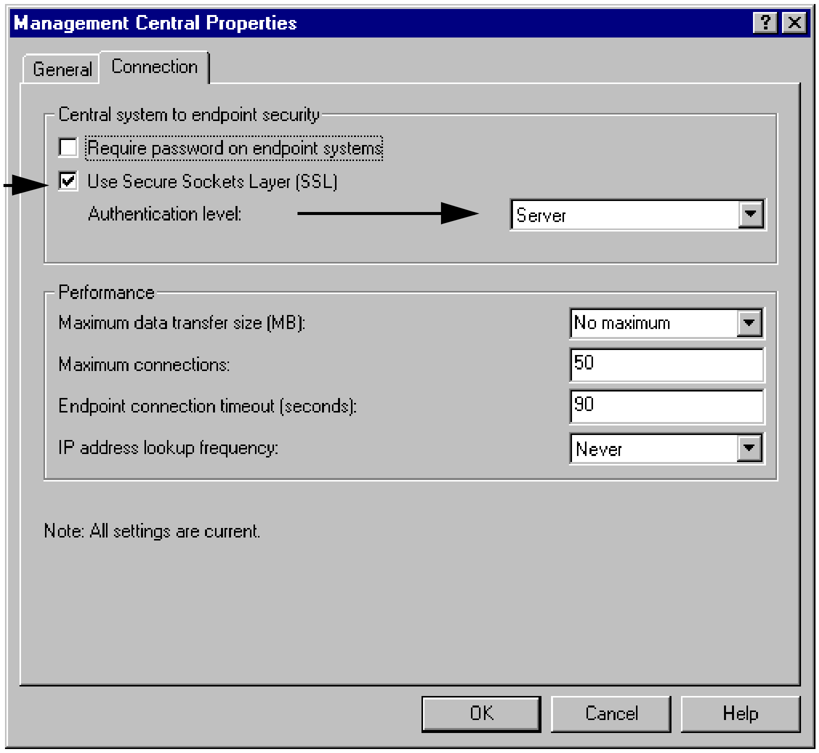
11. Repeat the steps until the central and all endpoint systems have a server certificate assigned to the Management Central server.

6.3.5 Configuring Management Central

Configure the Management Central server to use SSL and Server Authentication:

1. In AS/400 Operations Navigator, right-click **Management Central** and select **Properties**.

2. Click the **Connection** tab.



Management Central Properties

General | Connection

Central system to endpoint security

□ Require password on endpoint systems

☑ Use Secure Sockets Layer (SSL)

Authentication level: Server

Performance

Maximum data transfer size (MB): No maximum

Maximum connections: 50

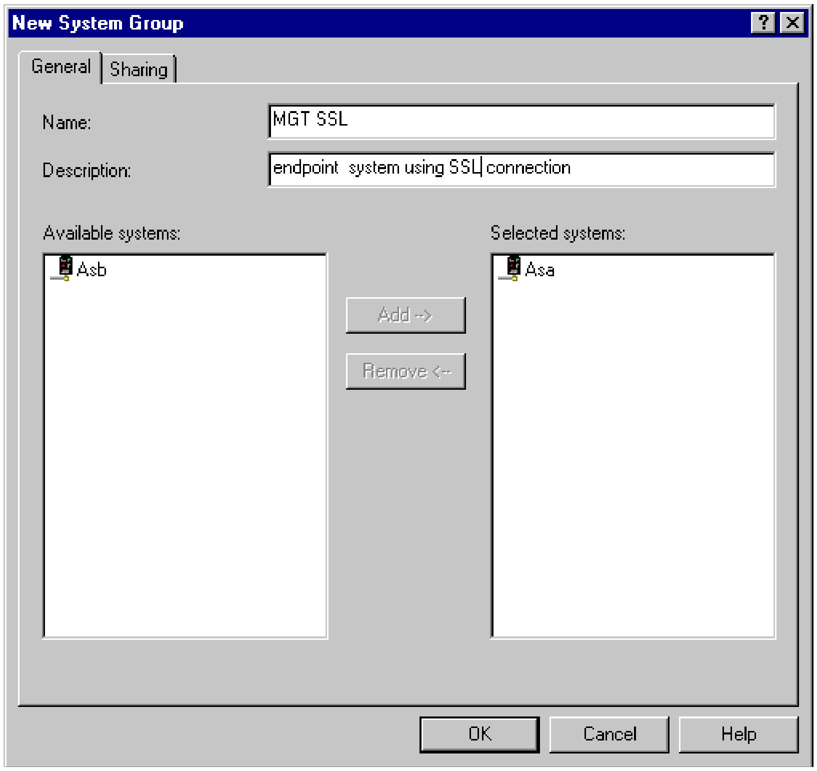
Endpoint connection timeout (seconds): 90

IP address lookup frequency: Never

Note: All settings are current.

Figure 202. Management Central Properties

3. Select **Use Secure Sockets Layer (SSL)**.
4. For the Authentication level, specify **Server**.
5. Click **OK** to set the value on the central system. Note that all endpoint systems need to be explicitly configured for using SSL.
6. In AS/400 Operations Navigator, expand **Management Central**.
7. Right-click **AS/400 System Groups** and select **New System Group.**



Name: MGT SSL

Description: endpoint system using SSL connection

Available systems: Asb

Selected systems: Asa

Figure 203. New System Group

8. Define a new system group that includes all AS/400 endpoint systems to which you want to connect using SSL, and click **OK**.

   Refer to *Management Central: A Smart Way to Manage AS/400 Systems*, SG24-5407 for special considerations if you still have V4R3 systems in your network.

9. Refresh the list of system groups to display your new group.

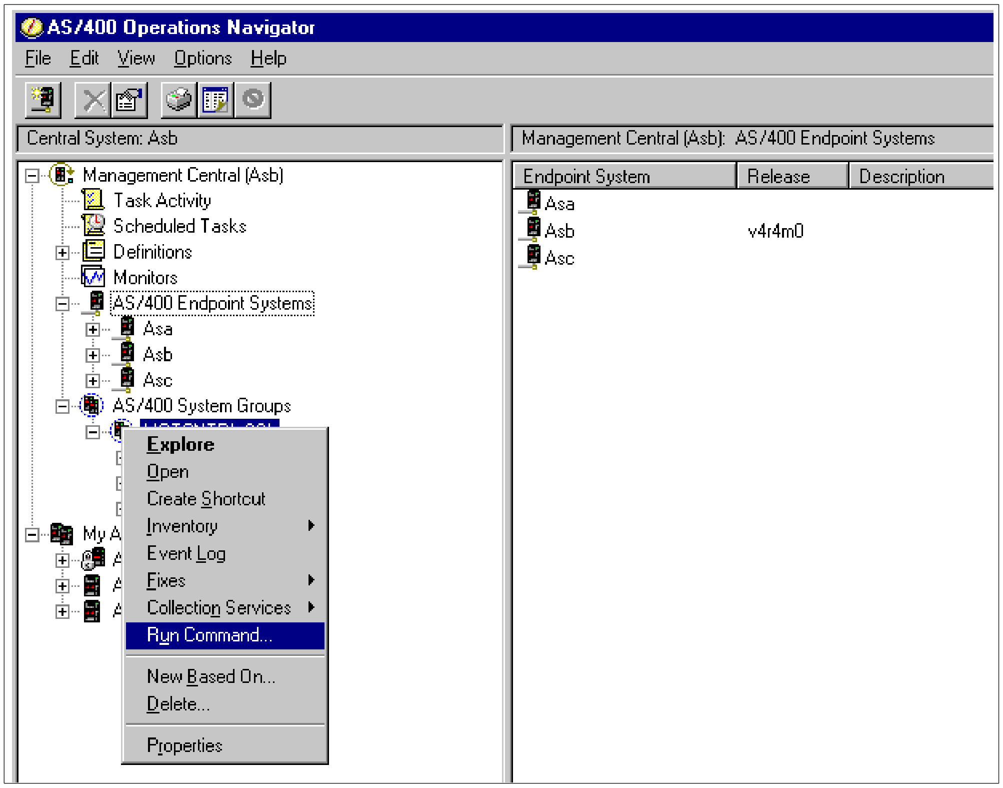
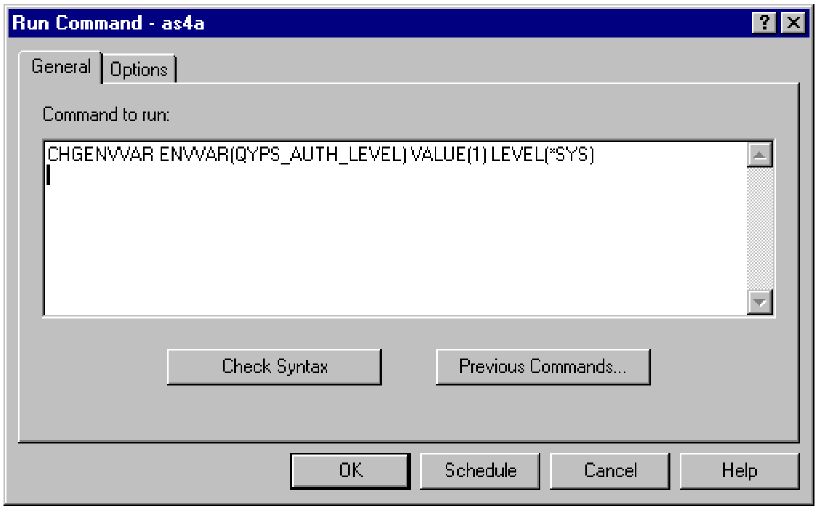


Figure 204. Run command through Management Central

10.Right-click the new system group you have created and select **Run Command**.



```
CHGENVVAR ENVVAR(QYPS_AUTH_LEVEL) VALUE(1) LEVEL(*SYS)
```

Figure 205. Run Command window

11.Enter the following command to be performed on the system:

```
CHGENVVAR ENVVAR(QYPS_AUTH_LEVEL) VALUE(1) LEVEL(*SYS)
```

This command actually changes the Management Central server's authentication behavior.

If you use Management Central the first time on an endpoint system, the environment variable QYPS_AUTH_LEVEL does not exist. Therefore, you need to run the following command on those systems:

```
ADDENVVAR ENVVAR(QYPS_AUTH_LEVEL) VALUE('1') LEVEL(*SYS)
```

If you fail to add the environment variable first, the Task Activity report of Management Central shows the Run Command action as Failed.

You may also encounter communication problems in the Task Activity report when you do not follow exactly the order of configuring and restarting Management Central.

12. Click **OK**.

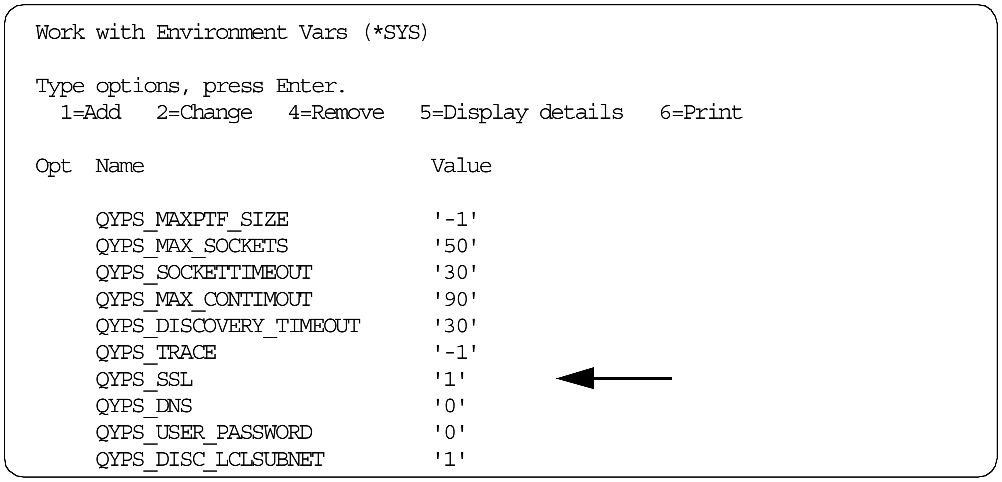
    The Management Central client sends this command to all AS/400 systems that are defined in this endpoint group.

6.3.6 Verifying a SSL connection

Perform the following steps to verify that Management Central is correctly configured for SSL and that it is using SSL for the communication between the central and the endpoint system.

1. Use the AS/400 command `NETSTAT *CNN` to check that port numbers 5555, 5566, and 5577 are in Listen state. Refer to Table 5 on page 212 for the description of each port.
2. Be sure that the environment variables are set correctly. Use the following command on all systems that are in the Management Central network:

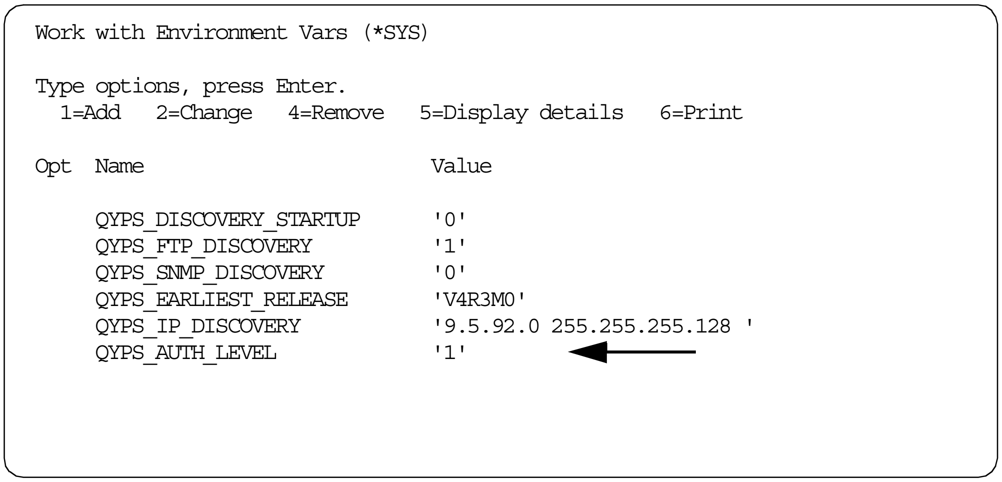
   ```
   WRKENVVAR LEVEL(*SYS)
   ```



```
Work with Environment Vars (*SYS)

Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display details   6=Print

Opt  Name                        Value

     QYPS_MAXPTF_SIZE            '-1'
     QYPS_MAX_SOCKETS            '50'
     QYPS_SOCKETTIMEOUT          '30'
     QYPS_MAX_CONTIMOUT          '90'
     QYPS_DISCOVERY_TIMEOUT      '30'
     QYPS_TRACE                  '-1'
     QYPS_SSL                    '1'
     QYPS_DNS                    '0'
     QYPS_USER_PASSWORD          '0'
     QYPS_DISC_LCLSUBNET         '1'
```

Figure 206. WRKENVVAR (1 of 2)

Make sure the Environment variable `QYPS_SSL` is set to 1 and scroll forward until the QYPS_AUTH_LEVEL variable is shown.

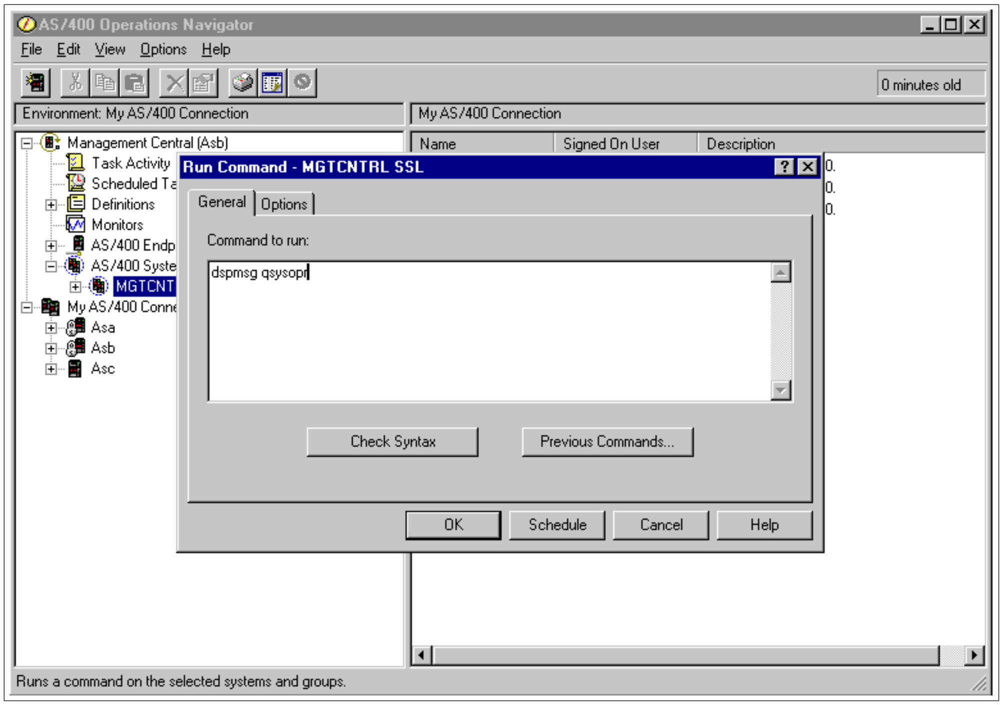


```
Work with Environment Vars (*SYS)

Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display details   6=Print

Opt  Name                        Value

     QYPS_DISCOVERY_STARTUP      '0'
     QYPS_FTP_DISCOVERY          '1'
     QYPS_SNMP_DISCOVERY         '0'
     QYPS_EARLIEST_RELEASE       'V4R3M0'
     QYPS_IP_DISCOVERY           '9.5.92.0 255.255.255.128 '
     QYPS_AUTH_LEVEL             '1'
```

Figure 207. WRKENVVAR (2 of 2)

Make sure the Environment variable QYPS_AUTH_LEVEL is set to 1 (Server Authentication).

3. To verify that the central system is communicating with the endpoint system using SSL, you have to run a Management Central task. The easiest way is to use again the Run Command option as shown in Figure 208.

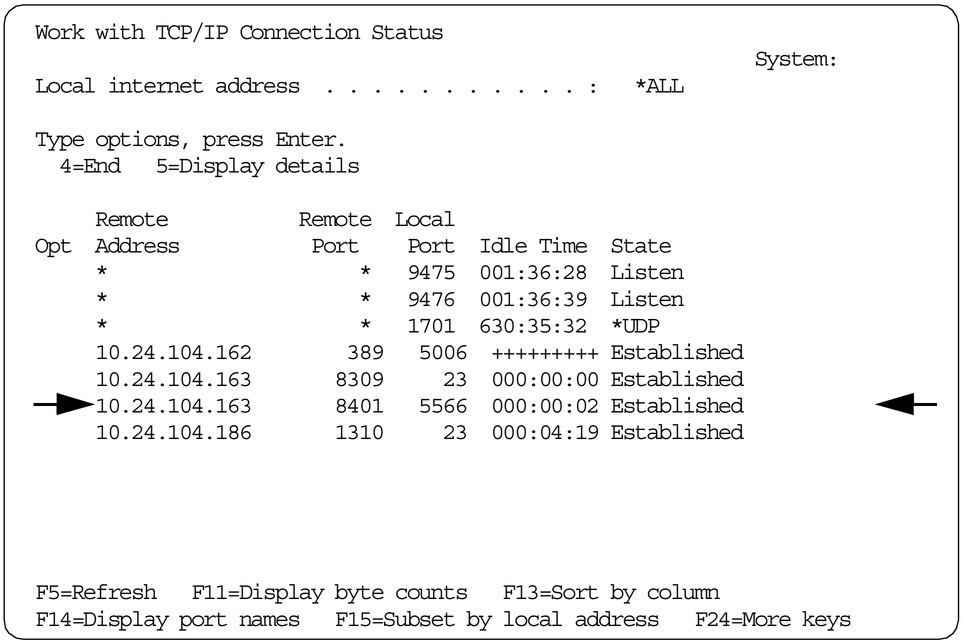


Command to run: dspmsg qsysopr

Figure 208. Run Command for SSL verification

4. Enter the command DSPMSG QSYSOPR and click **OK**.

5. Check on each system in the Management Central network that the port for SSL is being used for running the command. Use the AS/400 system command NETSTAT *CNN again to verify the correct port.



```
Work with TCP/IP Connection Status
                                                              System:
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote  Local
Opt  Address           Port    Port  Idle Time  State
     *                     *   9475  001:36:28  Listen
     *                     *   9476  001:36:39  Listen
     *                     *   1701  630:35:32  *UDP
     10.24.104.162       389   5006  +++++++++ Established
     10.24.104.163      8309     23  000:00:00 Established
     10.24.104.163      8401   5566  000:00:02 Established
     10.24.104.186      1310     23  000:04:19 Established




F5=Refresh   F11=Display byte counts   F13=Sort by column
F14=Display port names   F15=Subset by local address   F24=More keys
```

If port 5566 is shown as the local port on the endpoint system and the remote port on the central system and the environment variables are set correctly, SSL with server authentication is used for Management Central connections.

6.4 Enabling SSL for LDAP on the AS/400 system

On the AS/400 system you can set up a Lightweight Directory Access Protocol (LDAP) server or you can publish, for example user data, to an LDAP server. The Operations Navigator can access the LDAP server on the AS/400 system using SSL, and the LDAP server on the AS/400 can publish information to another LDAP server using SSL. Also, an LDAP-enabled client such as the Netscape address book application is able to connect to the LDAP server on the AS/400 system using SSL. LDAP with SSL support has been available since OS/400 V4R3. The following table shows the port numbers used for LDAP connections:

Table 6. The LDAP server port numbers

Connection	Port number	Service name
No SSL	389	not assigned
SSL	636	not assigned

In DCM there are two application IDs related to LDAP on the AS/400 system:

QIBM_GLD_DIRSRV_SERVER

This application ID is used for the LDAP directory services server. For example, the Netscape address book uses this server to access the LDAP directory.

QIBM_GLD_DIRSRV_PUBLISHING

This application ID is used for directory publishing services, such as publishing directory data to an LDAP server.

6.4.0.1 Implementation tasks overview

To use the LDAP services with SSL, you must perform these tasks:

1. Be sure that you have all of the required license programs installed.

   Refer to 6.4.2, “Prerequisites” on page 221 for the list of license programs.

2. Prepare a CA certificate and server certificate.

   Refer to Chapter 5, “Digital Certificate Manager for AS/400” on page 107.

3. Set up IBM AS/400 Client Access Express to use SSL.

   This is an optional task and may be used to protect the configuration traffic between the IBM AS/400 Client Access Express and the AS/400 system. Refer to 6.2, “Enabling SSL for IBM AS/400 Client Access Express” on page 187 to set up SSL for IBM AS/400 Client Access Express.

4. Set up the LDAP servers on your AS/400 system to use SSL.

5. Set up the Netscape address book to access the AS/400 LDAP server.

   This is an optional task to prove that SSL can be used by an LDAP client to access the directory on an LDAP server.

6.4.1 Objective

The objective of this section is to show you how to configure the LDAP server to use SSL. The scenario is that the Operations Navigator connects to the LDAP server on the AS/400 system with SSL and an LDAP-enabled client such as the Netscape address book application connects to the LDAP server on the AS/400 system also using SSL.

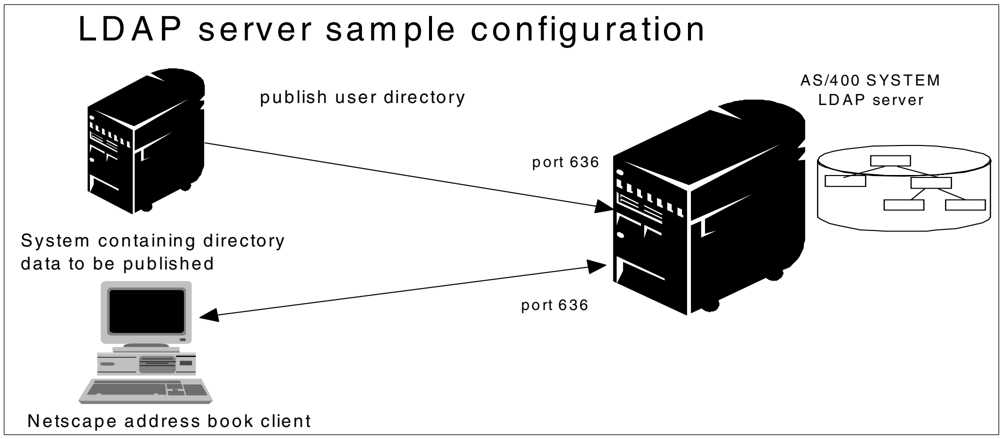

LDAP server sample configuration
publish user directory
AS/400 SYSTEM
LDAP server
port 636
System containing directory
data to be published
port 636
Netscape address book client

Figure 209. LDAP server sample configuration

6.4.2 Prerequisites

The following license programs must be installed for this scenario:

AS/400 license programs

- 5769 SS1 option 34 OS/400 - Digital Certificate Manager
- 5769 SS1 option 32 OS/400 - Directory Services
- 5769 DG1 IBM HTTP Server for AS/400
- Either 5769 AC1,2,3 Crypto Access Provider for AS/400

- Either 5769 CE1,2,3 Client Encryption (optional)
- 5769 XE1 Client Access/400 Express for Windows

PC programs

- Netscape Communicator

6.4.3 Configuring the AS/400 system

To enable SSL for LDAP services on the AS/400 system, you have to perform several tasks. In the first task you have to assign server certificates to the LDAP servers. There are two application IDs in DCM related to LDAP that can have a certificate assigned to them. Once a certificate is assigned to the LDAP server, the server is automatically enabled for SSL. The second task is to configure the LDAP publishing services for SSL.

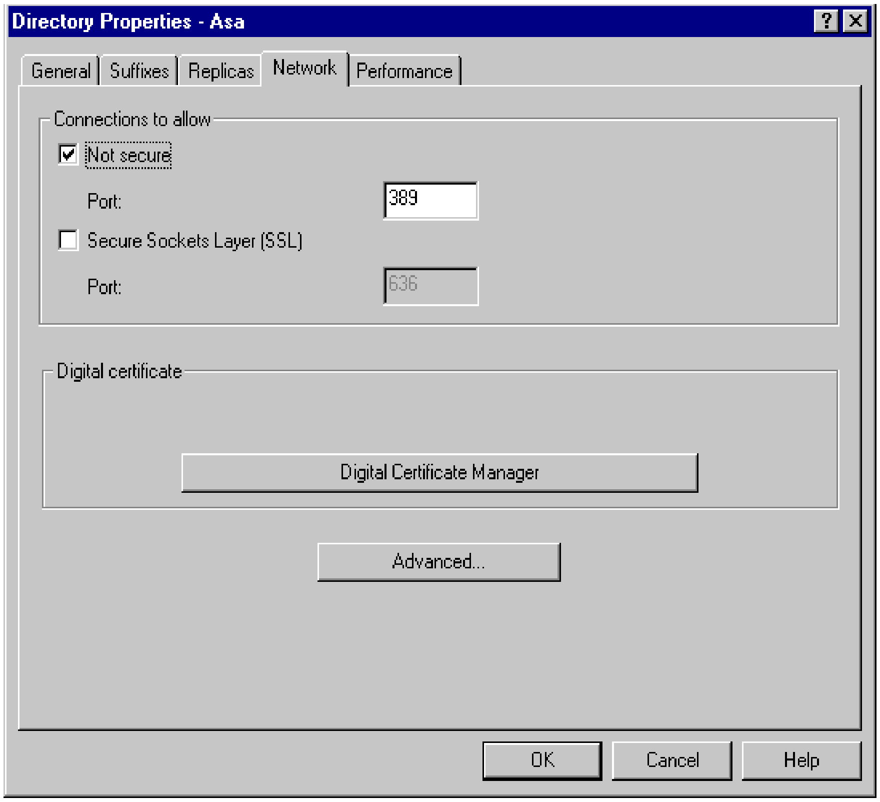
6.4.4 Assigning a server certificate to the LDAP server

To assign a server certificate to your LDAP server, use the Digital Certificate Manager interface. You can launch the Digital Certificate Manager using one of the following methods:

- From the Internet folder in Operations Navigator
- From the Network window of the directory server's Properties dialog
- From the AS/400 Tasks page

To launch it from the Network window, follow these steps:

1. In Operations Navigator, expand **Network** -> **Servers** -> **TCP/IP**.
2. Right-click **Directory** and select **Properties**.
3. Click the **Network** tab.



Connections to allow

☑ Not secure

Port: 389

□ Secure Sockets Layer (SSL)

Port: 636

Digital certificate

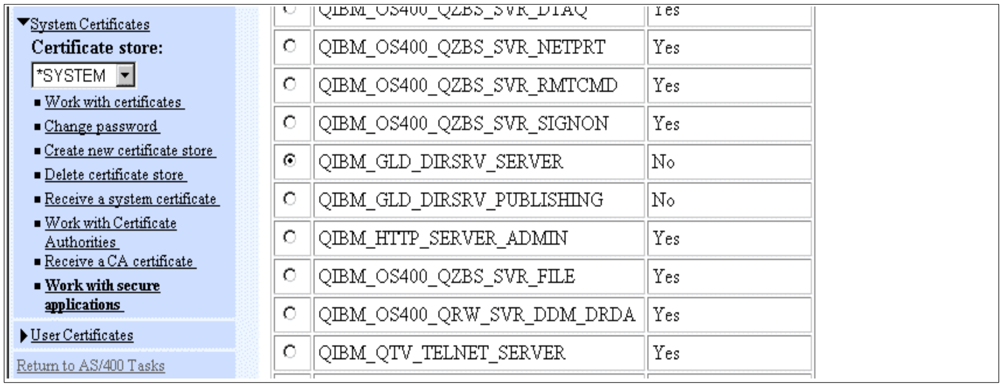
Figure 210. Directory Properties

4. Click the **Digital Certificate Manager** button.

   Digital Certificate Manager will launch in your default Internet browser.

5. Click **System Certificates**.

6. Click **Work with secure applications**.



Certificate store: *SYSTEM

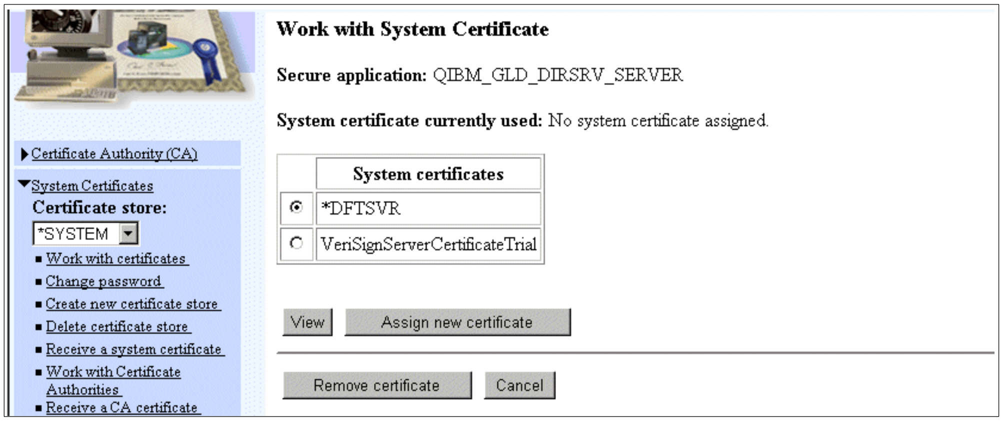
○	QIBM_OS400_QZBS_SVR_DTAQ	Yes
○	QIBM_OS400_QZBS_SVR_NETPRT	Yes
○	QIBM_OS400_QZBS_SVR_RMTCMD	Yes
○	QIBM_OS400_QZBS_SVR_SIGNON	Yes
●	QIBM_GLD_DIRSRV_SERVER	No
○	QIBM_GLD_DIRSRV_PUBLISHING	No
○	QIBM_HTTP_SERVER_ADMIN	Yes
○	QIBM_OS400_QZBS_SVR_FILE	Yes
○	QIBM_OS400_QRW_SVR_DDM_DRDA	Yes
○	QIBM_QTV_TELNET_SERVER	Yes

Figure 211. Work with Secure Applications window

7. Select the application ID **QIBM_GLD_DIRSRV_SERVER.**

   Note that once the certificate is assigned to the application ID QIBM_GLD_DIRSRV_SERVER, the LDAP server is automatically enabled for SSL. To change the SSL port used by the LDAP server, refer to 6.4.5, “Configuring LDAP services for SSL” on page 224.

8. Click **Work with system certificate**.



Work with System Certificate

Secure application: QIBM_GLD_DIRSRV_SERVER

System certificate currently used: No system certificate assigned.

	System certificates
●	*DFTSVR
○	VeriSignServerCertificateTrial

Figure 212. Work with System Certificate window

9. Select the certificate from the list that you want the LDAP server to use to establish SSL connections.

10. Click **Assign new certificate**.

11. DCM displays a confirmation message. Click **OK**.

12. If you want to publish directory information to another LDAP server over SSL, you must also assign a certificate to the application ID QIBM_GLD_DIRSRV_PUBLISHING . This also includes publishing directory data from the AS/400 system on which the LDAP server is running. To do this, repeat the steps taken for assigning the certificate to QIBM_GLD_DIRSRV_SERVER.

13. Restart the LDAP server.

    To reflect these changes to the LDAP server, you must restart it using the following commands:

    To stop: `ENDTCPSVR SERVER(*DIRSVR)`

    To start: `STRTCPSVR SERVER(*DIRSVR)`

    You can also restart the server through the Operations Navigator using the path **Network->Servers->TCP/IP->Directory**.

Note

When restarting the LDAP server on the AS/400 system, be sure that there is no active connection for port 389 (if SSL was already enabled, check also for port 636) using the AS/400 command `NETSTAT *CNN`. If there is still a connection active for one of the ports, the LDAP server will end automatically after restart.

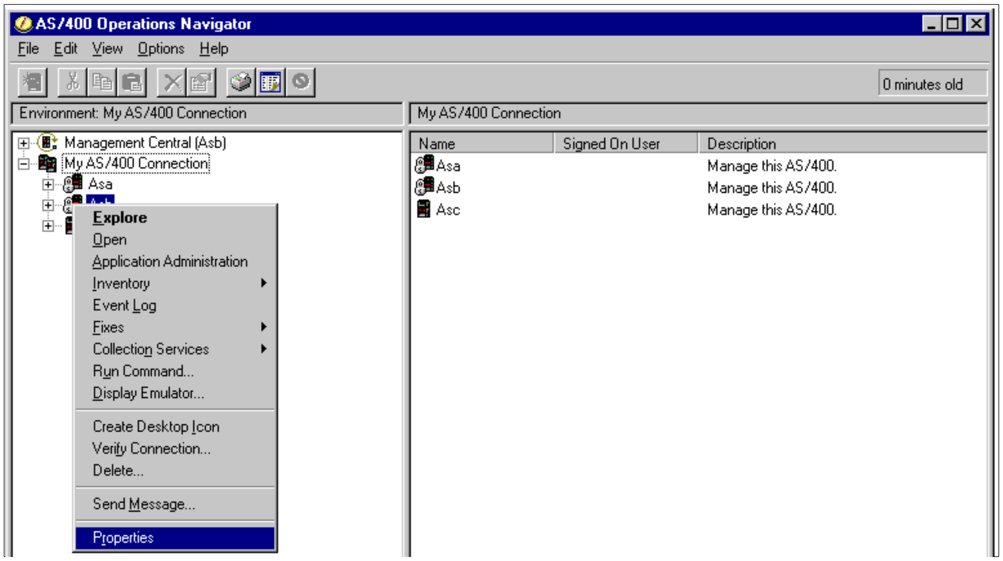
6.4.5 Configuring LDAP services for SSL

There are two LDAP services that can be configured for SSL. These are the LDAP server and the publishing server. If you want to use the AS/400 system only as an LDAP server, you only have to configure the LDAP server for SSL and not the publishing server and vice versa. That means that either the LDAP server, the publishing server, or both can be configured for SSL connections.

6.4.5.1 Configure the LDAP publishing services for SSL

To configure the LDAP publishing services from Operations Navigator, perform the following steps:

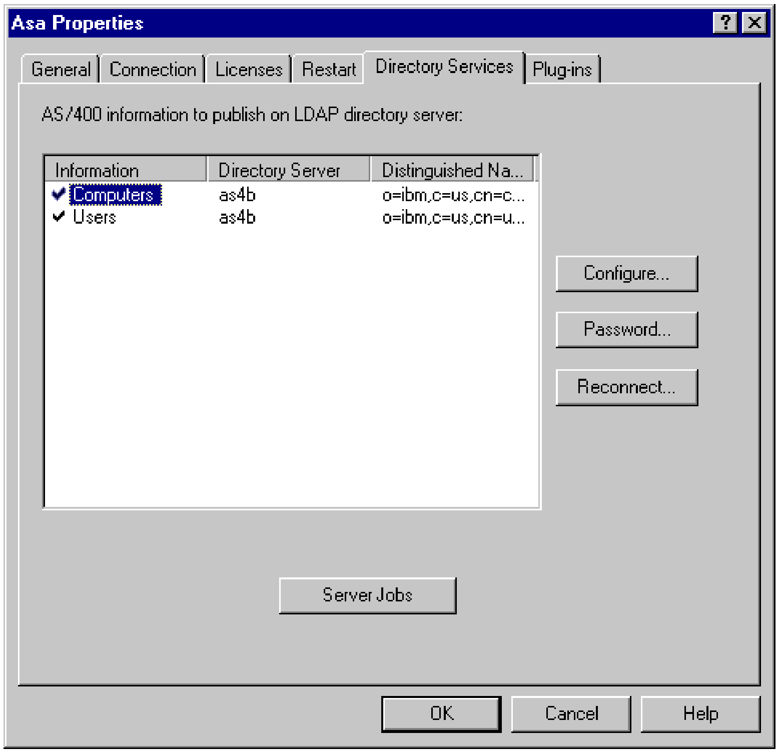
1. Start the Operations Navigator.
2. Right-click your **AS/400 Connection** and select **Properties**.



Name	Signed On User	Description
Asa		Manage this AS/400.
Asb		Manage this AS/400.
Asc		Manage this AS/400.

Figure 213. Operations Navigator - connection properties

3. Select the **Directory Services** tab.

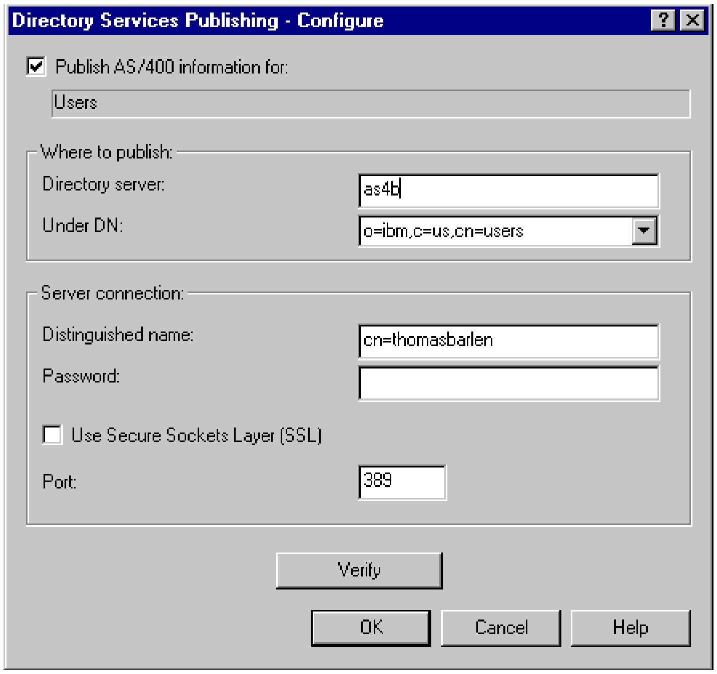


AS/400 information to publish on LDAP directory server:

Information	Directory Server	Distinguished Na...
✓ Computers	as4b	o=ibm,c=us,cn=c...
✓ Users	as4b	o=ibm,c=us,cn=u...

Figure 214. Directory Services properties

4. Select the information to be published and you want to configure SSL for, and click **Configure**.



Directory Services Publishing - Configure

☑ Publish AS/400 information for:

Users

Where to publish:

Directory server: as4b

Under DN: o=ibm,c=us,cn=users

Server connection:

Distinguished name: cn=thomasbarlen

Password:

☐ Use Secure Sockets Layer (SSL)

Port: 389

Figure 215. Directory Services Publishing -Configure window

5. Check **Use Secure Socket Layer (SSL)**.

   The Port number changes automatically from 389 to 636.

6. Click **OK** to save the new settings.

7. Click **OK** to close the properties window.

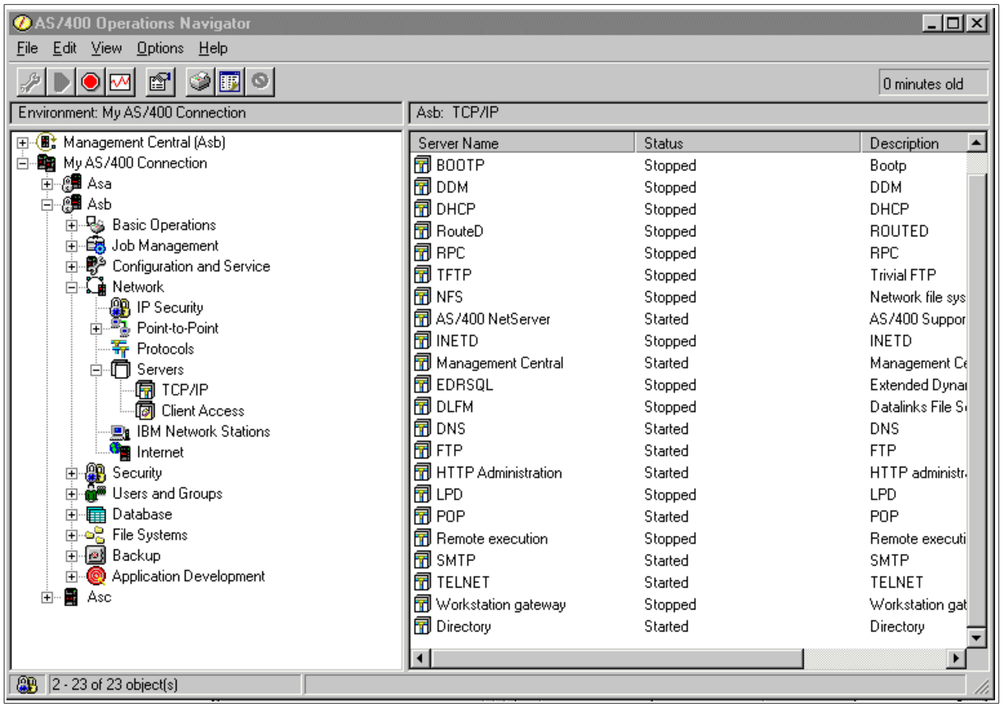
6.4.5.2 Configure the LDAP server for SSL

The LDAP server is automatically enabled for SSL when a certificate is assigned to it and listens by default to the secured port 636. Through the following steps, you can change the SSL port for the LDAP server.

To configure the LDAP server from Operations Navigator, perform the following steps:

1. Start the Operations Navigator.

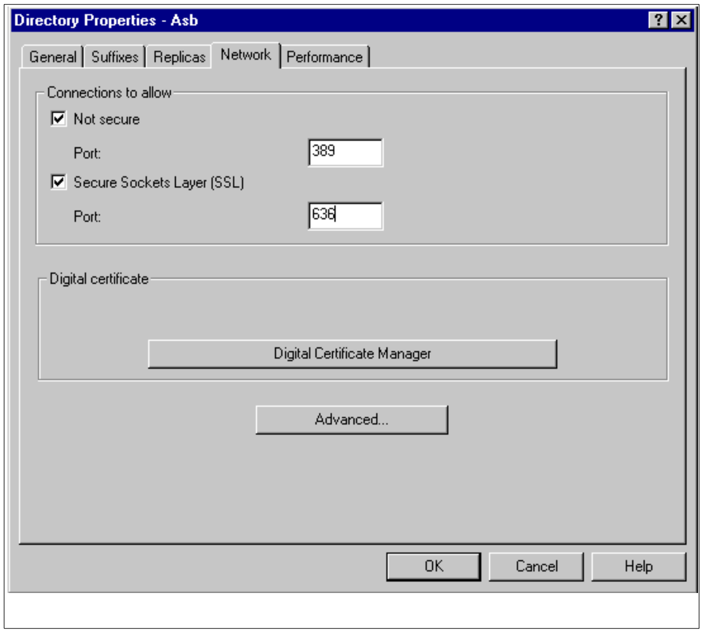
2. Expand the tree on the AS/400 connection you want to configure the LDAP server to **Network->Servers->TCP/IP**.



Server Name	Status	Description
BOOTP	Stopped	Bootp
DDM	Stopped	DDM
DHCP	Stopped	DHCP
RouteD	Stopped	ROUTED
RPC	Stopped	RPC
TFTP	Stopped	Trivial FTP
NFS	Stopped	Network file sys
AS/400 NetServer	Started	AS/400 Suppor
INETD	Stopped	INETD
Management Central	Started	Management Ce
EDRSQL	Stopped	Extended Dynai
DLFM	Stopped	Datalinks File S
DNS	Started	DNS
FTP	Started	FTP
HTTP Administration	Started	HTTP administr
LPD	Stopped	LPD
POP	Started	POP
Remote execution	Stopped	Remote executi
SMTP	Started	SMTP
TELNET	Started	TELNET
Workstation gateway	Stopped	Workstation gat
Directory	Started	Directory

Figure 216. Operations Navigator - Directory server

3. Right-click the **Directory** server and select **Properties**.
4. Click the **Network** tab.
5. Select the port parameter under **Secured Socket Layer (SSL)**.



Connections to allow

☑ Not secure

Port: 389

☑ Secure Sockets Layer (SSL)

Port: 636

Figure 217. Operations Navigator - Directory server properties

6. Change the port number, if you want to use a port other than the well-known port for LDAP SSL connections.

Note

The SSL support for the LDAP server cannot be enabled or disabled from the properties window in OS/400 V4R4 or higher. To enable SSL for the LDAP server you have to assign a certificate to the application ID `QIBM_GLD_DIRSRV_SERVER`. To disable SSL for an LDAP server you have to remove the certificate in DCM from the secured application `QIBM_GLD_DIRSRV_SERVER`.

7. Click **OK** to save the changes.

To activate the changes you have to restart the LDAP server by using the following AS/400 commands:

Stop the server: `ENDTCPSVR SERVER(*DIRSRV)`
Start the server: `STRTCPSVR SERVER(*DIRSRV)`

Remember to check for active LDAP connections using the `NETSTAT *CNN` command. If there is still an active connection, the server will end but does not start again.

6.4.6 Configuring the Netscape address book

You can add additional directory servers to the Netscape address book. This allows you to access, for example an LDAP directory on an AS/400 system. Perform the following steps to add an entry for the AS/400 LDAP server using SSL for secured communication.

1. Launch the Netscape Navigator.
2. Open **Communicator->Address Book**.

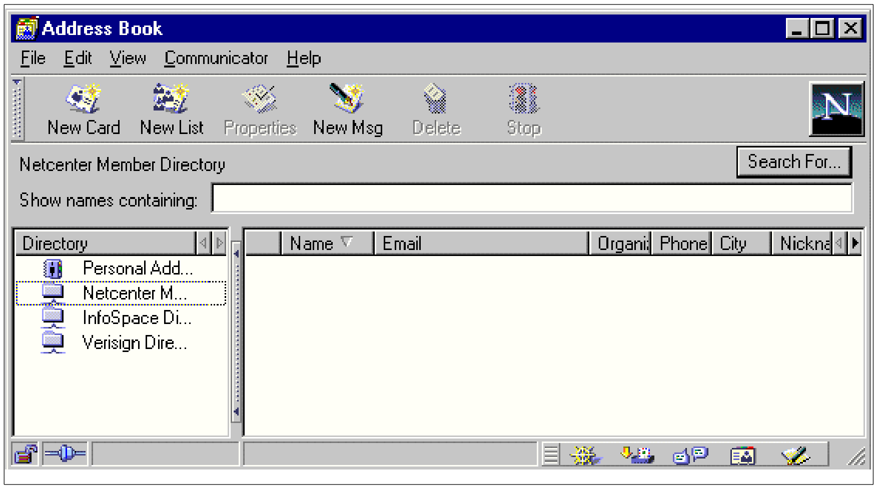
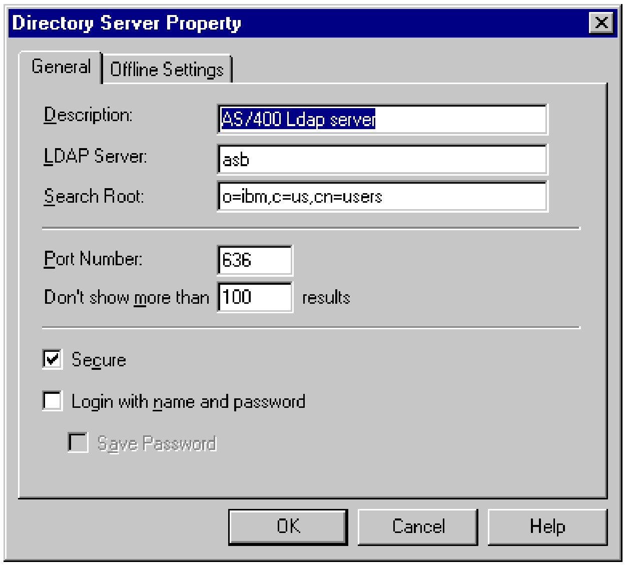


Figure 218. Netscape address book (nonsecure)

3. Click **File->New Directory** to create an entry for the AS/400 LDAP directory.



Description: AS/400 Ldap server

LDAP Server: asb

Search Root: o=ibm,c=us,cn=users

Port Number: 636

Don't show more than 100 results

☑ Secure

☐ Login with name and password

☐ Save Password

Figure 219. Directory Server Properties window

Enter the required parameters as shown in the following table:

Table 7. Netscape address book directory properties

Parameter	Value	Description
Description	AS/400 ASB Directory	Describes the LDAP directory
LDAP Server	ASB	IP address of host name of the LDAP server
Search Root	o=ibm,c=us,cn=users	Directory path containing the user data on the LDAP server
Port number	636	SSL port of the LDAP server
Don’t show more ...	100	Amount of entries to be displayed in the result window
Secure	Enabled	Specifies that the address book uses the SSL protocol to establish a connection to the LDAP server.

4. Click **OK** to save the new entry.

Note that enabling the Secure parameter does not automatically change the port number from 389 to 636. The Login with name and password parameter is only needed when the LDAP directory is protected.

6.4.7 Verifying LDAP connections

The following procedures can be used to determine if the LDAP connections are protected by using the SSL protocol.

6.4.7.1 Checking the LDAP server site

1. Use the `NETSTAT *CNN` command to check that the SSL port which is by default 636 is in the Listen status.

2. When LDAP clients or LDAP publishing systems establish a connection, check that the local port in the NETSTAT display for those connections is 636 (or another port if the LDAP server does not uses the well-known port).

6.4.7.2 Checking on an AS/400 system that publishes directory data

1. Use the `NETSTAT *CNN` command to check that the remote port for the LDAP connection uses port 636 and not 389. The LDAP connection can be identified by the user profile used for this connection and by the remote address. The user profile must be *QDIRSRV*.
2. Check also that the following jobs are running in subsystem QSYSWRK:

   QGLDPUBA

   This job is referred to as a *Publishing Agent*. It is the job that is responsible for publishing information about a system's users and the computer system itself to an LDAP directory. Publishing Agent is a term that could apply to any job that publishes some type of information to a directory; this is just one instance.

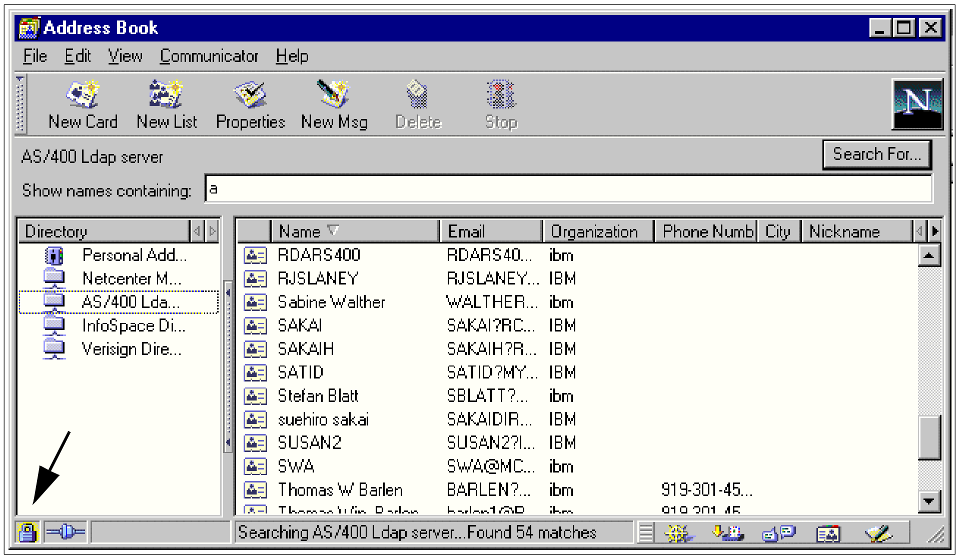
   QGLDPUBE

   This job is referred to as the *Publishing Engine*. It is the job that processes publishing requests made via the QgldPubDirObj API. When a Publishing Agent makes a publishing request, the target LDAP server may or may not be available at that time. This job isolates the business of retrying publishing requests in such a situation in one place, so every Publishing Agent does not have to reinvent that logic.

   If you encounter problems when trying to publish data to an LDAP server, check the joblog of these jobs also.

6.4.7.3 Checking the Netscape address book connection

1. Start the Netscape Communicator.
2. Select **Communicator->Address book** or press CTRL+SHIFT+2 to open the address book. Select the **AS/400 LDAP** directory and enter a name in the **Show names containing** field to initiate the LDAP directory search.



AS/400 Ldap server

Show names containing: a

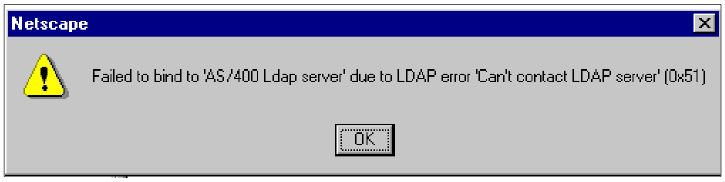
Name	Email	Organization	Phone Numb	City	Nickname
RDARS400	RDARS40...	ibm			
RJSLANEY	RJSLANEY...	IBM			
Sabine Walther	WALTHER...	ibm			
SAKAI	SAKAI?RC...	IBM			
SAKAIH	SAKAIH?R...	IBM			
SATID	SATID?MY...	IBM			
Stefan Blatt	SBLATT?...	ibm			
suehiro sakai	SAKAIDIR...	IBM			
SUSAN2	SUSAN2?I...	IBM			
SWA	SWA@MC...	ibm			
Thomas W Barlen	BARLEN?...	ibm	919-301-45...		

Searching AS/400 Ldap server...Found 54 matches

Figure 220. Netscape Address Book window

The padlock in the lower left corner of the Address Book window indicates that the connection between the Netscape LDAP client and the LDAP server on the AS/400 system is protected by SSL.

If you get the message shown in Figure 221 when trying to search the LDAP directory, the most likely reason is that the CA certificate is not installed on the Netscape browser. Therefore, check that the CA certificate of the server certificate is installed in the browser certificate database.



Netscape

Failed to bind to 'AS/400 Ldap server' due to LDAP error 'Can't contact LDAP server' (0x51)

Figure 221. LDAP server connection fail message

6.5 Enabling SSL for IBM eNetwork Personal Communications

The Secure Telnet server is supported from OS/400 V4R4 or higher. There are two major Telnet client products that support SSL.

- PC5250 included in the Client Access Express.

  Refer to 6.2, “Enabling SSL for IBM AS/400 Client Access Express” on page 187 for instructions on how to enable SSL for PC5250 in IBM AS/400 Client Access Express.

- IBM eNetwork Personal Communications V4R3

There is currently no client authentication supported. Only server certificates are used to authenticate the server and establish the SSL connection.

The following table shows the port numbers used for Telnet connections.

Table 8. The Telnet server port numbers

Connection	Port number	Service name
No SSL	23	telnet
SSL	992	telnet-ssl

6.5.0.1 Implementation tasks overview

The implementation tasks to enable SSL for IBM eNetwork Personal Communications are as follows:

1. Be sure that you have all of the required license programs installed.

   Refer to 6.5.2, “Prerequisites” on page 232 for the list of required license programs.

2. Prepare a CA certificate and server certificate.

   Refer to Chapter 5, “Digital Certificate Manager for AS/400” on page 107 for instructions on how to set up certificates on the AS/400 system.

3. Set up the Secure Telnet server on your AS/400 system to use SSL.
4. Set up IBM eNetwork Personal Communications for SSL connections.

6.5.1 Objective

The objective of this section is to show you how to configure the Secure Telnet server to use SSL. This scenario uses the IBM eNetwork Personal Communications product as the Telnet client software. A server certificate issued by a private CA is used for establishing SSL connection.

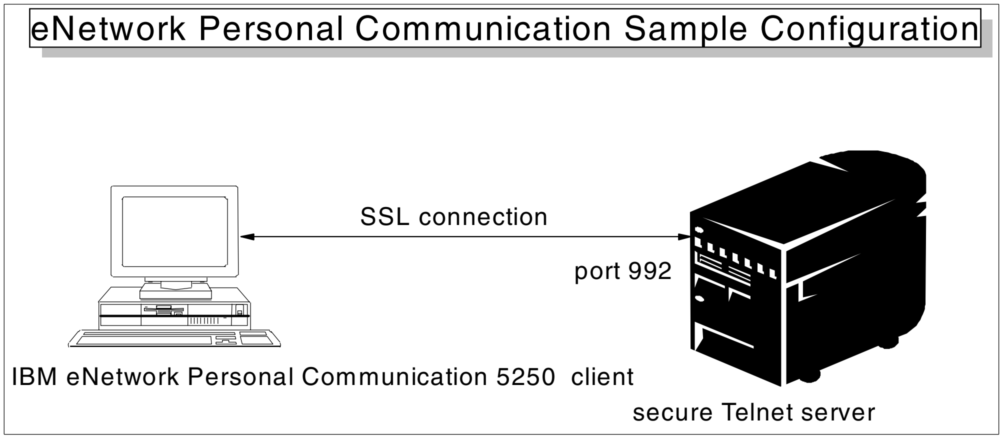

eNetwork Personal Communication Sample Configuration
SSL connection
port 992
IBM eNetwork Personal Communication 5250 client
secure Telnet server

Figure 222. Secure Telnet sample configuration

6.5.2 Prerequisites

The following license programs must be installed for this scenario:

AS/400 license programs

- Digital Certificate Manager (DCM), option 34 of OS/400 (5769-SS1)
- TCP/IP Connectivity Utilities for AS/400 (5769-TC1)
- IBM HTTP server for AS/400 (5769-DG1)
- One of the IBM Cryptographic Access Provider products:

  5769-AC1 (40-bit)

  5769-AC2 (56-bit)

  5769-AC3 (128-bit)

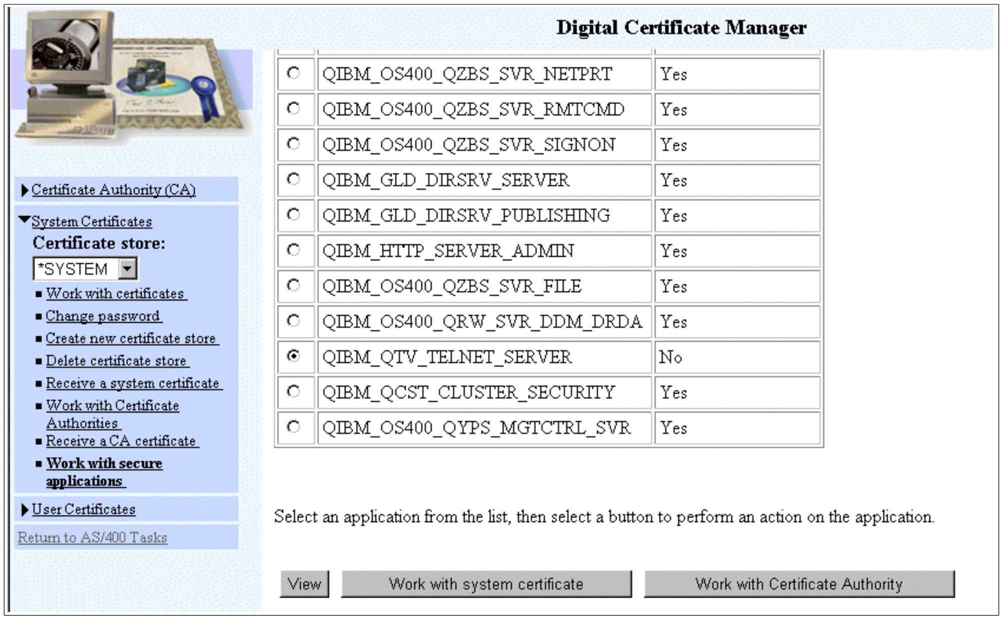
PC license programs

- IBM eNetwork Personal Communications V4R3

6.5.3 Configuring the AS/400 system

You must associate a server certificate with the secure Telnet server application ID. This automatically enables the Telnet server for SSL connections. No further actions need to be done. Perform the following steps to associate the certificate with the Telnet server:

1. Start the Digital Certificate Manager through the Operations Navigator or the AS/400 Tasks page.
2. Click **System Certificates**.
3. Click **Work with secure applications**.

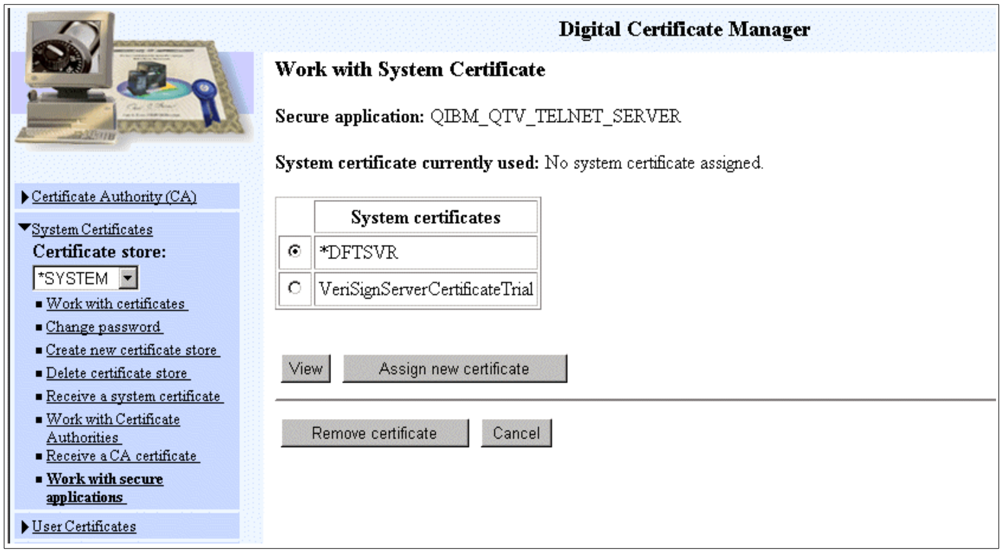

Digital Certificate Manager
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Work with system certificate
Work with Certificate Authority

○	QIBM_OS400_QZBS_SVR_NETPRT	Yes
○	QIBM_OS400_QZBS_SVR_RMTCMD	Yes
○	QIBM_OS400_QZBS_SVR_SIGNON	Yes
○	QIBM_GLD_DIRSRV_SERVER	Yes
○	QIBM_GLD_DIRSRV_PUBLISHING	Yes
○	QIBM_HTTP_SERVER_ADMIN	Yes
○	QIBM_OS400_QZBS_SVR_FILE	Yes
○	QIBM_OS400_QRW_SVR_DDM_DRDA	Yes
●	QIBM_QTV_TELNET_SERVER	No
○	QIBM_QCST_CLUSTER_SECURITY	Yes
○	QIBM_OS400_QYPS_MGTCTRL_SVR	Yes

Select an application from the list, then select a button to perform an action on the application.

Figure 223. Work with Secure Applications

4. Select the application ID **QIBM_QTV_TELNET_SERVER.**
5. Click **Work with system certificate**.



Work with System Certificate

Secure application: QIBM_QTV_TELNET_SERVER

System certificate currently used: No system certificate assigned.

	System certificates
●	*DFTSVR
○	VeriSignServerCertificateTrial

Figure 224. Work with System Certificate window

6. Select the certificate from the list that you want the secure Telnet server to use to establish SSL connections between the Telnet server and client.
7. Click **Assign new certificate**.
8. DCM displays a confirmation message. Click **OK**.
9. Restart the Telnet server.

   To activate these changes to the Telnet server, you must restart it using the following commands:

To stop: `ENDTCPSVR SERVER(*TELNET)`

To start: `STRTCPSVR SERVER(*TELNET)`

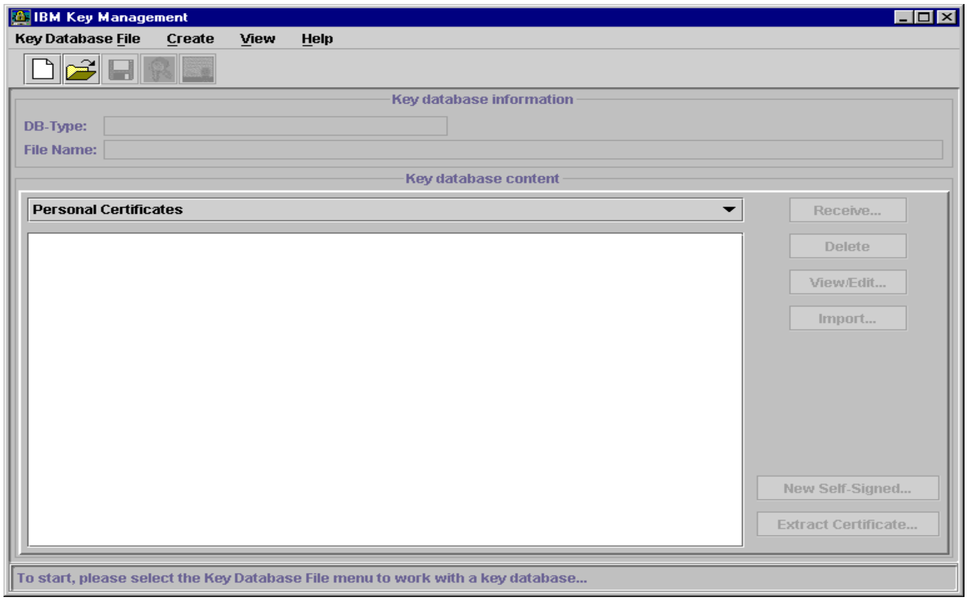
> **Note**
>
> Take extra care when ending the Telnet server on the AS/400 system. All active Telnet sessions will also be ended.

6.5.4 Configuring the PC

First, you must import the private CA certificate into the key database file. The IBM eNetwork Personal Communications has its own key database file. Then you have to configure the particular emulation session to use SSL. Note that you do not have to perform these steps if you are using a server certificate that is issued by a well-known CA. Perform the following steps to add a private CA certificate to the key database:

1. Start the IBM Key Management program in the IBM eNetwork Personal Communications folder using the following default path:

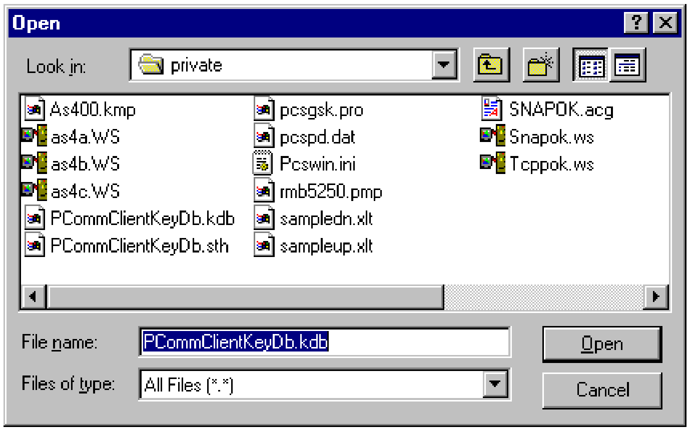
   Start->Programs->IBM Personal Communications->Utilities->Certificate Management



To start, please select the Key Database File menu to work with a key database...

Figure 225. IBM Key Management

2. Click **Key Database File->Open**.



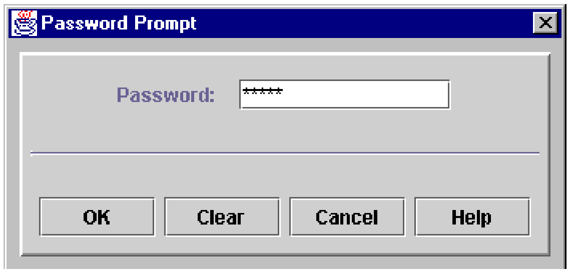
Look in: private

File name: PCommClientKeyDb.kdb

Files of type: All Files (*.*)

Figure 226. Open a default key database file

3. Select the key database file **PCommClientKeyDb.kdb** and click **Open**.



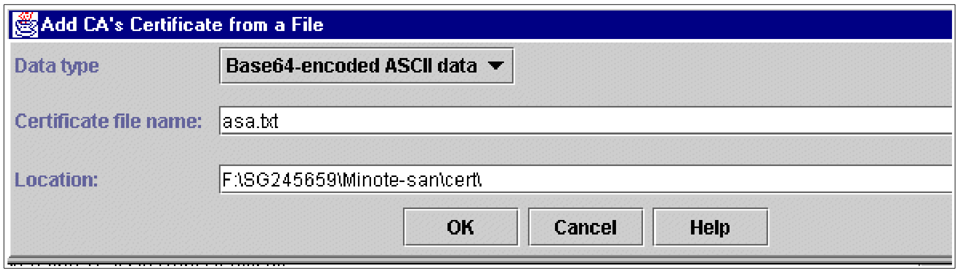
Password: *****

Figure 227. Password prompt

4. Enter the password and click **OK**. By default, the password is `pcomm`.

   The currently installed CA certificates are displayed.

5. Click **Add** on the right side of the Key Management window to add a new CA certificate to the key database.



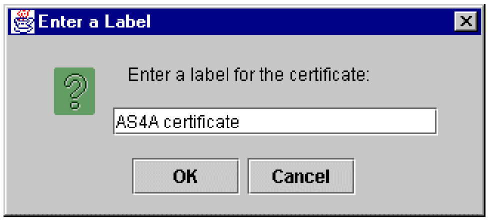
Data type: Base64-encoded ASCII data

Certificate file name: asa.txt

Location: F:\SG245659\Minote-san\cert\

Figure 228. Import file selection window

6. Enter the path name and the file name of the CA certificate you want to import and Click **OK**. Refer to 5.5, “Managing a Certificate Authority” on page 128 to see how to create a PC file containing the CA certificate. Follow the instructions to install a CA certificate on your PC using the copy and paste method.



Enter a Label

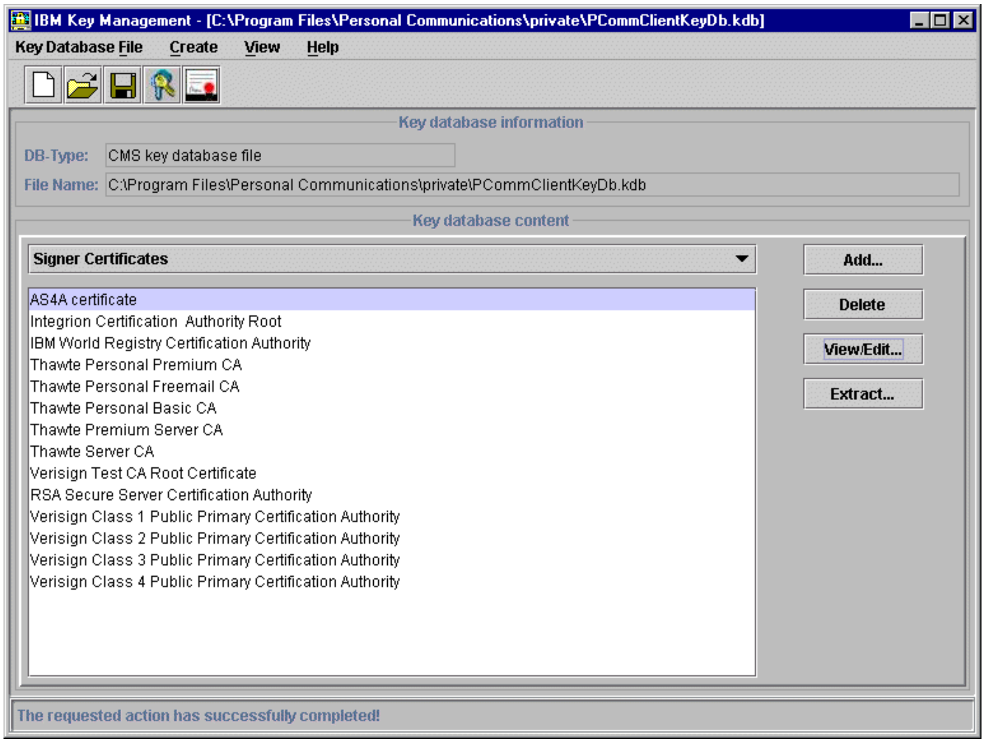
Enter a label for the certificate:

AS4A certificate

Figure 229. Certificate label name input window

7. Enter a label for the certificate and click **OK**.

   The certificate is stored as a trusted root in the key database file.



IBM Key Management - [C:\Program Files\Personal Communications\private\PCommClientKeyDb.kdb]

Key database information

DB-Type: CMS key database file

File Name: C:\Program Files\Personal Communications\private\PCommClientKeyDb.kdb

Key database content

Signer Certificates

AS4A certificate
Integrion Certification Authority Root
IBM World Registry Certification Authority
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
Verisign Test CA Root Certificate
RSA Secure Server Certification Authority
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority
Verisign Class 4 Public Primary Certification Authority

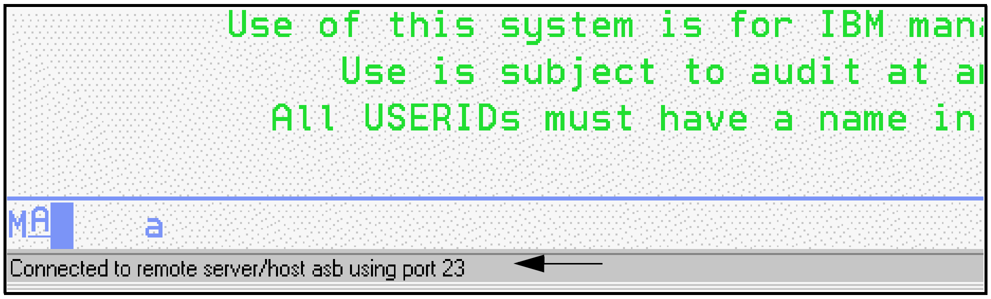
The requested action has successfully completed!

Figure 230. IBM Key Management main window

8. Click **View/Edit** to confirm the imported certificate’s contents.

The key database on your PC now has the private CA certificate and it is registered as a trusted root.

9. Start a Personal Communications (PCOM) session that you want to set up for SSL.

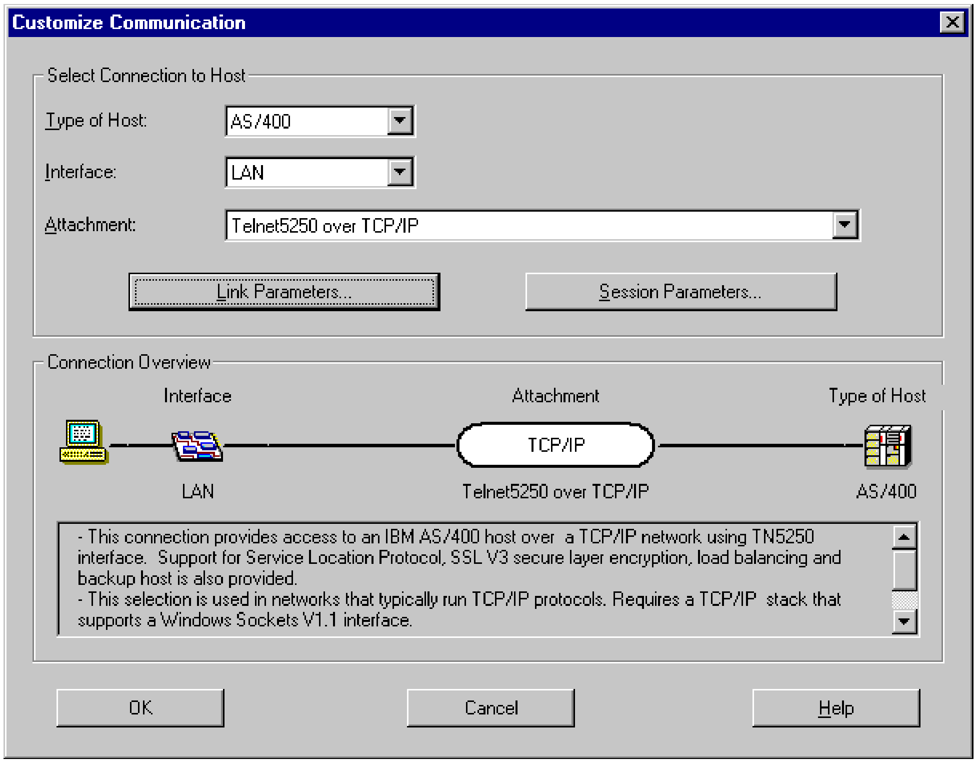


```
          Use of this system is for IBM man
               Use is subject to audit at a
            All USERIDs must have a name in
MA      a
Connected to remote server/host asb using port 23
```

Figure 231. Unsecured Telnet connection

At this time the used port 23 indicates that the emulation session is not using SSL.

10.Open **Communication->Configure**.



Customize Communication

Select Connection to Host

Type of Host: AS/400

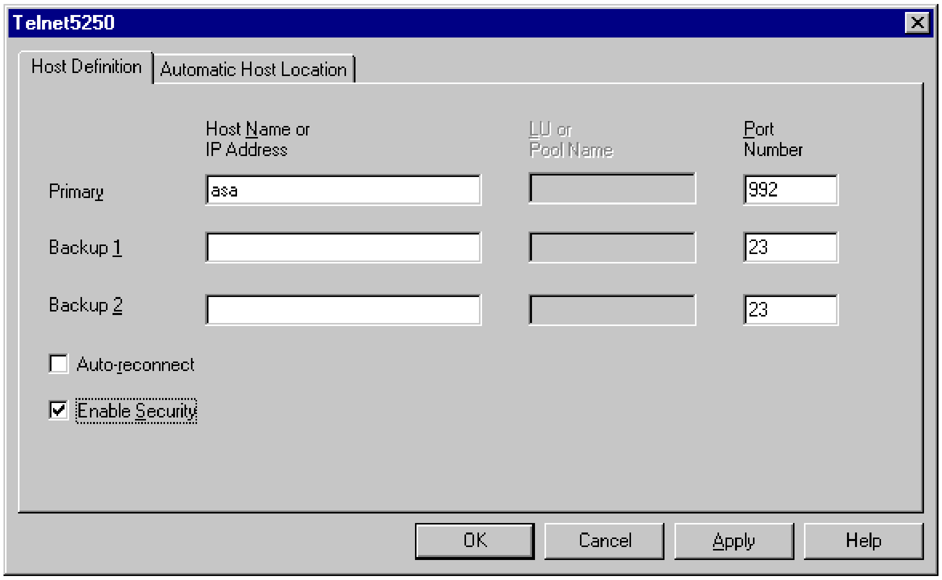
Interface: LAN

Attachment: Telnet5250 over TCP/IP

- This connection provides access to an IBM AS/400 host over a TCP/IP network using TN5250 interface. Support for Service Location Protocol, SSL V3 secure layer encryption, load balancing and backup host is also provided.
- This selection is used in networks that typically run TCP/IP protocols. Requires a TCP/IP stack that supports a Windows Sockets V1.1 interface.

Figure 232. Customize Communication window.

11.Click **Link Parameters**.



	Host Name or IP Address	LU or Pool Name	Port Number
Primary	asa		992
Backup 1			23
Backup 2			23

☐ Auto-reconnect

☑ Enable Security

Figure 233. Telnet5250 window

12. Change the Port number from `23` to `992` and select the **Enable Security** check box.

13. Click twice **OK** to save the changes and confirm the message indicating that the communication will be ended.

    The session restarts automatically and establishes a secured connection. Remember to save the session profile with the new settings.

6.5.5 Verifying the SSL connection

The following procedures can be used to determine if the Telnet connection is protected using the SSL protocol.

On the AS/400 system:

1. Use the `NETSTAT *CNN` command and check that the TCP port 992 is in the Listen state.

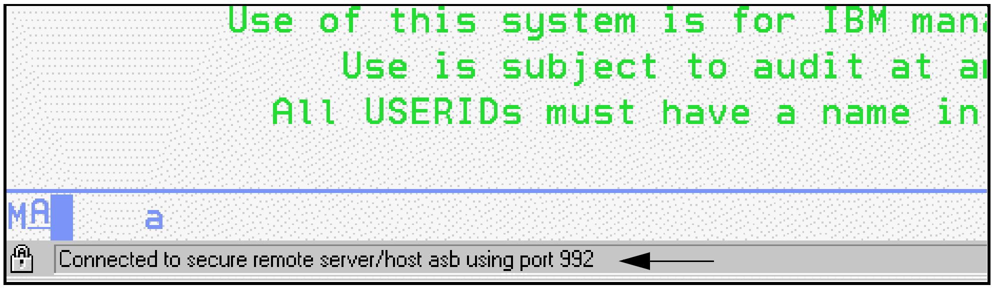
```
Remote             Remote  Local
Address             Port    Port  Idle Time  State
*                      *     992  000:11:41  Listen
```

2. When a Telnet session is established, use the `NETSTAT *CNN` command to check that the Telnet client has a connection through port 992 and not 23.

```
Remote             Remote  Local
Address             Port    Port  Idle Time  State
10.17.62.92          1308    992  000:00:00  Established
```

On the PC:

1. Start a Telnet session that is configured for SSL. Check the status bar at the bottom of the 5250 session window.



```
Use of this system is for IBM man
    Use is subject to audit at a
  All USERIDs must have a name in
```

Connected to secure remote server/host asb using port 992

Figure 234. PC5250 using a SSL connection

The padlock indicates that the 5250 emulation is secured using the SSL protocol. In addition the message shows that port 992 is used for this connection.

6.6 Enabling SSL for IBM SecureWay Host On-Demand

SecureWay Host On-Demand (HOD) V4.0 provides access to various Telnet servers such as 5250, 3270, or VT emulation servers through Java applets loaded into a Web browser. SSL encryption and server authentication provides secure connections between the emulator and the AS/400 system or downloaded from the AS/400 server to the browser in the client. No software except for the browser needs to be installed in the client PC.

This section covers how to configure the AS/400 Telnet server for SSL and the configuration of HOD sessions to use SSL. You can also set up the Redirector of HOD to use SSL. But this is outside the scope of this redbook and not supported by the server on the AS/400 system. Further information on the IBM SecureWay Host On-Demand product and its configuration is located in the redbook *Host On-Demand 4.0*, SG24-2149 and at the following URL:

`http://www.software.ibm.com/network/hostondemand/library/`

The following table shows the port numbers used for Telnet connections.

Table 9. The Telnet server port number

Connection	Port number	Service name
No SSL	23	telnet
SSL	992	telnet-ssl

SecureWay Host On-Demand provides several clients for different purposes. The following table lists the clients and HTML file names to start each client on the browser.

Table 10. The SecureWay Host On-Demand client type and HTML name

Client	HTML
Administration client	HODAdmin.html
Cached client	HODCached.html
Download client	HOD.html
Download client with REsQ!Net/LE Interface	HODResqnet.html

Client	HTML
Function On-Demand client	HODThin.html
Function On-Demand client with REsQ!Net/LE Interface	HODThinResqnet.html
Problem Determination client	HODDebug.html
Database On-Demand client	HODDatabase.html

6.6.0.1 Implementation tasks overview

To protect the SecureWay Host On-Demand Telnet sessions with SSL, you must perform these tasks:

1. Be sure that you have all of the required license programs installed.
   Refer to 6.6.2, “Prerequisites” on page 241 for further information.
2. Prepare a CA certificate and server certificate.
   Refer to Chapter 5, “Digital Certificate Manager for AS/400” on page 107.
3. Set up the SecureWay Host On-Demand server on your AS/400 system to use SSL.

6.6.1 Objective

The objective of this section is to show you how to configure Host On-Demand sessions to use the SSL protocol for secured communication. You can also configure the HTTP server to use SSL in order to secure the download of the Host On-Demand Web pages and applets. Refer to Chapter 4, “Securing the HTTP Server for AS/400” on page 35 for detailed information on setting up the HTTP server for SSL. Figure 235 shows an overview of the environment discussed in this section.

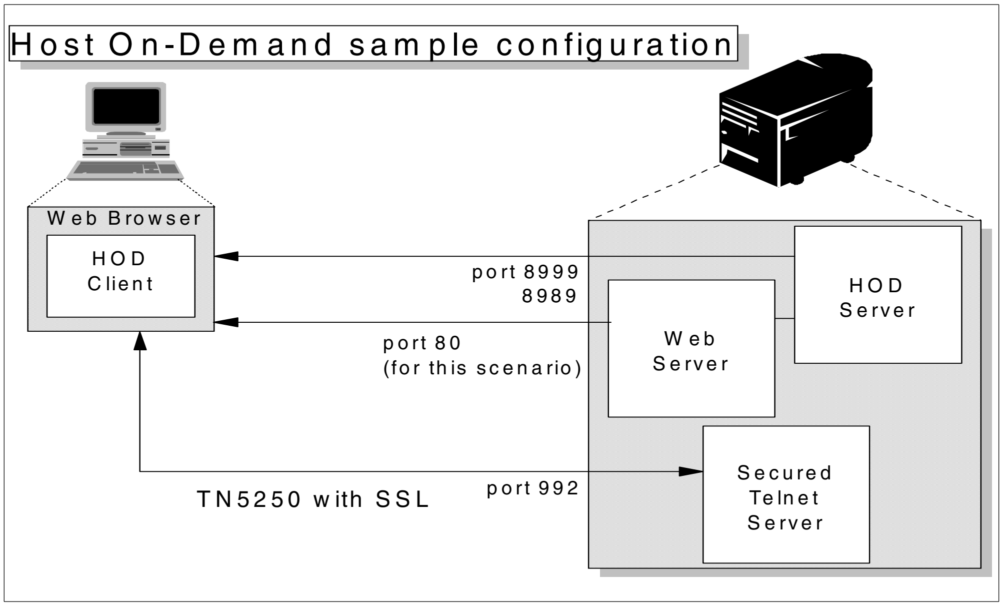


Figure 235. Host On-Demand sample configuration

There are several ports involved when using Host On-Demand with secured Telnet sessions. If you are using the Host On-Demand server behind a firewall, be sure to permit the traffic to those ports. If you are using the Host On-Demand Redirector, be sure to enable those ports through the firewall.

Table 11. Host On-Demand scenario port summary

Port	Description
992	Telnet server port for secured connections (SSL)
80	HTTP server port. In this scenario the HOD is set up in the default server instance. You may also use your own server instance, which listens then to a different port from the well-known port for HTTP requests.
8999	Host On-Demand configuration port.
8989	Host On-Demand administration port.

6.6.2 Prerequisites

The following AS/400 license programs must be installed for this scenario:

- Digital Certificate Manager (DCM), option 34 of OS/400 (5769-SS1)
- TCP/IP Connectivity Utilities for AS/400 (5769-TC1)
- IBM HTTP server for AS/400 (5769-DG1)
- One of the IBM Cryptographic Access Provider products:

  5769-AC1 (40-bit)

  5769-AC2 (56-bit)

  5769-AC3 (128-bit)
- AS/400 Java Toolkit (5769JV1)
- QShell Interpreter, option 30 of OS/400 (5769-SS1)
- Secure Way Host On-Demand CD V4.2 (5648-C54)

6.6.3 Configuring a Host On-Demand session profile

In this scenario, the SecureWay Host On-Demand server is installed on an AS/400 system. The following steps take you through the process of creating a Host On-Demand user environment and how to create and enable a session profile for SSL.

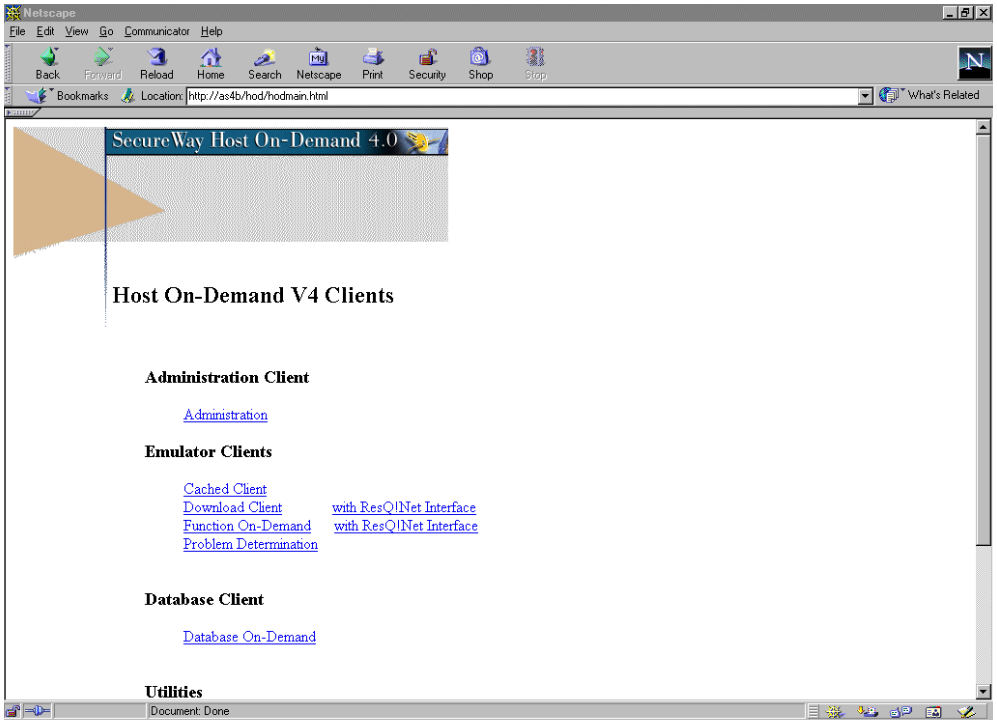
1. Start a Web browser and open the **SecureWay Host On-Demand** main window using the following URL:

   `http://as4b/HOD/hodmain.html`

   or if you are using a server instance with a port number other than 80 specify the following URL:

   `http://as4b:port number/HOD/hodmain.html`

   Note that `as4b` is the host name of the AS/400 system. It is also assumed that the Host On-Demand server is installed using the default installation paths and configuration, particularly the Pass directive in the HTTP configuration, which should be `Pass /HOD/* /QIBM/ProdData/hostondemand/HOD/*`.


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://as4b/hod/hodmain.html
What's Related
SecureWay Host On-Demand 4.0
Document: Done

Host On-Demand V4 Clients

Administration Client

Administration

Emulator Clients

Cached Client
Download Client with ResQ!Net Interface
Function On-Demand with ResQ!Net Interface
Problem Determination

Database Client

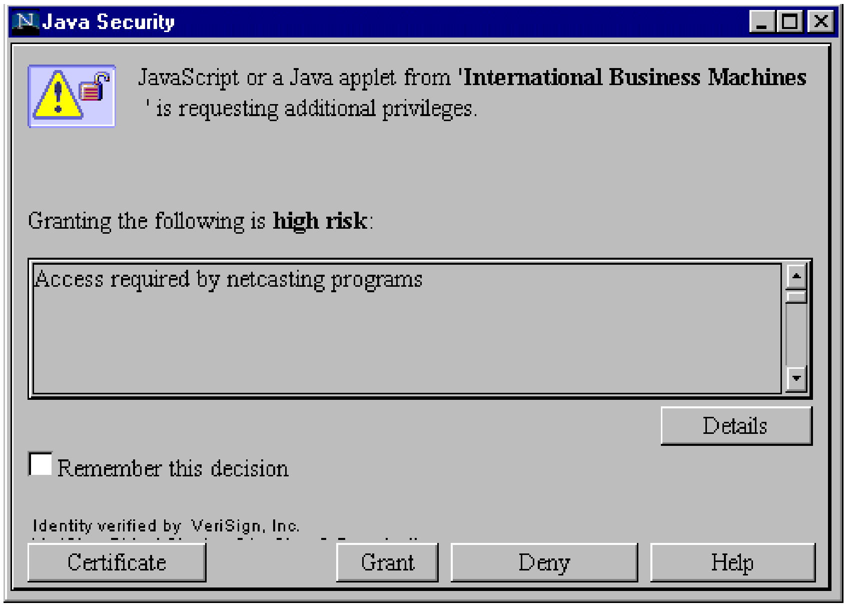
Database On-Demand

Utilities

Figure 236. The SecureWay Host On-Demand main window

2. To create a new SecureWay Host On-Demand user account, click **Administration**.

   At this time the Java Virtual Machine will be started on your browser and some Java applets are downloaded.



JavaScript or a Java applet from '**International Business Machines** ' is requesting additional privileges.

Granting the following is **high risk**:

Access required by netcasting programs

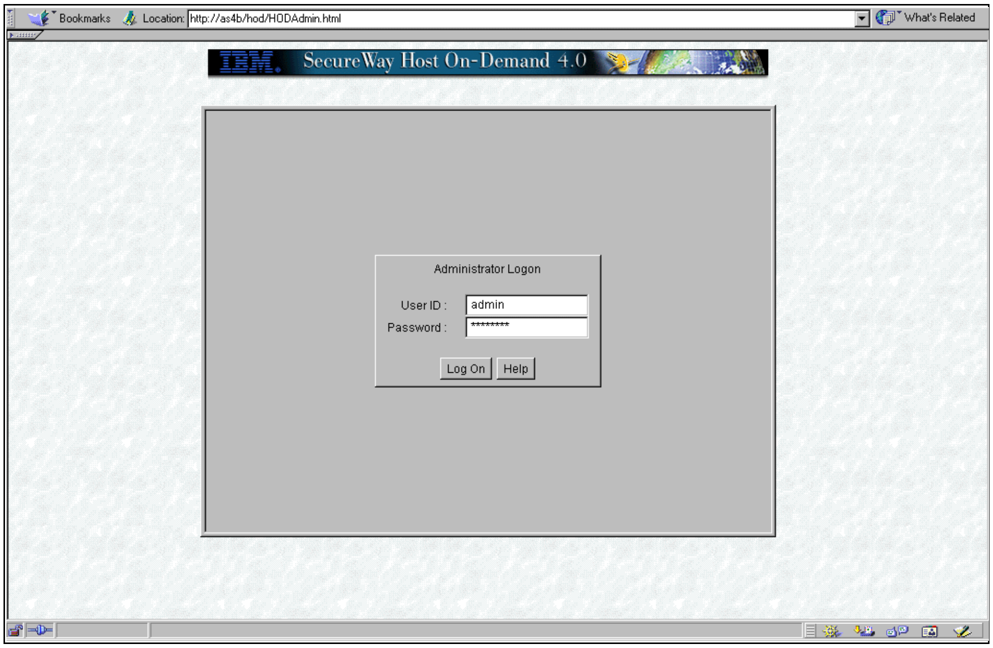
□ Remember this decision

Identity verified by VeriSign, Inc.

Figure 237. Java Security Information window

The Netscape browser, when running applets, presents a Java Security window asking if the user wants to allow the execution of the applet.

3. Click **Grant** on the Java Security window. To avoid this message in the future, also select **Remember this decision**. The signer information of this applet will then be stored in the browser security information.



Location: http://as4b/hod/HODAdmin.html

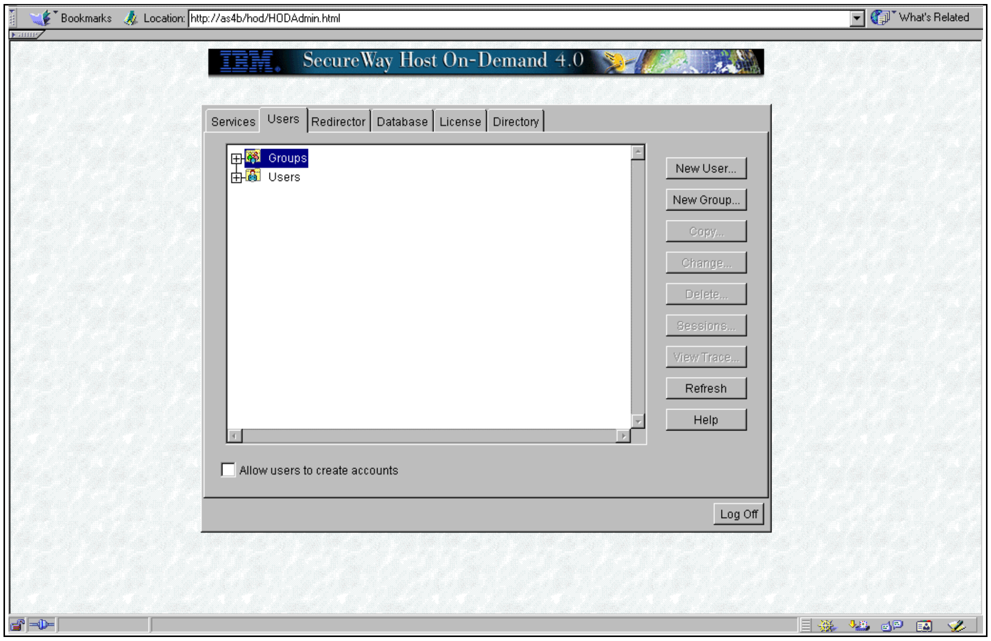
Administrator Logon

User ID : admin

Password : ********

Figure 238. Administrator Logon panel

4. Enter the user ID and password. By default, the user ID is `admin` and the Password is `password`. The administrator main window is displayed.

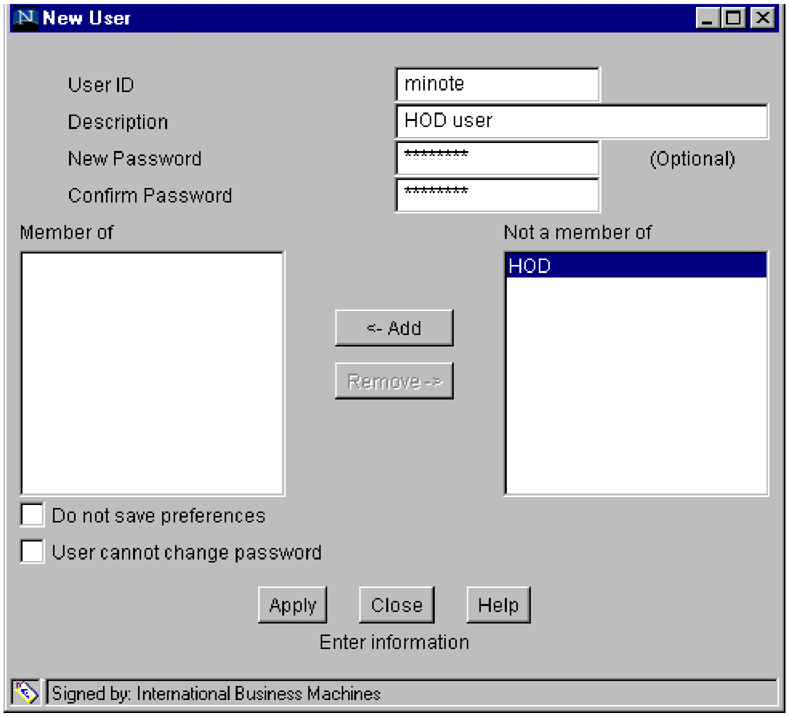


Location: http://as4b/hod/HODAdmin.html

□ Allow users to create accounts

Figure 239. The SecureWay Host On-Demand administrator main window

5. Select the **Users** tab and click **New User**.



New User

User ID: minote

Description: HOD user

New Password: ********* (Optional)

Confirm Password: *********

Member of:

Not a member of: HOD

□ Do not save preferences

□ User cannot change password

Enter information

Signed by: International Business Machines

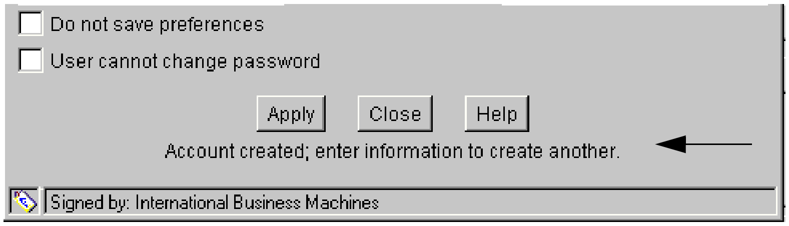
Figure 240. New User entry window

6. Enter the user ID, description and password.

   The user that is created in Host On-Demand is not related to an AS/400 user profile. The user account is only used to store user configurations and control user access to various Host On-Demand functions. A Host On-Demand user has to enter the user and password when contacting the Host On-Demand server to start a function, such as a Telnet session.

7. Select **HOD** under Not a member of and click **Add**. The new user will be added to the system default group HOD.

8. Click **Apply**. The user account is created and a confirmation message displayed.



□ Do not save preferences

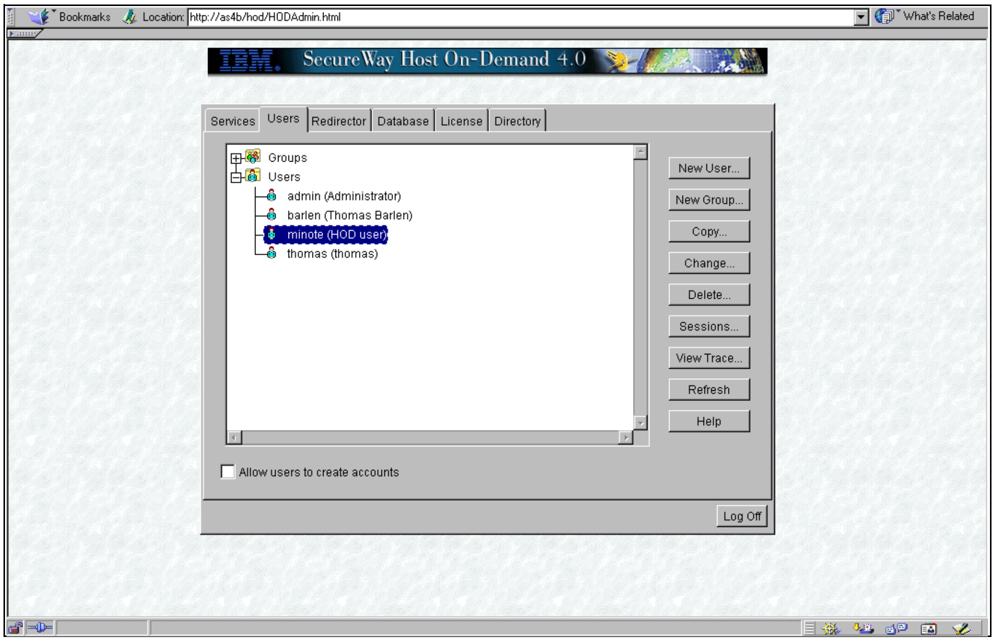
□ User cannot change password

Account created; enter information to create another.

Signed by: International Business Machines

Figure 241. Confirmation message

9. Click **Close** to return to the SecureWay Host On-Demand administration main window.



Location: http://as4b/hod/HODAdmin.html

SecureWay Host On-Demand 4.0

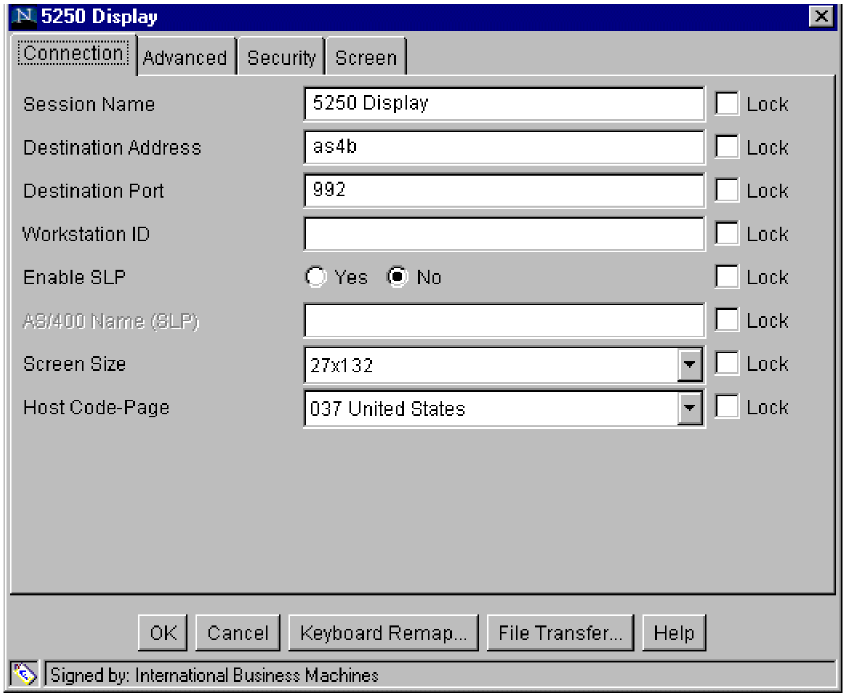
- Groups
- Users
  - admin (Administrator)
  - barlen (Thomas Barlen)
  - minote (HOD user)
  - thomas (thomas)

□ Allow users to create accounts

Figure 242. SecureWay Host On-Demand users

10.Select the user you want to configure Telnet sessions for and click **Sessions**.

11.At the next window, click **5250 Display**. The 5250 Display window is displayed.



5250 Display

Session Name	5250 Display	□ Lock
Destination Address	as4b	□ Lock
Destination Port	992	□ Lock
Workstation ID		□ Lock
Enable SLP	○ Yes ● No	□ Lock
AS/400 Name (SLP)		□ Lock
Screen Size	27x132	□ Lock
Host Code-Page	037 United States	□ Lock

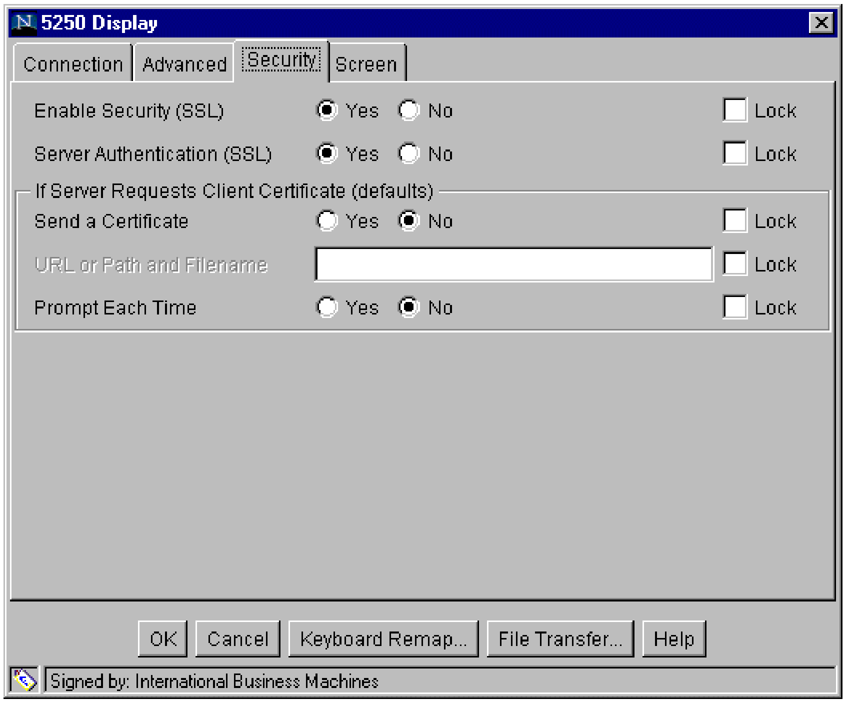
Signed by: International Business Machines

Figure 243. 5250 Display Configuration window

12.Enter the following information.

Destination Address	The Telnet server host name or IP address.
Destination Port	992

13.Select the **Security** tab.



Enable Security (SSL) ● Yes ○ No □ Lock

Server Authentication (SSL) ● Yes ○ No □ Lock

If Server Requests Client Certificate (defaults)

Send a Certificate ○ Yes ● No □ Lock

URL or Path and Filename □ Lock

Prompt Each Time ○ Yes ● No □ Lock

Figure 244. 5250 Display Security entry window

14. Select **Yes** for the parameter Enable Security (SSL) and Server Authentication (SSL). Server Authentication is used to check if the common name in the server certificate matches the host name specified for destination host.

15. Click **OK**. The 5250 session is created on the SecureWay Host On-Demand server.

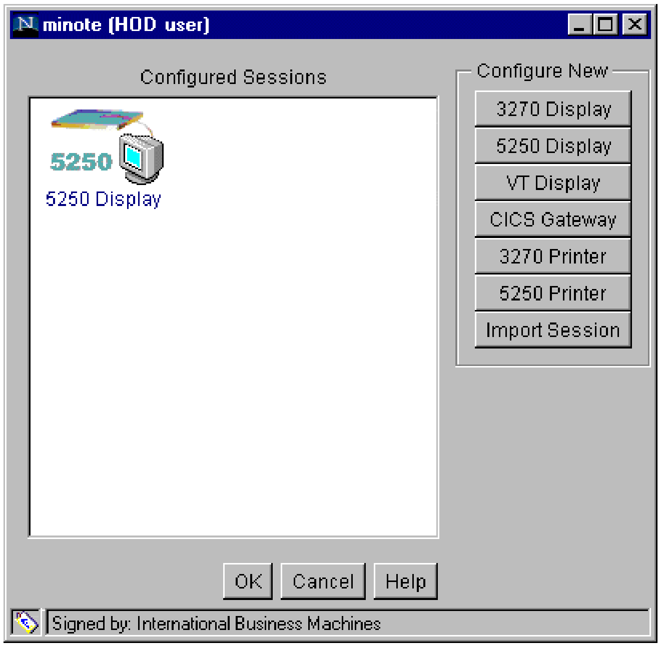


Figure 245. 5250 Display configuration

16. Click **OK** to return to the SecureWay Host On-Demand administration main window.

Follow the next steps to complete the setup to use SSL for Host On-Demand Telnet sessions.

6.6.4 Create a CA certificate

Since this scenario shows how to set up Host On-Demand to trust server certificates issued by private CAs, a private CA must be set up. The detailed steps are shown in 5.4, “Setting up a local Certificate Authority” on page 118. If you already have the private CA certificate on your AS/400 system or using a well-known CA, you can skip this step.

6.6.5 Assign a server certificate to the secure Telnet server

A server certificate needs to be assigned to all Telnet servers to which Telnet sessions over SSL will be established. That means, for example, if you have three AS/400 systems installed in your network and the session traffic has to be protected by SSL, you have to have a server certificate issued for each of the systems. And each particular server certificate must be assigned to the system’s Telnet server.

The detailed steps are shown in 6.5.3, “Configuring the AS/400 system” on page 232. If you have already assigned the server certificate to the secure Telnet server, you can skip this step.

6.6.6 Create the certificate class for the SecureWay Host On-Demand

The certificate class is needed by SecureWay Host On-Demand to store trusted root CA certificates that are not in the list of well-known CAs. On PC client products, such as IBM eNetwork Personal Communications or IBM AS/400 Client Access Express, the certificates are stored in key databases on the PC. Since Host On-Demand Telnet clients are downloadable as applets from the Host On-Demand server, the certificate class file resides on that server. The file name for the certificate class is CustomizedCAs.class and must be placed in the directory /QIBM/ProdData/hostondemad/HOD/.

There are two methods to add a private CA certificate to the CustomizedCAs.class file.

- Adding a CA certificate using the IBM Key Management utility.
- Adding a CA certificate using a Java utility keyrng.

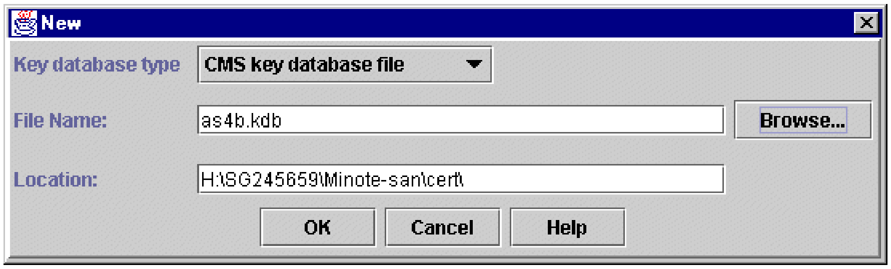
Note

The steps to add a CA certificate to the CustomizedCAs.class must only be performed if you are using a server certificate that has been issued by private or intranet CAs. If you are using a server certificate issued by a well-know CA, skip these steps. You can check which well-known CA certificates are supported by Host On-Demand by starting, for example a non-SSL 5250 session and click **Communication->Security** and select **Show CAs trusted by client.** A list of all trusted CAs is displayed.

6.6.6.1 Adding a CA certificate using the IBM Key Management utility

We assume you already have the CA certificate of your private CA stored in the Base64 encoded form in a PC file. To import a CA certificate into the certificate class file you need to have a tool, such as the Key Management Utility program. This is part of Host On-Demand. You can also use the Key Management utilities provided with IBM AS/400 Client Access Express or IBM eNetwork Personal Communications. We are using the Key Management utility from IBM AS/400 Client Access Express. To create the certificate class, perform these steps.

1. Start *the* IBM Key Management in the Clients Access Express window.
2. Select **Key Database File** -> **New**.
3. In the File Name field enter a name for the key database file where the private CA certificate will be stored. The Location can be any directory of your choice. Note that this file does not need to be transferred to the server. It is only used to extract the CA certificates into the certificate class file.



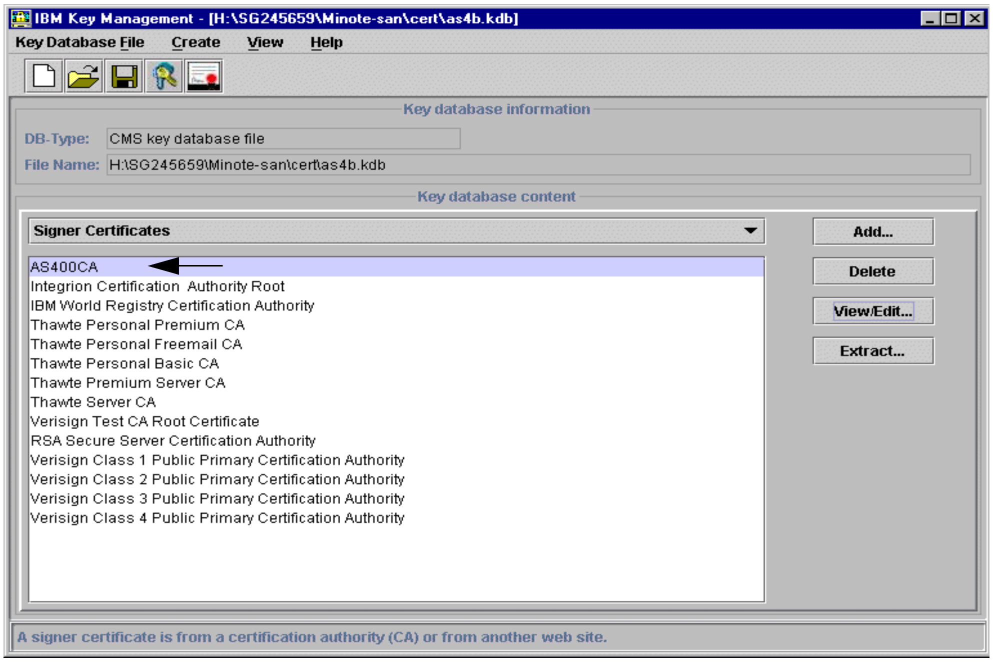
Key database type: CMS key database file

File Name: as4b.kdb

Location: H:\SG245659\Minote-san\cert\

Figure 246. New key database name entry

4. Click **OK**.
5. Enter `CA400` in the Password and Confirm Password fields and click **OK**. The password is used to protect the key database.
6. Click **Add**.
7. Click **Browse** to find the text file where the private CA certificate is stored. The CA certificate must be in the Base64 format. Refer to 5.5, “Managing a Certificate Authority” on page 128 to see how an AS/400 CA certificate is exported into a PC file using the copy and paste method.
8. Select the file and click **Open**.
9. Click **OK**. A window is displayed requesting a label under which the CA certificate is stored in the key database.
10. Enter a label for the CA certificate, for example, `AS400CA` and click **OK**.



IBM Key Management - [H:\SG245659\Minote-san\cert\as4b.kdb]

Key database information

DB-Type: CMS key database file

File Name: H:\SG245659\Minote-san\cert\as4b.kdb

Key database content

Signer Certificates

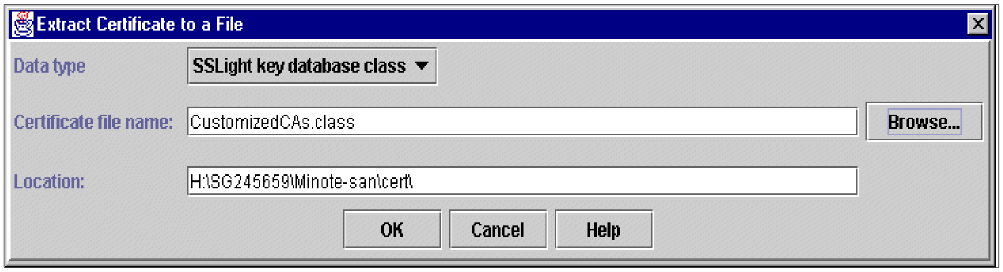
AS400CA
Integrion Certification Authority Root
IBM World Registry Certification Authority
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
Verisign Test CA Root Certificate
RSA Secure Server Certification Authority
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority
Verisign Class 4 Public Primary Certification Authority

A signer certificate is from a certification authority (CA) or from another web site.

Figure 247. The IBM Key Management window

Now you need to extract the CA certificates and store them in the CustomizedCAs.class.

11.Click **Extract**.



Extract Certificate to a File

Data type: SSLight key database class

Certificate file name: CustomizedCAs.class

Location: H:\SG245659\Minote-san\cert\

Figure 248. Extract Certificate to a File window

12.Set the Data Type to SSLight key database class, Certificate file name to CustomizedCAs.class and the Location can be any directory of your choice.

13.Click **OK**.

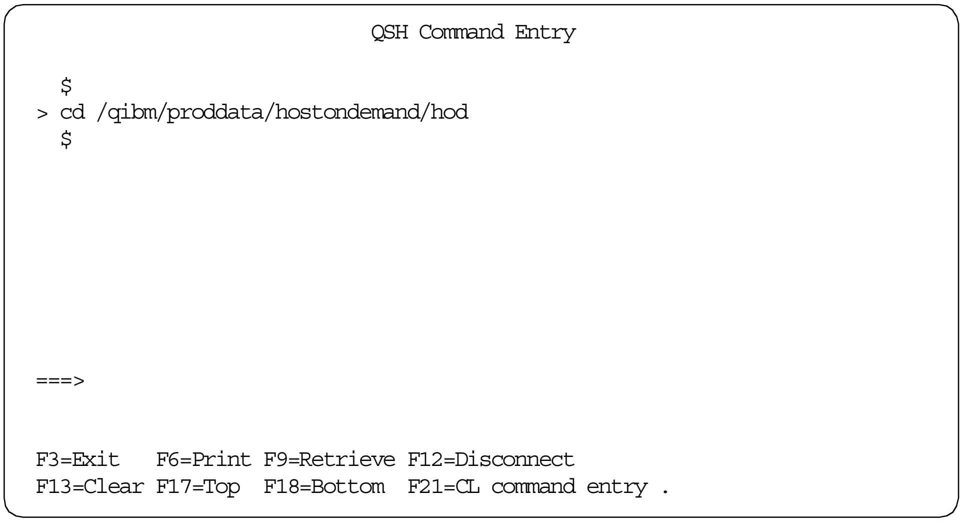
14.Transfer this class file to the following IFS directory using, for example the AS/400 NetServer function.

Directory: /QIBM/ProdData/hostondemand/HOD/

6.6.6.2 Adding a CA certificate using the keyrng utility

The Java classes provided with the SecureWay Host On-Demand product also include a keyrng class. This class contains methods that can be used to update or create the CustomizedCAs.class file in the /QIBM/ProdData/hostondemand/HOD directory. You can either run this utility from a PC that has a JDK installed or from the AS/400 QShell interface. Perform the following steps to add a private CA certificate to the CustomizedCAs.class file.

1. Sign on to the AS/400 system that has the Host On-Demand server installed.
2. Enter the AS/400 command `QSH` to start the QShell and change the current directory to /QIBM/ProdData/hostondemand/HOD as shown in Figure 249.



```
                             QSH Command Entry

  $
> cd /qibm/proddata/hostondemand/hod
  $










===>


F3=Exit   F6=Print F9=Retrieve F12=Disconnect
F13=Clear F17=Top  F18=Bottom  F21=CL command entry .
```

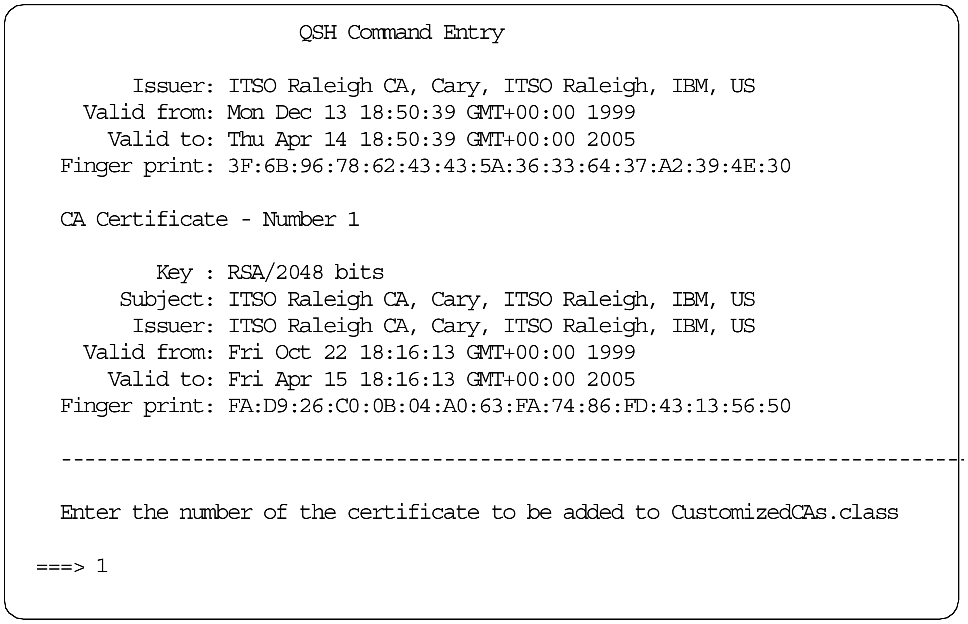
Figure 249. AS/400 QShell

The CD command sets the current directory to the Host On-Demand product directory which is a required step to run the keyrng utility. The keyrng.class resides in the com/ibm/hodsslight/tools directory which is a subdirectory of the current directory.

3. Run the following Java command to add the CA certificate to the CustomizedCAs.class file:

```
java -classpath . com.ibm.hodsslight.tools.keyrng CustomizedCAs connect
as4a:9476
```

In this case the private CA is configured on the system AS4A. The port 9476 identifies the secured port of the sign-on host server. The command retrieves the site and CA certificate and displays the information on the AS/400 display.



```
                    QSH Command Entry

       Issuer: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
   Valid from: Mon Dec 13 18:50:39 GMT+00:00 1999
     Valid to: Thu Apr 14 18:50:39 GMT+00:00 2005
 Finger print: 3F:6B:96:78:62:43:43:5A:36:33:64:37:A2:39:4E:30

 CA Certificate - Number 1

         Key : RSA/2048 bits
      Subject: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
       Issuer: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
   Valid from: Fri Oct 22 18:16:13 GMT+00:00 1999
     Valid to: Fri Apr 15 18:16:13 GMT+00:00 2005
 Finger print: FA:D9:26:C0:0B:04:A0:63:FA:74:86:FD:43:13:56:50

 ----------------------------------------------------------------------------

 Enter the number of the certificate to be added to CustomizedCAs.class

===> 1
```

If you have no online connection to the system where the CA is running, you can also add a CA certificate to the CustomizedCAs.class by performing the following command:

```
java -classpath . com.ibm.hodsslight.tools.keyrng CustomizedCAs add --ca
/webserver/certasa.der
```

where `/webserver/certasa.der` is the qualified path of the file that contains the CA certificate in binary DER data format (also referred to as binary X509 certificate format). Note that the BASE64 encoded format is not support by this utility.

4. Select the CA certificate, which in this case is the option 1 and press Enter.

   A completion message indicates that the CA certificate has been successfully added to the CustomizedCAs.class.

```
> 1
  Adding the CA Certificate - 1 to CustomizedCAs.class
  Done.
  $
```

5. To verify that the CA certificate is stored correctly, perform the following command:

```
java -classpath . com.ibm.hodsslight.tools.keyrng CustomizedCAs  verify
```

   The verification process displays the CA certificate data that is stored in the CustomizedCAs.class.

```
 ------------------------- Key ring entry: 1 -------------------------

   Entry type: CA Certificate

         Key : RSA/2048 bits
      Subject: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
       Issuer: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
   Valid from: Fri Oct 22 18:16:13 GMT+00:00 1999
     Valid to: Fri Apr 15 18:16:13 GMT+00:00 2005
 Finger print: FA:D9:26:C0:0B:04:A0:63:FA:74:86:FD:43:13:56:50
```

In order to activate the changes, you have to reload the Host On-Demand client on the browser. The best way to ensure having the CustomizedCAs.class downloaded to the PC is to close your Web browser and start it again.

6.6.7 Verifying the SSL connection

In our scenario, we will use a download client of the SecureWay Host On-Demand, so you do not need to configure the PC. You just have to have a Java-enabled browser such as Netscape Navigator.

To start the SecureWay Host On-Demand client on your browser, perform the following steps:

1. Go to the following URL on your browser:

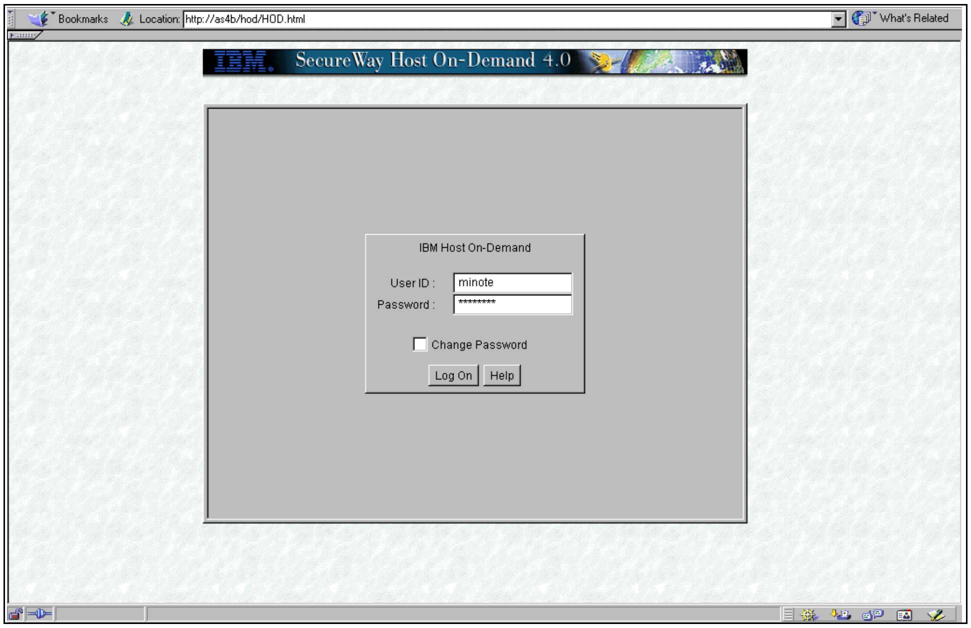
   `http://as4b/HOD/hod.html`

   or if you are using a different port from the well-known port 80, specify the port number used in your HTTP configuration:

   `http://as4b:port number/HOD/hod.html`

   Note that `as4b` is the host name of the AS/400 system. It is also assumed that the Host On-Demand server is installed using the default installation paths and configuration. In particular the Pass directive in the HTTP configuration that should be `Pass /HOD/* /QIBM/ProdData/hostondemand/HOD/*`.

   The SecureWay Host On-Demand logon window is displayed.


Bookmarks
Location: http://as4b/hod/HOD.html
What's Related
IBM. SecureWay Host On-Demand 4.0
IBM Host On-Demand

User ID : minote
Password : ********

Figure 250. The Secure Way Host On-Demand logon window

2. Enter the user ID and password of the user you have registered on the SecureWay Host On-Demand administration window, and click **Log On**.

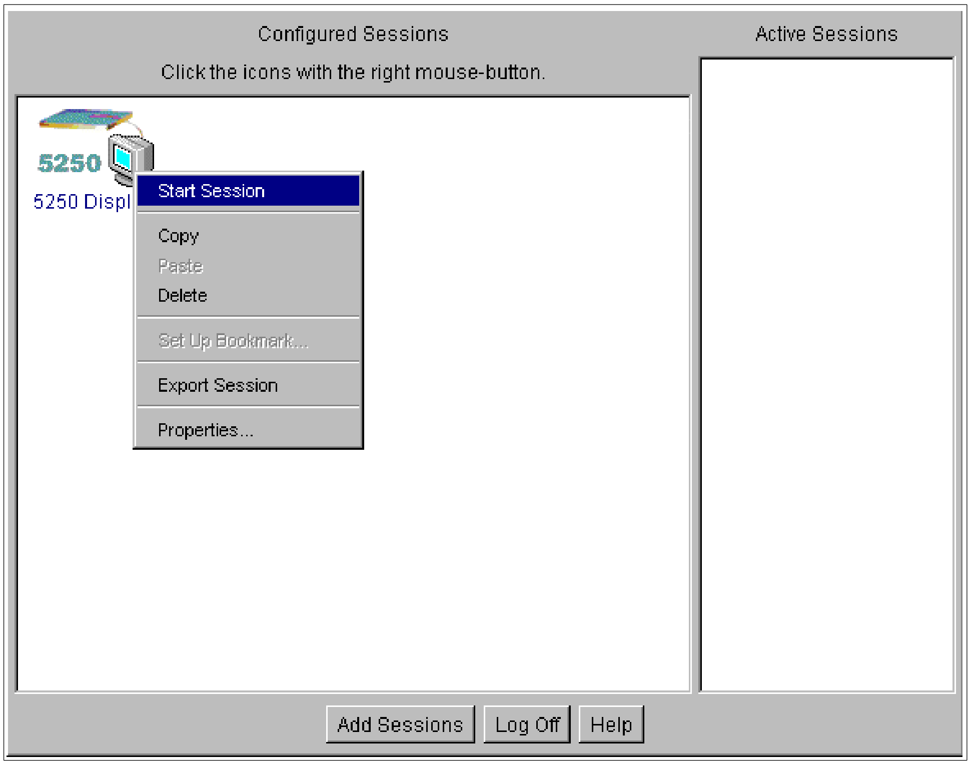


Figure 251. The SecureWay Host On-Demand user window

3. Right-click the **5250 Display** icon and select **Start Session**. At this time the 5250 emulator applets are downloaded from the SecureWay Host On-Demand server to the browser. After the download completed, the 5250 emulator window is displayed. On the bottom right of the emulator window the message bar indicates a secured connection as shown in Figure 252.

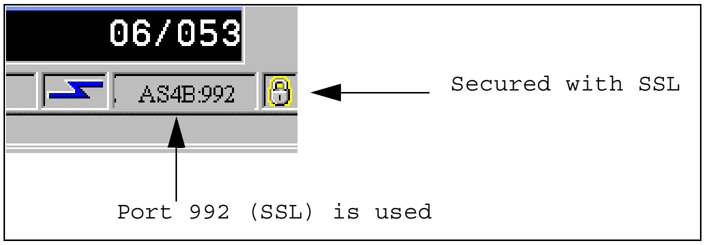


Figure 252. The SecureWay Host On-Demand 5250 emulator status message bar

The padlock indicates that the 5250 emulation is secured using the SSL protocol. In addition the next message shows that port 992 is used for this connection.

If you encounter problems while establishing the session, check with the AS/400 `NETSTAT *CNN` command that the port 992 is in the Listen state. Also be sure to have the HTTP server running and that the Host On-Demand server jobs QHODSVM and QJVACMDSRV are running in the QSYSWRK subsystem, which is the default subsystem. If you changed settings with the `CFGHODSVM` command, check for the jobs in the configured subsystem.

6.7 Enabling the AS/400 Toolbox for Java to use SSL

The AS/400 Toolbox for Java enables Java applications to access resources on the AS/400 system. With these classes, you can write client/server Java applications and applets. You can also run Java applications that use the AS/400 Toolbox for Java on the AS/400 Java Virtual Machine (JVM).

The AS/400 Toolbox for Java provides the following three objects:

- jt400.zip

  This allows the Java application program to access the AS/400 system.

- sslightu.zip or sslightx.zip

  These provide SSL support for Java applications.

- SSLTools.zip

  This allows you to download the CA certificate in the KeyRing.class file.

The AS/400 Toolbox for Java uses the AS/400 servers, such as the TCP host servers, as access points to the system. Each server job sends and receives data streams on a socket connection. To connect to the server, you just have to use an `AS400()` object in your Java code. That object handles connecting to the server. Also, you can set up a secure AS/400 connection by creating an instance of a SecureAS400() object instead of using an AS400() object.

Note

Only the JDBC driver classes have their own connection method. If you want to use SSL on the JDBC driver, you must set the JDBC property to use the SSL connection. By default, the security property is disabled. To activate the security function on the JDBC driver, add the following parameter in your code:

<nonsecure>

```
connection = DriverManager.getConnection ("jdbc:as400://" + system);
```

<secure>

```
connection = DriverManager.getConnection ("jdbc:as400://" + system +
";secure = true");
```

When the Java application establishes the secure connection to the server, they refer to the KeyRing.class in the jt400.zip. The KeyRing.class has already included the well-known CA certificates, such as the VeriSign and so on.

6.7.0.1 Implementation tasks overview

To use the AS/400 Toolbox for Java with SSL, you must perform these tasks:

1. Be sure to have all of the required license programs installed.

   Refer to 6.7.2, “Prerequisites” on page 255 for a list of those license programs.

2. Prepare a CA certificate and server certificate.

   Refer to Chapter 5, “Digital Certificate Manager for AS/400” on page 107.

3. Set up the TCP host servers on your AS/400 system to use SSL.

Refer to 6.2, “Enabling SSL for IBM AS/400 Client Access Express” on page 187.

4. Set up the Java program to use SSL on your PC.

6.7.1 Objective

The objective of this section is to show you how to configure a Java program using the AS/400 Toolbox for Java classes to use the SSL protocol for their communication. The following chart is an overview of this scenario. The sample Java code has the following functions:

- Connect to the secure sign-on server on the AS/400 system.
- Connect to the secure remote command server on the AS/400 system.
- Send and receive the encrypted data such as user ID, password, and OS/400 command.

A private CA is used that issues a server certificate for the AS/400 system.

The sample code is listed in Appendix D, “Sample Java program using SSL” on page 397.

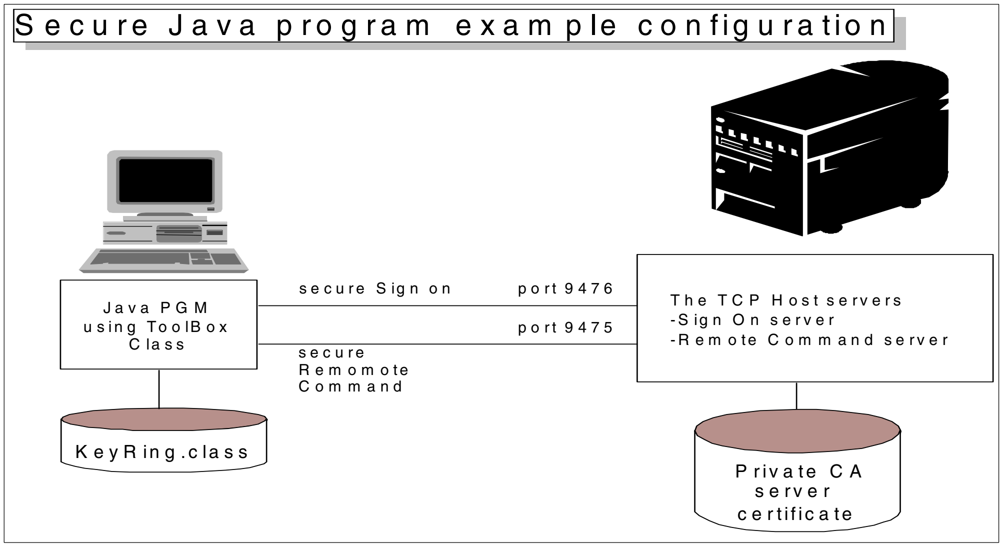


Figure 253. Secure Java sample configuration

6.7.2 Prerequisites

The following license programs must be installed for this scenario:

AS/400 license programs

- Digital Certificate Manager (DCM), option 34 of OS/400 (5769-SS1)
- TCP/IP Connectivity Utilities for AS/400 (5769-TC1)
- IBM HTTP server for AS/400 (5769-DG1)
- AS/400 ToolBox for Java (5769-JC1)
- One of the IBM Cryptographic Access Provider products:

  5769-AC1 (40-bit)

5769-AC2 (56-bit)

5769-AC3 (128-bit)

- At least one of the AS/400 products:

  5769-CE1 (40-bit)

  5769-CE2 (56-bit)

  5769-CE3 (128-bit)

  Encryption classes are included in these products.

PC programs

Java Development Kit (JDK) 1.1.x

6.7.3 Configuring the AS/400 system

We assume that a server certificate is already obtained from the private CA and is available along with the CA certificate on the AS/400 system. The detailed creation steps are shown in 5.4, “Setting up a local Certificate Authority” on page 118.

All host servers that are used by the AS/400 Toolbox for Java need to be enabled for SSL. That means a server certificate must be assigned to the various host servers. Refer to 6.2.3, “Configuring the AS/400 system” on page 190 to assign the server certificate with the TCP/IP host servers.

6.7.4 Configuring the PC

To enable the Java program using the AS/400 Toolbox for Java classes to establish connections with SSL, follow these steps:

1. Download the AS/400 Toolbox for Java classes (jt400.zip) to your PC.

   This file contains the AS/400 Toolbox for Java classes that are needed in the sample Java program.

   File: jt400.zip

   Location: /QIBM/ProdData/HTTP/Public/jt400/lib

   If you have already installed IBM AS/400 Client Access Express on your PC, you can skip this step, because the files are then already downloaded to the C:\Program Files\IBM\Client Access\jt400\lib\ directory.

2. Download the SSL component classes and the tools class to your PC.

   This file enables the Java program to use SSL connections.

   File: sslightu (128-bit), or sslightx.zip (40 or 56-bit)

   Location: /QIBM/ProdData/HTTP/Public/jt400/SSLnm (nm=40,56,128)

   If you have already installed IBM AS/400 Client Access Express on your PC, you can skip this step, because the files are already downloaded to the C:\Program Files\IBM\Client Access\jt400\lib\directory:

3. Set up the CLASSPATH variable on your PC.

   You must add the following location name:

   ```
   CLASSPATH=c:\Program Files\IBM\Client Access\jt400\lib\jt400.zip;
   ```

   ToolBox for Java classes

```
c:\jdk1.1.8\lib\classes.zip;
c:\jdk1.1.8\bin;
c:\jdk1.1.8;
.;          your Java program location
c:\Program Files\IBM\Client Access\jt400\lib\sslightu.zip; ->
            SSL classes
c:\Program Files\IBM\Client Access\jt400\lib\SSLTools.zip ->
            SSL tool classes
```

4. Set up the KeyRing file for the AS/400 Toolbox for Java.

   The AS/400 Toolbox for Java classes refer to the KeyRing.class file when establishing an SSL connection. The CA certificate of the authority that has issued the server certificate that is used by the connection partner must be in that file. The well-known CAs have already been included in the KeyRing.class file in the jt400.zip archived class file. If you are using a private CA server certificate, you must also add the private CA certificate into the KeyRing class file. Perform the following steps to add the certificate to the KeyRing.class file:

   a. Create the following directory on your PC:

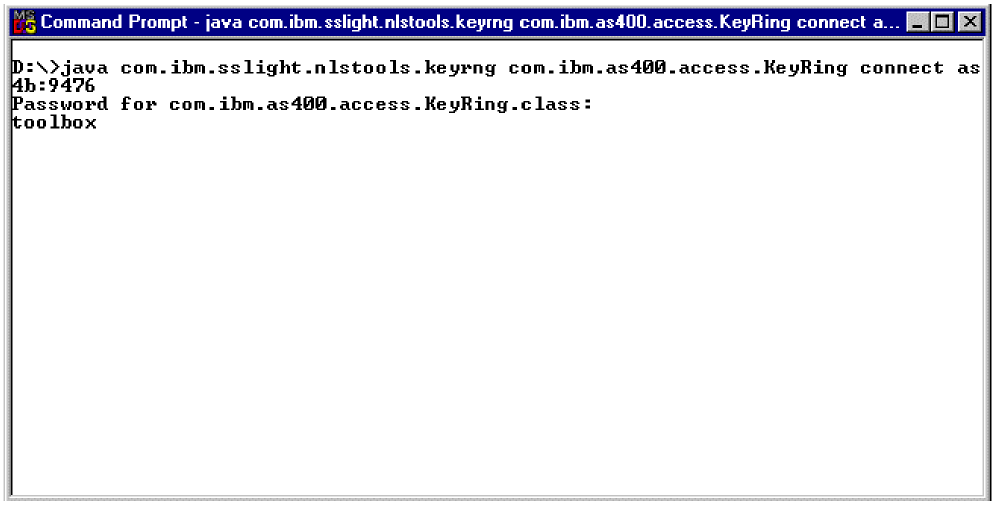
      ```
      MD C:\com\ibm\as400\access
      ```

      The directory represents the path structure of the KeyRing.class in the jt400.zip file. It can be on any disk drive but has to be specified from the root. It cannot be a subdirectory of an existing directory.

   b. Run the SSL tool to receive the private CA certificate.

      This tool downloads the CA certificate from the AS/400 system into the KeyRing class file on your PC. Enter the following command in a DOS window:

      ```
      C:\>java com.ibm.sslight.nlstools.keyrng com.ibm.as400.access.KeyRing
      connect <systemname> : <port>
      ```


Command Prompt - java com.ibm.sslight.nlstools.keyrng com.ibm.as400.access.KeyRing connect a...

```
D:\>java com.ibm.sslight.nlstools.keyrng com.ibm.as400.access.KeyRing connect as
4b:9476
Password for com.ibm.as400.access.KeyRing.class:
toolbox
```

Figure 254. Java SSL tool

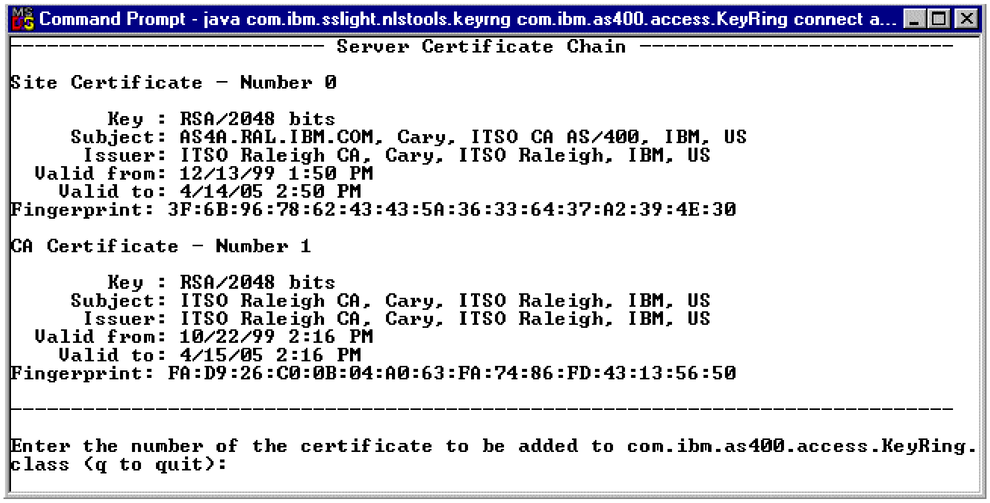
Note

The keyrng tool from the SSLTools can also be performed using the QShell interface on the AS/400 system. To do this, enter the command `QSH` from an AS/400 command prompt, set the CLASSPATH as shown in this section, and perform the same command as shown in Figure 254. This is especially useful if you do not have a JDK installed on the PC where you are going to update the KeyRing.class file.

The system specified on this command has to be the system, where the private CA is set up. The port 9476 is the secured port of the AS/400 sign-on host server. Note that the command has to be performed from the root directory where the directory structure from step 1a is on.

c. Enter the password `toolbox` and press Enter.

The password to be entered here is fixed and cannot be changed.

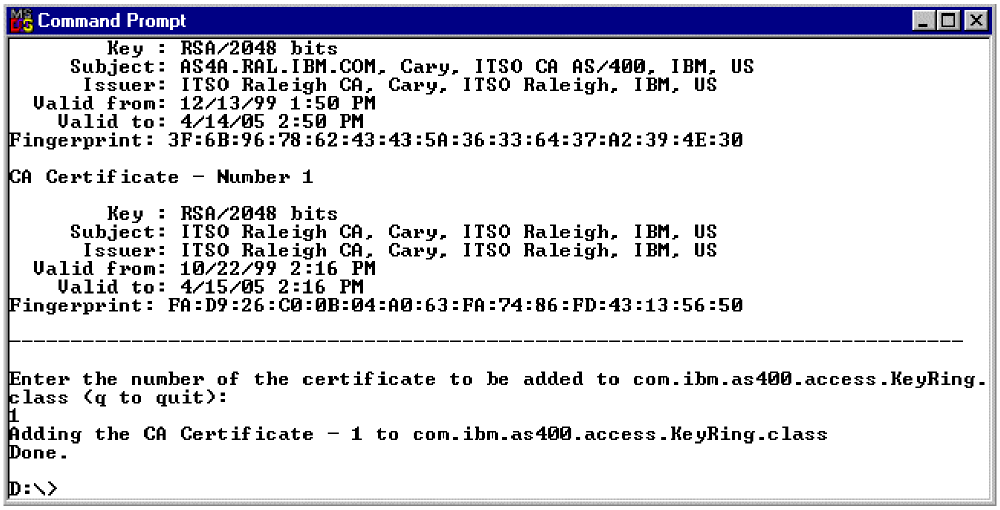

Command Prompt - java com.ibm.sslight.nlstools.keyrng com.ibm.as400.access.KeyRing connect a...

```
-------------------------- Server Certificate Chain --------------------------

Site Certificate - Number 0

        Key : RSA/2048 bits
     Subject: AS4A.RAL.IBM.COM, Cary, ITSO CA AS/400, IBM, US
      Issuer: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
  Valid from: 12/13/99 1:50 PM
    Valid to: 4/14/05 2:50 PM
Fingerprint: 3F:6B:96:78:62:43:43:5A:36:33:64:37:A2:39:4E:30

CA Certificate - Number 1

        Key : RSA/2048 bits
     Subject: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
      Issuer: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
  Valid from: 10/22/99 2:16 PM
    Valid to: 4/15/05 2:16 PM
Fingerprint: FA:D9:26:C0:0B:04:A0:63:FA:74:86:FD:43:13:56:50

------------------------------------------------------------------------------

Enter the number of the certificate to be added to com.ibm.as400.access.KeyRing.
class (q to quit):
```

Figure 255. Selection display

d. Select to download the private CA certificate.

You must choose the **CA certificate.** Do not select Site Certificate. For example, in this case, enter 1.

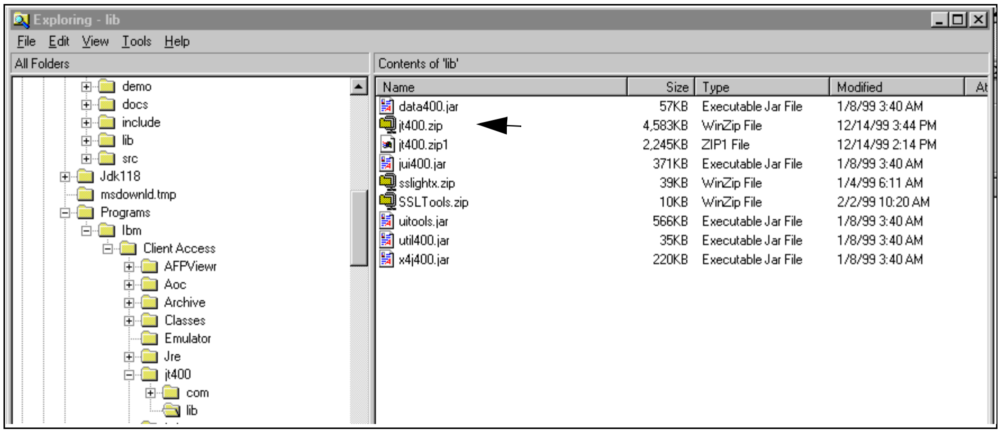


```
        Key : RSA/2048 bits
     Subject: AS4A.RAL.IBM.COM, Cary, ITSO CA AS/400, IBM, US
      Issuer: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
  Valid from: 12/13/99 1:50 PM
    Valid to: 4/14/05 2:50 PM
Fingerprint: 3F:6B:96:78:62:43:43:5A:36:33:64:37:A2:39:4E:30

CA Certificate - Number 1

        Key : RSA/2048 bits
     Subject: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
      Issuer: ITSO Raleigh CA, Cary, ITSO Raleigh, IBM, US
  Valid from: 10/22/99 2:16 PM
    Valid to: 4/15/05 2:16 PM
Fingerprint: FA:D9:26:C0:0B:04:A0:63:FA:74:86:FD:43:13:56:50

------------------------------------------------------------------------------

Enter the number of the certificate to be added to com.ibm.as400.access.KeyRing.
class (q to quit):
1
Adding the CA Certificate - 1 to com.ibm.as400.access.KeyRing.class
Done.

D:\>
```

Figure 256. Completion message

The SSL tool creates the KeyRing.class file in the directory you created (com.ibm.as400.access). This class now also contains the private CA certificate.

5. The next step replaces the existing KeyRing.class file with the new file within the jt400.zip file. The jt400.zip file contains the AS/400 Toolbox for Java classes and resides in the Client Access directory as shown in Figure 257.

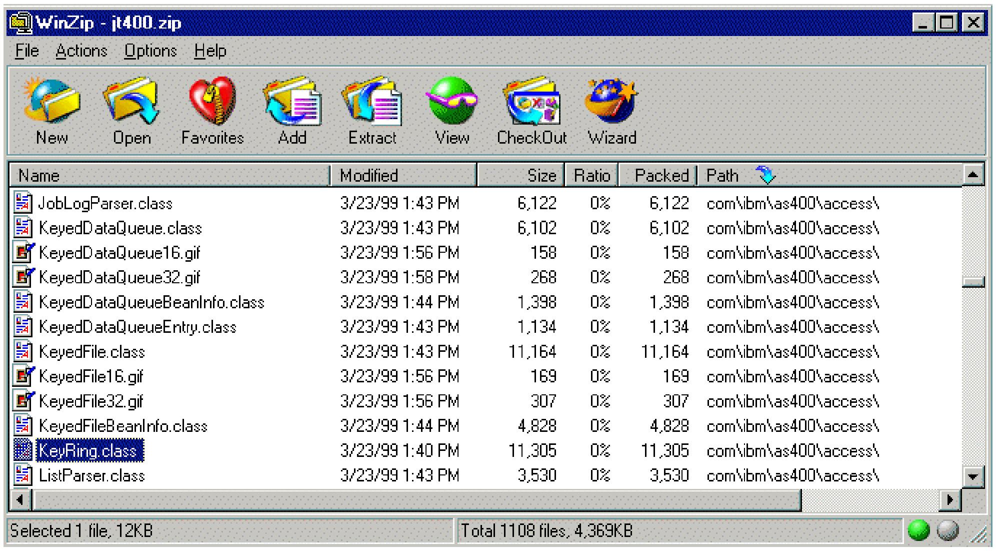


Name	Size	Type	Modified
data400.jar	57KB	Executable Jar File	1/8/99 3:40 AM
jt400.zip	4,583KB	WinZip File	12/14/99 3:44 PM
jt400.zip1	2,245KB	ZIP1 File	12/14/99 2:14 PM
jui400.jar	371KB	Executable Jar File	1/8/99 3:40 AM
sslightx.zip	39KB	WinZip File	1/4/99 6:11 AM
SSLTools.zip	10KB	WinZip File	2/2/99 10:20 AM
uitools.jar	566KB	Executable Jar File	1/8/99 3:40 AM
util400.jar	35KB	Executable Jar File	1/8/99 3:40 AM
x4j400.jar	220KB	Executable Jar File	1/8/99 3:40 AM

Figure 257. Directory of jt400.zip file

In this scenario, we have installed WinZip 7.0. This product enables the user to double-click a zip file to open the archive. If you are using another utility to work with zip files, the steps to replace a file within a zip file might be different.

6. Double-click **jt400.zip** to open the Toolbox archive.



Name	Modified	Size	Ratio	Packed	Path
JobLogParser.class	3/23/99 1:43 PM	6,122	0%	6,122	com\ibm\as400\access\
KeyedDataQueue.class	3/23/99 1:43 PM	6,102	0%	6,102	com\ibm\as400\access\
KeyedDataQueue16.gif	3/23/99 1:56 PM	158	0%	158	com\ibm\as400\access\
KeyedDataQueue32.gif	3/23/99 1:58 PM	268	0%	268	com\ibm\as400\access\
KeyedDataQueueBeanInfo.class	3/23/99 1:44 PM	1,398	0%	1,398	com\ibm\as400\access\
KeyedDataQueueEntry.class	3/23/99 1:43 PM	1,134	0%	1,134	com\ibm\as400\access\
KeyedFile.class	3/23/99 1:43 PM	11,164	0%	11,164	com\ibm\as400\access\
KeyedFile16.gif	3/23/99 1:56 PM	169	0%	169	com\ibm\as400\access\
KeyedFile32.gif	3/23/99 1:56 PM	307	0%	307	com\ibm\as400\access\
KeyedFileBeanInfo.class	3/23/99 1:44 PM	4,828	0%	4,828	com\ibm\as400\access\
KeyRing.class	3/23/99 1:40 PM	11,305	0%	11,305	com\ibm\as400\access\
ListParser.class	3/23/99 1:43 PM	3,530	0%	3,530	com\ibm\as400\access\

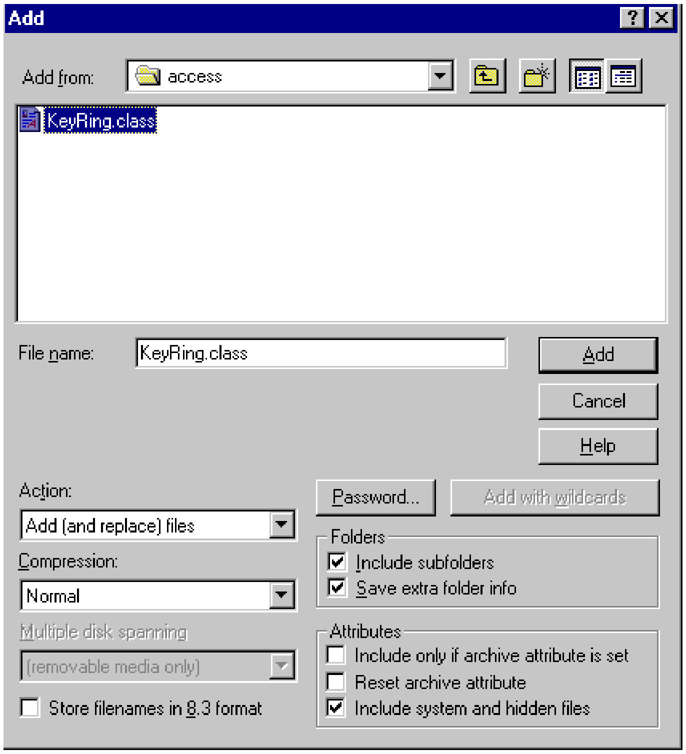
Selected 1 file, 12KB

Total 1108 files, 4,369KB

Figure 258. Archive contents of jt400.zip

Note the file date in the Modified column. After you replaced the file, this date should change.

7. Select the **KeyRing.class** file and click the **Add** button on the navigation bar.



Add from: access

KeyRing.class

File name: KeyRing.class

Action: Add (and replace) files

Compression: Normal

Multiple disk spanning: (removable media only)

☐ Store filenames in 8.3 format

Folders
☑ Include subfolders
☑ Save extra folder info

Attributes
☐ Include only if archive attribute is set
☐ Reset archive attribute
☑ Include system and hidden files

Figure 259. Adding/Replacing the KeyRing.class file

Select the file **\com\ibm\as400\access\KeyRing.class** and the options shown in Figure 259. Click **Add**.

Note

It is important to have the KeyRing.class file in the \com\ibm\as400\access directory. If you select the file from another directory, the KeyRing.class file will not be replaced in the jt400.zip file. Instead the new file will be added to the end of the archive, because the path is different. You may also use the CwbCoSSL utility to update the KeyRing.class file in the Client Access product subdirectory \IBM\Client Access\Classes\com\ibm\as400\access. Due to the different path of the existing KeyRing.class file in the archive, this file needs to be copied into the \com\ibm\as400\access directory. Refer to 6.2.4.1, “Configuring Client Access Express for SSL” on page 192 for further information about the CwbCoSSL utility.

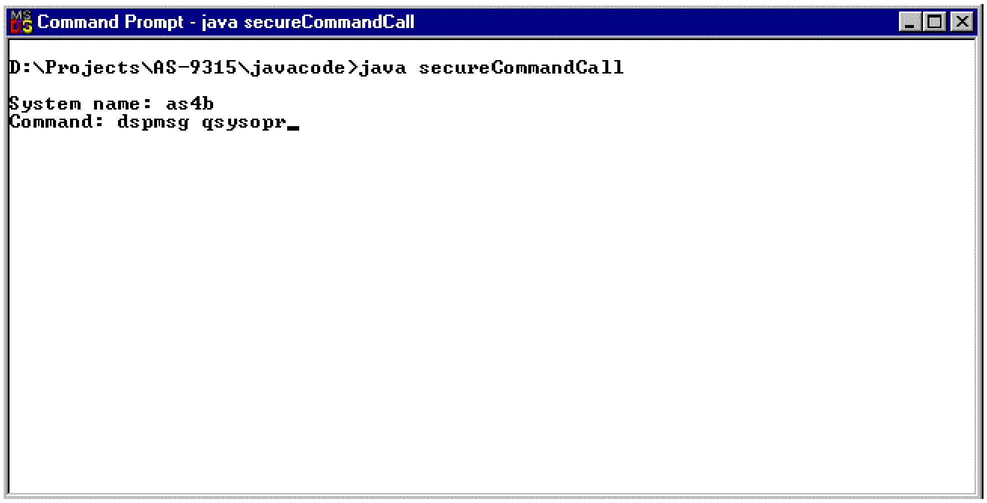
The changed date in the archive for the KeyRing.class file indicates a successful update. Close the archive.

6.7.5 Verifying the SSL connection using a sample Java program

To successfully verify an SSL connection, you need to enable a secured connection in your Java code. Refer to Appendix D, “Sample Java program using SSL” on page 397 for sample applications using the AS/400 Toolbox for Java to communicate over SSL. Perform the following steps to verify an SSL connection:

1. Use the `NETSTAT *CNN` command on an AS/400 command prompt to check that the appropriate server ports are in the Listen state. Table 4 on page 188 shows the SSL ports used by the AS/400 host servers.
2. Open a DOS window.
3. To run the Java sample program used in this example, enter:

   ```
   java secureCommandCall.
   ```

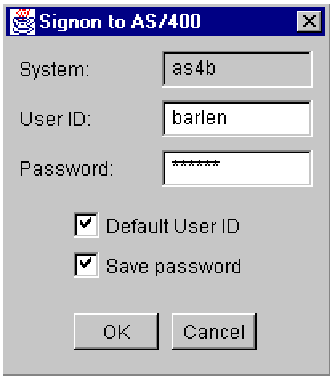


```
D:\Projects\AS-9315\javacode>java secureCommandCall

System name: as4b
Command: dspmsg qsysopr_
```

Figure 260. Sample Java program

Enter the system name of the AS/400 system to which an SSL connection will be established and the OS/400 command to be performed on that system.

The AS/400 Toolbox for Java SecureAS400() object has several constructors. If you choose the constructor that requires no parameter, a sign-on prompt is automatically presented on your display.


Signon to AS/400

System: as4b

User ID: barlen

Password: ******

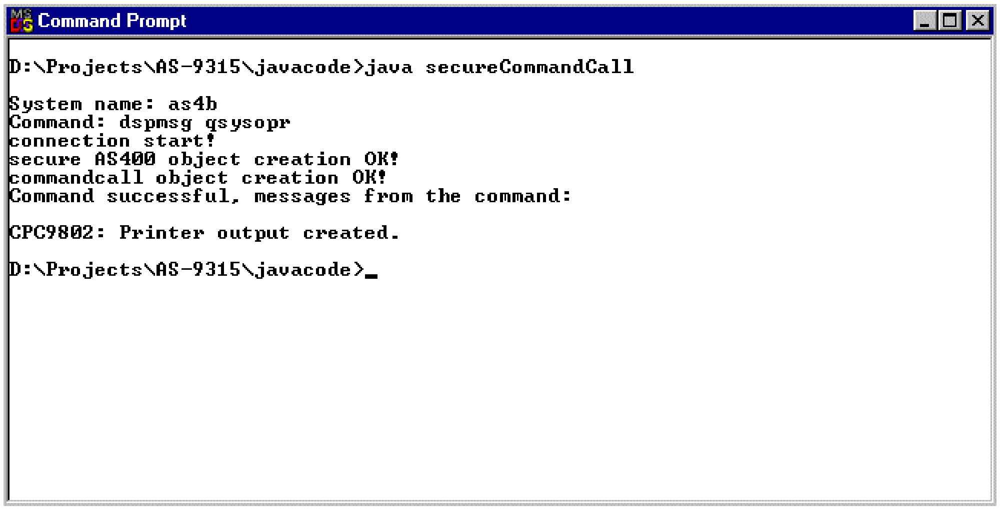
☑ Default User ID

☑ Save password

Figure 261. Sign-on window

4. Enter the user ID and password and click **OK**.

   The Java program establishes an SSL connection to the AS/400 system using the Toolbox classes. After establishing the SSL connection, the Java program sends the user ID and password encrypted to the secure host sign-on server. Then the command is sent to the secure host remote command server.

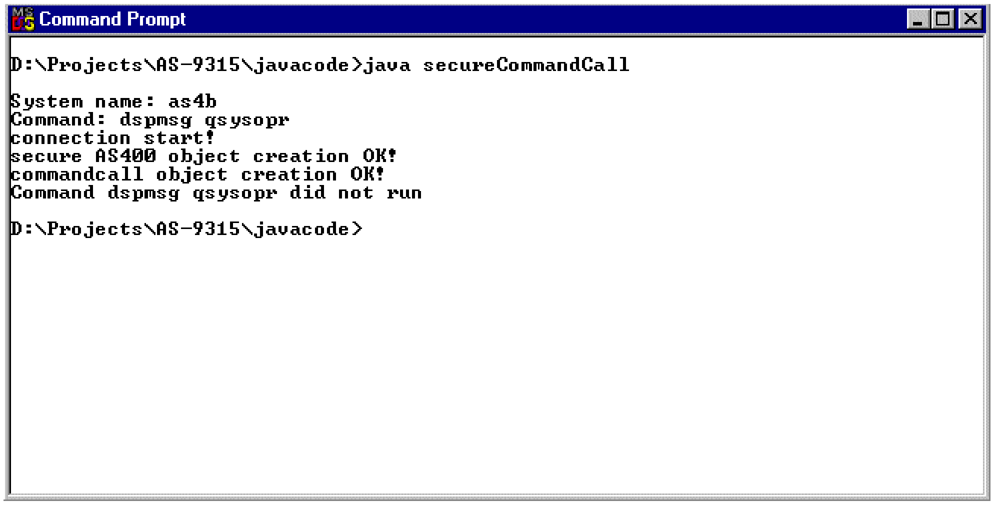


```
D:\Projects\AS-9315\javacode>java secureCommandCall

System name: as4b
Command: dspmsg qsysopr
connection start!
secure AS400 object creation OK!
commandcall object creation OK!
Command successful, messages from the command:

CPC9802: Printer output created.

D:\Projects\AS-9315\javacode>_
```

Figure 262. Result of the secureCommandCall program

The command performed in this example creates a spoolfile containing the contents of the QSYSOPR message queue.

If the appropriate CA certificate is not included in the KeyRing.class file, the previous program call shows the following message:



```
D:\Projects\AS-9315\javacode>java secureCommandCall

System name: as4b
Command: dspmsg qsysopr
connection start!
secure AS400 object creation OK!
commandcall object creation OK!
Command dspmsg qsysopr did not run

D:\Projects\AS-9315\javacode>
```

Figure 263. Program call result when the CA certificate is missing

This means that the SSL connection failed during initialization. Assuming that logging is enabled in the QSYS/QZBSJOBD job description, the sign-on host server shows the following message:

```
CPIAD08   40    12/14/99   16:05:20   QZBSCOMM    QSYS    *STMT    QZBSCOMM
   From module . . . . . . . . :   QZBSCOMM
   From procedure  . . . . . . :   SndCPIAD08__FiN21
   Statement . . . . . . . . . :   2604
   To module . . . . . . . . . :   QZBSCOMM
   To procedure  . . . . . . . :   SndCPIAD08__FiN21
   Statement . . . . . . . . . :   2604
   Message . . . . . :   Host server communications error occurred on
     SSL_Handshake().
   Cause . . . . . :   Error code -16 was received while processing the
     SSL_Handshake() function for the host server communications. Recovery  .
     :   See any previously listed message(s) to determine the cause of the
     error; if necessary, correct the error and issue the request again. .
```

6.8 Enabling SSL for DDM and DRDA

You can also secure Distributed Data Management (DDM) and Distributed Relational Database Architecture (DRDA) connections using the SSL protocol. It can be used to interoperate with clients such as AS/400 Toolbox for Java and Client Access OLE DB Provider that support SSL for record level access, and with any DRDA application requester products or DDM file I/O clients provided by independent software vendors (ISV) that support SSL. To use SSL with the AS/400 DDM/DRDA TCP/IP server, the client must be configured to connect to the well-known port 448 on the server.

Table 12 shows the IP ports and associated service names used by DRDA and DDM on the AS/400 system.

Table 12. Port numbers used by DDM and DRDA

Connection	Port number	Server	Service name
No SSL	446	DRDA	drda
No SSL	447	DDM	ddm
SSL	448	DDM/DRDA	ddm-ssl

The DDM/DRDA server jobs run in the QSYSWRK subsystem. Be sure to have them started in order to access the database on the AS/400 system using these services.

The server jobs are:

QRWTLSTN DRDA/DDM listener job that listens for incoming DRDA/DDM requests on the ports listed in Table 12.

QRWTSRVR This job processes DRDA/DDM requests which are assigned from the listener job.

6.8.0.1 Implementation tasks overview

To use DDM and DRDA with SSL, you must perform these tasks:

1. Be sure to have all of the required license programs installed.

   Refer to 6.8.2, “Prerequisites” on page 265 for a list of those license programs.

2. Prepare a CA certificate and server certificate.

   Refer to Chapter 5, “Digital Certificate Manager for AS/400” on page 107.

3. Set up the DDM server on your AS/400 system to use SSL.

6.8.1 Objective

The objective of this section is to show you how to enable SSL for DDM and DRDA connections. A private CA is used that issues a server certificate for the DDM/DRDA TCP server on the AS/400 system. Figure 264 shows the environment that is described in this section.

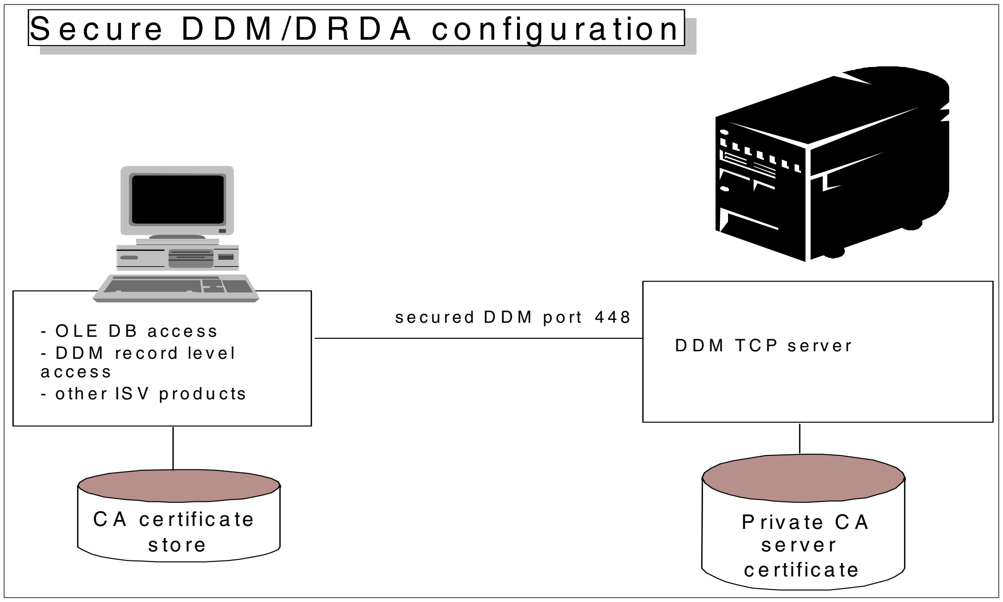


Figure 264. Secure DDM/DRDA connection.

6.8.2 Prerequisites

The following AS/400 license programs must be installed for this scenario:

- Digital Certificate Manager (DCM), option 34 of OS/400 (5769-SS1)

  Used to assign a server certificate to the DDM TCP server.

- TCP/IP Connectivity Utilities for AS/400 (5769-TC1)
- IBM HTTP server for AS/400 (5769-DG1)

  Used to run the Digital Certificate Manager.

- One of the IBM Cryptographic Access Provider products:

  5769-AC1 (40-bit)

  5769-AC2 (56-bit)

  5769-AC3 (128-bit)

- If you are using the AS/400 Toolbox for Java or other Client Access utilities to securely access the database with DDM, you need at least one of the following AS/400 products:

  5769-CE1 (40-bit)

  5769-CE2 (56-bit)

  5769-CE3 (128-bit)

  Encryption classes are included in these products.

6.8.3 Configuring the AS/400 system

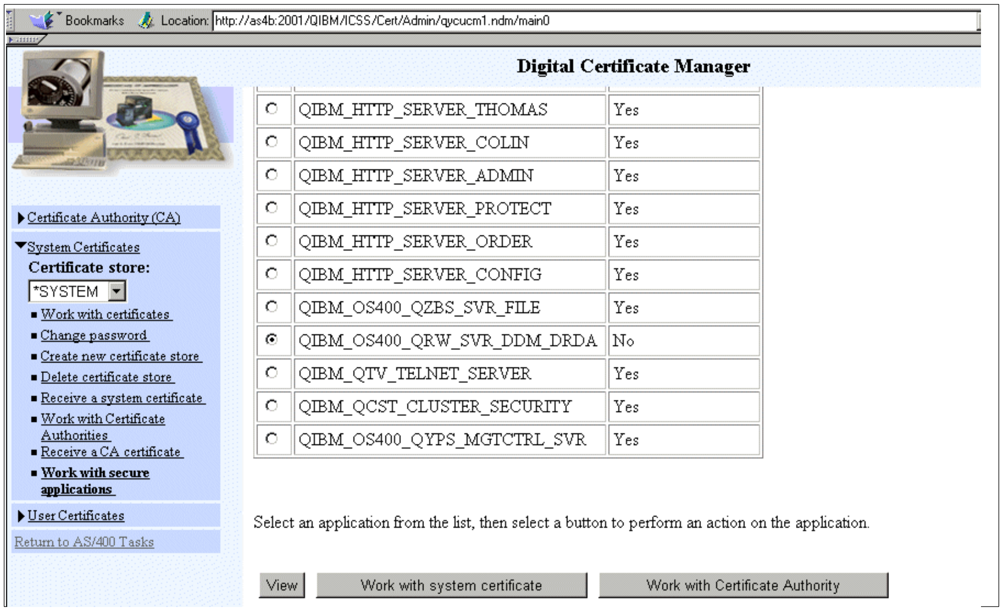
We assume that a server certificate has already been obtained from the private CA and is available along with the CA certificate on the AS/400 system. Refer to Chapter 5, “Digital Certificate Manager for AS/400” on page 107 for a detailed description of how to create a private Certificate Authority and a server certificate.

To enable SSL for DDM/DRDA, you have to assign a server certificate to the DDM/DRDA TCP server. The following steps take you through this process:

1. Start the AS/400 Tasks page by entering the following URL in your Web browser:

```
http://as400hostname:2001/ (Specify 2010 when using the SSL admin port)
```

2. Click the **Digital Certificate Manager** link.
3. Expand **System Certificates**. Enter the certificate store password when prompted.
4. Click **Work with secure applications**.


Bookmarks
Location:
Digital Certificate Manager
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Work with system certificate
Work with Certificate Authority

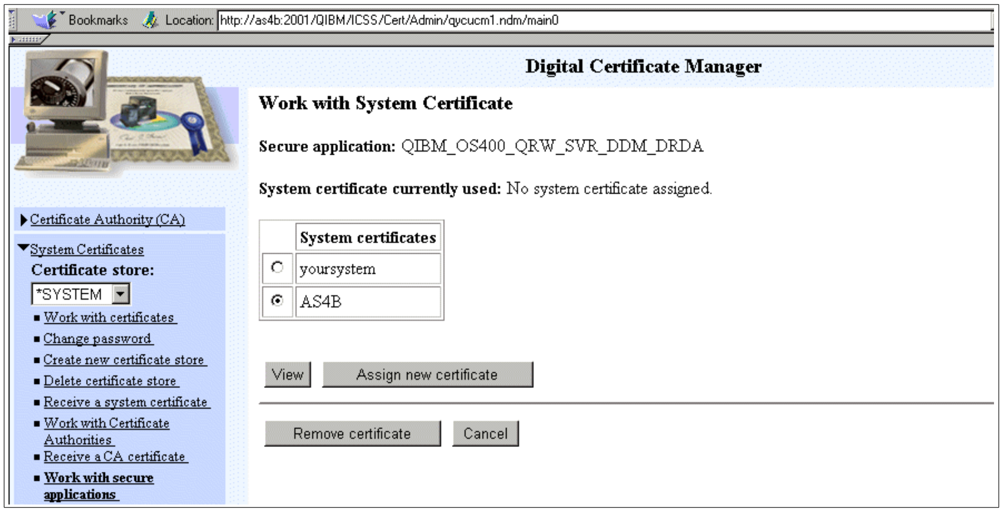
Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

○	QIBM_HTTP_SERVER_THOMAS	Yes
○	QIBM_HTTP_SERVER_COLIN	Yes
○	QIBM_HTTP_SERVER_ADMIN	Yes
○	QIBM_HTTP_SERVER_PROTECT	Yes
○	QIBM_HTTP_SERVER_ORDER	Yes
○	QIBM_HTTP_SERVER_CONFIG	Yes
○	QIBM_OS400_QZBS_SVR_FILE	Yes
●	QIBM_OS400_QRW_SVR_DDM_DRDA	No
○	QIBM_QTV_TELNET_SERVER	Yes
○	QIBM_QCST_CLUSTER_SECURITY	Yes
○	QIBM_OS400_QYPS_MGTCTRL_SVR	Yes

Select an application from the list, then select a button to perform an action on the application.

Figure 265. DCM - Work with secure applications - DDM/DRDA

5. Select DDM/DRDA TCP server application ID **QIBM_OS400_QRW_SVR_DDM_DRDA** and click **Work with system certificate**.



Bookmarks
Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
View
Assign new certificate
Remove certificate
Cancel

Digital Certificate Manager

Work with System Certificate

Secure application: QIBM_OS400_QRW_SVR_DDM_DRDA

System certificate currently used: No system certificate assigned.

	System certificates
○	yoursystem
●	AS4B

Figure 266. Assign a server certificate to the DDM/DRDA server

6. Select the server certificate that is to be assigned to the DDM/DRDA server, in this case **AS4B** and click **Assign new certificate**.

   A completion message indicates that the server certificate is successfully assigned to DDM/DRDA TCP server.

7. Click **Work with secure applications** again, select the **QIBM_OS400_QRW_SVR_DDM_DRDA** application ID and click **Work with Certificate Authority** to be sure that the appropriate CAs are marked as trusted.

Be sure to have the DDM/DRDA TCP server started. Perform the following command from the AS/400 command prompt to start the server:

```
STRTCPSVR SERVER(*DDM)
```

6.8.4 Configuring the PC

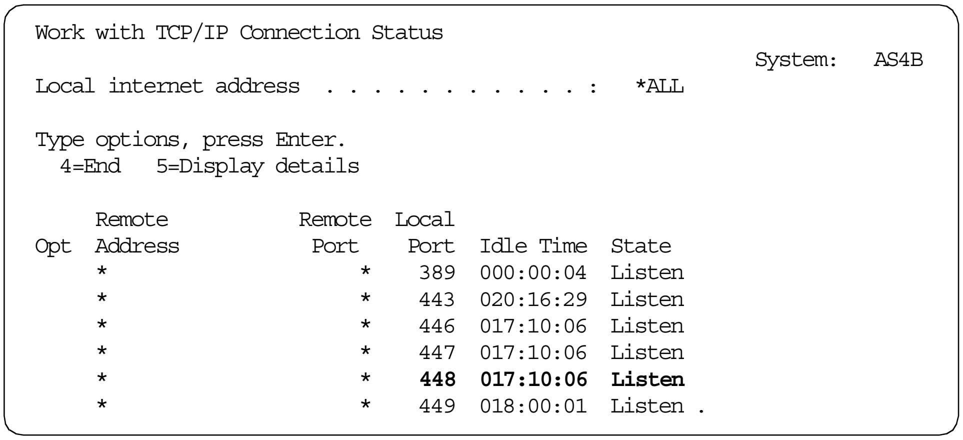
Depending on the client application that is accessing the DDM/DRDA server on the AS/400 system using the SSL protocol, the client application have to accept the server certificate. For example, if you are accessing the AS/400 database with AS/400 Toolbox for Java classes using record level access, the CA certificate of the private CA has to be in the KeyRing.class (Refer to 6.7, “Enabling the AS/400 Toolbox for Java to use SSL” on page 254). When using Client Access to access the AS/400 database through DDM, the CA certificate must also be registered as a trusted root in the Client Access key database (Refer to 6.2, “Enabling SSL for IBM AS/400 Client Access Express” on page 187).

Other client applications may have other processes in place to check if the CA that issued the server certificate is trusted by that application. Refer to the individual product documentation in order to accept a server certificate that is issued by a CA that is not registered.

6.8.5 Verifying SSL on the DDM/DRDA server

After the DDM/DRDA server is configured to support SSL connections, perform the following steps to verify that the server is listening to the appropriate port:

1. Use the AS/400 command `NETSTAT *CNN` to check that port 448 is in the Listen state.



```
Work with TCP/IP Connection Status
                                                             System:   AS4B
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote          Remote  Local
Opt  Address          Port    Port  Idle Time  State
     *                    *    389  000:00:04  Listen
     *                    *    443  020:16:29  Listen
     *                    *    446  017:10:06  Listen
     *                    *    447  017:10:06  Listen
     *                    *    448  017:10:06  Listen
     *                    *    449  018:00:01  Listen .
```

Figure 267. DDM/DRDA port status

   If port 448 does not appear in the list of listening ports, be sure that the DDM/DRDA TCP servers are started. The two jobs, QRWTLSTN and QRWTSRVR are running in the QSYSWRK subsystem. By default, you do not see the QRWTSRVR job. You have to press the F14 key to expand the list of running jobs to see this job. Use the command `STRTCPSVR SERVER(*DDM)` to start the DDM/DRDA servers.

2. When a connection using the SSL protocol is established, check that port 448 is used for this connection.

Part 3. Using digital certificates in user applications

Chapter 7. Introducing digital certificates in user applications

As you have seen in previous chapters, the AS/400 system supports the Secured Socket Layer (SSL) protocol together with digital certificates for most of the server applications provided in OS/400. The Digital Certificate Manager (DCM) is the central application to manage digital certificates on the AS/400 system. However, OS/400 license programs, such as DCM can only provide functions that are commonly used. That means, even if these license programs provide many functions to create, manage, and use digital certificates in an AS/400 environment, user applications may have specific needs that require additional programming.

To use and manage digital certificates in user applications, the AS/400 system provides a set of application programming interfaces (APIs) that can be used in Original Program Model (OPM) and Integrated Language Environment (ILE) programming environments, such as RPG. Refer to Chapter 3, “Introducing digital certificate management APIs” on page 25 for an introduction to these APIs.

Of course, the AS/400 system also provides the support for digital certificates in Java programs. Whether you are using the IBM WebSphere Application Server to run Java servlets, or using the AS/400 Toolbox for Java, or writing Java applications that are communicating over sockets, the AS/400 system supports classes to use digital certificates for this kind of application.

7.1 Basic considerations

There are several considerations to be taken into account when planning to use or manage digital certificates in user applications. First of all you have to decide whether you want to use only server certificates or both, server and client certificates. If you are using server certificates only (which means the certificate can be used to authenticate the server by the client and to establish an SSL connection) there is in most cases no need for modifying the application. But when you use client certificates as well you need to code additional functions in your program. With client certificates you can authenticate a client user within your system or application. They also allow control of access to your application.

7.1.1 Using server certificates only

As previously stated, a server certificate is used during session establishment of an SSL connection. Depending on what kind of application you are running on the AS/400 system, you may have to perform additional steps to use SSL with certificates for this application.

7.1.1.1 Running a Web application based on HTTP Server for AS/400

A user Web application that uses Common Gateway Interface (CGI) programs needs no modification to use server certificates only. When you enable the HTTP server instance to use SSL, the HTTP Configuration and Administration utility automatically adds an application ID for this server instance to the list of secure applications in DCM. Once the application ID for this server instance is available in DCM, you can associate a server certificate with that application. When a user establishes a connection using the HTTPS protocol with the server, the assigned server certificate is used to establish the connection and authenticate the server by the client.

7.1.1.2 Using sockets applications in an ILE environment

A sockets application uses the sockets API to establish a connection between the server and the client. The sockets API is located in the communications model between the application and the transport layers. The sockets API is not a layer in the communication model; it is an API that allows applications to interface with the transport or networking layers of the typical communications model.

When using a sockets application with SSL, you have to register the application in DCM using the Register Application for Certificate Use (QSYRGAP, QsyRegisterAppForCertUse) API. This makes the application known to DCM and you can then use DCM to associate a server certificate with this application. SSL connections in sockets applications are then established using the SSL_Init_Application() API. This API, which was introduced with V4R4, takes the application ID as an input parameter and retrieves the associated server certificate including the private key from the certificate store. The private key, which never leaves the server system, is used for encrypting and decrypting data that was encrypted or being decrypted by the public key of the server certificate.

7.1.1.3 Running Java servlets with IBM WebSphere Application Server

The IBM WebSphere Application Server is a Java servlet-based Web application server that helps you deploy and manage Web applications on the AS/400 system. On the AS/400 system the WebSphere application server works in conjunction with the IBM HTTP Server for AS/400. That means the IBM HTTP Server for AS/400 is the access point to the WebSphere Application Server. Therefore, you do not need to modify your servlets to use SSL with server certificates only. The only requirement to use server certificates with servlets running under the WebSphere Application Server is to associate a server certificate with the HTTP server instance.

7.1.2 Using client certificates

Client certificates can be used to authenticate the client user and to control access to the system or application. Depending on what you want to achieve with client certificates, you have to perform additional programming in your application. For example, if you want to store a client certificate into a validation list, your application needs to be modified to perform this task.

7.1.2.1 Running a Web application based on HTTP Server for AS/400

The IBM HTTP Server for AS/400 can be configured to request a client certificate during SSL session establishment. The client certificate is then automatically stored into environment variables that can be accessed through CGI programs. If configured, the server authenticates a client’s certificate and grants access to protected resources. In this case, the user application does not need to be modified. All the configuration is done in the HTTP server configuration.

As soon as you want to use, for example, attributes of a client certificate to control access to a database, you need to write routines in your application to read the required information from the environment variables. Refer to Chapter 4, “Securing the HTTP Server for AS/400” on page 35 for more information about the HTTP server configuration and using certificates to control access to AS/400 resources.

Based on a sample application, this chapter explains how to use and manage client certificates in user applications.

7.1.2.2 Using sockets applications in an ILE environment

When using client authentication in sockets applications the server must be set up for SSL as mentioned in 7.1.1, “Using server certificates only” on page 271. In addition you have to specify that client authentication is required when defining the SSL_Handshake() function of the SSL APIs. Refer to Chapter 9 of *OS/400 UNIX-Type APIs V4R4*, SC41-5875 for detailed information on defining the SSL_Handshake() function and how to obtain the client certificate. Once the client certificate (also referred to as the peer certificate) is received, the digital certificate and validation list APIs can be used to further process and manage the certificate on the AS/400 system.

7.1.2.3 Running Java servlets with IBM WebSphere Application Server

In addition to the security directives in the HTTP server configuration, which allow, for example, to check for valid client certificates, you can use and manage client certificates in Java servlets. The first task in a user application is to receive the client certificate. This is done by using the getAttribute() method from the ServletRequest interface of the javax.servlet package. Once the certificate is received, you can use other methods to, for example, encode or parse the client certificate.

Refer to Chapter 9, “Sample application: using certificates in Java” on page 337 for explanations of how to use and manage client certificates in servlets. The sample application in that chapter uses the WebSphere Application Server.

7.2 Introducing the sample application

We have created a sample application in order to demonstrate the use of some of the functions for managing client certificates on the AS/400 system and to provide working code that can be copied and modified as required.

The application is provided for two programming language environments:

- CGI REXX and RPG programs, where digital certificate and validation list APIs are used in ILE RPG programs.
- Java servlets that are running under control of the WebSphere Application Server. The servlets and a Java program that uses the AS/400 Toolbox for Java demonstrate how to use client certificates in a Java environment.

This section describes the application interfaces and functions that are common in both the REXX/RPG and Java application.

The application will service the following scenario:

- We are hosting a Web site that offers services to our clients and our suppliers.
- Both services require secure communications. Clients must be registered before they are able to use the services. For the registration process they have to possess a valid client certificate. Also, they have to give a credit card number and an e-mail address.
- We plan to have a large number of clients. A validation list will hold the certificates of these clients. The HTTP server and the application programs will use the validation list for client authentication.
- We have a small number of suppliers and they work closely with us. The applications allowed to each supplier may vary. We will create a user profile for

each supplier and associate the supplier's certificate with the user profile. AS/400 system authorities will be used to control the applications these clients can access. We will also have a directory for each supplier that they can access using a Web browser. These will also be secured using AS/400 system authorities so that each supplier can access only its own directory.

The sample application performs the following functions:

- Registering a new client or supplier.
- Displaying a registered client's orders.

  Or displaying a customized error window to unregistered clients and to clients with a pending registration request.
- Displaying the contents of a supplier's directory.

  Or displaying a customized error window to users who are not suppliers.
- Allowing clients and suppliers to maintain some of the information held about them.
- Renewing (which means replacing) certificates for registered clients and suppliers.

The sample application consists of:

- HTML pages
- An HTTP server configuration
- User programs
  - CGI programs written in REXX
  - Programs written in RPG using APIs to perform the various functions required.

  Or:
  - Java servlets
  - Java program
  - WebSphere Application Server configuration
- A client file and an orders file
- Validation lists to hold certificates for pending and accepted clients.
- A couple of data areas
- A library to hold all the application objects
- An IFS directory to hold the suppliers' directories
- A user profile to hold the common authorities of user profiles created for suppliers

The entire sample application with its sources is available from the IBM Redbooks Web site. Refer to Appendix E, "Using the additional material" on page 401 for information in how to find and get the material from the Web.

Some utilities used in the REXX/RPG sample application are downloaded from the IBM AS/400 Technical Studio at the following URL:

`http://www.as400.ibm.com/tstudio/workshop/snippets/snippets.htm`

7.2.1 Disclaimer

This is not a complete system.

It does not do all the things a working client management system would need to do. It does not handle all the error conditions that could occur. Its procedure for renewing certificates has security weaknesses. But it's supposed to show the principles for renewing (which is actually replacing) certificates for an account.

However, our intent is not to create a full working system but instead to demonstrate the use of system functions for handling certificates in a realistic context.

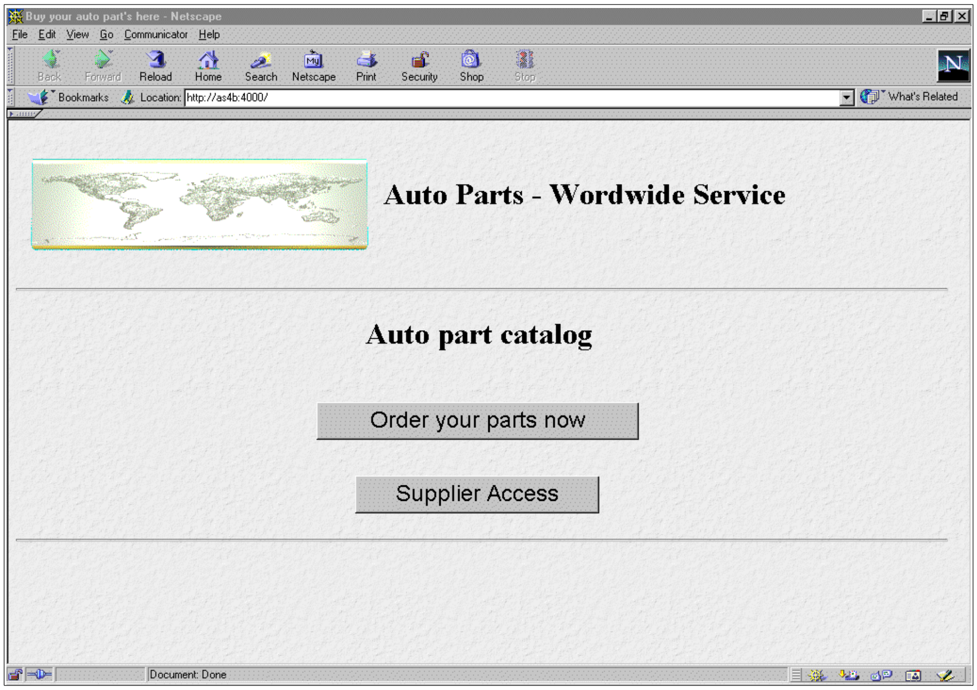
Please use the programs in this system to understand how to use those functions and possibly as a basis for your own programs. Do not try to use the system as it stands in a production environment.

7.3 Sample application interfaces and flow

This section describes the user interfaces and functions of the sample application. It also provides an overview of the logical flow that clients and suppliers have to follow to get access to the application.

7.3.1 Main window

The sample application shown in this chapter offers clients and suppliers a Web-based user interface. They are presented with an unprotected initial window as shown in Figure 268. The Web browser used to test the application was Netscape's Communicator 4.7.



Location: http://as4b:4000/

Auto Parts - Wordwide Service

Auto part catalog

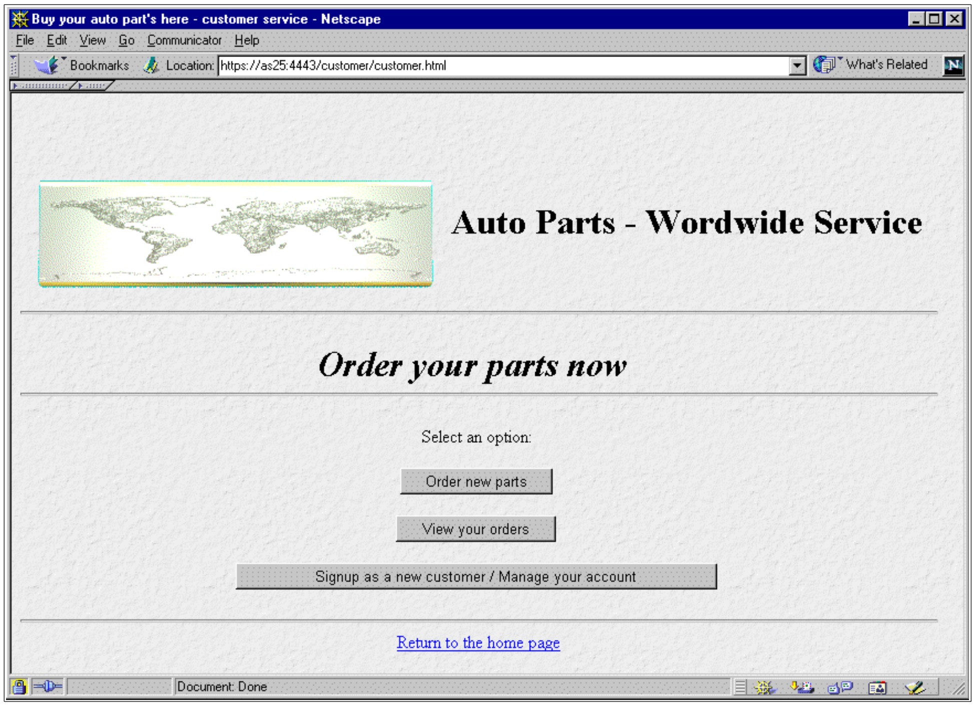
Document: Done

Figure 268. Initial window

Order your parts now is the entry link for our clients. **Supplier access** is the link for suppliers. The parts catalog is not active. Note that this window is accessed using the HTTP protocol. No SSL is used yet.

7.3.2 Client’s main window

On the initial window, click **Order your parts now** to display the base window for our clients. This window is protected using SSL so the user has to present a valid client certificate to see it.



Buy your auto part's here - customer service - Netscape

Location: https://as25:4443/customer/customer.html

Auto Parts - Wordwide Service

Order your parts now

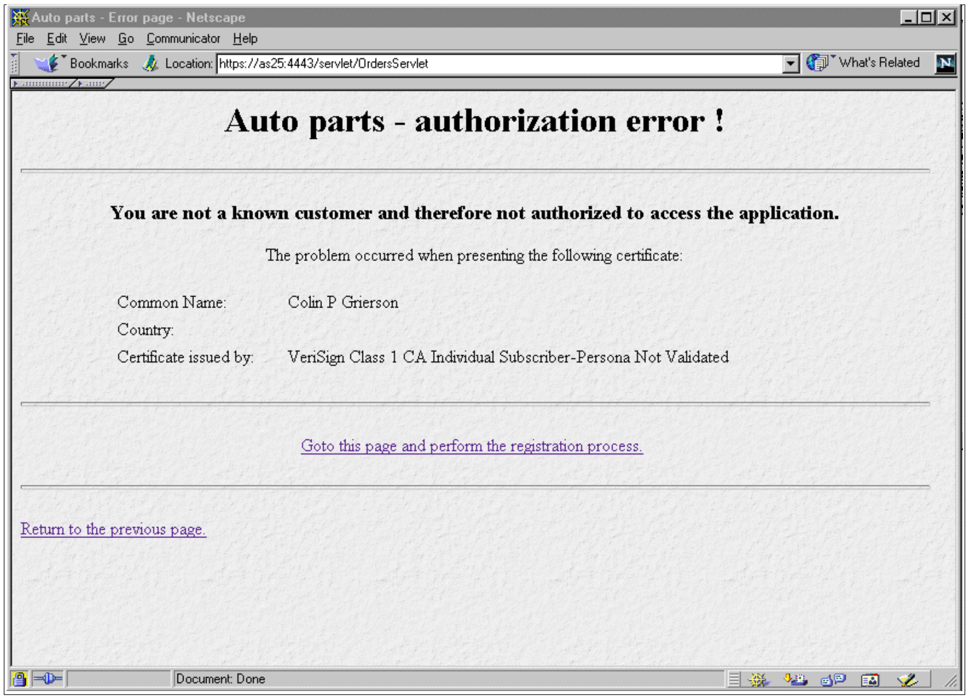
Select an option:

Return to the home page

Document: Done

Figure 269. Client main window

If you try to use one of the options **Order new parts** or **View your orders** without having registered, the following error window is displayed.


Auto parts - Error page - Netscape
File Edit View Go Communicator Help
Bookmarks Location: https://as25:4443/servlet/OrdersServlet
What's Related

Auto parts - authorization error !

You are not a known customer and therefore not authorized to access the application.

The problem occurred when presenting the following certificate:

Common Name:	Colin P Grierson
Country:	
Certificate issued by:	VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

Goto this page and perform the registration process.

Return to the previous page.

Figure 270. Not registered error window

The Common Name, Country and CA is retrieved from the presented client certificate.

We could use HTTP protection setups to secure these options but this would not allow us to give a personalized and useful friendly error window. Instead, we do the checking in a program and format the preceding window as required.

7.3.2.1 REXX/RPG application

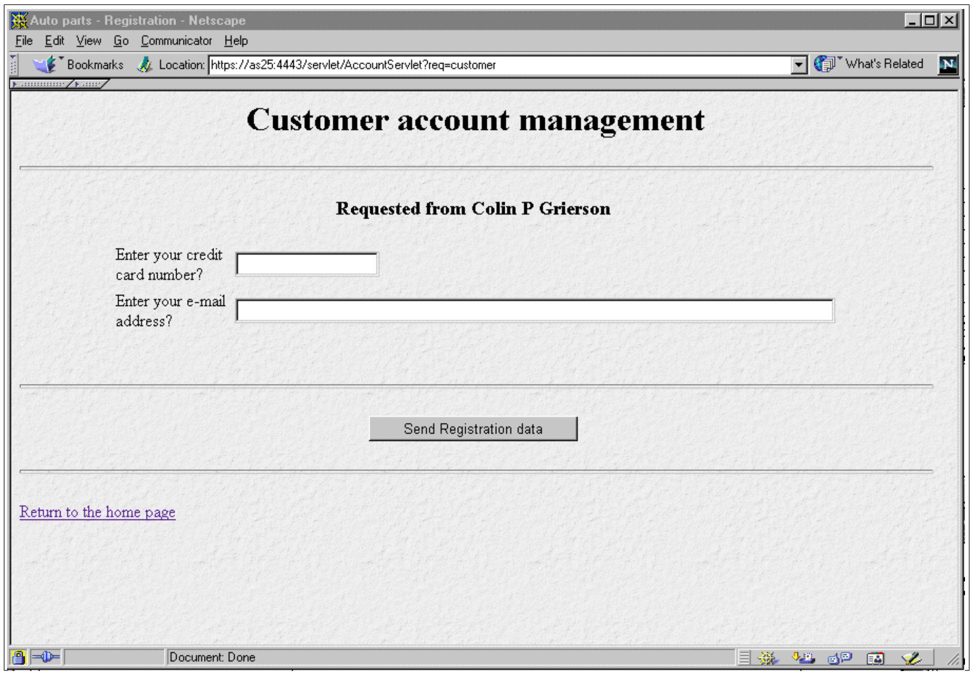
The REXX CGI procedure REQCLT1 gets invoked when the user clicks one of the buttons on the client main window. This procedure calls the RPG program CHKCERVLDL, which is used to check if the client's certificate is in the appropriate validation list.

7.3.2.2 Java application

Depending on the button pressed, different servlets are invoked. For example, if the client clicks the **View your orders** button, the OrdersServlet starts. The servlet uses the checkForCertificateInVLDL method of the ClientCertificates class to check if the client certificate is in the appropriate validation list.

7.3.3 Registration

Click the option **Signup as a new customer/Manage your account** to display the registration window. If the client user is not registered yet, the registration window is displayed as shown in Figure 271.


Auto parts - Registration - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: https://as25:4443/servlet/AccountServlet?req=customer
What's Related
Send Registration data
Document: Done

Customer account management

Requested from Colin P Grierson

Enter your credit card number?

Enter your e-mail address?

Return to the home page

Figure 271. Client registration/Account management

The client has already presented their certificate so we retrieve their name from that certificate. Remember that not all CAs validate all of the fields that go into a certificate, so the user name that is put into the certificate may or may not be a good idea to use. In this system we just ask for a credit card number and e-mail address. In a production system you would probably need more information than this, such as the client's address, phone number, and so on.

This window is also used for account maintenance. If a client returns to this window the system displays their current details and allows the client to change them.

REXX/RPG application

The REXX CGI procedure CLTREQ1 is invoked when the user clicks the **Signup as a new customer/Manage your account** button.

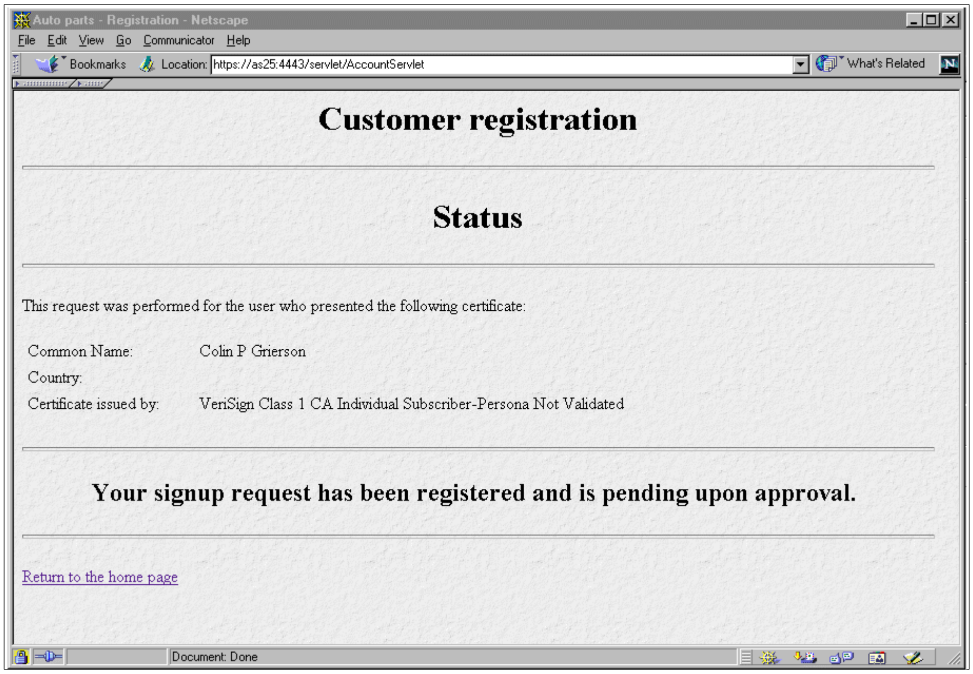
Since this window is also used to update account data, the procedure checks first if the client certificate is stored in the ACCEPTED or PENDING validation list. If the certificate is present in one of the validation lists, the user is already registered and the account number will be displayed. Note that the available buttons change if the user already exists. In the case of a new user, the client user has to click the **Send Registration data** button to register the client certificate along with the information provided on the registration window.

Then the RPG program REGCLT2 is used to record a new registration request or change the details of an existing client.

Java application

The AccountServlet is used to register new and manage existing user accounts. This servlet first checks if a user account already exists for the presented client certificate. The necessary data is obtained using the AuthenticatedUser class. This class is also used to finally update the account database.

Click **Send registration data** to record the new data or changes to existing data. The following confirmation is displayed.


Auto parts - Registration - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: https://as25:4443/servlet/AccountServlet
What's Related
Document: Done

Customer registration

Status

This request was performed for the user who presented the following certificate:

Common Name:	Colin P Grierson
Country:	
Certificate issued by:	VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

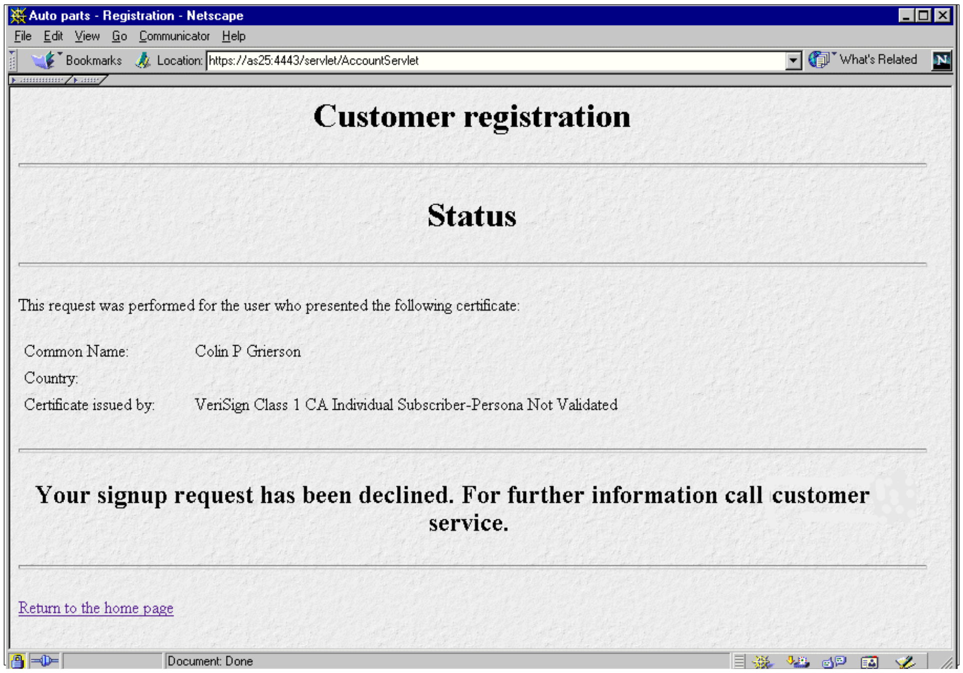
Your signup request has been registered and is pending upon approval.

Return to the home page

Figure 272. Registration confirmation

The client management staff periodically reviews pending registrations. They perform the relevant checks, and either accept or decline the request. When a registration is approved the client's status is changed. Also, their certificate is moved from the validation list for pending registrations to the validation list for approved (that is, accepted) clients. If a registration is declined we maintain client details, including the certificate handle, so that further registration requests can be automatically rejected as shown in Figure 273.

.



Auto parts - Registration - Netscape
File Edit View Go Communicator Help
Bookmarks Location: https://as25:4443/servlet/AccountServlet
What's Related

Customer registration

Status

This request was performed for the user who presented the following certificate:

Common Name:	Colin P Grierson
Country:	
Certificate issued by:	VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

Your signup request has been declined. For further information call customer service.

Return to the home page

Figure 273. Automatic rejection of a registration request

REXX/RPG application

The RPG program APPCLTREG is used to accept or decline registration requests.

Java application

The java program RegistrationAdmin is used on a PC to accept or decline registration requests.

7.3.4 Registered client options

From the client main window, shown in Figure 269 on page 276, click the option **View your orders** to display your current orders. This option is built into the application to demonstrate how to relate client certificates with actual data stored in a database. The basic flow for viewing orders is as follows:

1. A client user enters the application through a Web browser and presents the client certificate.
2. A program on the server retrieves the client certificate and gets the certificate handle. Then the program searches for an account record that contains the certificate handle and retrieves the client account number. Once the client account number is known, it will be used to retrieve all client orders that match this account number.
3. The CGI program sends the client's order data back to the browser.

Note

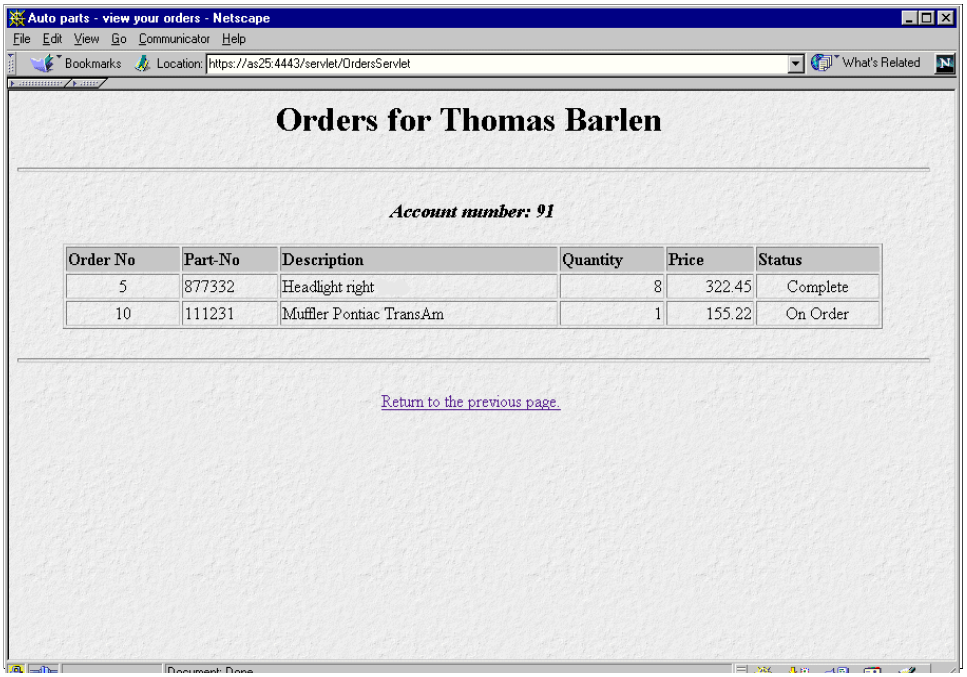
When you test the application, a new client account number will be assigned to each new registered client. Therefore, you have to change the account number of some records in the ORDDTLP file in order to get order data displayed when clicking the **View your orders** option. For example, you can use SQL on the AS/400 system to change the account number in the order file:

```
STRSQL
UPDATE SALES/ORDDTLP SET DTLCLTNUM = 34 WHERE DTLCLTNUM = 33
```

where `SET DTLCLTNUM` defines the new value and `WHERE DTLCLTNUM` the value of the records to be changed. Perform the following SQL statement to update all records in the order file:

```
UPDATE SALES/ORDDTLP SET DTLCLTNUM = 34
```

You can also use the `UPDDTA FILE(SALES/ORDDTLP)` command on the OS/400 command prompt to update the file.


Auto parts - view your orders - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: https://as25:4443/servlet/OrdersServlet
What's Related
Document: Done

Orders for Thomas Barlen

Account number: 91

Order No	Part-No	Description	Quantity	Price	Status
5	877332	Headlight right	8	322.45	Complete
10	111231	Muffler Pontiac TransAm	1	155.22	On Order

Return to the previous page.

Figure 274. Client orders

REXX/RPG application

When clicking the **View your orders** button, the REXX procedure REQCLT1 retrieves the client name from the environment variable HTTPS_CLIENT_CERT_COMMON_NAME. Remember that not all CAs validate all of the fields that go into a certificate. If you are using a common name, be sure that the CAs trusted by the application verify the field as needed; otherwise, may be the CA should not be trusted. The procedure then calls the RTVCLTDTA RPG program to retrieve the client account number. This data is displayed as heading information on the order details window. In the next step the procedure calls the RPG program RTVCLTORD to retrieve the orders for the current client. The order details are displayed in a table.

Java application

The OrdersServlet is used to perform the request to view client orders.

Clicking the option **Order new parts** displays a message that the online service is not yet active.

7.3.5 Renewing a client's certificate

Renewing is a misnomer; actually we must replace an old certificate with a new one. The problem is how to link the two certificates. A browser will present only one certificate at a time so we need a two-step process with a secure way of linking the steps. The steps involved in this process are:

1. User enters the application with the current client certificate.
2. The user takes the option to change the account certificate.
3. The user gets some information that identifies this particular change request.
4. All browser windows must be closed.
5. The user starts the browser again and enters a specific window using the new certificate to perform the second phase of the change request. The information given in step 3 is used to complete the change request and associate the new certificate with the account.

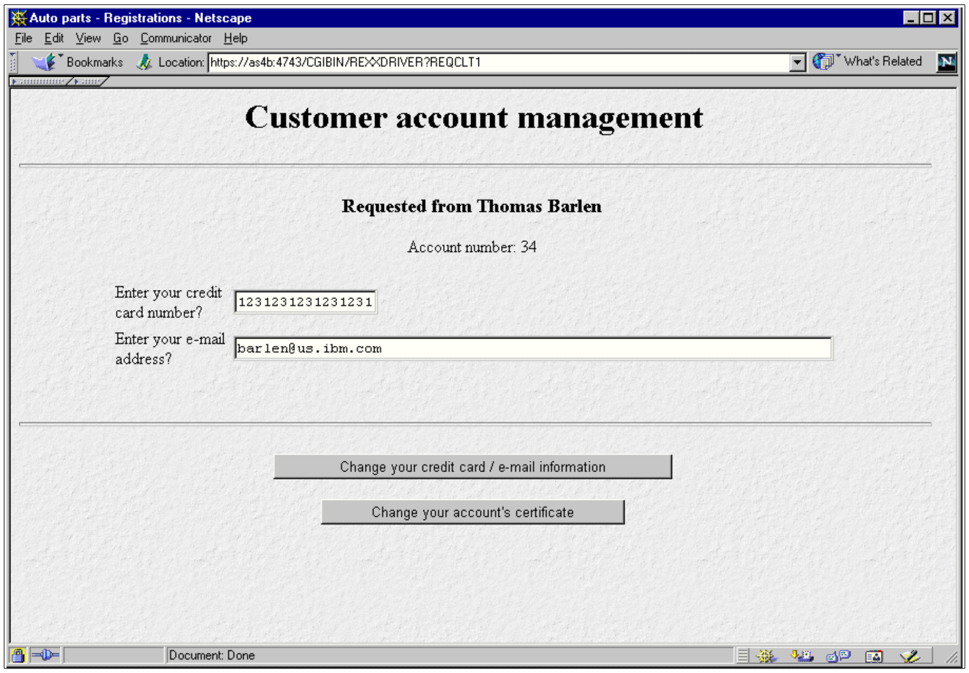
One reason for renewing or replacing a client certificate would be if the certificate is going to expire and the client has already obtained a new one. Then the new certificate needs to be associated with the client account.

The sample applications covered in this book have slightly different methods implemented to renew (replace) a client certificate. Therefore, this chapter contains separate sections for the RPG and the Java application.

7.3.5.1 Replacing a client certificate using the REXX/RPG application

The method used in the REXX/RPG application requires the user to manually perform the most important steps involved in replacing a client certificate.

To replace your certificate with a new one, click the option **Signup as a new customer/Manage your account** on the client main window. The account management window appears:


Auto parts - Registrations - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: https://as4b:4743/CGIBIN/REXXDRIVER?REQCLT1
What's Related

Customer account management

Requested from Thomas Barlen

Account number: 34

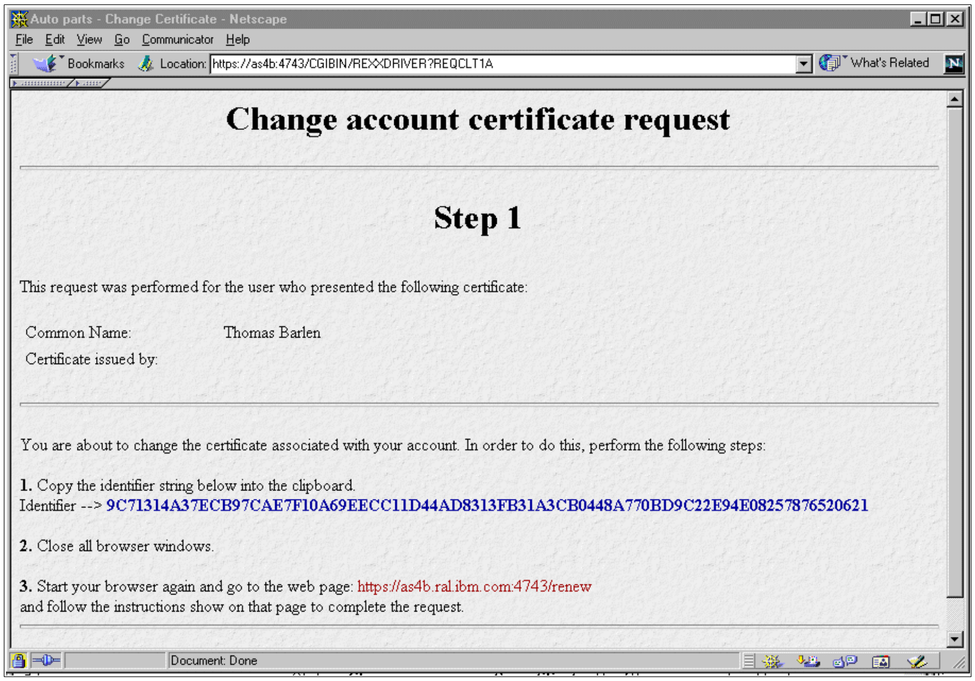
Enter your credit card number? 1231231231231231

Enter your e-mail address? barlen@us.ibm.com

Change your credit card / e-mail information
Change your account's certificate
Document: Done

Figure 275. Renewing a certificate

Click **Change your account's certificate**. The Change account certificate request window is displayed as shown in Figure 276. Note that this option is only available to clients that are registered as accepted clients. If the client user already enters the window with its new client certificate, only the Send Registration data button is displayed as would be the case for new users. This is because client users are identified by their certificate. And a new certificate (even if it contains the same attributes) gets a new serial number and expiration date and therefore is different from the old certificate.


Auto parts - Change Certificate - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: https://as4b:4743/CGIBIN/REXXDRIVER?REQCLT1A
What's Related
Document: Done

Change account certificate request

Step 1

This request was performed for the user who presented the following certificate:

Common Name:	Thomas Barlen
Certificate issued by:	

You are about to change the certificate associated with your account. In order to do this, perform the following steps:

1. Copy the identifier string below into the clipboard.
Identifier --> **9C71314A37ECB97CAE7F10A69EECC11D44AD8313FB31A3CB0448A770BD9C22E94E0825787652062l**

2. Close all browser windows.

3. Start your browser again and go to the web page: https://as4b.ral.ibm.com:4743/renew
and follow the instructions show on that page to complete the request.

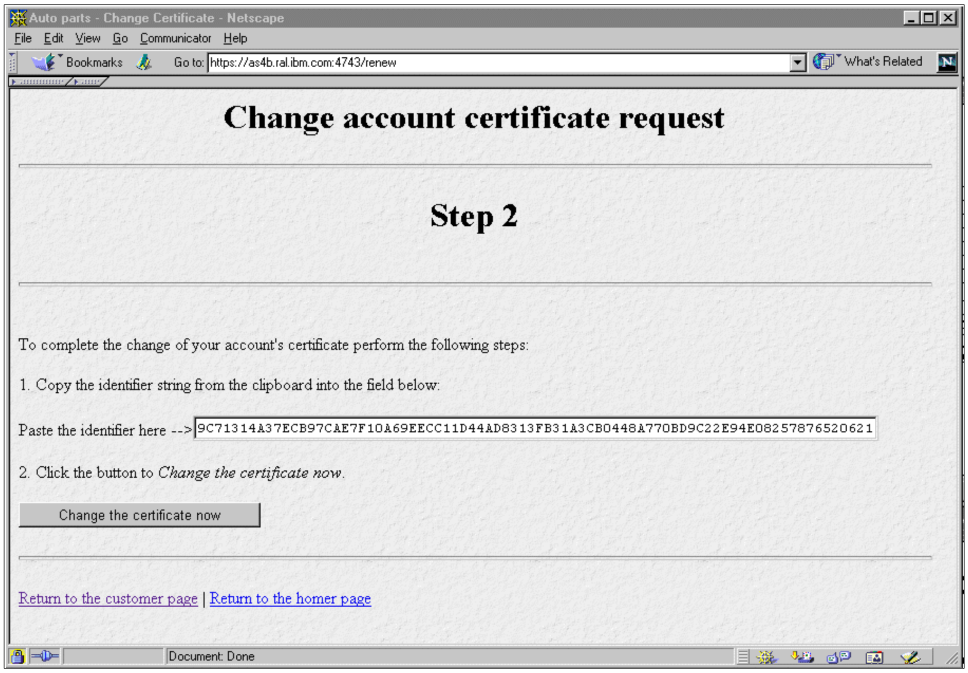
Figure 276. Renewing a certificate - step 1

The REXX procedure REQCLT1A calls the RPG program RTVCLTDTA. This program retrieves the client's account data including the certificate handle. The certificate handle will then be displayed on the Web browser along with instructions on how to proceed with the request.

Note the link to go to the next step, `https://as4b.ral.ibm.com:4743/renew`, then select and copy the identifier string `9C71314A37ECB`.... into the clipboard.

Close all open browser windows. This is necessary so that it does not automatically reuse your current certificate when you go to the link `https://as4b.ral.ibm.com:4743/renew`.

Restart your browser and go to the link `https://as4b.ral.ibm.com:4743/renew`. When requested for a certificate be sure to select your new certificate. The following window appears:


Auto parts - Change Certificate - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: https://as4b.ral.ibm.com:4743/renew
What's Related
Document: Done

Change account certificate request

Step 2

To complete the change of your account's certificate perform the following steps:

1. Copy the identifier string from the clipboard into the field below:

Paste the identifier here --> 9C71314A37ECB97CAE7F10A69EECC11D44AD8313FB31A3CB0448A770BD9C22E94E0825787652O621

2. Click the button to *Change the certificate now*.

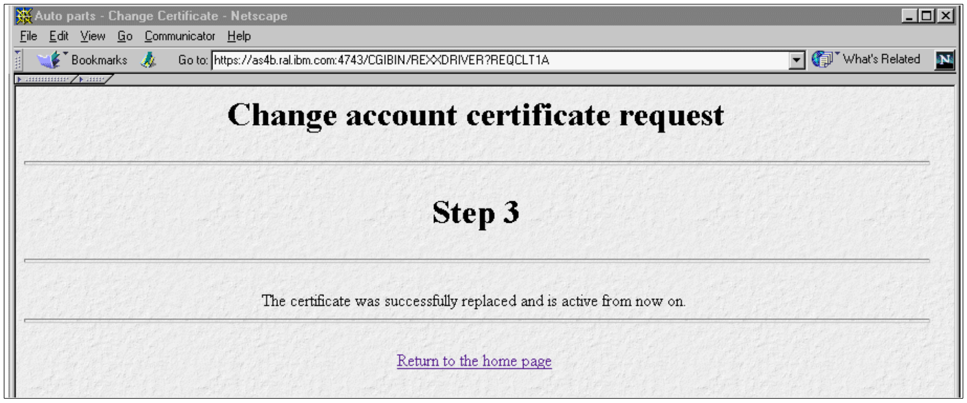
Return to the customer page | Return to the homer page

Figure 277. Renewing a certificate - step 2

Paste in the identifier you previously copied and click **Change the certificate now**.

The REXX procedure REQCLT1A is invoked. It calls the RPG program RENCLTCER, which is used to swap the certificates for the client.

The following window appears to confirm the change.


Auto parts - Change Certificate - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: https://as4b.ral.ibm.com:4743/CGIBIN/REXXDRIVER?REQCLT1A
What's Related

Change account certificate request

Step 3

The certificate was successfully replaced and is active from now on.

Return to the home page

Figure 278. Renewing a certificate, completion

From now on you must use the new certificate to enter the application.

The method we have used illustrates how a certificate might be replaced in a secure manner. However, the method used in the REXX/RPG application has a security weakness and could be made more convenient.

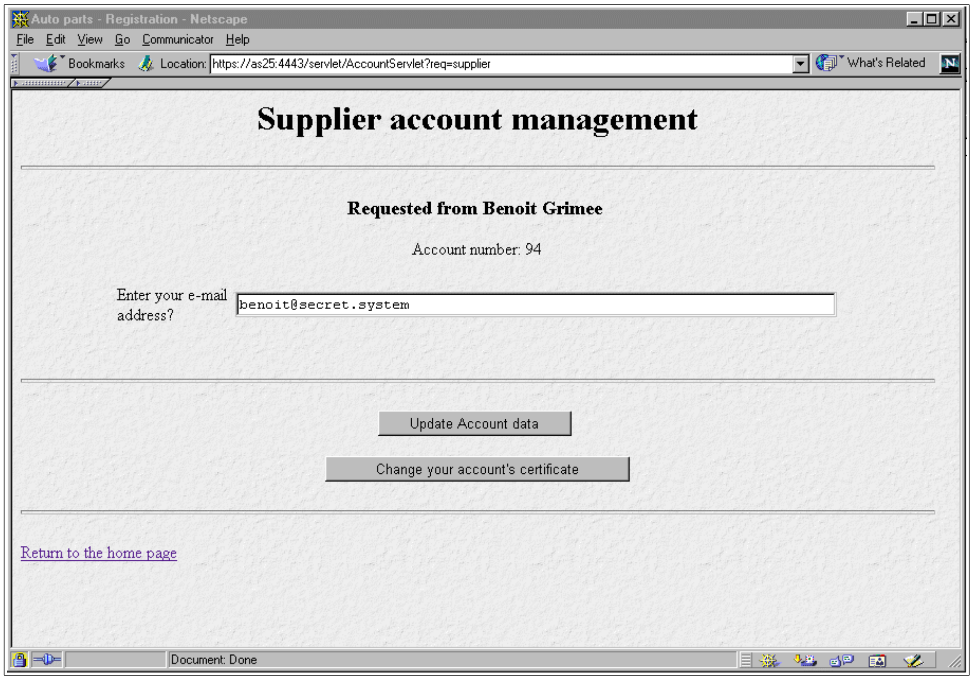
- The security weakness is the use of the handle as the link between the old and new certificates. This is convenient but our client's certificate handles are stored in the client master file so if someone obtains a copy of this file, they could then use the handles to "renew" another client's certificate with their own. A better link would be a random number with some mechanism to limit the time during which it can be used. The Java application addresses the security issues discussed in this section.

- Having to copy and reenter the handle, or whatever value is used as a link, is a bit messy. Using a cookie, as implemented in the Java application, to store the value on the client's browser would be a neater and easier-to-use solution.

7.3.5.2 Replacing a client certificate using the Java application

The security weakness problem discussed for the RPG application is addressed in the Java application. For example, a cookie is used to store the request identifier on the client's PC. Also the request identifier now consists of the certificate handle and a random number. The random number changes every time a new request to change the certificate is initiated. To make this process even more secure, the request identifier is stored in a hashtable in the servlet that processes the request. Also the cookie expires after one day and cannot be used to replace the certificate. We have chosen 24 hours to provide enough time to complete the request for users in different time zones. As long as the servlet stays active in memory, the user can complete the change request by reentering the Web browser with the new certificate. As soon as the new client certificate is active, the cookie value is removed from the client's browser and the request identifier deleted from the hashtable in the servlet.

Click **Signup as a new customer / Manage your account** on the client main window or on **Signup as a new supplier / Manage your account** on the supplier main window. The account management window appears:


Auto parts - Registration - Netscape
File Edit View Go Communicator Help
Bookmarks
Location:
What's Related

https://as25:4443/servlet/AccountServlet?req=supplier

Supplier account management

Requested from Benoit Grimee

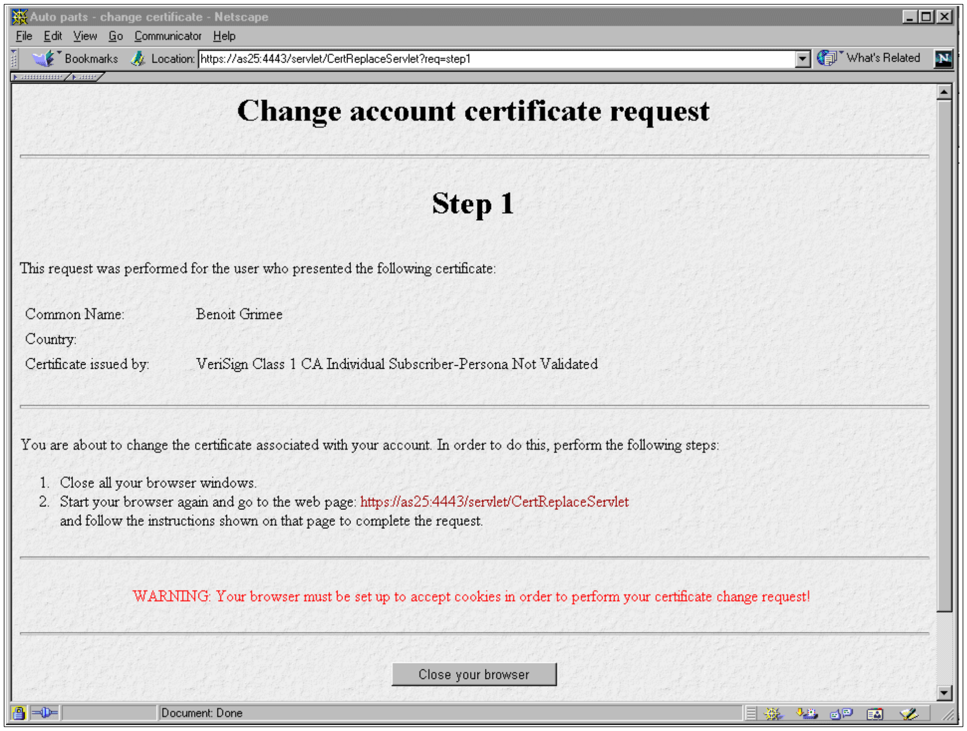
Account number: 94

Enter your e-mail address? benoit@secret.system

Update Account data
Change your account's certificate
Return to the home page
Document: Done

Figure 279. Account Management window

Click **Change your account's certificate**. The Change account certificate request window is displayed as shown in Figure 280. Note that this option is only available to clients that are registered as accepted clients. If the client user already enters the window with its new client certificate, only the Send Registration data button is displayed as it would be the case for new users. This is because client users are identified by their certificate. A new certificate (even if it contains the same attributes) gets a new serial number and expiration date and therefore is different from the old certificate.


Auto parts - change certificate - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: https://as25:4443/servlet/CertReplaceServlet?req=step1
What's Related
Document: Done

Change account certificate request

Step 1

This request was performed for the user who presented the following certificate:

Common Name:	Benoit Grimee
Country:	
Certificate issued by:	VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

You are about to change the certificate associated with your account. In order to do this, perform the following steps:

1. Close all your browser windows.
2. Start your browser again and go to the web page: https://as25:4443/servlet/CertReplaceServlet and follow the instructions shown on that page to complete the request.

WARNING: Your browser must be set up to accept cookies in order to perform your certificate change request!

Close your browser

Figure 280. Changing a client certificate - step 1

The CertReplaceServlet is used to change client certificates. It retrieves the certificate handle and generates a random number. This information is combined into a change request ID that is stored in a hashtable in the servlet and as a cookie on the browser.

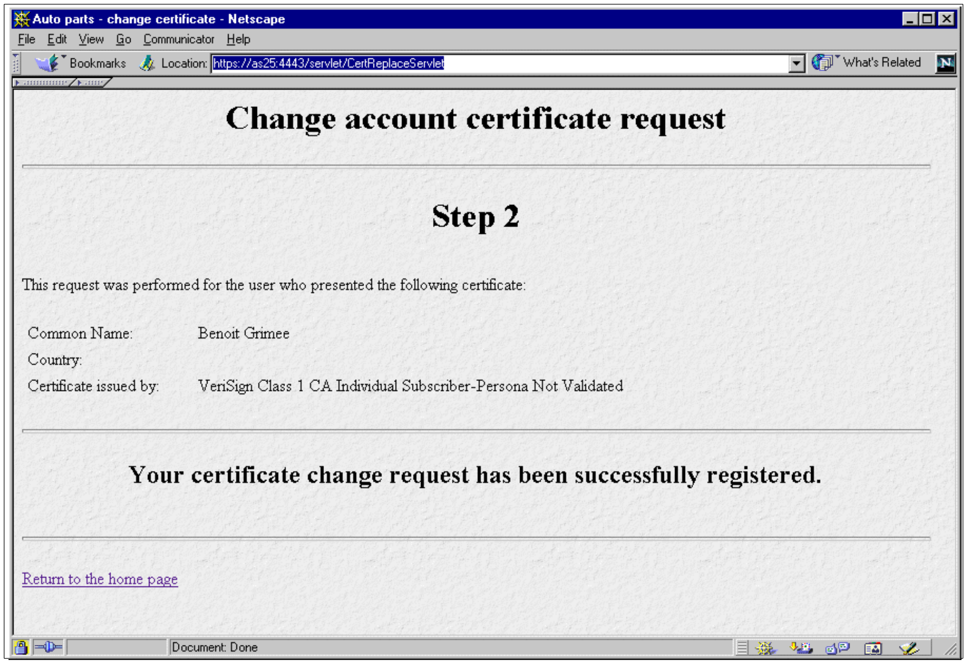
Copy the `https://as25:4443/servlet/CertReplaceServlet` link into the clipboard and click **Close your browser**. A window appears to confirm ending the browser. Note that this technique requires the browser to be configured to accept cookies. Otherwise, the servlet is not able to write the cookie data to the browser and step 2 of the change request will fail.

All browser windows need to be closed in order to select the new certificate when performing step 2 of the change request.

Start the browser again and paste the link from the clipboard into the browser's URL line. The CertReplaceServlet is invoked again and automatically reads the change request ID from the browser's cookie. It then swaps the certificate handles in the account database, deletes the old certificate from the ACCEPTED validation list, and adds the new one to it.

In the case of a supplier, the old certificate association is removed from the user profile and the new certificate is associated with the user profile.

After the change request has finished, a completion message is displayed.


Auto parts - change certificate - Netscape
File Edit View Go Communicator Help
Bookmarks Location: https://as25:4443/servlet/CertReplaceServlet
What's Related

Change account certificate request

Step 2

This request was performed for the user who presented the following certificate:

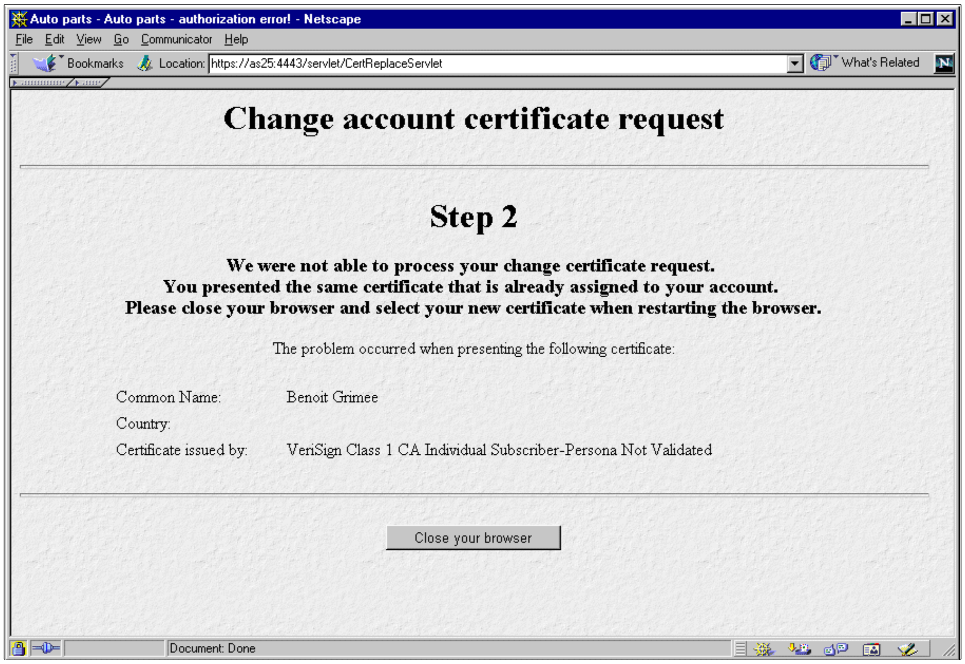
Common Name:	Benoit Grimee
Country:	
Certificate issued by:	VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

Your certificate change request has been successfully registered.

Return to the home page

Figure 281. Changing a client certificate - step 2

If the user selected the old certificate during step 2, the following error message is displayed.


Auto parts - Auto parts - authorization error! - Netscape
File Edit View Go Communicator Help
Bookmarks Location: https://as25:4443/servlet/CertReplaceServlet
What's Related

Change account certificate request

Step 2

We were not able to process your change certificate request.
You presented the same certificate that is already assigned to your account.
Please close your browser and select your new certificate when restarting the browser.

The problem occurred when presenting the following certificate:

Common Name:	Benoit Grimee
Country:	
Certificate issued by:	VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

Figure 282. Changing a client certificate - step 2 error message

Another way to provide the change request ID to the client user would be to send the ID in an e-mail note to the client.

7.3.6 Registration of a new supplier

Suppliers must also have a client certificate and must be registered in order to use the application. The steps to register a new supplier are basically the same as for clients. In addition an AS/400 user profile and a supplier directory will be created. The client certificate will be associated with the user profile. Permissions will be granted to the supplier's user profile to allow a supplier to access only its own directory. Care should be taken when approving suppliers if a user profile will be created. Problems could arise if the supplier is called QSYS, QSECOFR, and so on. Problems could also arise if duplicates are not handled correctly (two competitors should not be able to use the same directory).

To perform a supplier registration, select the **Supplier access** link on the initial window. Then select **Signup as a new supplier / Manage your account**. In this sample application we request only the supplier's e-mail address.

REXX/RPG application

New suppliers register in the same way as the clients do (Refer to 7.3.3, "Registration" on page 277). The client management staff has to approve the registration using the APPCLTREG program. Then the program ASSCERUSR must be used to create a user profile and a directory for the supplier. Further it associates the supplier's certificate with their user profile.

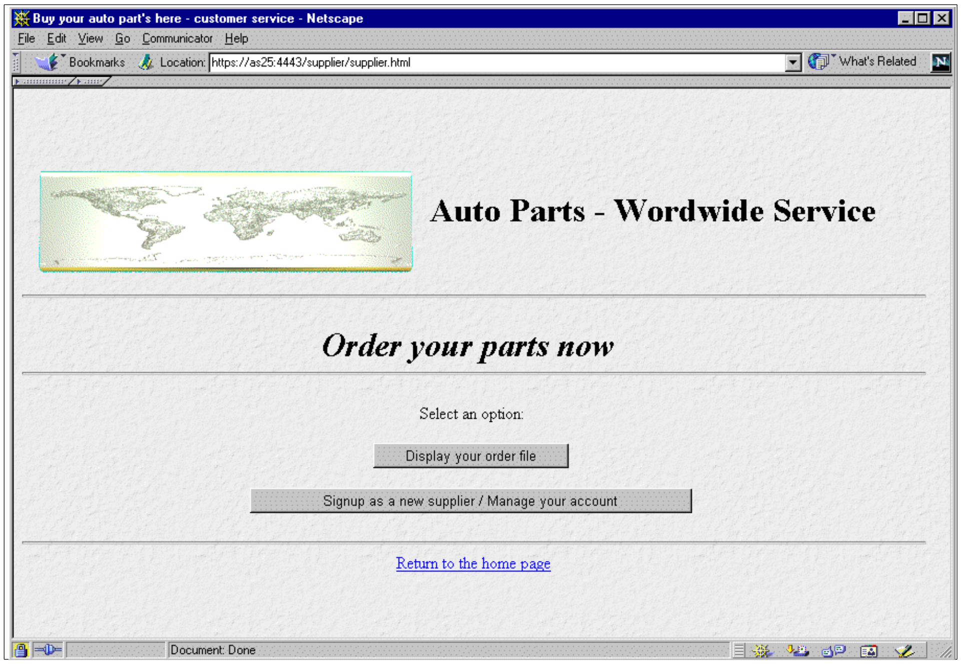
Java application

The supplier registration also uses the RegistrationAdmin java program to register a supplier.

7.3.7 Displaying supplier order files

This option demonstrates how AS/400 object authorities can be used to control access to objects accessed by Internet applications. In the following example, a supplier can use the Web browser to list order files stored in the supplier's directory on the AS/400 system. The goal is that even if supplier A knows the directory path to the directory of supplier B, supplier A should not be allowed to browse supplier's B directory. To accomplish this, the client certificate needs to be associated to an AS/400 user profile as performed during supplier registration.

Click the option **Supplier access** on the initial window to display the suppliers main window as follows:


Buy your auto part's here - customer service - Netscape
File Edit View Go Communicator Help
Bookmarks Location: https://as25:4443/supplier/supplier.html
What's Related
Document: Done

Auto Parts - Wordwide Service

Order your parts now

Select an option:

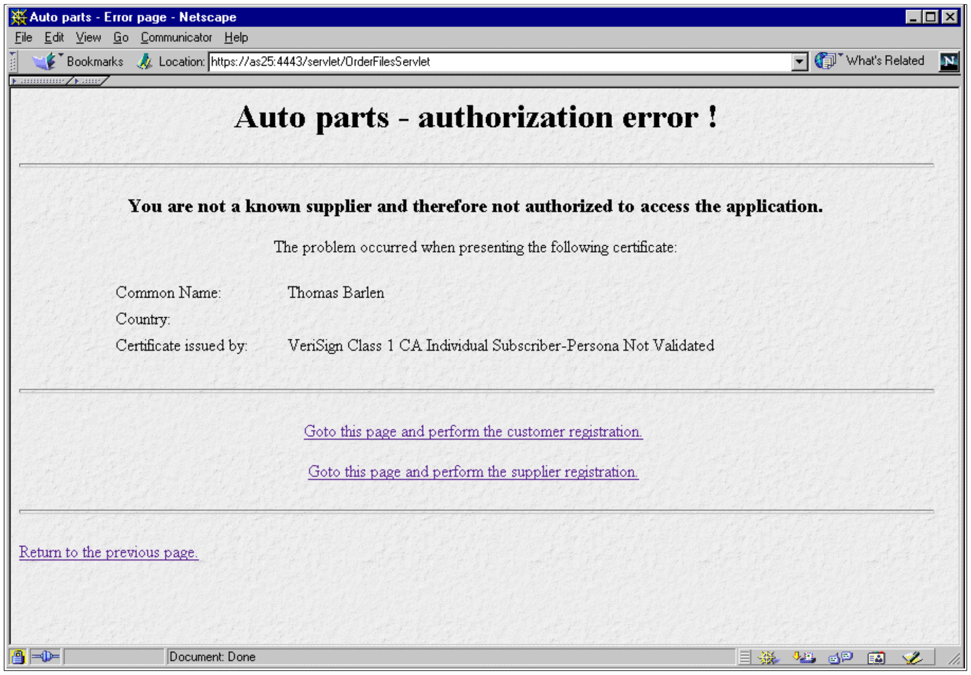
Display your order file

Signup as a new supplier / Manage your account

Return to the home page

Figure 283. Suppliers main window

If a client who is not a supplier clicks **Display your order files,** the following display appears:


Auto parts - Error page - Netscape
File Edit View Go Communicator Help
Bookmarks Location: https://as25:4443/servlet/OrderFilesServlet
What's Related
Document: Done

Auto parts - authorization error !

You are not a known supplier and therefore not authorized to access the application.

The problem occurred when presenting the following certificate:

Common Name:	Thomas Barlen
Country:	
Certificate issued by:	VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

Goto this page and perform the customer registration.

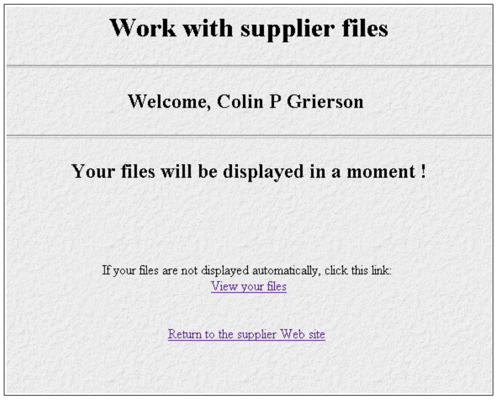
Goto this page and perform the supplier registration.

Return to the previous page.

Figure 284. Not a valid supplier

However, a valid supplier gets access to its own directory. The RPG application presents for a short time an information window as shown in Figure 285. The supplier is then automatically redirected to its directory.

The java application immediately shows the supplier’s directory.



Work with supplier files

Welcome, Colin P Grierson

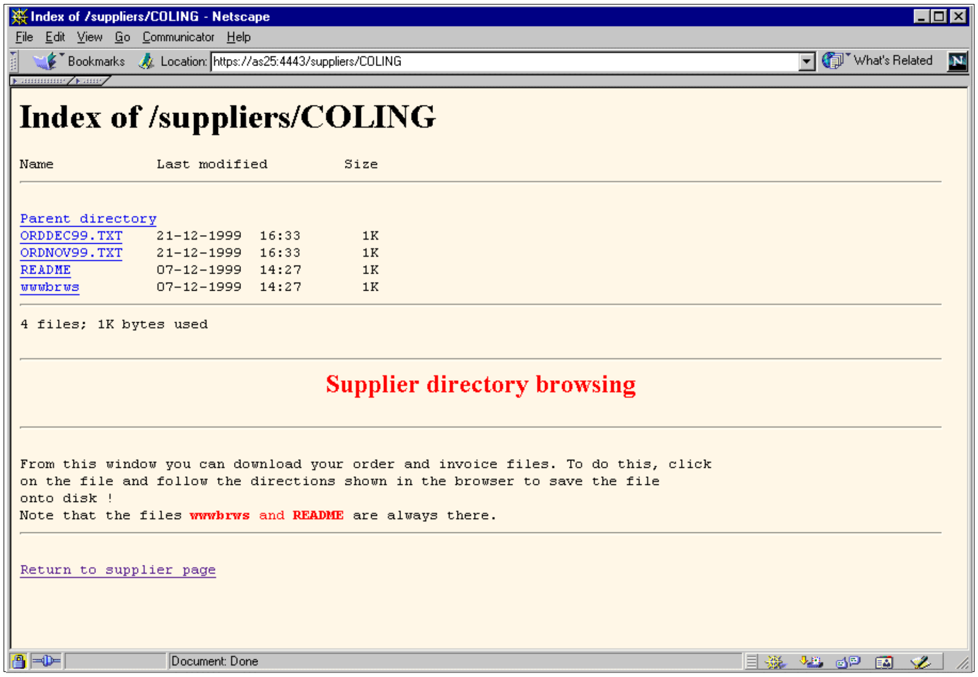
Your files will be displayed in a moment !

If your files are not displayed automatically, click this link:
View your files

Return to the supplier Web site

Figure 285. Displaying supplier files 1

From the directory displayed on the browser the supplier can, for example, download order files. For the sample application, we configured the HTTP server to allow selective directory browsing. That means if a file named *wwwbrws* is stored in the directory and no HTML file name is specified in the URL, the HTTP server sends the directory list to the Web browser.



Location: https://as25:4443/suppliers/COLING

Index of /suppliers/COLING

```
Name              Last modified         Size

Parent directory
ORDDEC99.TXT      21-12-1999  16:33       1K
ORDNOV99.TXT      21-12-1999  16:33       1K
README            07-12-1999  14:27       1K
wwwbrws           07-12-1999  14:27       1K

4 files; 1K bytes used
```

Supplier directory browsing

```
From this window you can download your order and invoice files. To do this, click
on the file and follow the directions shown in the browser to save the file
onto disk !
Note that the files wwwbrws and README are always there.

Return to supplier page
```

Figure 286. Displaying supplier files 2

Note the URL request: `https://as25:4443/suppliers/COLING`

The application takes the client certificate and retrieves the user profile name with which this client certificate is associated. Next the application builds the URL request string to be sent to the Web browser. The URL request consists of the following elements:

Protocol type HTTPS, which is the HTTP protocol secured with SSL.

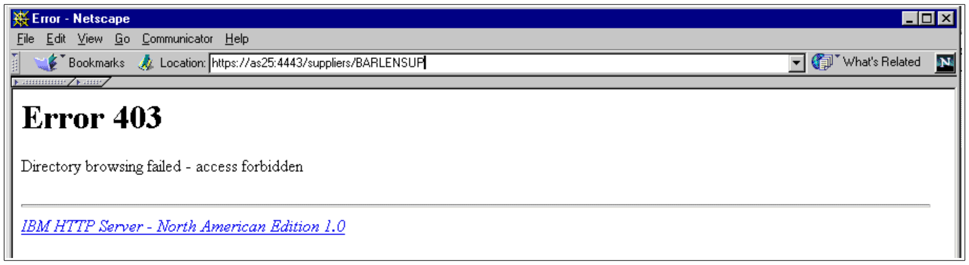
Hostname Host name or IP address of the AS/400 system.

Port The SSL port of the HTTP server instance.

Common directory In the sample application all individual supplier directories are stored under the common directory *suppliers*.

Supplier directory The supplier directory has the same name as the supplier's user profile. Each supplier has access only to its own directory.

If one supplier specifies by chance a directory name of another supplier, the following message is displayed.



https://as25:4443/suppliers/BARLENSUP

Error 403

Directory browsing failed - access forbidden

IBM HTTP Server - North American Edition 1.0

Figure 287. Unauthorized access to supplier directory

As you can see, the permissions granted to the directory prevented the access to it. To accomplish this, the HTTP server has an appropriate Protect directive configured. Refer to Chapter 8, "Sample application: using APIs with ILE RPG" on page 295 and Chapter 9, "Sample application: using certificates in Java" on page 337 for the HTTP server configuration.

REXX/RPG application

Clicking the **Display your order file** link invokes the REQSUP1 REXX procedure. The procedure checks first by calling the CHKCERVLDL program if the request comes from a registered user. Then it uses the RTVCLTDTA program to check if the user is a registered supplier. If both conditions are true, it calls the RTVCERUSR program to retrieve the AS/400 user profile name. Next the procedure builds the URL request string for directory browsing and sends it to the client's Web browser.

Java application

When clicking the **Display your order file** link, the OrderFilesServlet is invoked to process the request. The OrderFilesServlet uses the AuthenticatedUser class to retrieve the client's account data. Among the returned data is the client status or role. If it is a valid supplier, the servlet sends the redirect request to the Web browser.

7.3.8 Other supplier options

In the sample application the supplier can also use the customer or client options.

This concludes the demonstration of the sample application.

7.3.9 HTML pages used in the sample application

The HTML pages of the sample application are used only to demonstrate how digital certificates can be used in user applications. Therefore, they are built in a simple manner. The HTML sources are included in the sample application code that can be downloaded from the Internet. Refer to Appendix E, “Using the additional material” on page 401 for a description of how to obtain the code.

This section explains some techniques used in the HTML pages of the sample application.

Most of the HTML pages contain JavaScript routines to avoid hardcoded URL links as shown in Figure 288. The only hardcoded value is the port number 4743 that is used for HTTPS requests.

```
<html>
<head>
   <title>Buy your auto part's here</title>
</head>
<body background="./images/backdrop.gif">
<FORM>
<SCRIPT LANGUAGE="JavaScript">
//get the host name in order to avoid hard coding of the host name in the
urls called in this HTML page
      var host = self.location.host;    // assign hostname or IP address to
                                        host
      var index = host.indexOf( ":" ) ; // gets the position of the :
      if ( index >= 0 ) {               // if a port was used (:) then do
          host = host.substr( 0 , index ) ; // assign host name up to :
        }
      var url = "https://" + host + ":4743";// construct the host part of
                                              URL

</SCRIPT>
<br><img SRC="./images/worldban.gif" BORDER=0 height=125 width=390
align=CENTER><b><font size=+3>Auto Parts - Wordwide Service</font></b>
...
...
<INPUT TYPE=BUTTON VALUE="Order your parts now" onClick="self.location =
url +'/customer/customer.html'">
```

Figure 288. JavaScript to avoid hardcoded URL links

The next technique is used to prevent caching of HTML pages. Web browsers usually use memory and disk caches to store resources that have been recently used. If a Web user clicks the **Back** button in the browser, a cached version of the previous window will be displayed. Sometimes this leads to big problems. Of course, the Web browser can be configured for no caching. But this is not desirable in all cases.

We encountered a problem with caching when a client user performed a new registration. For example, the user entered the registration form and filled out the credit card number and e-mail address and clicked **Send registration data**. A confirmation message was displayed. When now clicking the **Back** button in the browser, the previous window is shown again. But the user already has a pending registration. So this is wrong. The user must get the updated version of the window, in this case with changed buttons to update the account.

To prevent this problem we implemented the highlighted statements as shown in Figure 289.

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<meta http-equiv="Expires" CONTENT="Sat, 20 Nov 1965">// of course the
                            pages are always expired using this date
   <meta http-equiv="Pragma" CONTENT="no-cache">     // also used to
prevent caching
   <title>Buy your auto part's here - customer service</title>
</head>
```

Figure 289. Prevent caching in HTML pages

These tags were tested with the Netscape browser. If you are using Microsoft’s Internet Explorer you may also want to add the following Meta tag:

```
<META HTTP-EQUIV="Cache-Control" CONTENT="no cache">
```

Chapter 8. Sample application: using APIs with ILE RPG

This chapter explains how digital certificate and validation list Application Programming Interfaces (APIs) are used in an ILE RPG environment. Refer to Chapter 7, “Introducing digital certificates in user applications” on page 271 for a general description of the program functions and flow of the sample application.

The documents used when this application was developed were:

HTTP Server for AS/400 Webmaster's Guide V4R4, GC41-5434

OS/400 Security APIs V4R4, SC41-5872

Web Programming Guide V4R4, GC41-5435

All APIs used in this application are defined and called within ILE RPG programs. REXX procedures are used as CGI programs to build the interface between the browser and the AS/400 application.

8.1 Setting up the environment

This section shows the commands and sources used to create the environment to run the application. Program logic and source information are not covered in this section. They are described in 8.2, “Program specifications” on page 307 and 8.5, “Working with APIs” on page 317.

8.1.1 The sample application system environment

For the REXX/RPG sample application we used a simple network environment as shown in Figure 290. Both systems are connected to an intranet.

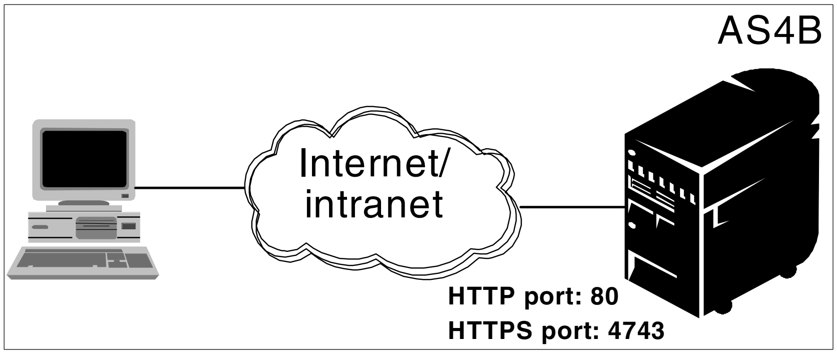


Figure 290. Network environment

The following software environment is used on the AS/400 system:

- OS/400 V4R4 with the cumulative PTF tape C9230440 and the additional PTFs SF58303, MF22714, and the HTTP group PTF SF99026. The PTFs listed here show the PTF level used when writing and testing the application. You may install the newest cumulative PTF level on your AS/400 system.
- Digital Certificate Manager (DCM), option 34 of OS/400 (5769-SS1)
- TCP/IP Connectivity Utilities for AS/400 (5769-TC1)
- IBM HTTP server for AS/400 (5769-DG1)
- IBM Cryptographic Access Provider product (5769-AC3)

- ILE RPG for AS/400 (5769-RG1)

The following software products are used on the PC:

- Microsoft Windows NT 4.0 Service Pack 4
- Netscape Communicator 4.7

8.1.2 Obtaining and restoring the sample application

Refer to Appendix E, “Using the additional material” on page 401 for information on how to download the application code from the Internet. The README.HTML file that is part of the Web material contains detailed instructions on how to restore the application.

8.1.3 Creating the required AS/400 objects

The sample application requires certain objects to be created on the AS/400 system. This section describes how those objects are created and the purpose of them. Figure 291 shows the source of a CL program that contains all OS/400 commands to create the application environment except the programs themselves.

```
PGM
CRTVLDL VLDL(SALES/PENDING)  TEXT('Certificates from pending registration  +
requests')
CRTVLDL VLDL(SALES/ACCEPTED) TEXT('Certificates from registered clients')
CRTUSRPRF USRPRF(SALESOWN) PASSWORD(*NONE) TEXT('Demonstration system user')
crtdtaara nxtcltnum *dec 7 text('Next client number')
CRTUSRPRF USRPRF(SALESGRP) PASSWORD(*NONE) INLMNU(*SIGNOFF) TEXT('Group +
authorities for Internet supplier users')
crtdtaara intsupdir *char 50 text('Dir in which Internet supplier dir''s are +
created')
CRTDIR DIR('/Suppliers') DTAAUT(*EXCLUDE) OBJAUT(*NONE)
chgaut 'suppliers' salesgrp dtaaut(*rx) objaut(*objref)
CRTPF FILE(CLTMASP) SIZE(10000 10000 100) AUT(*CHANGE)
crtlf cltmasl0
crtlf cltmasl1
CRTPF FILE(ORDDTLP) SIZE(1000000 30000 1000) AUT(*CHANGE)
crtlf orddtll0
crtlf orddtll1
CHGOBJOWN  OBJ(SALES) OBJTYPE(*LIB) NEWOWN(SALESOWN)
CHGOBJOWN  OBJ(SALES/PENDING) OBJTYPE(*VLDL) +
                          NEWOWN(SALESOWN)
CHGOBJOWN  OBJ(SALES/ACCEPTED) OBJTYPE(*VLDL) +
                          NEWOWN(SALESAUT)
GRTOBJAUT  OBJ(SALES/*ALL) OBJTYPE(*ALL) USER(SALESOWN) +
                          AUT(*ALL)
RVKOBJAUT  OBJ(SALES) OBJTYPE(*LIB) USER(*PUBLIC) +
                          AUT(*ALL)
ENDPGM
```

Figure 291. AS/400 objects required for the sample configuration

The purpose of the various objects that are created using the CL program are:

- `CRTVLDL VLDL(SALES/PENDING) TEXT('Certificates from pending registration requests')`

  The validation list PENDING is used to hold all client certificates for Internet or intranet users who performed the registration as a new customer or supplier.

Once the registration request has been approved or declined by the admin staff, the client certificate will be removed from this validation list.

- `CRTVLDL VLDL(SALES/ACCEPTED) TEXT('Certificates from registered clients')`

  The validation list ACCEPTED holds all client certificates of customers or suppliers whose registration request has been approved.

- `CRTUSRPRF USRPRF(SALESOWN) PASSWORD(*NONE) TEXT('Demonstration system user common authorities')`

  The user profile SALESOWN will be the owner of all objects belonging to the sample application. It has no functional impact on the application itself.

- `crtdtaara nxtcltnum *dec 7 text('Next client number')`

  The dataarea NXTCLTNUM is used to keep track of the client's account numbers. It will be updated everytime a new registration request is performed and hold the next available client account number.

- `CRTUSRPRF USRPRF(SALESGRP) PASSWORD(*NONE) INLMNU(*SIGNOFF) TEXT('Group + authorities for Internet supplier users')`

  The user profile SALESGRP is used as a group profile for all supplier user profiles. It gets permissions to the IFS directories used to store the supplier order files.

- `crtdtaara intsupdir *char 50 text('Dir in which Internet supplier dir''s are + created')`

  The data area INTSUPDIR contains a directory name under which the individual supplier directories are created. The RPG programs refer to this data area when accessing supplier directories. Note that the parent directory name, in this case `Suppliers`, is hardcoded in the HTTP server configuration in the appropriate PASS statement.

- `CRTDIR DIR('/Suppliers') DTAAUT(*EXCLUDE) OBJAUT(*NONE)`

  The IFS directory that contains all supplier directories.

- `chgaut '/suppliers' salesgrp dtaaut(*rx) objaut(*objref)`

  Grant appropriate authorities for the suppliers directory to the SALESGRP group profile.

- `CRTPF FILE(CLTMASP) SIZE(10000 10000 100) AUT(*CHANGE)`

  `crtlf cltmasl0`

  `crtlf cltmasl1`

  Physical and logical files that contain the account data for customers and suppliers.

The source for CTLMASP is as follows:

```
********** Beginning of data **********************************************
   * CLTMASP    Client master
   *
  A          R CLTMAS                    TEXT('Client master')
   *
  A            CLTNUM         7  0       COLHDG('Client')
  A                                      EDTCDE(Z)
  A                                      CMP(GT 0)
  A                                      TEXT('Client number')
   *
  A            CLTNAME       30          COLHDG('Name')
  A                                      REFSHIFT(A)
  A                                      TEXT('Client name')
   *
  A            CLTSTS         1          COLHDG('Sts')
  A                                      TEXT('Status A=Accpeted, P=Pending +
  A                                      D=Declined, U=User prf')
  A                                      VALUES('A' 'P' 'D' 'U')
   *
  A            CLTCRD        16  0       COLHDG('Credit card')
  A                                      CMP(GT 0)
  A                                      TEXT('Credit card number')
   *
  A            CLTEMAIL      70          COLHDG('E-mail' 'address')
  A                                      REFSHIFT(A)
  A                                      TEXT('Client email address')
   *
  A            CLTHDL        40          COLHDG('Certificate' 'Handle')
  A                                      TEXT('Client''s certificate handle')
************* End of data **************************************************
```

Figure 292. CTLMASP source

The source for CTLMASL0 is as follows:

```
*************** Beginning of data **********************************
    * Primary access path over the Client master
    * Unique key by Client number
    *
   A                                      UNIQUE
   A          R CLTMAS                    PFILE(CLTMASP)
    *
   A          K CLTNUM
****************** End of data *************************************
```

Figure 293. CTLMASL0 source

The source for CTLMASL1 is as follows:

```
*************** Beginning of data ***************************************
    * Access path over the Client master keyed by certificate handle.
    *
   A          R CLTMAS                    PFILE(CLTMASP)
    *
   A          K CLTHDL
****************** End of data ******************************************
```

Figure 294. CTLMASL1 source

Beware

The default for the CRTPF command is SIZE(10000 1000 3). In our experience this causes occasional problems when files become full. The useful purpose of the SIZE attribute is to stop a rogue application. It is best to set the size so high that only a rogue application will ever hit the limit.

-
  ```
  CRTPF FILE(ORDDTLP) SIZE(1000000 30000 1000) AUT(*CHANGE)
  crtlf orddtll0
  crtlf orddtll1
  ```

  The physical and logical files containing the order details. Since the application does not contain an order entry system, the records were added manually. The data is used for the View your orders option of the customer main window.

  The source for ORDDTLP is as follows:

```
********** Beginning of data *********************************************
   *
  A          R ORDDTL                    TEXT('Order Details')
   *
  A            DTLORDNUM      7  0       COLHDG('Order')
  A                                      TEXT('Order number')
   *
  A            DTLLINE        3  0       COLHDG('Order Line')
  A                                      TEXT('Order line')
  A                                      CMP(GT 0)
   *
  A            DTLPRTNUM      7  0       COLHDG('Part')
  A                                      TEXT('Part number ordered')
  A                                      CMP(GT 0)
   *
  A            DTLDESC       30          COLHDG('Part description')
  A                                      REFSHIFT(A)
  A                                      TEXT('Part desc.  Default from +
  A                                      master, may change')
   *
  A            DTLQTY         5  0       COLHDG('Quantity')
  A                                      TEXT('Number ordered')
  A                                      CMP(GT 0)
   *
  A            DTLPRICE       7  2       COLHDG('Price')
  A                                      TEXT('Unit price')
  A                                      CMP(GE 0)
   *
  A            DTLCLTNUM      7  0       COLHDG('Client')
  A                                      CMP(GT 0)
  A                                      TEXT('Client number')
   *
  A            DTLSTS         1          COLHDG('Status')
  A                                      TEXT('Status: P=Packed, S=Shipped +
  A                                      C=Complete, O=On order')
  A                                      VALUES('O' 'P' 'S' 'C')
```

Figure 295. ORDDTLP source

The source for ORDDTLL0 is as follows:

```
*************** Beginning of data **********************************
       * Primary access path over the orders details
   * Unique key by Order, and Order line
   *
  A                                        UNIQUE
  A          R ORDDTL                      PFILE(ORDDTLP)
   *
  A          K DTLORDNUM
  A          K DTLLINE
****************** End of data *************************************
```

Figure 296. ORDDTLL0 source

The source for ORDDTLL1 is as follows:

```
*************** Beginning of data ***************************************
   * Primary access path over the orders details
   * Unique key by Order, and Order line
   *
  A          R ORDDTL                      PFILE(ORDDTLP)
   *
  A          K DTLCLTNUM
  A          K DTLORDNUM
  A          K DTLLINE
****************** End of data ******************************************
```

Figure 297. ORDDTLL1 source

-
  ```
  CHGOBJOWN  OBJ(SALES) OBJTYPE(*LIB) NEWOWN(SALESOWN)
  CHGOBJOWN  OBJ(SALES/PENDING) OBJTYPE(*VLDL) +
  NEWOWN(SALESOWN)
  CHGOBJOWN  OBJ(SALES/ACCEPTED) OBJTYPE(*VLDL) +
  NEWOWN(SALESOWN)
  GRTOBJAUT  OBJ(SALES/*ALL) OBJTYPE(*ALL) USER(SALESOWN) +
  AUT(*ALL)
  RVKOBJAUT  OBJ(SALES) OBJTYPE(*LIB) USER(*PUBLIC) +
  AUT(*ALL)
  ```

  Change permissions for objects of the sample application.

8.1.4 Setting up the HTTP server

For the sample application we use a welcome window that is served unprotected, which means the SSL protocol is not used. This window, which is the WelcomeSales.html page, is served through the DEFAULT HTTP server instance. This server instance listens to the well-known port 80 for incoming HTTP requests. The following directives are required in the DEFAULT server instance for this application:

```
Welcome WelcomeSales.html
Pass /* /webserver/sales/public/*
AlwaysWelcome On
Enable GET
```

The welcome window provide the options Order your parts now and Supplier access. Both options, when clicked, switch to the HTTPS protocol and send the appropriate URL requests to a HTTP server instance that listens to port 4743. We created a separate server instance SALES, which serves the application itself. With this concept, we are able to allow Web users to enter the application by using a well-known port and then use a server instance that serves only our sample application. The application HTTP server configuration is shown in Figure 298.

```
# HTTP CONFIGURATION FILE
Protect /suppldir/* {
      PasswdFile %%SYSTEM%%
      ACLOverride Off
      PostMask All
      GetMask All
      AuthType Cert
      UserID %%CLIENT%%
}
Welcome WelcomeSales.html
HostName AS4B.RAL.IBM.COM
BindSpecific Off
Port 4680
UserID SALESOWN
DNS-Lookup Off
# Imbeds CGI html
Imbeds On SSIOnly
AlwaysWelcome On
DirAccess Selective
NormalMode On
# Do not change or delete the following AppName directi
AppName QIBM_HTTP_SERVER_SALES
SSLMode On
SSLPort 4743
SSLClientAuth Required
AccessLog /webserver/sales/logs/access.log 2000
CacheAccessLog /webserver/sales/logs/cache.log 2000
ProxyAccessLog /webserver/sales/logs/proxy.log 2000
AgentLog /webserver/sales/logs/agent.log 2000
RefererLog /webserver/sales/logs/referer.log 2000
AccessLogArchive Purge
AccessLogExpire 30
AccessLogSizeLimit 0
AccessLogExcludeMimeType image/gif
ErrorLog /webserver/sales/logs/error.log 2000 *DFT *DFT
CgiErrorLog /webserver/sales/logs/cgierror.log 2000
ErrorLogArchive Purge
ErrorLogExpire 30
ErrorLogSizeLimit 0
Disable CONNECT
Disable DELETE
Disable PUT
Enable GET
Enable HEAD
Enable OPTIONS
Enable POST
Enable TRACE
Pass /renew /webserver/sales/client/renew.html
Pass /customer/* /webserver/sales/client/*
Pass /suppldir/* /suppliers/*
Pass /supplier/* /webserver/sales/supplier/*
Pass /images/* /webserver/sales/public/images/*
Exec /cgibin/* /qsys.lib/sales.lib/*.PGM
DirShowDate On
DirShowCase On
DirShowSize On
DirShowBytes On
DirShowOwner Off
DirShowDescription On
DirShowMinLength 15
DirShowMaxLength 25
DirReadme Bottom
```

Figure 298. SALES HTTP server configuration

The highlighted server directives are crucial to our application and will be explained in more detail. All other directives are default directives or are not important to run the application. We enabled all kind of logging functions to get as much information as possible to debug the application.

The description of the most important server directives are as follows:

8.1.4.1 Common settings

The following server directives are used to allow access to the appropriate application data and programs:

- `Pass /renew /webserver/sales/client/renew.html`

  This PASS directive maps step 2 of the certificate change process directly to the appropriate HTML page.

- `Pass /customer/* /webserver/sales/client/*`

  Maps customer requests to the appropriate directories and files on the server. The directory structure is hidden from outside the server.

- `Pass /supplier/* /webserver/sales/supplier/*`

  Maps supplier requests to the appropriate directories and files on the server. The directory structure is hidden from outside the server.

- `Pass /images/* /webserver/sales/public/images/*`

  Customer and supplier HTML pages contain images, such as the company's logo. Since these images are common for both customers and suppliers, they are stored in a common directory. This PASS directive gives proper access to the images. Also this directory structure is hidden from outside the server.

- `Exec /cgibin/* /qsys.lib/sales.lib/*.PGM`

  Allows access and defines the location to the CGI programs used in the sample application.

- `CgiErrorLog /webserver/sales/logs/cgierror.log 2000`

  This directive defines the location of the error log for CGI programs. This log contains useful information when one of the CGI programs encounter a problem.

-
  ```
  Enable GET
  Enable POST
  ```

  These are the two request methods used in the sample application.

8.1.4.2 Supplier access

The following server directives are required to allow suppliers to list their own order files using a Web browser:

-
  ```
  Protect /suppldir/* {
     PasswdFile %%SYSTEM%%
     ACLOverride Off
     PostMask All
     GetMask All
     AuthType Cert
     UserID %%CLIENT%%
     }
  ```

The Protect directive protects the directory and subdirectories of the suppldir directory for incoming URL requests, such as `https://as4b.ral.ibm.com:4743/suppldir/barlensp1`. The inline definitions for this protect statement require a client certificate that is associated with an AS/400 user profile. For example, when a supplier presents its client certificate, the authority checking will be done using the user profile with which that certificate is associated.

This means for the sample application that normal customers are not able to browse any supplier directory at all.

- `DirAccess Selective`

  When a new supplier is registered, a user profile and a supplier directory is created. A wwwbrws file is copied into the new supplier directory. The DirAccess Selective directive allows directory browsing only when a wwwbrws file is present in the directory to be browsed. This setting allows a supplier to browse their order files.

- `Pass /suppldir/* /suppliers/*`

  This PASS directive maps incoming URL requests containing the /suppldir/* path to the IFS directory /suppliers/*. This allows us to hide the actual directory structure.

- `DirReadme Bottom`

  When a supplier browses its directory, text is shown at the bottom of the browser window. In the sample application the supplier gets a description of the files displayed on the browser and instructions on how to proceed. This directive defines where the text will be shown on the browser window. The text itself is stored in a file named README, which itself is located in the supplier directory.

8.1.4.3 Security

The following server directives are required to support the SSL protocol for this server instance:

- `AppName QIBM_HTTP_SERVER_SALES`

  Is the application ID that is listed under Work with secure applications in the Digital Certificate Manager (DCM). A server certificate must be assigned to this application ID to enable SSL for this server instance.

- `SSLMode On`
  `SSLPort 4743`

  The previous two directives enable the SSL protocol for the server instance and define the port that is used for HTTPS client requests.

- `SSLClientAuth Required`

  Specifies that client authentication is required. No access is permitted without presenting a client certificate when using the HTTPS protocol.

8.1.5 IFS Objects

The HTML files used in this sample application are stored in an Integrated File System (IFS) directory structure. Also the README and wwwbrws files that are used for supplier access are stored in an IFS directory.

The locations of the objects and their meaning are as follows:

Table 13. IFS objects for the HTTP server

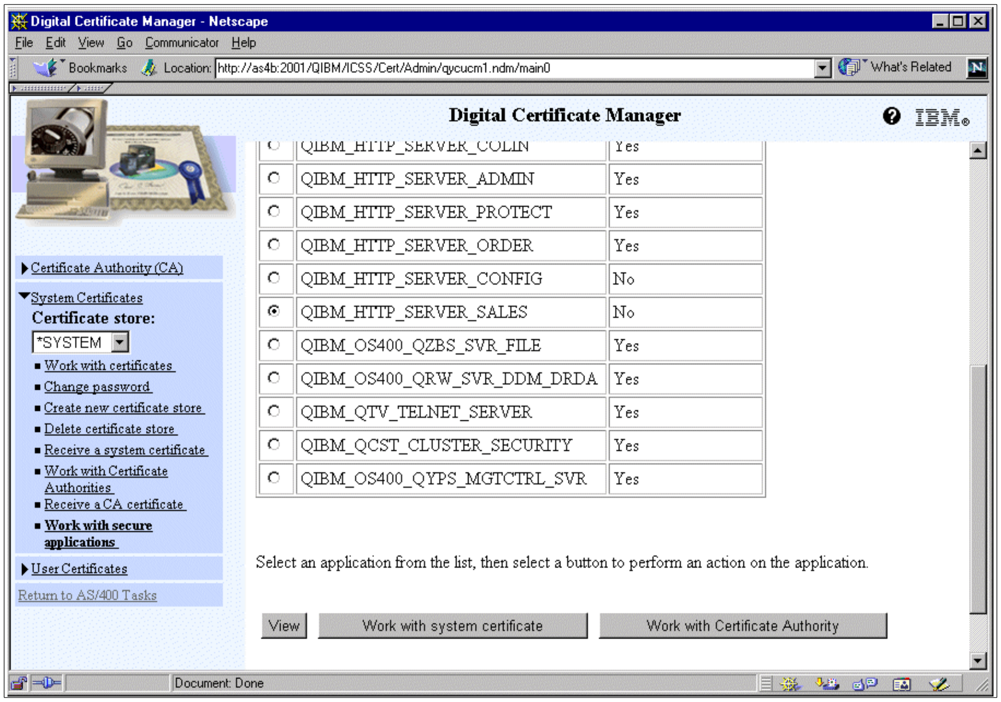
Directory	File	Description
/webserver/sales		Main directory for HTTP server
/webserver/sales/public	WelcomeSales.html	Welcome window
/webserver/sales/public/images	backdrop.gif	Image of Web window background
/webserver/sales/public/images	worldban.gif	World banner for Web window
/webserver/sales/client	Customer.html	Customer main window
/webserver/sales/client	renew.html	Certificate renew window for customers and suppliers
/webserver/sales/supplier	supplier.html	Supplier main window
/supplier (1)		Parent directory for supplier directories
/supplier/	wwwb (1)	Copy source for creating the wwwbrws file in an individual supplier directory
/supplier/	Readm (1)	Copy source for creating the README file in an individual supplier directory

(1) Note that these objects need *RX authorities for the SALESGRP group user profile.

8.1.6 Assigning a server certificate to the HTTP server instance

One requirement to enable SSL for the SALES HTTP server instance is to assign a server certificate to it. For the sample application we used an AS/400 system as a private Certificate Authority (CA). The HTTP Configuration and Administration utility had to be used to enable SSL for the SALES server instance in order to get the application ID added to DCM. The following steps take you through the process of assigning the server certificate to the SALES HTTP server instance.

1. Start a Web browser and enter the URL `http://as4b:2001/` to start the AS/400 Tasks page.
2. Select **Digital Certificate Manager** (DCM) and expand **System Certificates**.
3. Click on **Work with secure applications**.

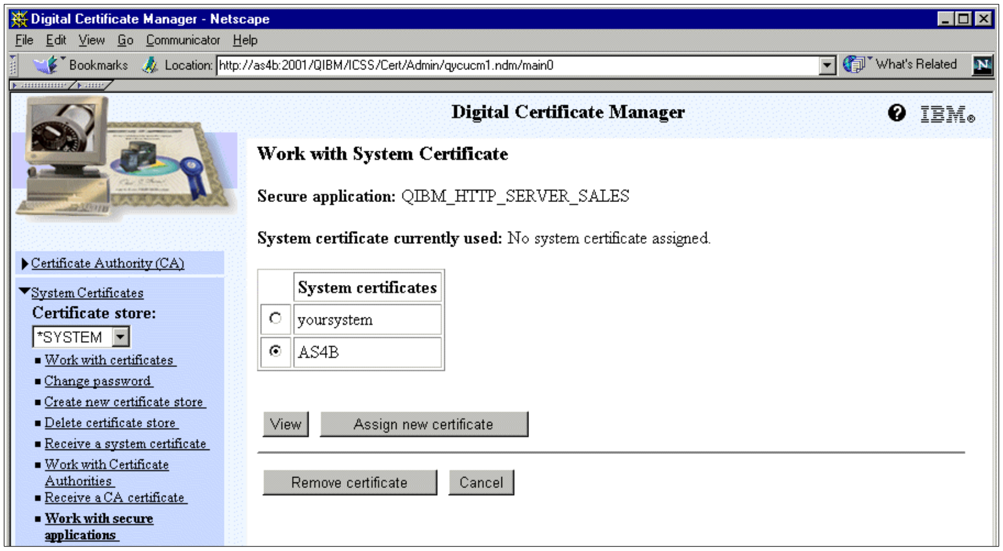

Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM.
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Work with system certificate
Work with Certificate Authority
Document: Done

○	QIBM_HTTP_SERVER_COLIN	Yes
○	QIBM_HTTP_SERVER_ADMIN	Yes
○	QIBM_HTTP_SERVER_PROTECT	Yes
○	QIBM_HTTP_SERVER_ORDER	Yes
○	QIBM_HTTP_SERVER_CONFIG	No
●	QIBM_HTTP_SERVER_SALES	No
○	QIBM_OS400_QZBS_SVR_FILE	Yes
○	QIBM_OS400_QRW_SVR_DDM_DRDA	Yes
○	QIBM_QTV_TELNET_SERVER	Yes
○	QIBM_QCST_CLUSTER_SECURITY	Yes
○	QIBM_OS400_QYPS_MGTCTRL_SVR	Yes

Select an application from the list, then select a button to perform an action on the application.

Figure 299. DCM - Work with secure applications - step 1

4. Select the QIBM_HTTP_SERVER_SALES application ID and click **Work with system certificate**. Note that the application ID appears only when the HTTP Configuration and Administration utility was used to configure SSL for the SALES server instance.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM.
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
View
Assign new certificate
Remove certificate
Cancel

Work with System Certificate

Secure application: QIBM_HTTP_SERVER_SALES

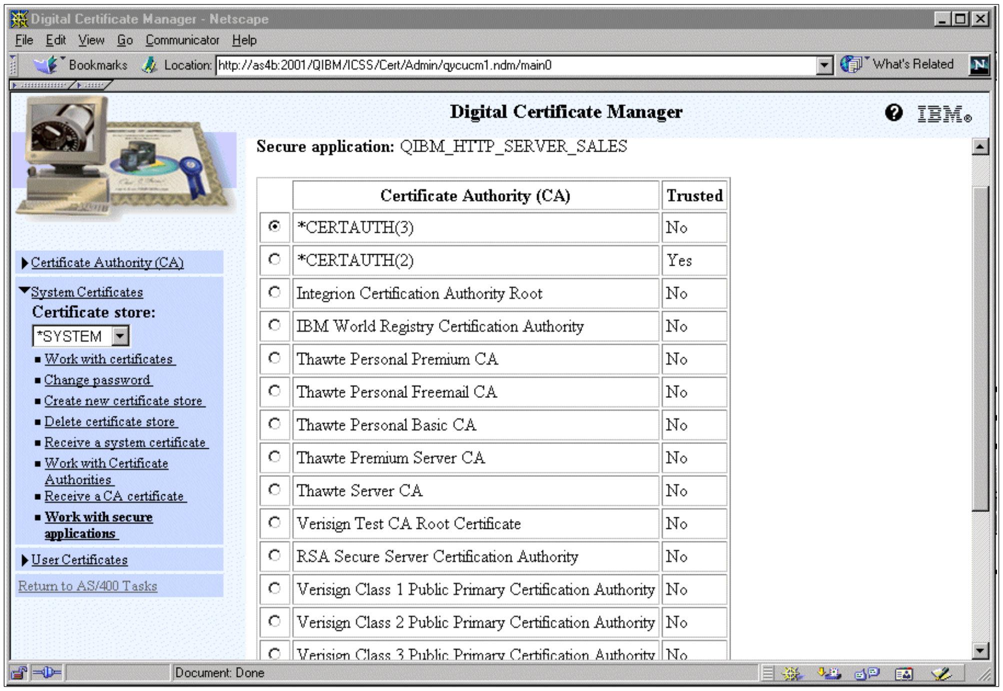
System certificate currently used: No system certificate assigned.

	System certificates
○	yoursystem
●	AS4B

Figure 300. DCM - Work with secure applications - step 2

5. Select a server certificate that is to be assigned to the server instance and click **Assign new certificate**. When the completion message appears, click **OK**.

6. The list of secure applications is displayed again. Select the **QIBM_HTTP_SERVER_SALES** application ID again and click **Work with Certificate Authority**.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Location: http://as4b:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
Document: Done

Secure application: QIBM_HTTP_SERVER_SALES

	Certificate Authority (CA)	Trusted
●	*CERTAUTH(3)	No
○	*CERTAUTH(2)	Yes
○	Integrion Certification Authority Root	No
○	IBM World Registry Certification Authority	No
○	Thawte Personal Premium CA	No
○	Thawte Personal Freemail CA	No
○	Thawte Personal Basic CA	No
○	Thawte Premium Server CA	No
○	Thawte Server CA	No
○	Verisign Test CA Root Certificate	No
○	RSA Secure Server Certification Authority	No
○	Verisign Class 1 Public Primary Certification Authority	No
○	Verisign Class 2 Public Primary Certification Authority	No
○	Verisign Class 3 Public Primary Certification Authority	No

Figure 301. DCM - Work with secure applications - step 3

7. The CA that issued the server certificate that is assigned to the SALES server instance is automatically marked as trusted. All the CA certificates from which the application should accept client certificates must be marked as trusted. For example, if a Web user enters the application with a client certificate that was issued by VeriSign, the VeriSign CA certificate must be set up as trusted. Otherwise, the client will not be able to connect.

   Since we are using client certificates issued by the VeriSign Class 1 Public Primary Certification Authority, select **VeriSign Class 1 Public Primary Certification Authority** and click **Trust**. Repeat this step for all CAs the application should trust.

For more details on DCM refer to Chapter 5, “Digital Certificate Manager for AS/400” on page 107.

8.2 Program specifications

This section describes the various programs and other objects that are part of the sample application.

8.2.1 REXX procedures

This application uses REXX procedures as CGI programs. Within those REXX procedures, calls are made to other programs. These programs are the ILE RPG programs written to demonstrate how to use the certificate and validation lists APIs. Further utility programs are used to performs the input and output operation from and to the user’s Web browser. You can find more information about the utility programs in 8.2.2, “CGI utility programs” on page 308.

Since these REXX procedures only provide some application logic and no calls to APIs at all, the sources are not included in this section. But they are included in the sample application code that can be downloaded from the Internet. Refer to Appendix E, “Using the additional material” on page 401 for further instructions to obtain the application code from the Internet.

The sample application uses the following three REXX procedures:

REQCLT1

This procedure is invoked from the customer main window. It performs the following main functions:

- Order new parts (returns only a message that this option is not available)
- View your orders
- Entry point to sign up new customers and update current accounts

REQCLT1A

The procedure is invoked through the REQCLT1 and REGSUP1 procedures when a request is made to:

- Sign up a new customer or supplier
- Update a current account
- Perform a certificate renewal change request

REQSUP1

The procedure REQSUP1 is invoked from the supplier main window. It is responsible for performing the following application functions:

- Browsing the supplier order files
- Entry point to sign up new suppliers and update current accounts

All the REXX procedures are built using the template procedure as a base, as described in the next section

8.2.2 CGI utility programs

The REXX CGI programs used in the sample application are based on utility programs and templates that are available on the IBM AS/400 Technical Studio Web site.

The following list contains the main utility programs that are used in the sample application:

- GETENV obtains environment variable values.
- STDIN reads data from standard in.
- STDOUT writes data to standard out.
- REXXDRIVER is the CGI entry program that calls the REXX procedures specified in HTTP requests through the FORM parameter.
- TEMPLATE is a REXX procedure that provided the basic structure of the REXX procedures used in this application. It contains input, output, and environment subroutines.

The programs that are previously described including the service programs and source code are available on the AS/400 Web Builder's Workshop's Snippets Web site. For more information see:

```
http://www.as400.ibm.com/techstud/workshop/snippets/snippets.htm
```

For completeness we have provided the programs and sources in the material that can be downloaded from the Internet. Refer to Appendix E, “Using the additional material” on page 401 for further information.

8.2.3 Approve or decline registration: APPCLTREG

The process of deciding to accept or decline a registration request is handled by an application our client management department uses. APPCLTREG is called by that application to accept or decline a particular request. Enter the following command to run the program from an OS/400 command prompt:

```
CALL PGM(APPCLTREG) PARM(X'0000034F' A X)
```

where `X’0000034F’` represent the account number of the new user to be accepted or declined. The `A` is used to accept a registration request and `D` to decline a request. The last parameter is used to hold the parameter that is returned from the program and can be any value.

Parameters

1. Requires client account number and action, Accept or Decline
2. Returns action code. “Error1”, “Error2”, or “Okay”
    - “Error1” = Account not found
    - “Error2” = Account status is not “Pending”

Specification

1. Get account details
2. If account is not found return "Error1"
3. If account status is not "Pending”:

   >>Unlock data base record

   >>Return "Error2"
4. If request is "Accept”:

   >>Get certificate from pending validation list

   >>Add certificate to accepted validation list

   >>Set status to "Accepted”
5. Else (request is "Decline”):

   >>Set status to “Declined”
6. Update data base
7. Remove certificate from pending validation list
8. Return "Okay"

APIs used

The following APIs are used in this program:

QSYFDVLE	Find Validation List Entry

QsyAddVldlCertificate	Add Validation List Certificate
QsyRemoveVldlCertificate	Remove Validation List Certificate

8.2.4 Associate a certificate with a user profile: ASSCERUSR

Our suppliers work closely with us and have access to a number of our applications. The number of suppliers is not large and the applications they are authorized to vary. Also we have a directory for each supplier that can be used for transferring files from the server to the client. To handle this situation we create an AS/400 user profile for each supplier and associate their certificate with this. We can then use AS/400 system authorities to control the applications individual suppliers can access and to secure the suppliers directories.

To register, suppliers make a registration request in the normal way. After approving the registration our client management department can take another option that calls ASSCERUSR. This creates the supplier’s user profile, creates the supplier’s directory, and associates the supplier’s certificate with their user profile. Enter the following command to run the program from an OS/400 command prompt:

```
CALL PGM(ASSCERUSR) PARM(X'0000021F' usrprf X)
```

where `X’0000021F’` represent the account number of the user to be registered as a supplier. The parameter `usrprf` specifies the name of the user profile to be created for the supplier. The last parameter is used to hold the parameter that is returned from the program and can be any value.

Parameters

1. Requires client account number and user profile name
2. Returns action code. “Error1”, “Error2”, “Error3”, or “Okay”
   - “Error1” = Client account number not found
   - “Error2” = Client status is not “Accepted”
   - “Error3” = A user profile of the name given already exists

Specification Part1:

This part is written in ILE CL.

1. If the named user profile already exists - return “Error3”
2. Create the user profile:

   - with no password, so it cannot be used to sign on

   - with group profile SALESGRP for common authorities
3. Create a private directory for the user profile:

   - this is created within the directory named in the data area INTSUPDIR

   - the directory name is the same as the user profile name

   - no public authority
4. Give the new user authority to the new directory
5. Call part2, which is written in ILE RPG
6. If an error code is returned, delete the user profile and directory

Specification Part2:

This part is written in ILE RPG.

1. Get client details from data base:

   >>Error if not found - return "Error1"

   >>Error if status not "Accepted" - Return "Error2"

2. Get client's certificate
3. Associate it with the given user profile
4. Update the account status to "U" - "User profile"

APIs used

The following APIs are used in this program:

QSYFDVLE	Find Validation List Entry
QsyAddUserCertificate	Adds a client certificate to a user profile

8.2.5 Check if certificate is on a validation list: CHKCERVLDL

CHKCERVLDL is a utility that CGI programs may use to check if the current client’s certificate is on a particular validation list.

Parameters

1. Requires a validation list name
2. Returns action code. “Yes” or “No”

Specification

1. Obtain user's certificate from environment
2. Translate from EBCIDIC back to ASCII
3. Check if certificate is on the given validation list

   - If so return “Yes”

   - If no return “No”

API used

The following API is used in this program:

QsyCheckVldlCertificate	Check Validation List Certificate

8.2.6 Registration update program: REGCLT2

REGCLT2 is called to record a registration request or to update a client’s credit card number and email address.

Parameters

1. Requires e-mail address and credit card number

   A REXX program is used to call REGCLT2. When the credit card number field is all numeric REXX passes it as packed decimal. Otherwise REXX passes it as character. In order to get a consistent result we prefix a character to the start of the string in the REXX program and discard it again here.

2. Returns action code. “Pending”, “Updated”, “Decline”, or “Error”

Specification

1. If credit card number is not all digits, return "Error"

2. Obtain user's certificate from environment
3. Translate from EBCIDIC back to ASCII
4. Parse certificate to obtain handle and user's name
5. If the certificate handle is already on file

   >>If certificate was previously declined, return “Decline”

   >>Else update the client's information and return "Updated"
6. Else

   >>Obtain and update the next client number

   >>Write client details to client master with status "P"

   >>Format the path name to the validation list for pending registrations

   >>Store certificate in the validation list

   >>Return "Pending"

APIs used

The following APIs are used in this program:

QsyParseCertificate	Parse Certificate
QsyAddVldlCertificate	Add Validation List Certificate

8.2.7 Renew an expiring certificate with a new one: RENCLTCER

Certificates have finite lifetimes, generally one to three years. Once a certificate has expired it is unusable. Before it expires you need to get a new certificate and somehow replace the old one with the new.

We have set up a system to do this as follows:

1. A client comes to our site using their old certificate and initiates the renewal procedure. We give them a copy of their certificate handle as an 80-character hexadecimal string.
2. The client leaves our system and closes its browser.
3. The client returns to our system using its new certificate and goes to the window for completing the certificate renewal.
4. The client enters the copy of its handle that we gave it previously, probably using cut and paste. We then check that the handle matches an existing certificate and, if so, replace the existing certificate with the client’s current certificate.

NOTE

We use the handle of the old certificate as the link to the client's existing details. This is simple in concept and works well. However, because we hold the certificate handles in our database, it is not very secure. If anyone got a copy of our client master file they could use the information there to "renew" any existing client's certificate with their own. A better system would be to generate some random identifier, valid for only a short period, and use this to link the old and new certificates.

Since the purpose of this system is to demonstrate the use of APIs relevant to certificates we are not going to worry about this security weakness. But if you are creating a production system, you should!

Speaking of security, you should also protect the application library and the files against unauthorized access.

A more elegant solution would be to use cookies on the client's browser so they do not have to cut and paste the certificate handle or whatever is used as an identifier. This method requires that the client user has configured the browser to accept cookies.

Parameters

1. Requires current certificate handle as an 80-character hexadecimal string
2. Returns action code. “Error1”, “Error2”, or “Okay”

- “Error1” = handle is not valid
- “Error2” = new certificate is the same as the old certificate

Specification

1. Change the handle back to a 40 long character string
2. Use this to retrieve the client's details
3. Exit with 'Error1" if not found
4. Obtain the client's new certificate from environment
5. Translate from EBCIDIC to ASCII
6. Parse to obtain the new certificate’s handle
7. If handle has not changed (that is, still using old certificate), exit with “Error2”
8. Update the client master file with the new handle
9. If the old certificate is in the pending validation list

   >>Remove it

   >>Add the new certificate
10. If the old certificate is in the accepted validation list

    >>Remove it

    >>Add the new certificate
11. If the old certificate is associated with a user profile

    >>Remove the association

>>Associate the new certificate with the user profile

12. Return

APIs used

The following APIs are used in this program:

QsyParseCertificate	Parse Certificate
QsyCheckVldlCertificate	Check Validation List Certificate
QsyRemoveVldlCertificate	Remove Validation List Certificate
QsyAddVldlCertificate	Add Validation List Certificate
QsyFindCertificateUser	Finds the user that is associated with a certificate.
QsyRemoveUserCertificate	Removes a certificate from an OS/400 user profile.
QsyAddUserCertificate	Adds a client certificate to a user profile

8.2.8 Retrieve the user a certificate is associated with: RTVCERUSR

RTVCERUSR is a utility that CGI programs may use to obtain the user profile name associated with the current client certificate. This is useful for us because suppliers have directories that have the same name as the user profile associated with their certificate.

Parameters

1. Returns:
   - User profile name, Char 10
   - Blank if the current client certificate is not associated with a user profile.

Specification

1. Obtain current client's certificate from environment
2. Translate from EBCIDIC to ASCII
3. Find the user profile the presented client certificate is associated with
4. Return the user profile or blank if none

API used

The following API is used in this program:

QsyFindCertificateUser	Finds the user that is associated with a certificate.

8.2.9 Retrieve a client's details: RTVCLTDTA

RTVCLTDTA is a utility that CGI programs may use to retrieve the details of the current client.

1. Returns action code. “Okay”
2. Returns client's details:
   a. Account number, Char 7, right adjusted
   b. Name, Char 30
   c. Credit card number, Char 16

d. Credit card number, Char 19, formatted as nnnn-nnnn-nnnn-nnnn

e. E-mail address, Char 70

f. Status, Char 1
   - P = Pending acceptance
   - A = Accepted
   - D = Declined
   - U = Accepted and associated with a user profile

g. Status, Char 8
   - Pending = Pending acceptance
   - Accepted = Accepted
   - Declined = Declined
   - User prf = Accepted and associated with a user profile

h. Certificate handle in hexadecimal format, Char 80

Specification

1. Obtain user's certificate from environment
2. Parse to obtain certificate handle
3. Use handle to get client details from data base
4. Format client details
5. Return client details

API used

The following API is used in this program:

QsyParseCertificate	Parse Certificate

8.2.10 Retrieve a client’s orders: RTVCLTORD

RTVCLTORD is a utility that CGI programs may use to retrieve the details of orders belonging to the current client.

> **Note**
>
> This program must not be created with the default setting of activation group *NEW. When activation group *NEW is used, a new activation group is created when the program is called. The activation group is destroyed, along with the program variables and open file information, when the program exits. This prevents the program from returning more than one record. See “Activation groups” on page 317.

1. Input/Output: Control code, Char 7
   - If given “NEW”, the program initializes and returns the client’s first order
   - If given blank, the program returns the next order for the current client
   - Returns “Error” if given other than “NEW” or blank
   - Returns blank if an order was found and returned
   - Returns “END” if no further orders were found

2. Output:
    a. Order number, Char 7 right adjusted, blank filled
    b. Order line, Char 3 right adjusted, blank filled
    c. Part number, Char 7 right adjusted, blank filled
    d. Part description, Char 30
    e. Quantity ordered, Char 5 right adjusted, blank filled
    f. Price, Char 8 right adjusted, blank filled, e.g. ___24.50
    g. Customer number, Char 7 right adjusted, blank filled
    h. Status description, Char 8
        - Packed
        - Shipped
        - Complete
        - On order

Specification

1. If control code is not "NEW" or blank, return "Error"
2. If control code is "NEW"

    >>Obtain user's certificate from environment

    >>Translate certificate from EBCIDIC to ASCII

    >>Parse to obtain the handle

    >>Use the handle to get the client's account code

    >>Get the first order detail record for the client
3. Else if control code is blank

    >>Get the next order detail record for the client
4. If an order detail record was found

    >>Set the control code to blank

    >>Format the return parameters
5. Else

    >>Set the control code to "END"
6. Return

API used

The following API is used in this program:

QsyParseCertificate	Parse Certificate

8.3 System source

The source files QRPGLESRC, QCLSRC, QREXSRC, and QDDSSRC have been used to hold the source for programs and files. Refer to Appendix E, “Using the additional material” on page 401 for information on how to obtain the application source code.

All source members have the same name as the corresponding programs.

The source member PROTOTYPES in QRPGLESRC holds data structures and prototypes used in the ILE RPG programs we have written. The member CGIPROTYPS holds data structures and prototypes used in the ILE RPG programs we have copied from the AS/400 Web Builder's Workshop's Snippets Web site. For more information see:

`http://www.as400.ibm.com/techstud/workshop/snippets/snippets.htm`

The source member CREATERPG in QCLSRC holds the commands used for creating the programs.

8.4 Activation groups

We have used activation group *CALLER for the programs previously described. Calling a program for the first time is far slower than recalling an active program. For the first call, the program must be located and initiated, files must be located and opened, and so on. Our programs are utilities and are likely to be called many times so we want them to remain active once they have been called.

To do this we must not use the default of ACTGRP(*NEW). ACTGRP(*NEW) for a program causes a new activation group to be created when the program is called and deleted when the program returns. This does a very good job of tidying up, closing the program, removing the storage that held variables, closing all the files, and so on - but it is not what we want here.

We could use named activation groups, which create a separate area for each activation group we create. These activation groups persist until we explicitly delete them using the RCLACTGRP command or until the job ends.

We have chosen to use ACTGRP(*CALLER), which causes our utility programs to use the same activation group as the program that calls them. When this activation group is deleted, the calling program and our utilities will all be closed down. This seems the most appropriate option for utility type programs such as those we have created.

8.5 Working with APIs

This section discusses the useful, interesting, and odd things we found about the various APIs we used. Most of the APIs are described in detail in *OS/400 Security APIs V4R4,* SC41-5872 and require the service program QSYDIGID. Where an API is described in another manual, or requires another service program, we will state this.

Where possible we have used the API procedures, for example, QsyAddVldlCertificate, instead of the API programs, such as QSYADDVC. The procedures run marginally faster and are more in the *modern* style. Also there are more traps to the procedures than the programs. If you can handle the procedures you can handle the programs but the reverse is not necessarily so.

8.5.1 Prototypes and parameter lengths

Many of the APIs have parameters of arbitrary length and another parameter that states the length to be used. If you specify a character field of a specific length on the API's prototype then the compiler will check that you always call the API using a variable of that length. This is not good because in fact the length of the parameter is not fixed and you may want to use different length variables in different situations.

The best way we found to get around this was to define the parameters as a pointer passed by value. For example $P1 and $Qusec as follows:

```
 * Prototype for QExample, which...........
See .... to find the prototype details.
D Example         pr                 extproc('QsyExample')
D $P1                            *   Value
D $P1Len                        9b 0
D $Qusec                         *   Value
```

Figure 302. Sample prototype using pointers

Then when calling the procedure we pass the address of the variables. For example:

```
C                 callp     Example(%addr(Parm1):Parm1Len:%addr(Qusec)
```

Figure 303. Sample calling a procedure using pointers

Because they are of indefinite length we have defined both variable $P1 and $Qusec to be pointer types. When we call the sample procedure the actual length of Parm1 is specified by the variable Parm1Len and the actual length of Qusec is specified in the first 4 bytes of the structure.

8.5.2 Differences between procedures and programs

Speed

Calls to programs are marginally slower than calls to procedures. This is not an effect worth worrying about unless the number of calls is going to be large. One or two calls per transaction is not a problem. A much larger effect is closing programs, exiting RPG programs with the LR indicator on, or using activation group *NEW. These cause a program to have to be found, opened, its files found and opened, and so on every time it is called. Do not close programs that will be used frequently within a job.

Parameters passed by value

Programs always use parameters passed by reference. Procedures may use parameters passed by reference or by value. Some of the certificate API procedures pass some parameters by value. Finding this took some time and finding where to find the details even more.

In the library QSYSINC are a number of source files containing copy code for the various languages that can be used on the AS/400 system. The file QSYSINC/QRPGLESRC should contain copy code defining the prototypes for the certificate APIs. However it does not.

The source member QSYDIGID has the definitions for the procedures in the service program QSYDIGID. It contains the data structures and a heading “Prototypes”. And that is all. Just the heading.

For the service program QHTTPSVR/QZHBCGI, which contains the API for retrieving environment variables, it is even worse. No member is present at all.

However the C copy code file “H” does have both members and the members include the prototype definitions. If you look in these you will see something like the following:

```
QBFC_EXTERN void QsyAddVldlCertificate(
                   char    *Vldl_pathname,
                   int      Length_of_path,
                   char    *Certificate,
                   int      Type,
                   int      Length_of_certificate,
                   void    *Error_code);
```

Figure 304. C copy code prototype for QsyAddVldlCertificate

The parameters match what are documented in the API reference manual. The main thing to note is the presence or absence of the *.

When a * is present it means the parameter is passed by reference, that is, a pointer to the parameter is passed. This is the default for RPG.

When there is no * the parameter is passed by value. An example of this is the following prototype where $VldlPathLen, $CertType, and $CertLen are all passed by value.

```
 * Prototype for QsyAddVldlCertificate, which adds a certificate to a validation l
 * See QSYSINC/H member QSYDIGID to find the prototype details.
D AddCert         pr                  extproc('QsyAddVldlCertificate')
D $VldlPath                     40
D $VldlPathLen                   9b 0 Value
D $Cert                      32767
D $CertType                      9b 0 Value
D $CertLen                       9b 0 Value
D $Qusec                                    like(Qusec)
```

Figure 305. RPG prototype for QsyAddVldlCertificate

No changes are needed on the procedure call for parameters passed by value.

We have created a member, PROTOTYPES, in QRPGLESRC for the APIs we have used.

Variable parameter length

Because parameters to programs must always be passed by reference, not by value, the technique discussed previously in 8.5.1, “Prototypes and parameter lengths” on page 318 cannot be used for programs in order to define a parameter of arbitrary length.

If you want to have multiple calls to a program using variables of different lengths you cannot use a single prototype with defined lengths. You can define multiple prototypes, or you can abandon using prototypes and use the CALL operation code instead of CALLP.

8.5.3 Error structure

The standard API error structure can be set so errors result in an escape message being sent to the program or so the error details are recorded in the error structure.

For testing we found it best to set the bytes provided to zero so escape messages are sent. We could then read the message in the joblog and display the second level text if we wanted to. This is good for debugging. However if you want your programs to handle error conditions you will need to use the error structure.

We obtained the error structure definition by copying in QSYSINC/QRPGLESRC member QUSEC. This is a very basic structure as follows:

```
DQUSEC            DS
D*                                               Qus EC
D QUSBPRV                1      4B 0
D*                                               Bytes Provided
D QUSBAVL                5      8B 0
D*                                               Bytes Available
D QUSEI                  9     15
D*                                               Exception Id
D QUSERVED              16     16
```

Figure 306. QUSEC standard error structure

If you want your programs to use the error structure to trap, analyze, and respond to errors you may need to define more of the error structure so the information you need is available.

See the source code for RTVCERUSR for a minimal example of handling errors using the error structure. See *AS/400 System API Reference V4R4,* SC41-5801 for further details.

8.6 Description of the APIs used in the sample application

Application programming interfaces (APIs) allow programmers to use system functions that are mostly not available as OS/400 system commands. This section contains the information needed to implement the certificate and validation list APIs used in the sample application.

8.6.1 QsyAddVldlCertificate

QsyAddVldlCertificate (also available as the program QSYADDVC)can be used to add a certificate to a validation list. It has the following parameters:

1. **Validation list path**

   Despite validation lists only existing in QSYS.LIB, this API requires the validation list name to be given as a fully qualified path name such as /QSYS.LIB/DEM.LIB/PENDING.VLDL. However, you can still use *LIBL as part of the path. For example /QSYS.LIB/*LIBL.LIB/PENDING.VLDL.

2. **Validation list path length**

   The number of characters in the path name. Exactly. Excluding trailing blanks. Use %len(%trim(PathName)) to get this.

3. **Certificate data**

4. **Certificate type**

1 = ANSI, which is how most of the certificate APIs will give you a certificate.

3 = Base 64 encoded. This is how the Get-Environment-Variable API returns a certificate.

5. **Certificate length**

   This is always given by the API that gives you the certificate. The lengths we have seen are around 1000 - 2000 bytes so our buffer size of 32767 seems fairly safe.

6. **Error structure**

Example

Figure 307 shows the prototype definitions for the API.

```
 * Prototype for QsyAddVldlCertificate, which adds a certificate to a validation
list.
 * See QSYSINC/H member QSYDIGID to find the prototype details.
D AddVldlCert     pr                  extproc('QsyAddVldlCertificate')
D $Vldlpath                        *   value
D $VldlpathLen                    9b 0 value
D $Cert                            *   value
D $Certtype                       9b 0 value
D $Certlen                        9b 0 value
```

Figure 307. QsyAddVldlCertificate prototype

Figure 308 shows the definitions of the data structures and the API call.

```
D VldlPath        s             40
D VldlPathLen     s              9b 0
D Cert            s          32767
D CertLen         s              9b 0
D CertType        s              9b 0 inz(3)

C                   callp     AddVldlCert(%addr(VldlPath):VldlPathLen:
C                                 %addr(Cert):CertType:Certlen:
C                                 %addr(Qusec))
```

Figure 308. QsyAddVldlCertificate data structures and call

8.6.2 QsyRemoveVldlCertificate

QsyRemoveVldlCertificate (also available as the program QSYRMVVC) can be used to remove a certificate from a validation list. It is very similar to QsyAddVldlCertificate and has the following parameters:

1. **Validation list path**

   Despite validation lists only existing in QSYS.LIB, this API requires the validation list name to be given as a fully qualified path name such as /QSYS.LIB/DEM.LIB/PENDING.VLDL. However, you can still use *LIBL as part of the path. For example /QSYS.LIB/*LIBL.LIB/PENDING.VLDL.

2. **Validation list path length**

   The number of characters in the path name. Exactly. Excluding trailing blanks. Use %len(%trim(PathName)) to get this.

3. **Certificate data or Certificate handle**

4. **Certificate type**

1 = ANSI, which is how most of the certificate APIs will give you a certificate.

2 = Certificate handle. The certificate handle is used as the key to the validation list entry. If you have the certificate handle you should use this, because it is faster than giving a certificate.

3 = Base 64 encoded. This is how the Get-Environment-Variable API returns a certificate.

5. **Certificate, or certificate handle, length**

   This is always given by the API that gives you the certificate. The lengths we have seen for certificates are around 1000 - 2000 bytes so our buffer size of 32767 seems fairly safe. Certificate handles are always 40 bytes long and the developers tell us this will not change.

6. **Error structure**

Example

Figure 309 shows the prototype definitions for the API

```
 * Prototype for QsyRemoveVldlCertificate, which removes a certificate
 * from a validation list.
 * See QSYSINC/H member QSYDIGID to find the prototype details.
D RmvVldlCert     pr                extproc('QsyRemoveVldlCertificate')
D $Vldlpath                       *   value
D $VldlpathLen                   9b 0 value
D $Cert                           *   value
D $Certtype                      9b 0 value
D $Certlen                       9b 0 value
D $Qusec                          *   value
```

Figure 309. QsyRemoveVldlCertificate prototype

Figure 310 shows the definitions of the data structures and the API call.

```
D VldlPath        s             40
D VldlPathLen     s              9b 0
D Cert            s          32767
D CertLen         s              9b 0
D CertType        s              9b 0 inz(3)

C                   callp     RmvVldlCert(%addr(VldlPath):VldlPathLen:
C                                 %addr(Cert):CertType:Certlen:
C                                 %addr(Qusec))
```

Figure 310. QsyRemoveVldlCertificate data structures and call

8.6.3 QSYFDVLE

QSYFDVLE is only available as a program, not as a procedure.

QSYFDVLE can be used to retrieve an entry from a validation list. Since certificates are held as validation list entries, and the key used is the certificate handle, we can use this to retrieve certificates from validation lists. The API for listing certificates held on a validation list has to work through all the certificates on the list, parsing them and checking if they match the selection criteria given. This can be very much slower than QSYFDVLE.

Unfortunately the parameters for this API are a bit complex and confusing. At least we found them so.

1. **Validation list name and library**

This requires a 20-character field with the validation list name left adjusted in the first 10 characters and the library name left adjusted in the second 10.

For example `'PENDING   *LIBL      '` You can use *LIBL and *CURLIB as library names.

2. **Entry ID**

   The key to the validation list entry, in our case a certificate handle. This parameter has the following structure:

   a. Length, in our case 40.

   b. CCSID, which the manual says is not used to find the entry and we set to 0.

   c. Entry ID, which in this case is a certificate handle.

3. **Attribute information requested**

   A validation list entry consists of a key, an encrypted part, a non-encrypted part, and a number of named attributes. The standard parts have limited lengths and this is why a certificate is held as an attribute. The API returns the attributes that are specified in the request. This parameter has the following structure:

   a. Number of attributes to be returned.

   b. Each attribute has the following structure:

      1. Length of attribute entry. In our case 36.

         This must be a multiple of 4. If not, you get the helpful message `One of the parameters is invalid.`

      2. Attribute location. In our case 0 (which means, the validation list).

      3. Attribute type. In our case 0 (which means, system defined).

      4. Displacement to attribute ID. Value = 24. No other value is possible.

      5. Length of the attribute ID. In our case this is 11.

      6. Bytes provided for the attribute data. This refers to the space provided in parameter 5, the return attribute information. In our case we set this to 32767.

      7. The attribute ID. The name of the attribute to be returned. In our case *QsyX509Cert*. However, remember to put this in a 12-byte field so that the length of the attribute entry works out to a multiple of 4 bytes.

4. **Validation list entry data**

   This is 1724 bytes and has a defined structure. However, we do not use this.

5. **Attribute information returned**

   The information for the attributes requested in parameter 3. All fields are output. It has the following structure for each of the attributes that are requested:

   a. Length of entry

      The total length of data returned for this attribute, including this field.

      In the manual this parameter has the same name, Length of attribute entry as the field describing the total length of an attribute entry in the attribute information requested parameter. This was a bit confusing to us.

   b. Bytes returned

The actual number of bytes returned including padding.

c. Bytes available

The number of bytes available to return including padding. This should match the Bytes returned value. If not you do not get all of the attribute data returned - which would invalidate a certificate.

d. Length of attribute

The actual length of the attribute, in our case the certificate. Due to padding this may not be the same as bytes returned.

e. CCSID of attribute

f. Attribute value

In our case this is the certificate.

6. **Error structure**

Example

Figure 311 shows the prototype definitions for the API.

```
 * Prototype for QSYFDVLE, which retrieves an entry from a validation list.
 * Because this is a program all parameters are passed by reference
 * NOTE.  The structures used are set for retrieving a certificate not
 * any validation list entry
D RtvVldlCert     pr                  extpgm('QSYFDVLE')
D $VldlNameLib                  20
D $VldlId                                    like(VldlId)
D $VldlAtr                                   like(VldlAtr)
D $VldlData                                  like(VldlData)
D $VldlAtrR                                  like(VldlAtrR)
D $Qusec                                     like(Qusec)
```

Figure 311. QSYFDVLE prototype

Figure 312 shows the definitions of the data structures and the API call.

```
 * Structures used by get validation list entry  QSYFDVLE
 * NOTE.  These are set for retrieving a certificate - not a general
 * validation list entry
D VldlPendingLib   s            20    inz('PENDING   *LIBL     ')

D VldlID          ds
D VldlIDlen                      9b 0 inz(40)
D VldlIDCcsid                    9b 0 inz(0)
D VldlHandle                    40

D VldlAtr         ds
D VldlAtrNum                     9b 0 inz(1)
D VldlAtrLen                     9b 0 inz(36)
D VldlAtrLocn                    9b 0 inz(0)
D VldlAtrType                    9b 0 inz(0)
D VldlAtrIdDisp                  9b 0 inz(24)
D VldlAtrIdLen                   9b 0 inz(11)
D VldlAtrLenPrv                  9b 0 inz(32767)
D VldlAtrId                     12    inz('QsyX509Cert ')

D VldlData        s           1724

D VldlAtrR        ds
D VldlAtrRLen                    9b 0
D VldlAtrRLenRtn                 9b 0
D VldlAtrRLenAvl                 9b 0
D VldlAtrRLenAtr                 9b 0
D VldlAtrRCcsid                  9b 0
D VldlAtrRData               32767

C                   callp     RtvVldlCert(VldlPendingLib:VldlID:VldlAtr:
C                                VldlData:VldlAtrR:Qusec)
```

Figure 312. QSYFDVLE data structures and call

8.6.4 QsyAddUserCertificate

QsyAddUserCertificate (also available as the program QSYADDUC) can be used to associate a certificate with a user profile. You can then use the HTTP protection directive that limits access to only certificates that are associated with user profiles. You can also specify that the associated user profile is used to process requests. This allows you to use AS/400 authorities to control the access allowed to Internet users.

QsyAddUserCertificate has the following parameters:

1. **User profile name**

   Ten characters. The name of the user profile to which the certificate is to be associated with.

2. **Certificate data**
3. **Certificate type**

   1 = ANSI, which is how most of the certificate APIs will give you a certificate.

   3 = Base 64 encoded. This is how the Get-Environment-Variable API returns a certificate.

4. **Certificate length**

This is always given by the API that gives you the certificate. The lengths we have seen are around 1000 - 2000 bytes so our buffer size of 32767 seems fairly safe.

5. **Error structure**

Example

Figure 313 shows the prototype definitions for the API.

```
 * Prototype for QsyAddUserCertificate, which adds a certificate to a user profil
 * See QSYSINC/H member QSYDIGID to find the prototype details.
D AddUserCert     pr                  extproc('QsyAddUserCertificate')
D $UserProfile                  10
D $Cert                           *   value
D $Certtype                      9B 0 value
D $Certlen                       9B 0 value
D $Qusec                          *   value
```

Figure 313. QsyAddUserCertificate prototype

Figure 314 shows the definitions of the data structures and the API call.

```
D #UserProfile    s             10
D Cert            s          32767
D CertLen         s              9b 0
D CertType        s              9b 0 inz(3)

 * Add the certificate to the user profile.
C                   callp     AddUserCert(#UserProfile:%addr(Cert):
C                                  CertType:CertLen:%addr(Qusec))
```

Figure 314. QsyAddUserCertificate data structures and call

8.6.5 QsyRemoveUserCertificate

QsyRemoveUserCertificate (also available as the program QSYRMVUC) removes the association of a certificate with a user profile. It has the following parameters:

1. **User profile name**

   Ten characters. The name of the user profile to which the certificate is associated with.

2. **Certificate data or certificate handle**

3. **Certificate type**

   1 = ANSI, which is how most of the certificate APIs will give you a certificate.

   2 = Certificate handle. The certificate handle is used as the key to the validation list entry. If you have the certificate handle you should use this as it is faster than using a certificate.

   3 = Base 64 encoded. This is how the Get-Environment-Variable API returns a certificate.

4. **Certificate or certificate handle length**

   This is always provided by the API that gives you the certificate. The lengths we have seen for certificates are around 1000 - 2000 bytes so our buffer size of 32767 seems fairly safe. Certificate handles are always 40 bytes long and the developers tell us this will not change.

5. **Error structure**

Example

Figure 315 shows the prototype definitions for the API.

```
 * Prototype for QsyRemoveUserCertificate, which removes a certificate
 * from a user profile.
 * See QSYSINC/H member QSYDIGID to find the prototype details.
D RmvUserCert     pr                  extproc('QsyRemoveUserCertificate')
D $UserProfile                  10
D $Cert                           *   value
D $Certtype                      9B 0 value
D $Certlen                       9B 0 value
D $Qusec                          *   value
```

Figure 315. QsyRemoveUserCertificate prototype

Figure 316 shows the definitions of the data structures and the API call.

```
D #UserProfile    s             10
D Cert            s          32767
D CertLen         s              9b 0
D CertType        s              9b 0 inz(3)

 * Remove the certificate association with the user profile.
C                   callp     RmvUserCert(#UserProfile:%addr(Cert):
C                                  CertType:CertLen:%addr(Qusec))
```

Figure 316. QsyRemoveUserCertificate data structures and call

8.6.6 QsyCheckVldlCertificate

QsyCheckVldlCertificate (also available as the program QSYCHKVC) checks if a certificate is present on a particular validation list.

You can use a full certificate or a certificate handle to check the list. Using a certificate handle is faster. If you use a certificate the API internally parses the certificate to obtain the handle then uses this handle to check the validation list.

QsyCheckVldlCertificate has the following parameters:

1. **Validation list path**

   Despite validation lists only exist in the QSYS.LIB file system, this API requires the validation list name to be given as a fully qualified path name such as /QSYS.LIB/DEM.LIB/PENDING.VLDL. However, you can still use *LIBL as part of the path. For example /QSYS.LIB/*LIBL.LIB/PENDING.VLDL.

2. **Validation list path length**

   The number of characters in the path name. Exactly. Excluding trailing blanks. Use %len(%trim(PathName)) to get this value.

3. **Certificate data or Certificate handle**

4. **Certificate type**

   1 = ANSI, which is how most of the certificate APIs will give you a certificate.

   2 = Certificate handle. The certificate handle is used as the key to the validation list entry. If you have the certificate handle you should use this as it is faster than using a certificate.

   3 = Base 64 encoded. This is how the Get-Environment-Variable API returns a certificate.

5. **Certificate, or ceriticate handle, length**

This is always provided by the API that gives you the certificate. The lengths we have seen for certificates are around 1000 - 2000 bytes so our buffer size of 32767 seems fairly safe. Certificate handles are always 40 bytes long and the developers tell us this will not change.

6. **Return code**

   1 = the certificate is present on the validation list.

   0 = the certificate is not present.

7. **Error structure**

Example

Figure 317 shows the prototype definitions for the API.

```
 * Prototype for QsyCheckVldlCertificate which checks if a cert is
 * on a validation list
 * See QSYSINC/H member QSYDIGID to find the prototype details.
CheckCert       pr                 extproc('QsyCheckVldlCertificate')
D $VldlPath                      *   value
D $VldlPathLen                 9b 0 value
D $Cert                          *   value
D $Certtype                    9b 0 value
D $Certlen                     9b 0 value
D $ReturnCode                  9b 0
D $Qusec                         *   value
```

Figure 317. QsyCheckVldlCertificate prototype

Figure 318 shows the definitions of the data structures and the API call.

```
D Vldl            s             10    inz('*VLDL')
D VldlPath        s             40
D VldlPathLen     s              9b 0
D Cert            s          32767
D CertLen         s              9b 0
D Certtype        s              9b 0 inz(3)
D ReturnCode      s              9b 0

 *         Check if certificate is on the validation list
C                   callp     CheckCert(%addr(VldlPath):VldlPathLen:
C                                       %addr(Cert):CertType:CertLen:
C                                       ReturnCode:%addr(Qusec))
```

Figure 318. QsyCheckVldlCertificate data structures and call

8.6.7 QsyFindCertificateUser

QsyFindCertificateUser (also available as the program QSYFNDCU)returns the name of the user profile associated with a certificate.

You can use a full certificate or a certificate handle with this API. Using a certificate handle is faster. If you use a certificate the API internally parses the certificate to obtain the handle and then uses this handle to find the user profile.

QsyFindCertificateUser has the following parameters:

1. **Certificate data or Certificate handle**

2. **Certificate type**

   1 = ANSI, which is how most of the certificate APIs will give you a certificate.

2 = Certificate handle. The certificate handle is used as the key to the validation list entry. If you have the certificate handle you should use this as it is faster than using a certificate.

3 = Base 64 encoded. This is how the Get-Environment-Variable API returns a certificate.

3. **Certificate or ceriticate handle length**

   This is always provided by the API that gives you the certificate. The lengths we have seen for certificates are around 1000 - 2000 bytes so our buffer size of 32767 seems fairly safe. Certificate handles are always 40 bytes long and the developers tell us this will not change.

4. **User profile name**

   The name of the user profile associated with the certificate.

   Returns blank if no user profile is associated with the certificate. However, the system also generates the error message CPF227D. To handle the message ID you will need to use the error structure. The source code for the RTVCERUSR program contains an example of using the error structure. Refer also to *AS/400 System API Reference V4R4,* SC41-5801 for full details of using error structures.

5. **Error structure**

   The error structure has the following fields:

   a. Bytes provided. 4 bytes binary.

   b. Bytes available. 4 bytes binary.

   c. Error code. 7 characters.

   d. Reserved. 1 byte.

   e. And some additional fields that are in our case not relevant.

Example

Figure 319 shows the prototype definitions for the API.

```
 * Prototype for QsyFindCertificateUser, which finds the user profile,
 * if any, associated with a certificate.
 * See QSYSINC/H member QSYDIGID to find the prototype details.
D FindCertUser    pr                  extproc('QsyFindCertificateUser')
D $Cert                           *   value
D $Certtype                      9B 0 value
D $Certlen                       9B 0 value
D $UserProfile                  10
D $Qusec                          *   value
```

Figure 319. QsyFindCertificateUser prototype

Figure 320 shows the definitions of the data structures and the API call.

```
D Cert            s           32767
D CertLen         s               9b 0
D CertType        s               9b 0 inz(3)
D #UserProfile    s              10

 * Set the error structure length to 16 to trap errors returned in
 * case no user is associated
C                   eval      QusBPrv=16
C                   callp     FindCertUser(%addr(Cert):CertType:CertLen:
C                                   #UserProfile:%addr(Qusec))

C                   if        QuseI <> *blanks and QuseI <> 'CPF227D'
```

Figure 320. QsyCheckVldlCertificate data structures and call

8.6.8 QsyParseCertificate

QsyParseCertificate (also available as the program QSYPARSC) parses a certificate and returns the values of its components such as owner distinguished name, issuer distinguished name, and expiration date. It has the following parameters.

1. **Certificate data**
2. **Certificate type**

   1 = ANSI, which is how most of the certificate APIs will give you a certificate.

   3 = Base 64 encoded. This is how the Get-Environment-Variable API returns a certificate.
3. **Certificate length**

   This is always provided by the API that gives you the certificate. The lengths we have seen are around 1000 - 2000 bytes so our buffer size of 32767 seems fairly safe.
4. **Format of data to be returned**

   CERT0200 = All text fields available, translated into the job's CCSID.

   CERT0210 = All text fields available, not translated.
5. **Variable for data returned**

   The name of the variable to receive the parsed certificate data. This has the following structure:

   a. Returned length of certificate data.

   b. Available length of certificate data. This may be larger than the returned length of certificate data if the size of the variable provided was less than the size of the data available.

   c. Offset to certificate handle.

   d. Length of certificate handle.

   e. Offset to version.

   f. Length of version.

   g. Offset to serial number.

   h. Length of serial number.

   i. Offset to issuer's common name.

j. Length of issuer’s common name.

k. And so on for many more certificate attributes. See *OS/400 Security APIs V4R4,* SC41-5872 for details.

l. The parsed certificate data as specified by the offsets and lengths.

6. **Length of variable for data returned**

   The length of the variable to receive the parsed certificate data.

7. **Error structure**

Example

Figure 321 shows the prototype definitions for the API.

```
 * Prototype for QsyParseCertificate which parses a certificate
 * See QSYSINC/H member QSYDIGID to find the prototype details.
D ParseCert       pr                 extproc('QsyParseCertificate')
D $Cert                          *   value
D $Certtype                     9b 0 value
D $Certlen                      9b 0 value
D $Format                       8
D $Output                        *   value
D $OutputLen                    9b 0 value
D $Qusec                         *   value
```

Figure 321. QsyParseCertificate prototype

Figure 322 shows the definitions of the data structures and the API call.

```
D CertName        s             32    based(CertNamePtr)
D CertNameLen     s              9b 0 based(CertNameLenPtr)
D Cert            s          32767
D CertLen         s              9b 0
D CertType        s              9b 0 inz(3)
D ParseData       s                   like(Cert)
D ParseDataLen    s                   like(CertLen)
D                                     inz(%size(ParseData))
D ParseFmt        s              8    inz('CERT0200')
D Offset          s              9b 0 based(OffSetPtr)
D Handle          s             40    based(HandlePtr)

C                   callp     ParseCert(%addr(Cert):CertType:CertLen:
C                                   ParseFmt:%addr(ParseData):ParseDataLen:
C                                   %addr(Qusec))
C                   eval      OffsetPtr      = %addr(ParseData) + 8
C                   eval      HandlePtr      = %addr(ParseData) + Offset
C                   eval      OffsetPtr      = %addr(ParseData) + 104
C                   eval      CertNamePtr    = %addr(ParseData) + Offset
C                   eval      CertNameLenPtr = %addr(ParseData) + 108
```

Figure 322. QsyParseCertificate data structures and call

8.6.9 QtmhGetEnv

QtmhGetEnv is documented in the *Web Programming Guide V4R4,* GC41-5435. It requires the service program `QHTTPSVR/QZHBCGI` and is not available as a program.

QtmhGetEnv returns the value of a particular environment variable. Environment variables are used by the HTTP server to hold information that can be retrieved from a CGI program. One of the available environment variables is the client’s certificate. Others are various values from the certificate, fields returned from an HTML form, and so on.

When environment variables are returned they are translated into the job's current CCSID. However, certificates are not character data and should not be translated. We need to undo the translation to get a valid certificate. Because certificates are returned in base 64 encoding only a very limited character set is used. The translation can be performed with the API QDCXLATE using the translation table QASCII. See 8.6.10, "QDCXLATE" on page 333 for details on using the translation API.

QtmhGetEnv has the following parameters:

1. **Variable for data returned**

   The variable to hold the data returned.

2. **Length of variable for data returned**

   The length of the variable to hold the data returned.

3. **Length of environment variable returned**

   The length of the environment variable returned.

4. **Environment variable name**

   The name of the variable you want to be returned. For a certificate this is HTTPS_CLIENT_CERT. The various environment variables are documented in the *Web Programming Guide V4R4,* GC41-5435.

5. **Environment variable name length**

   The length of the environment variable name.

6. **Error structure**

Example

Figure 323 shows the prototype definitions for the API.

```
 * QtmhGetEnv This returns a variable from the "environment"
 * See QSYSINC/H member QZHBCGI to find the prototype details.
D GetEnvVar       pr                    extproc('QtmhGetEnv')
D $EnvRcvr                        *   value
D $EnvRcvrLen                    9b 0
D $EnvRspLen                     9b 0
D $EnvRqsName                     *   value
D $EnvRqsNameLen                 9b 0
D $Qusec                          *   value
```

Figure 323. QtmhGetEnv prototype

Figure 324 shows the definitions of the data structures and the API call.

```
D EnvName         s             50    inz('HTTPS_CLIENT_CERT')
D EnvNameLen      s              9b 0
D Cert            s          32767
D CertLenAvl      s              9b 0 inz(%size(Cert))
D CertLen         s              9b 0

C                   eval      EnvNameLen = %len(%trim(EnvName))
C                   callp     GetEnvVar(%addr(Cert):CertLenAvl:CertLen:
C                                   %addr(EnvName):EnvNameLen:%addr(Qusec))
```

Figure 324. QtmhGetEnv data structures and call

8.6.10 QDCXLATE

The QDCXLATE API is documented in *OS/400 National Language Support APIs V4R4,* SC41-5863. It is only available as a program.

QDCXLATE translates a string using a translation table.

When environment variables are returned they are translated into the job’s current CCSID. However, certificates are not character data and should not be translated. We need to undo the translation to get a valid certificate. Because certificates are returned in base 64 encoding only a very limited character set is used and this can be safely translated using the QASCII translation table.

QDCXLATE has the following parameters.

1. **Length of string**

   The length of the string to be translated.

2. **String to translate**

   The variable holding the string to be translated.

   > **Warning**
   >
   > QDCXLATE returns the translated string into the original variable

3. **Translation table**

   The name of the translation table to use. This must be given as a 20-character string with the table name left adjusted in the first 10 characters and the library name left adjusted in the second 10 characters.

   For example ‘`QASCII    QSYS      `’.

   Translation table QASCII does a basic conversion of EBCDIC to ASCII. QEBCDIC does the reverse. QSYSTRNTBL converts lower case to upper case. There are many special tables in the QUSRSYS library for conversions between CCSIDs.

Example

Figure 325 shows the prototype definitions for the API.

```
 * Prototype for QDCXLATE program which translates a string.
 * This is a program so all parameters are passed by reference
 * Because this is a program we cannot use pointer variables and must
 * declare the length of the string to translate.  Hence we have given
 * this the name XlateCert as the string length is set to what we are using
 * for certificates.
D XlateCert       pr                  extpgm('QDCXLATE')
D $StringLen                     5  0
D $String                    32767
D $Table                        10
```

Figure 325. QDCXLATE prototype

Figure 326 shows the definitions of the data structures and the API call.

```
D Cert            s         32767
D CertLen         s             9b 0
D QdcLen          s             5  0
D QAscii          s            10    inz('QASCII')

C                   eval      Qdclen = CertLen
C                   callp     XlateCert(QdcLen:Cert:QAscii)
```

Figure 326. QDCXLATE data structures and call

8.7 Administration tasks

In this sample application we assume that an administrator approves or declines user registration requests. This section shows you the steps to perform the registration for a customer and a supplier.

Note that this application provides two interface programs to perform the registration. It is not a complete administration utility. Therefore, you have to perform some manual steps that would not appear in a real production environment.

8.7.1 Registering a customer

A user must first submit a registration request before the administrator can approve or decline that request. Once a registration request is pending, the administrator has to perform the following steps:

1. Use the Data File Utility (DFU) or the Structured Query Language (SQL) interface to display the CLTMASP file. Note that you can not use a temporary DFU program, because the certificate handle cannot be displayed. Search for records with a P (Pending) in the CLTSTS (Sts) field. Write down the client number of this record.
2. Enter the following command to approve the registration request:

   ```
   CALL PGM(APPCLTREG) PARM(X'0000041F' A X)
   ```

   Where `0000041F` is the client number. For example, if there is a registration request pending for client number 66, you have to enter `0000066F`. The next parameter identifies the action. A stands for Approve and D for Decline. The X represents a field holding a return value, which is not used on a command line.

This concludes the customer registration process.

8.7.2 Registering a supplier

In our application, we consider a supplier also as a customer. Therefore, the customer registration must be done prior to the supplier registration. When a registration is processed for a customer, you can perform the following steps to extend a customer to a supplier:

1. Use the client number from the customer registration and perform the following command to register a supplier:

   ```
   CALL PGM(ASSCERUSR) PARM(X'0000021F' usrprf X)
   ```

Where `0000021F` represents the client number from the customer registration and `usrprf` the parameter for the user profile that will be created for the supplier.

This concludes the supplier registration process.

Chapter 9. Sample application: using certificates in Java

This chapter explains how client certificates can be used in Java applications. It demonstrates, for example, how certificates are added to validation lists, how certificates are associated with user profiles, and how to receive client certificates in the Java application. The Java application on the server runs as servlets under the WebSphere Application Server. Refer to Chapter 7, “Introducing digital certificates in user applications” on page 271 for a general description of the program functions and flow of the sample application.

The major resources used when this application was developed are:

- *HTTP Server for AS/400 Webmaster's Guide V4R4*, GC41-5434
- *Building AS/400 Client/Server Applications with Java*, SG24-2152
- *Building AS/400 Applications for IBM WebSphere Standard Edition 2.0*, SG24-5635
- `http://www.as400.ibm.com/tstudio/websphere/docs/as400v202/index.html` WebSphere Application Server for AS/400 online documentation.

Other publications are referenced in Appendix G, “Related publications” on page 405.

Important

The method to access a certificate with JDK 1.1.8 or lower is different from the methods used in JDK 1.2. We have implemented the administration utility application with JDK 1.1.8. You must be sure that you are running JDK 1.1.8 or JDK 1.1.7 and not JDK 1.2. You can test your JDK version by performing the following command:

```
java -version
```

This command can be performed on a PC at a DOS command prompt. On the AS/400 system you have to use the `QSH` command to enter the `QSHELL` command entry and then enter the `java -version` command.

9.1 Setting up the environment

This section shows the commands and sources used to create the environment to run the application. Program logic and source information are not covered in this section; they are described in 9.2, “The architecture of the application” on page 354.

9.1.1 The sample application system environment

For the Java sample application we used a simple network environment as shown in Figure 327. Both systems are connected to an intranet.

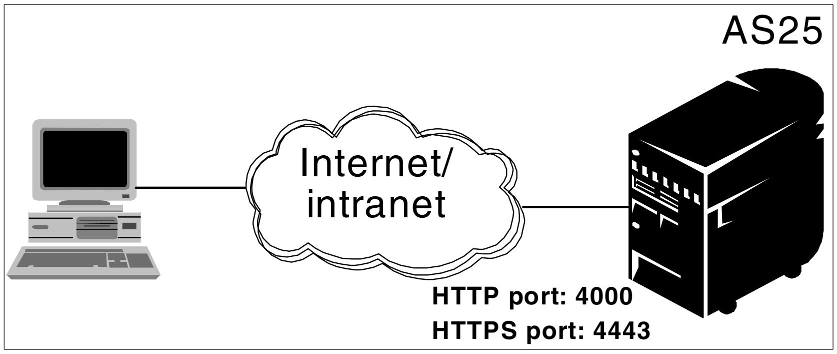


Figure 327. Network environment

The following software environment is used on the AS/400 system:

- OS/400 V4R4 with the cumulative PTF tape C9313440. The PTFs listed here show the PTF level used when writing and testing the application. You may install the newest cumulative PTF level on your AS/400 system.
- OS/400 - QShell Interpreter, option 30 of OS/400 (5769-SS1)
- Digital Certificate Manager (DCM), option 34 of OS/400 (5769-SS1)
- TCP/IP Connectivity Utilities for AS/400 (5769-TC1)
- IBM HTTP server for AS/400 (5769-DG1)
- IBM Cryptographic Access Provider product (5769-AC3)
- WebSphere Application Server for AS/400 (5769-AS1) Version 2.031, which is available by installing the group PTF SF99027

Note

When the sample application was written, we had problems receiving the client certificate into the Java application. PTF SF61070 solved this problem (APAR SA87275).

- AS/400 Toolbox for Java (5769-JC1)
- DB2 Query Mgr and SQL DevKit for AS/400 (5769-ST1)

The following software products are used on the PC:

- Microsoft Windows NT 4.0 Service Pack 4
- Netscape Communicator 4.7
- VisualAge for Java (used only for application development)

9.1.2 Obtaining and restoring the sample application

Refer to Appendix E, “Using the additional material” on page 401 for information on how to download the application code from the Internet. The README.HTML file that is part of the Web material contains detailed instructions on how to restore the application.

9.1.3 Creating the required AS/400 objects

The sample application requires certain objects to be created on the AS/400 system. This section describes how those objects are created and the purpose of them. Figure 328 shows the source of a CL program that contains all OS/400 commands to create the application environment except the programs themselves.

```
PGM
CRTVLDL VLDL(AS9315/PENDING)  TEXT('Certificates from pending registration  +
requests')
CRTVLDL VLDL(AS9315/ACCEPTED) TEXT('Certificates from registered clients')
CRTUSRPRF USRPRF(SALESOWN) PASSWORD(*NONE) TEXT('Demonstration system user')
crtdtaara nxtcltnum *dec 7 text('Next client number')
CRTUSRPRF USRPRF(SALESGRP) PASSWORD(*NONE) INLMNU(*SIGNOFF) TEXT('Group +
authorities for Internet supplier users')
CRTDIR DIR('/Suppliers') DTAAUT(*EXCLUDE) OBJAUT(*NONE)
chgaut 'suppliers' salesgrp dtaaut(*rx) objaut(*objref)
CRTPF FILE(CLTMASP) SIZE(10000 10000 100) AUT(*CHANGE)
CRTPF FILE(ORDDTLP) SIZE(1000000 30000 1000) AUT(*CHANGE)
CRTPF FILE(COUNTER) AUT(*CHANGE)
CHGOBJOWN  OBJ(AS9315) OBJTYPE(*LIB) NEWOWN(SALESAUT)
CHGOBJOWN  OBJ(AS9315/PENDING) OBJTYPE(*VLDL) +
                          NEWOWN(SALESOWN)
CHGOBJOWN  OBJ(AS9315/ACCEPTED) OBJTYPE(*VLDL) +
                          NEWOWN(SALESOWN)
GRTOBJAUT  OBJ(AS9315/*ALL) OBJTYPE(*ALL) USER(SALESAUT) +
                          AUT(*ALL)
RVKOBJAUT  OBJ(A9315) OBJTYPE(*LIB) USER(*PUBLIC) +
                          AUT(*ALL)
ENDPGM
```

Figure 328. AS/400 objects required for the sample configuration

The various objects that are created using the CL program are:

- `CRTVLDL VLDL(AS9315/PENDING) TEXT('Certificates from pending registration requests')`

  The validation list PENDING is used to hold all client certificates for Internet or intranet users who performed the registration as a new customer or supplier. Once the registration request has been approved or declined by the admin staff, the client certificate will be removed from this validation list.

- `CRTVLDL VLDL(AS9315/ACCEPTED) TEXT('Certificates from registered clients')`

  The validation list ACCEPTED holds all client certificates of customers or suppliers whose registration request has been approved.

- `CRTUSRPRF USRPRF(SALESOWN) PASSWORD(*NONE) TEXT('Demonstration system user common authorities')`

  The user profile SALESOWN will be the owner of all objects belonging to the sample application. It has no functional impact on the application itself.

- `CRTUSRPRF USRPRF(SALESGRP) PASSWORD(*NONE) INLMNU(*SIGNOFF) TEXT('Group + authorities for Internet supplier users')`

  The user profile SALESGRP is used as a group profile for all supplier user profiles. It gets permissions to the IFS directories used to store the supplier order files.

- `CRTDIR DIR('/Suppliers') DTAAUT(*EXCLUDE) OBJAUT(*NONE)`

  The IFS directory that contains all supplier directories.

- `chgaut '/suppliers' salesgrp dtaaut(*rx) objaut(*objref)`

Grant appropriate authorities for the suppliers directory to the INTSUPLIER group profile.

- `CRTPF FILE(CLTMASP) SIZE(10000 10000 100) AUT(*CHANGE)`

  Physical and logical files that contain the account data for customers and suppliers.

The source for CTLMASP is as follows:

```
********** Beginning of data **********************************************
   * CLTMASP    Client master
   *
  A          R CLTMAS                    TEXT('Client master')
   *
  A            CLTNUM         7  0       COLHDG('Client')
  A                                      EDTCDE(Z)
  A                                      CMP(GT 0)
  A                                      TEXT('Client number')
   *
  A            CLTNAME       30          COLHDG('Name')
  A                                      REFSHIFT(A)
  A                                      TEXT('Client name')
   *
  A            CLTSTS         1          COLHDG('Sts')
  A                                      TEXT('Status A=Accpeted, P=Pending +
  A                                      D=Declined, U=User prf')
  A                                      VALUES('A' 'P' 'D' 'U')
   *
  A            CLTCRD        16  0       COLHDG('Credit card')
  A                                      CMP(GT 0)
  A                                      TEXT('Credit card number')
   *
  A            CLTEMAIL      70          COLHDG('E-mail' 'address')
  A                                      REFSHIFT(A)
  A                                      TEXT('Client email address')
   *
  A            CLTHDL        40H         COLHDG('Certificate' 'Handle')
  A                                      TEXT('Client''s certificate handle')
************* End of data **************************************************
```

Figure 329. CTLMASP source

Beware

The default for the CRTPF command is `SIZE(10000 1000 3)`. In our experience this causes occasional problems when files become full. The useful purpose of the SIZE attribute is to stop a rogue application. It is best to set the size so high that only a rogue application will ever hit the limit.

- `CRTPF FILE(ORDDTLP) SIZE(1000000 30000 1000) AUT(*CHANGE)`

  The physical and logical files containing the order details. Since the application does not contain an order entry system, the records were added manually. The data are used for the View your orders option of the customer main window.

The source for ORDDTLP is as follows:

```
********** Beginning of data **********************************************
   *
  A          R ORDDTL                    TEXT('Order Details')
   *
  A            DTLORDNUM      7  0       COLHDG('Order')
  A                                      TEXT('Order number')
   *
  A            DTLLINE        3  0       COLHDG('Order Line')
  A                                      TEXT('Order line')
  A                                      CMP(GT 0)
   *
  A            DTLPRTNUM      7  0       COLHDG('Part')
  A                                      TEXT('Part number ordered')
  A                                      CMP(GT 0)
   *
  A            DTLDESC       30          COLHDG('Part description')
  A                                      REFSHIFT(A)
  A                                      TEXT('Part desc.  Default from +
  A                                      master, may change')
   *
  A            DTLQTY         5  0       COLHDG('Quantity')
  A                                      TEXT('Number ordered')
  A                                      CMP(GT 0)
   *
  A            DTLPRICE       7  2       COLHDG('Price')
  A                                      TEXT('Unit price')
  A                                      CMP(GE 0)
   *
  A            DTLCLTNUM      7  0       COLHDG('Client')
  A                                      CMP(GT 0)
  A                                      TEXT('Client number')
   *
  A            DTLSTS         1          COLHDG('Status')
  A                                      TEXT('Status: P=Packed, S=Shipped +
  A                                      C=Complete, O=On order')
  A                                      VALUES('O' 'P' 'S' 'C')
```

Figure 330. ORDDTLP source

- `CRTPF FILE(COUNTER) AUT(*CHANGE)`

  Create the counter file that can contains multiple counters. For this application the counter file is used to keep the next available account number for new customer or supplier registrations.

```
************** Beginning of data ****************************************
     * CLTNUM Order
     *
    A          R COUNT                     TEXT('Count')
     *
    A            CNTNAM        10          COLHDG('Counter')
    A                                      TEXT('Counter name')
     *
    A            CNTVAL         7  0       COLHDG('CounterVal')
    A                                      EDTCDE(Z)
    A                                      CMP(GT 0)
    A                                      TEXT('Counter value')
     *
    A          K CNTNAM
***************** End of data *******************************************
```

Figure 331. COUNTER source

- CHGOBJOWN OBJ(AS9315) OBJTYPE(*LIB) NEWOWN(SALESOWN)

```
CHGOBJOWN  OBJ(AS9315/PENDING) OBJTYPE(*VLDL) +
                          NEWOWN(SALESOWN)
CHGOBJOWN  OBJ(AS9315/ACCEPTED) OBJTYPE(*VLDL) +
                          NEWOWN(SALESOWN)
GRTOBJAUT  OBJ(ASA9315/*ALL) OBJTYPE(*ALL) USER(SALESOWN) +
                          AUT(*ALL)
RVKOBJAUT  OBJ(AS9315) OBJTYPE(*LIB) USER(*PUBLIC) +
                          AUT(*ALL)
```

  Change permissions for objects of the sample application.

There is also a user space required in the sample application. The name is CERTSPC. This user space is automatically created. It is used as a temporary storage to store a list of client certificates contained in a validation list. The class method getCertificateFromVLDL is using this user space.

9.1.4 Setting up the HTTP server

For the sample application we are using a welcome window that is served unprotected, that means, the SSL protocol is not used. This welcome window, which is the WelcomeSales.html window, is served through a server instance, called JAVASVR. This server instance listens to port 4000 for incoming HTTP requests.

The welcome window provides the options Order your parts now and Supplier access. Both options, when clicked, switch to the HTTPS protocol and send the appropriate URL requests to port 4443 of the JAVASVR server instance.

For this sample application we have chosen the port 4000 for HTTP requests, because the system we tested on was shared by several groups. In a real production environment, you would probably use an HTTP server instance that listens to the well-known port 80 for serving the welcome window. The application HTTP server configuration is shown in Figure 332.

```
# HTTP CONFIGURATION FILE
Protect /Suppliers/* {
      PasswdFile %%SYSTEM%%
      ACLOverride Off
      PostMask all
      GetMask all
      AuthType Cert
      UserID %%CLIENT%%
}
Service /*.jsp /QSYS.LIB/QAPPSVR.LIB/QZHJSVLT.SRVPGM:AdapterService
Service /servlet/* /QSYS.LIB/QAPPSVR.LIB/QZHJSVLT.SRVPGM:AdapterService
ServerInit /QSYS.LIB/QAPPSVR.LIB/QZHJSVLT.SRVPGM:AdapterInit /QIBM/ProdData/ +
      IBMWebAS/properties/bootstrap.properties
ServerTerm /QSYS.LIB/QAPPSVR.LIB/QZHJSVLT.SRVPGM:AdapterExit
Pass /IBMWebAS/* /QIBM/ProdData/IBMWebAS/web/*
Pass /Suppliers/* /Suppliers/*
Pass /* /QIBM/ProdData/IBMWebAS/web/*
Disable CONNECT
Disable DELETE
Disable PUT
Enable GET
Enable HEAD
Enable OPTIONS
Enable POST
Enable TRACE
HostName AS25
BindSpecific Off
Port 4000
UserID SALESOWN
DNS-Lookup Off
Imbeds Off SSIOnly
NormalMode On
# Do not change or delete the following AppName di
AppName QIBM_HTTP_SERVER_JAVASVR
SSLMode On
SSLPort 4443
SSLClientAuth Required
AlwaysWelcome On
DirAccess Selective
DirReadme Bottom
```

Figure 332. SALES HTTP server configuration

The highlighted server directives are crucial to our application and will be explained in more detail. All other directives are default directives or are not important for running the application.

The description of the most important server directives are as follows:

9.1.4.1 Common settings

The following server directives are used to allow access to the appropriate application data and programs.

- `Pass /* /QIBM/ProdData/IBMWebAS/web/*`

  Maps customer and supplier requests to the appropriate directory and files on the server. The ..../web directory contains the welcome window. Under this directory are the customer, supplier and image directories. The image directory contains image file that are used by all HTML pages. The directory structure is hidden from outside the server.

- `Enable GET`

  `Enable POST`

  These are the two request methods used in the sample application.

- `Port 4000`

  This port is used to serve the welcome window, which is not protected by SSL.

9.1.4.2 Supplier access

The following server directives are required to allow suppliers to list their own order files using a Web browser.

-
```
Protect /Suppldir/* {
   PasswdFile %%SYSTEM%%
   ACLOverride Off
   PostMask All
   GetMask All
   AuthType Cert
   UserID %%CLIENT%%
}
```

  The Protect directive protects the directory and subdirectories of the suppldir directory for incoming URL requests, such as `https://as25:4443/suppldir/barlen1`. The inline definitions for this protect statement require a client certificate that is associated with an AS/400 user profile. For example, when a supplier presents its client certificate, the authority checking will be done using the user profile with which that certificate is associated with.

  That means for the sample application that normal customers are not able to browse any supplier directory at all.

- `DirAccess Selective`

  When a new supplier is registered, a user profile and a supplier directory is created. A wwwbrws file is copied into the new supplier directory. The DirAccess Selective directive allows directory browsing only when a wwwbrws file is present in the directory to be browsed. This setting allows a supplier to browse their order files.

- `Pass /suppldir/* /suppliers/*`

  This PASS directive maps incoming URL requests containing the /suppldir/* path to the IFS directory /suppliers/*. This allows us to hide the actual directory structure.

- `DirReadme Bottom`

  When a supplier browses its directory, text is shown at the bottom of the browser window. In the sample application the supplier gets a description of the files displayed on the browser and instructions on how to proceed. This directive defines where the text will be shown on the browser window. The text itself is stored in a file named README, which itself is located in the supplier directory.

9.1.4.3 WebSphere

The following four directives are used to enable WebSphere under this HTTP server instance. The Java application uses Java servlets that run under the control of WebSphere.

```
Service /*.jsp /QSYS.LIB/QAPPSVR.LIB/QZHJSVLT.SRVPGM:AdapterService
Service /servlet/* /QSYS.LIB/QAPPSVR.LIB/QZHJSVLT.SRVPGM:AdapterService
ServerInit /QSYS.LIB/QAPPSVR.LIB/QZHJSVLT.SRVPGM:AdapterInit /QIBM/ProdData/ +
IBMWebAS/properties/bootstrap.properties
ServerTerm /QSYS.LIB/QAPPSVR.LIB/QZHJSVLT.SRVPGM:AdapterExit
```

9.1.4.4 Security

The following server directives are required to support the SSL protocol for this server instance.

- `AppName QIBM_HTTP_SERVER_JAVASVR`

  Is the application ID that is listed under Work with secure applications in the Digital Certificate Manager (DCM). A server certificate must be assigned to this application ID to enable SSL for this server instance.

- `SSLMode On`

  `SSLPort 4443`

  The previous two directives enable the SSL protocol for the server instance and define the port that is used for HTTPS client requests.

- `SSLClientAuth Required`

  Specifies that client authentication is required. No access is permitted without presenting a client certificate when using the HTTPS protocol. Note that the welcome window can be accessed without having an SSL connection.

9.1.5 IFS objects

The HTML files used in this sample application are stored in an Integrated File System (IFS) directory structure. Also the README and wwwbrws files that are used for supplier access are stored in an IFS directory.

The locations of the objects and their meaning are as follows:

Table 14. IFS objects for the HTTP server

Directory	File	Description
/QIBM/ProdData/IBMWebAS/web/		Main directory for HTTP server
/QIBM/ProdData/IBMWebAS/web/	Welcome.html	Welcome window
/QIBM/ProdData/IBMWebAS/web/images/	backdrop.gif	Image of Web window background
/QIBM/ProdData/IBMWebAS/web/images/	worldban.gif	World banner for Web windows
/QIBM/ProdData/IBMWebAS/web/customer/	Customer.html	Customer main window
/QIBM/ProdData/IBMWebAS/web/supplier/	Supplier.html	Supplier main window

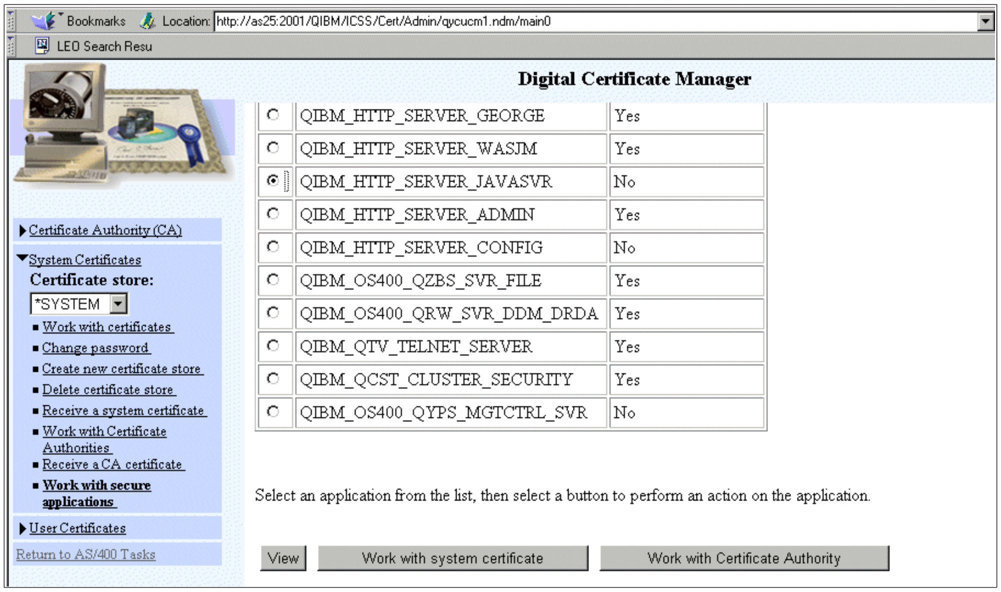
Directory	File	Description
/QIBM/ProdData/IBMWebAS/servlets/		Directory that holds the subdirectories containing the Java sample application.
/supplier (1)		Parent directory for supplier directories
/supplier/	wwwb (1)	Copy source for creating the wwwbrws file in an individual supplier directory.
/supplier/	Readm (1)	Copy source for creating the README file in an individual supplier directory.

(1) Note that these objects need *RX authorities for the SALESGRP group user profile.

9.1.6 Assigning a server certificate to the HTTP server instance

One requirement to enable SSL for the JAVASVR HTTP server instance is to assign a server certificate to it. For the sample application we used an AS/400 system as a private Certificate Authority (CA). The HTTP Configuration and Administration utility had to be used to enable SSL for the JAVASVR server instance in order to get the application ID added to DCM. The following steps take you through the process of assigning the server certificate to the JAVASVR HTTP server instance.

1. Start a Web browser and enter the URL `http://as25:2001/` to start the AS/400 Tasks page. Sign on to the Tasks page with a user profile that has *SECADM and *ALLOBJ authorities.
2. Start the **Digital Certificate Manager** (DCM) and expand **System Certificates**.
3. Click **Work with secure applications**.

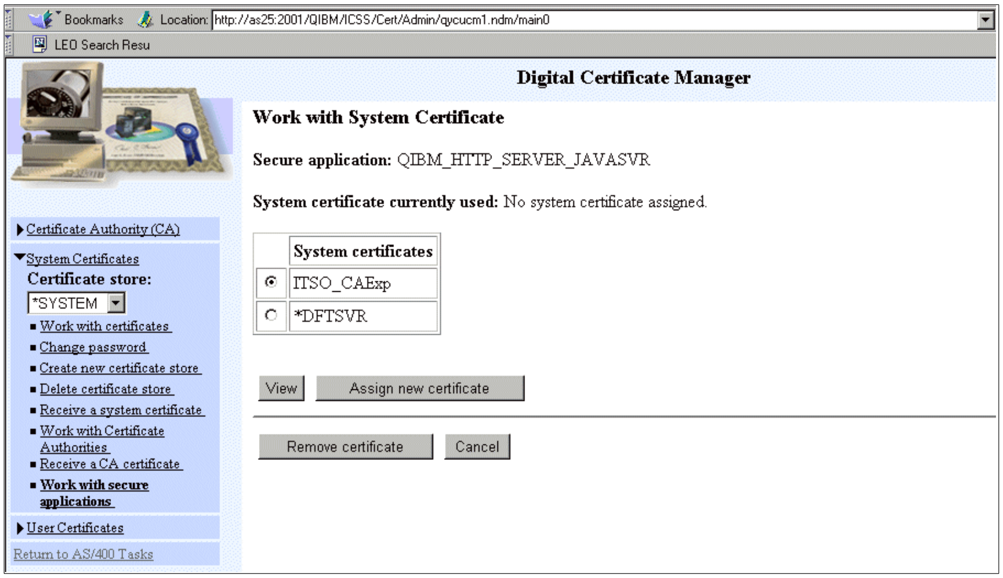

Bookmarks
Location: http://as25:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
LEO Search Resu
Digital Certificate Manager
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Work with system certificate
Work with Certificate Authority

○	QIBM_HTTP_SERVER_GEORGE	Yes
○	QIBM_HTTP_SERVER_WASJM	Yes
●	QIBM_HTTP_SERVER_JAVASVR	No
○	QIBM_HTTP_SERVER_ADMIN	Yes
○	QIBM_HTTP_SERVER_CONFIG	No
○	QIBM_OS400_QZBS_SVR_FILE	Yes
○	QIBM_OS400_QRW_SVR_DDM_DRDA	Yes
○	QIBM_QTV_TELNET_SERVER	Yes
○	QIBM_QCST_CLUSTER_SECURITY	Yes
○	QIBM_OS400_QYPS_MGTCTRL_SVR	No

Select an application from the list, then select a button to perform an action on the application.

Figure 333. DCM - Work with secure applications - step 1

4. Select the **QIBM_HTTP_SERVER_JAVASVR** application ID and click **Work with system certificate**. Note that the application ID only appears when the HTTP Configuration and Administration utility was used to configure SSL for the JAVASVR server instance.



Work with System Certificate

Secure application: QIBM_HTTP_SERVER_JAVASVR

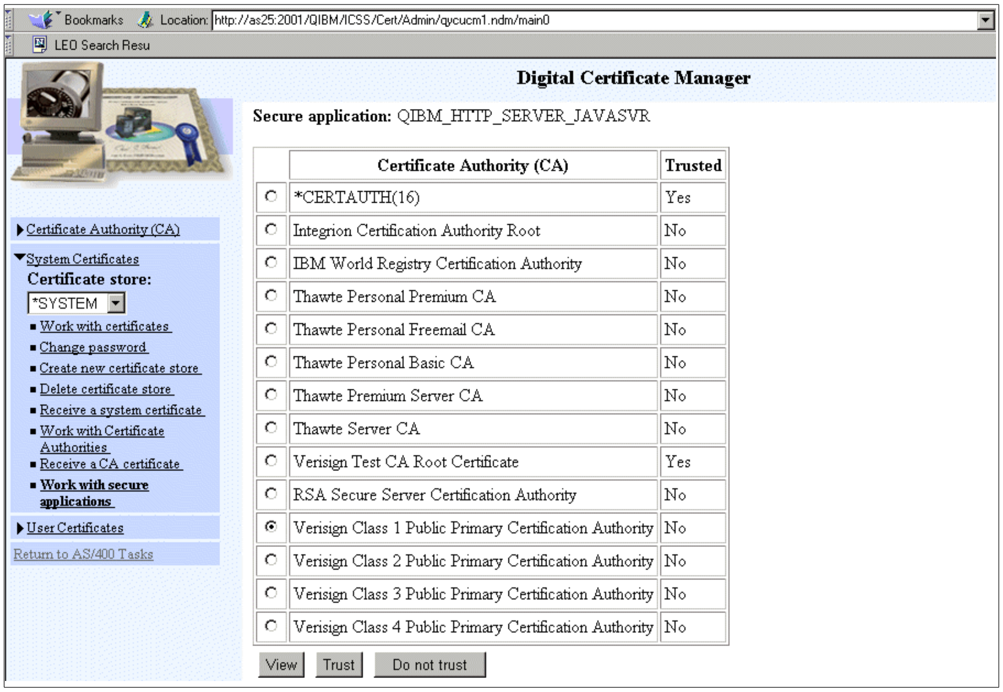
System certificate currently used: No system certificate assigned.

	System certificates
●	ITSO_CAExp
○	*DFTSVR

Figure 334. DCM - Work with secure applications - step 2

5. Select a server certificate that is to be assigned to the server instance and click **Assign new certificate**. When the completion message appears, click **OK**.

6. The list of secure applications is displayed again. Select the **QIBM_HTTP_SERVER_JAVASVR** application ID again and click **Work with Certificate Authority**.



Digital Certificate Manager

Secure application: QIBM_HTTP_SERVER_JAVASVR

	Certificate Authority (CA)	Trusted
○	*CERTAUTH(16)	Yes
○	Integrion Certification Authority Root	No
○	IBM World Registry Certification Authority	No
○	Thawte Personal Premium CA	No
○	Thawte Personal Freemail CA	No
○	Thawte Personal Basic CA	No
○	Thawte Premium Server CA	No
○	Thawte Server CA	No
○	Verisign Test CA Root Certificate	Yes
○	RSA Secure Server Certification Authority	No
●	Verisign Class 1 Public Primary Certification Authority	No
○	Verisign Class 2 Public Primary Certification Authority	No
○	Verisign Class 3 Public Primary Certification Authority	No
○	Verisign Class 4 Public Primary Certification Authority	No

Figure 335. DCM - Work with secure applications - step 3

7. The CA that issued the server certificate that is assigned to the JAVASVR server instance is automatically marked as trusted. All the CA certificates from which the application should accept client certificates must be marked as trusted. For example, if a Web user enters the application with a client certificate that was issued by VeriSign, the VeriSign CA certificate must be set as trusted. Otherwise, the client is not able to connect.

   Since we are using client certificates issued by the VeriSign Class 1 Public Primary Certification Authority, select **VeriSign Class 1 Public Primary Certification Authority** and click **Trust**. Repeat this step for all CAs the application should trust.

For more details on DCM refer to Chapter 5, “Digital Certificate Manager for AS/400” on page 107.

9.1.7 Configuring the WebSphere Application Server

We installed the application in a standard environment of the WebSphere Application Server. So no special classpath settings for the servlets are required. If you set up separate server instances with their own WebSphere directory structures, you need to modify the WebSphere configuration accordingly. Refer to the WebSphere documentation for further information on this subject.

Except for the administration utility, the rest of the sample application runs as Java servlets. The servlets are written to provide the most flexibility as possible. That means we avoided to hardcode system-dependent configuration values into the servlets. Instead we registered the servlets in WebSphere and specified the system-dependent values as parameters to the servlets.

The HTTP server directives that are required to enable the WebSphere Application Server under the HTTP server instance are listed in 9.1.4, “Setting up the HTTP server” on page 342.

It is assumed that the WebSphere Application Server is already installed according to the product installation instructions.

The following steps take you through the registration process of the servlets in the WebSphere Application Server:

1. Start a Web browser and enter the following URL:

   `http://as25:9090/` where `as25` is the AS/400 host name or IP address.

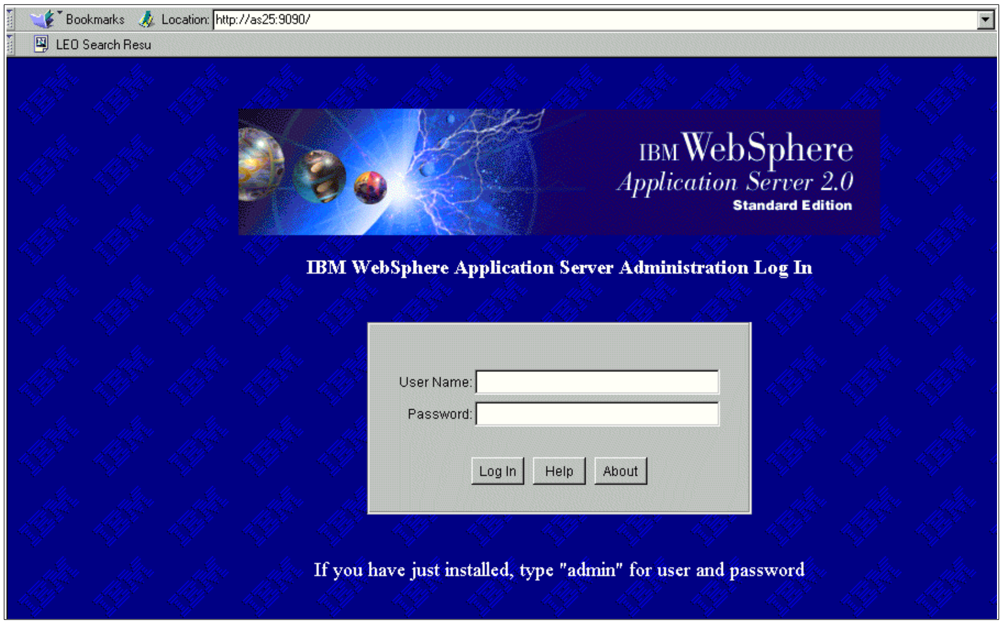
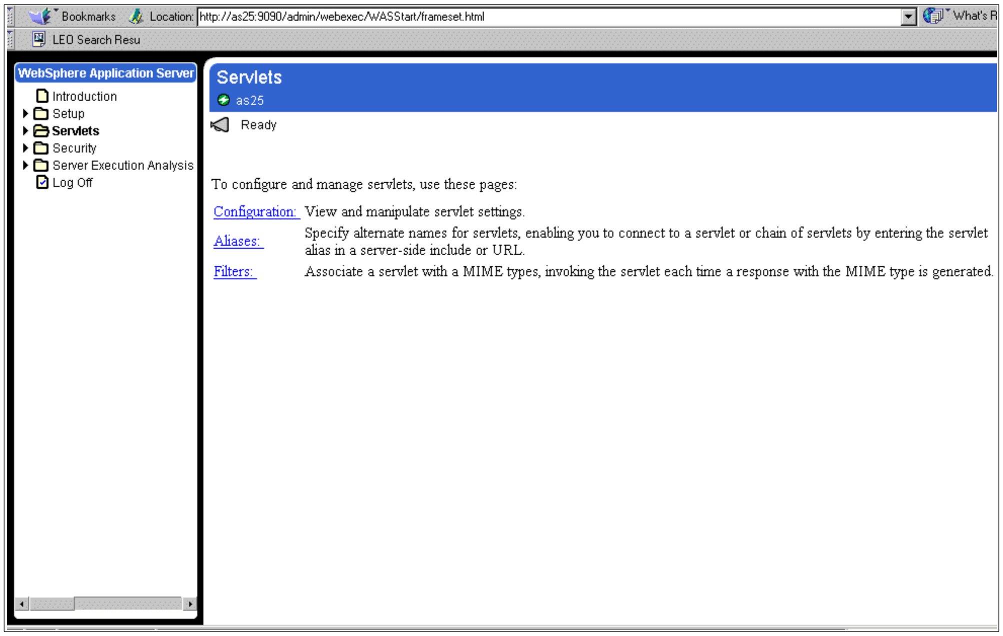

Bookmarks
Location: http://as25:9090/
LEO Search Resu
IBM WebSphere
Application Server 2.0
Standard Edition
IBM WebSphere Application Server Administration Log In
User Name:
Password:
Log In
Help
About
If you have just installed, type "admin" for user and password

Figure 336. WebSphere Administration Server Login

   Log in with the administrator user name and password. Note that we did not change the initial password and therefore signed on with `admin` as the user name and the password. After the user name and password is entered click **Log In**.

2. In the left pane of the window click **Servlets** to display the available options for servlets.


Bookmarks
Location: http://as25:9090/admin/webexec/WASStart/frameset.html
What's R
LEO Search Resu
WebSphere Application Server
Introduction
Setup
Servlets
Security
Server Execution Analysis
Log Off
Servlets
as25
Ready

To configure and manage servlets, use these pages:

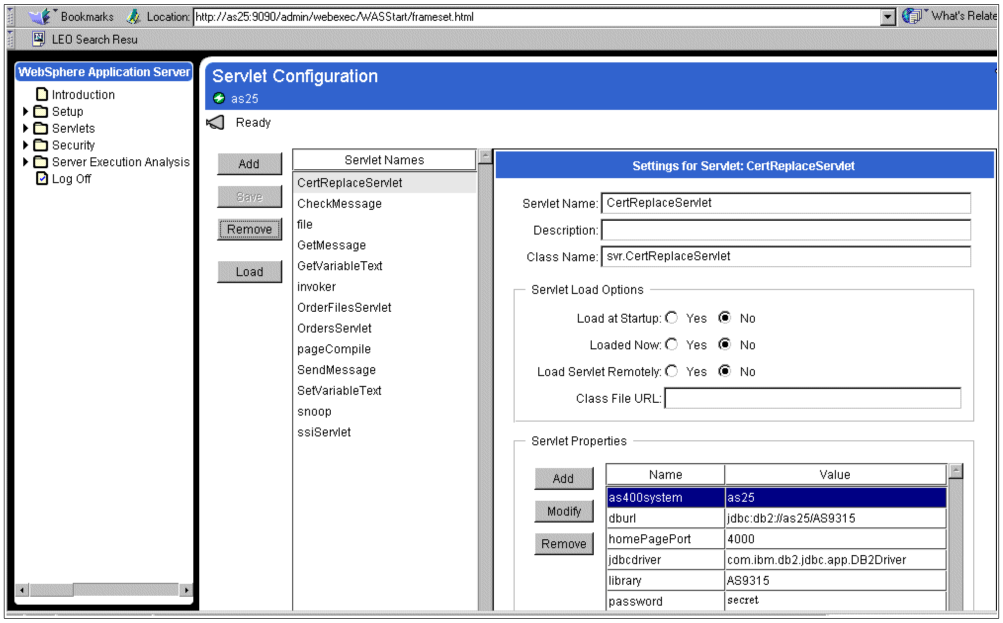
Configuration: View and manipulate servlet settings.

Aliases: Specify alternate names for servlets, enabling you to connect to a servlet or chain of servlets by entering the servlet alias in a server-side include or URL.

Filters: Associate a servlet with a MIME types, invoking the servlet each time a response with the MIME type is generated.

Figure 337. WebSphere Application Server - Servlets window

3. On the right pane of the window, click **Configuration**.



Settings for Servlet: CertReplaceServlet

Servlet Name: CertReplaceServlet

Description:

Class Name: svr.CertReplaceServlet

Servlet Load Options

Load at Startup: ○ Yes ● No

Loaded Now: ○ Yes ● No

Load Servlet Remotely: ○ Yes ● No

Class File URL:

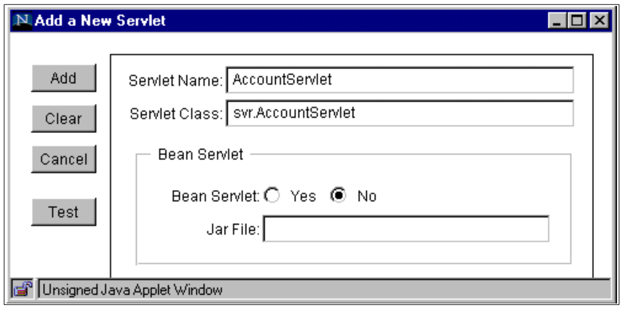
Servlet Properties

Name	Value
as400system	as25
dburl	jdbc:db2://as25/AS9315
homePagePort	4000
jdbcdriver	com.ibm.db2.jdbc.app.DB2Driver
library	AS9315
password	secret

Figure 338. WebSphere Application Server - Servlet Configuration overview

The middle pane of the window shows all currently registered servlets.

4. To register a servlet in WebSphere, click **Add** in the middle pane of the window.



Servlet Name: AccountServlet

Servlet Class: svr.AccountServlet

Bean Servlet

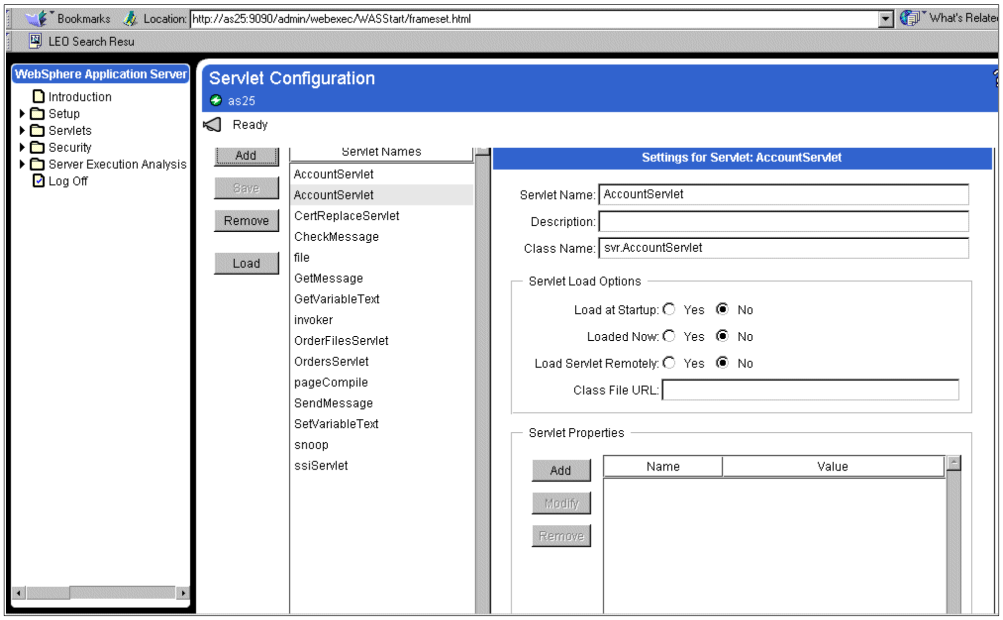
Bean Servlet: ○ Yes ● No

Jar File:

Figure 339. WebSphere Application Server - registering a servlet 1

Enter the servlet and class name. The servlets used in the sample application are not bean servlets. To register the AccountServlet enter `AccountServlet` in the Servlet Name parameter and `svr.AccountServlet` in the Class Name parameter. Select **No** for Bean Servlet.

5. Click **Add** to register the AccountServlet.



Servlet Name: AccountServlet

Description:

Class Name: svr.AccountServlet

Servlet Load Options

Load at Startup: ○ Yes ● No

Loaded Now: ○ Yes ● No

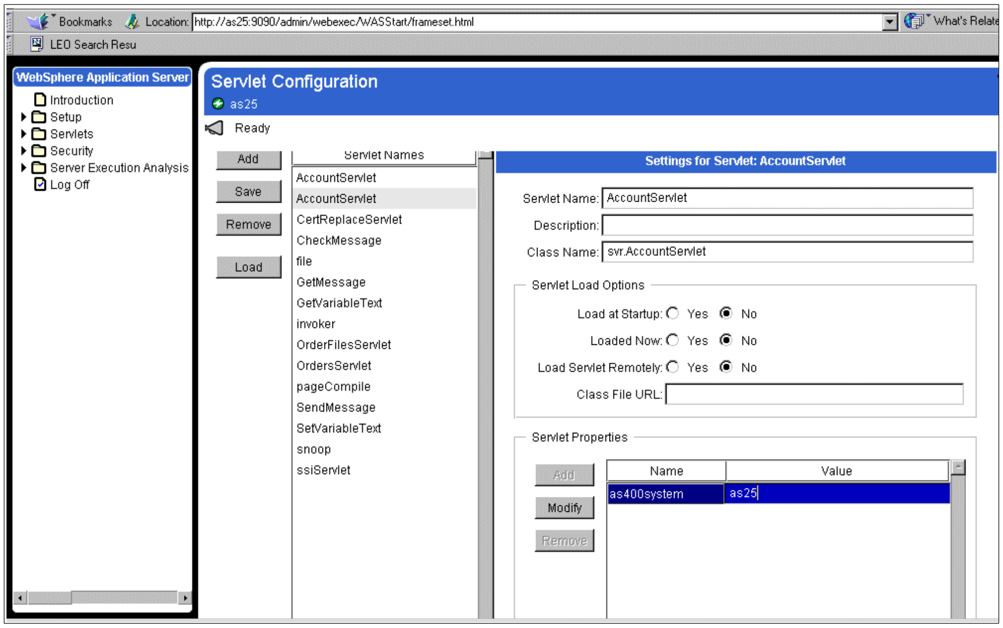
Load Servlet Remotely: ○ Yes ● No

Class File URL:

Servlet Properties

Figure 340. WebSphere Application Server - registering a servlet 2

6. Click **Add** on the Servlet Properties options to add the required parameter for the AccountServlet.



Servlet Configuration
as25

Settings for Servlet: AccountServlet

Servlet Name: AccountServlet
Description:
Class Name: svr.AccountServlet

Servlet Load Options
Load at Startup: ○ Yes ● No
Loaded Now: ○ Yes ● No
Load Servlet Remotely: ○ Yes ● No
Class File URL:

Servlet Properties

Name	Value
as400system	as25

Figure 341. WebSphere Application Server - registering a servlet 3

Enter `as400system` in the Name field and `as25` (your system name) in the Value field.

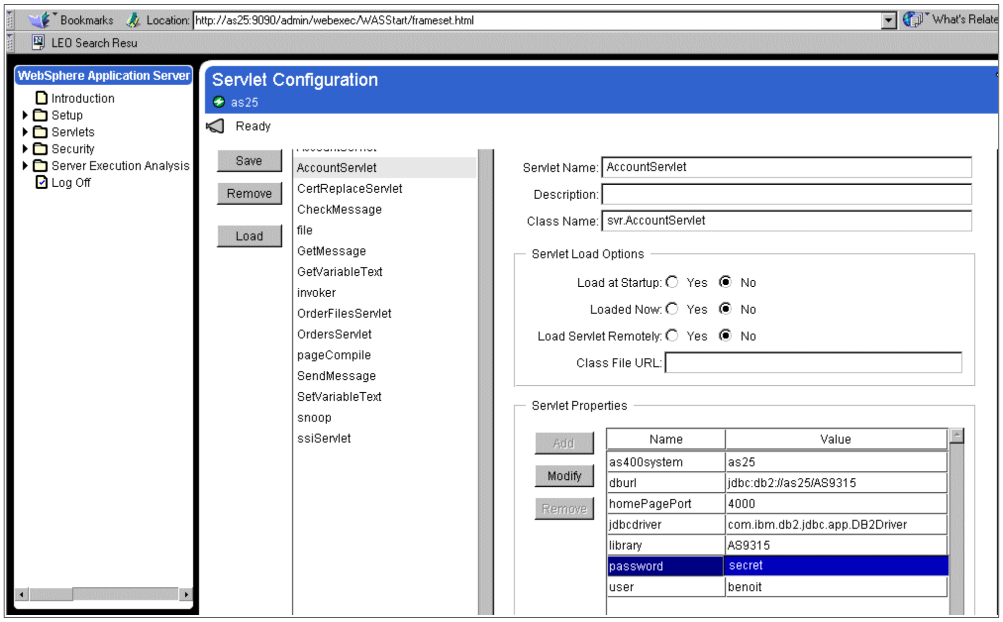
7. Press Enter to store the first property value.

8. Click **Add** on the Servlet Properties options again to add the rest of the required parameters for the AccountServlet. Repeat this step until all properties for the AccountServlet are set. Table 15 shows the values of the remaining properties to be added.

Table 15. AccountServlet properties

Remaining AccountServlet properties	
Name	**Value**
dburl	jdbc:db2://as25/AS9315 (Note that as25 is the system name and AS9315 is the library that contains the DB2 tables)
homePagePort	4000
jdbcdriver	com.ibm.db2.jdbc.app.DB2Driver
library	AS9315
password	(Password of the application user profile that is used for AS/400 Java Toolbox connections)
user	(User profile that is used for AS/400 Java Toolbox connections)

Figure 342 shows the AccountServlet with all properties set.


Bookmarks
Location: http://as25:9090/admin/webexec/WASStart/frameset.html
What's Related
LEO Search Resu
WebSphere Application Server
Introduction
Setup
Servlets
Security
Server Execution Analysis
Log Off
Save
Remove
Load
Add
Modify
Remove

Servlet Configuration
as25
Ready

AccountServlet
CertReplaceServlet
CheckMessage
file
GetMessage
GetVariableText
invoker
OrderFilesServlet
OrdersServlet
pageCompile
SendMessage
SetVariableText
snoop
ssiServlet

Servlet Name: AccountServlet
Description:
Class Name: svr.AccountServlet

Servlet Load Options
Load at Startup: ○ Yes ● No
Loaded Now: ○ Yes ● No
Load Servlet Remotely: ○ Yes ● No
Class File URL:

Servlet Properties

Name	Value
as400system	as25
dburl	jdbc:db2://as25/AS9315
homePagePort	4000
jdbcdriver	com.ibm.db2.jdbc.app.DB2Driver
library	AS9315
password	secret
user	benoit

Figure 342. WebSphere Application Server - Registered AccountServlet

9. Repeat the previous steps to register the remaining servlets of the sample application. Table 16 shows the parameter values to register the servlets. Note that for all servlets the value for Load at Startup and Load Servlet Remotely is No.

Table 16. Remaining application servlets

Servlet registration		
Servlet	**Parameter**	**Value**
CertReplaceServlet		
	Servlet Name	CertReplaceServlet
	Class Name	svr.CertReplaceServlet
	Servlet properties	
	as400system	as25 (your AS/400 server system)
	dburl	jdbc:db2://as25/AS9315 (Note that as25 is the system name)
	homePagePort	4000
	jdbcdriver	com.ibm.db2.jdbc.app.DB2Driver
	library	AS9315
	password	(Password of the application user profile that is used for AS/400 Java Toolbox connections)
	user	(User profile that is used for AS/400 Java Toolbox connections)
OrderFilesServlet		
	Servlet Name	OrderFilesServlet

Servlet registration		
	Class Name	svr.OrderFilesServlet
Servlet properties		
	as400system	as25 (your AS/400 server system)
	dburl	jdbc:db2://as25/AS9315 (Note that as25 is the system name)
	homePagePort	4000 (the HTTP server port)
	jdbcdriver	com.ibm.db2.jdbc.app.DB2Driver
	library	AS9315
	password	(Password of the application user profile that is used for AS/400 Java Toolbox connections)
	user	(User profile that is used for AS/400 Java Toolbox connections)
OrdersServlet		
	Servlet Name	OrdersServlet
	Class Name	svr.OrdersServlet
Servlet properties		
	as400system	as25 (your AS/400 server system)
	dburl	jdbc:db2://as25/AS9315 (Note that as25 is the system name)
	homePagePort	4000 (the HTTP server port)
	jdbcdriver	com.ibm.db2.jdbc.app.DB2Driver
	library	AS9315
	password	(Password of the application user profile that is used for AS/400 Java Toolbox connections)
	user	(User profile that is used for AS/400 Java Toolbox connections)

9.2 The architecture of the application

The following figure provides an overview of the different packages used to build the sample application.

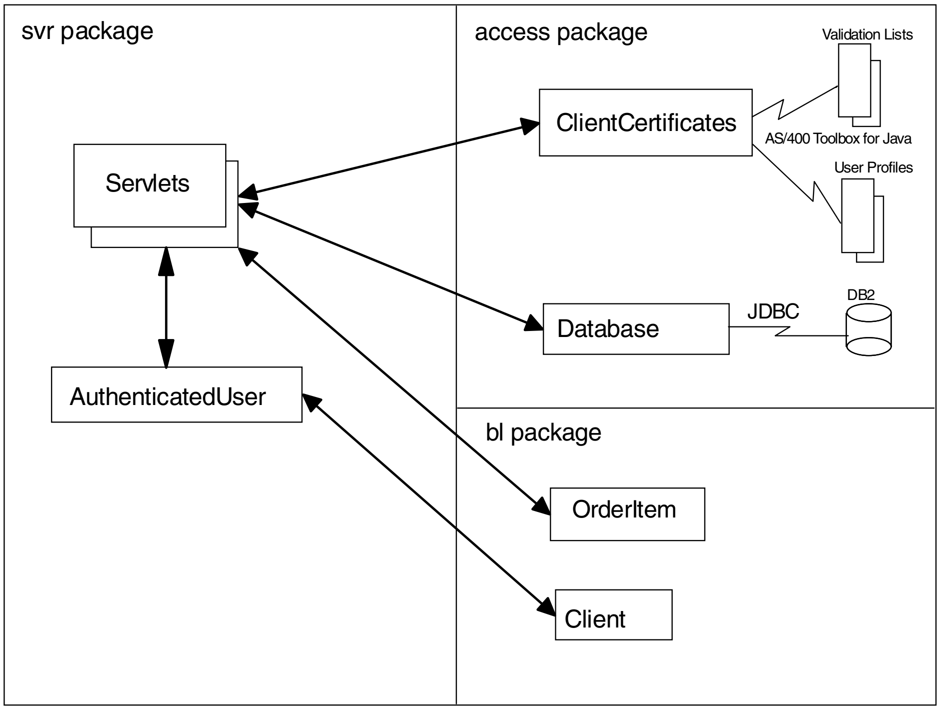


Figure 343. Servlet architecture

The application consists of multiple packages:

- **access package**

  This package is used by all the servlets and the certificate administration application and contains two main classes:

  - ClientCertificates.class

    This class is responsible for managing digital certificates. It is implemented using the AS/400 Toolbox for Java. The class contains several methods to manage certificates, for example getting or adding certificates into or from validation lists or user profiles.

  - Database.class

    This class is responsible for database access. The database access is implemented using JDBC.

  The other classes are used for error handling: ClientCertificatesException, CertificateNotPresentException, and DatabaseException classes.

- **bl package**

  This package contains two classes and represents the business logic:

  - Client.class

    This class represents a user account in the CLTMASP database.

  - OrderItem.class

    This class represents an order item in the ORDDTLP database. It is used by the OrdersServlet.

- **svr package**

This package contains the servlets running in the WebSphere environment and the AuthenticatedUser class used for authentication by the following classes:

- AccountServlet.class

  This servlet is used for the management of customer and supplier accounts: a new user can request a new account as a customer or as a supplier, the user can change its personal data information, or request a change of the certificate (this request is passed to the CertReplaceServlet). The servlet uses the Database and the ClientCertificates classes to access the required information.

- CertReplaceServlet.class

  This servlet is used for processing certificate replacement requests.

- OrdersServlet.class

  This servlet is used to display customer or supplier orders.

- OrderFilesServlet.class

  This servlet is used to display supplier's orders files.

The AuthenticatedUser class represents the data of the authenticated user: It contains the user certificate, the corresponding certificate handle, its role (new user, an existing customer, an existing supplier) and the user account information as a Client object. An AuthenticatedUser object is created every time a request to the servlets is made and performs the entire authentication process.

All the servlets are subclasses of the HttpsServlet class that extends the javax.servlet.http.HttpServlet class, the basic class used for writing servlets. This class contains some general methods used by every servlet.

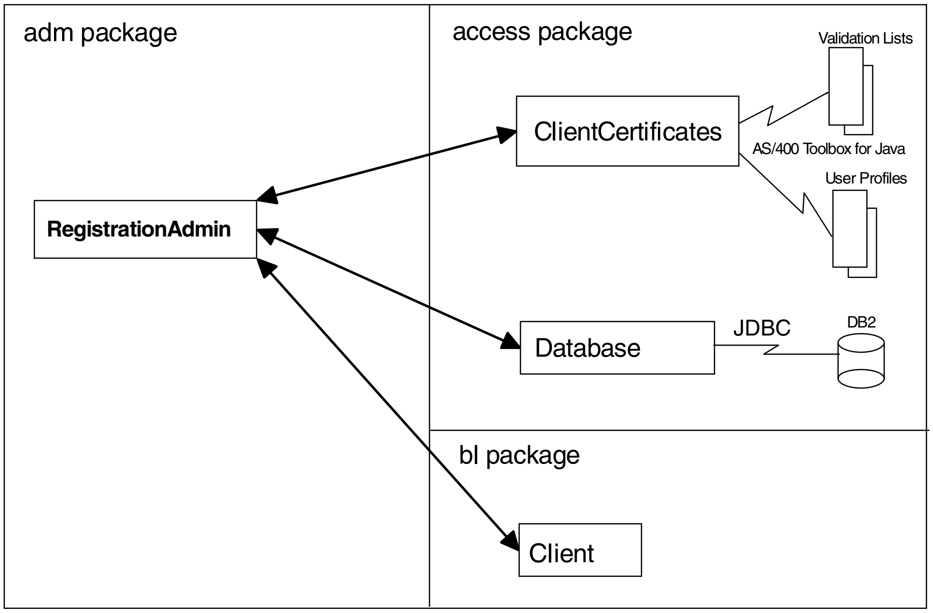


Figure 344. Registration Administration application architecture

- **adm package**

This package contains the RegistrationAdmin class that implements the user interface and the logic of the registration administration application. Note that this application uses the same packages as the servlets.

9.2.1 The access package

The access package contains the following classes.

9.2.1.1 ClientCertificates.class

This class is responsible for managing digital certificates. It uses the AS/400 Toolbox for Java for accessing the validation lists and the user profiles in the AS/400 system:

Table 17. The ClientCertificates methods

Method	Description
addCertificateToUP	The addCertificateToUP method adds a certificate to a user profile. It is used, for example, by the Registration Administration application for registering a certificate for a supplier.
addCertificateToVLDL	The addCertificateToVLDL method adds a certificate to a validation list. It is used, for example, by the AccountServlet for registering a certificate to the PENDING validation list when a user requests a customer registration.
checkForCertificateInVLDL	The checkForCertificateInVLDL method searches for a certificate in a validation list. It is used, for example, by the AuthenticatedUser class during the authentication phase of a servlet process.
getCertificateHandle	The getCertificateHandle method retrieves the AS/400 certificate handle that uniquely identifies this certificate.
getCertificateFromVLDL	The getCertificateFromVLDL method retrieves a certificate from a validation list by giving its handle as parameter.
deleteCertificateFromUP	The deleteCertificateFromUP method deletes a certificate from a user profile.
deleteCertificateFromVLDL	The deleteCertificateFromVLDL method deletes a certificate from a validation list.
getUserProfile	The getUserProfile method retrieves a user profile name of a user profile that has certificates associated by specifying an AS/400 certificate handle.

In order to improve performance, the connection to the AS/400 system is done during the initialization of the servlets. The servlets create a private `cltCert` ClientCertificate object attribute that is maintained during the whole servlet’s life cycle.

9.2.1.2 Database.class

This class is responsible for database access. The database access is implemented using JDBC. It contains several methods to access and maintain the database. Table 18 shows the methods of this class:

Table 18. The Database class methods

Method	Description
createNewAccount	The createNewAccount method is used by the AccountServlet when a user requests a new customer or supplier account. It increases a counter in the COUNTER table and uses this counter as the primary key to create a new record in the CLTMASP table. It sets the CLTSTS field to P for a pending registration request.
changeAccountStatus	The changeAccountStatus method is used by the Registration Administration application for changing the CLTSTS field of an account (CLTMASP table): A for an accepted customer, D for a declined user, U for an accepted supplier.
changeCertificateHandle	The changeCertificateHandle method changes the CLTSTS field of an account. It is used by the CertReplaceServlet when a certificate change request is processed.
updateAccount	The updateAccount method changes the account's information: CLTEMAIL and CLTCRD fields of CLTMASP.
deleteAccount	The deleteAccount method deletes an account from the CLTMASP table. It is used by the Registration Administration application.

getClient(byte[])
getClient(long)
	The getClient methods are used to retrieve a Client object representing an account record of the CLTMASP table. An account can be retrieved by specifying its AS/400 certificate handle (CLTHDL) or its client number (CLTNUM).

getAccounts	The getAccounts method retrieves all accounts with a specified status (CLTSTS) and returns them as an array of Client objects.
getOrders	The getOrders method retrieves all order records of a specific account by specifying its client number and returns them as an array of OrderItem objects.

In order to improve performance, the connection to the database is done when creating the `db` Database object and remains in a private attribute until the `db` Database object is destroyed. Servlets create the `db` Database attribute during their initialization.

9.2.2 The bl package

The bl package contains the following classes.

9.2.2.1 Client.class

This class represents a user account in the CLTMASP table. It contains a private attribute for each field:

Table 19. The Client.class attributes

Attribute	CLTMASP field
number commonName status creditCard email certificateHandle	CLTNUM CLTNAME CLTSTS CLTCRD CLTEMAIL CLTHDL

Each attribute has its own set and get method: setNumber, getNumber, and so on.

9.2.2.2 OrderItem.class

This class represents one record in the ORDDTLP database. It is used by the OrdersServlet for displaying orders. It contains an attribute for each field:

Table 20. The OrderItem.class attributes

Attribute	ORDDTLP field
orderNumber orderLine partNumber description quantity price clientNumber status	DTLORDNUM DTLLINE DTLPRTNUM DTLDESC DTLQTY DTLPRICE DTLCLTNUM DTLSTS

Each attribute has its own set and get method: setOrderNumber, getOrderNumber, and so on.

9.2.3 The svr package

The svr package contains the following classes.

9.2.3.1 HttpsServlet.class

The HttpsServlet class is the superclass of all the servlets. It contains some general methods used by all the servlets. It is used for creating the `db` Database object and the `cltCert` ClientCertificates object during the servlet initialization. Also, it is responsible for keeping these objects in memory during the whole life cycle of the servlets.

Table 21. The HttpsServlet.class attributes

Attribute	Description
db	Database object
cltCert	ClientCertificates object

Attribute	Description
homePagePort	It is the IP port the HTTP server listens to and which is specified in the URL request when accessing the application home page.
as400System	IP address or host name of the AS/400 system.
user	User ID used by the AS/400 Toolbox for Java and JDBC.
password	User ID’s password used by the AS/400 Toolbox for Java and JDBC.
jdbcDriver	JDBC driver used to access the database: com.ibm.db2.jdbc.app.DB2Driver
dbUrl	JDBC URL used to access the database: jdbc:db2://as25/AS9315 where as25 is the AS/400 host name and AS9315 is the library name where the tables are located.
library	Library name where the validation lists are located.

9.2.3.2 AccountServlet.class

The AccountServlet servlet class handles the registration process:

- New account request
- Update account information, such as credit card or e-mail data

9.2.3.3 CertReplaceServlet.class

The CertReplaceServlet servlet class handles the certificate replacement requests. It maintains the private `pendingCertificateReplaceRequest` hashtable attribute that contains all pending requests. The process of a certificate change is a two-step process:

1. The user must first present its current certificate. The servlet generates a random number and sends a cookie back to the user’s browser. This cookie contains the current AS/400 certificate handle and the random number. The contents of the cookie are stored in the pendingCertificateReplaceRequest hashtable .
2. After restarting the browser, the user presents its new certificate to the servlet. The cookie is sent automatically with the request. The servlet compares the cookie with the contents of the cookie stored in the pendingCertificateReplaceRequest hashtable. If the cookie matches, the certificate change process is continued and the cookie is removed from the user’s browser and from the hashtable.

9.2.3.4 OrdersServlet.class

The OrdersServlet class is used for displaying orders for an existing customer or supplier. It creates the user AuthenticatedUser object for every request sent by a client.

9.2.3.5 OrderFilesServlet.class

The OrderFilesServlet class is used for displaying supplier’s order files that are stored in an IFS directory of the AS/400 system. Every request to this servlet, if authorized during the authentication process, is redirected to the URL of the supplier’s home directory. It creates the user AuthenticatedUser object for every request.

9.2.3.6 AuthenticatedUser.class

The AuthenticatedUser class represents the data of the authenticated user. It contains the user certificate, the corresponding certificate handle, its role (new user, an existing customer, an existing supplier) and the user account information. An AuthenticatedUser object is created every time a request to the servlets is made.

Table 22. The AuthenticatedUser.class attributes

Attribute	Description
cert	This is the java.security.cert.X509Certificate object value of the certificate presented by the user. This value can be used to get individual fields of the certificate, such as the subject’s common name, country, and so on.
encodedCert	This is the ASN.1 encoded certificate value of the certificate presented by the user. This value is used by the AS/400 Toolbox for Java classes.
client	This is the Client object of the authenticated user.
certHandle	This is the AS/400 certificate handle value of the certificate presented by the user.
role	This is the account status of the authenticated user: ROLE_NEW_USER ROLE_PENDING_USER ROLE_ACCEPTED_CUSTOMER ROLE_ACCEPTED_SUPPLIER ROLE_DECLINED_USER

Each attribute has its own set and get method: setCert, getCert, and so on. The constructor of this class performs the authentication process. It retrieves the certificate presented by the user, checks for the certificate in the validation lists, and checks for the user’s role in the CLTMASP database.

9.3 Client certificate functions in the sample application

This section describes the various functions used in the application to work with client certificates. It contains code snippets that have the necessary lines of code to explain how the classes and methods are used to perform various tasks with client certificates.

9.3.1 Receiving the client certificate sent by the user’s browser

The client certificate is sent to the HTTP server during the SSL handshake. Usually a CGI program retrieves this certificate from the HTTPS_CLIENT_CERT CGI environment variable. But this CGI environment variable is not accessible through servlets.

The IBM WebSphere environment enables you to retrieve the client certificate sent by the user's browser to the HTTP server by using the getAttribute() method of the javax.servlet.http.HttpServletRequest class. This method called with the javax.net.ssl.peer_certificates attribute name retrieves the chain of X.509 certificates that authenticates the client. The result is an array of java.security.cert.X509Certificate objects. The X509Certificate class contains several methods to retrieve individual fields of the certificate.

Note

The JDK 1.1.8 used for developing the sample application does not contain the java.security.cert package! In order to be able to compile the servlets, you have to copy the x509v1.jar file located in the /QIBM/ProdData/IbmWebAs/lib directory of the AS/400 system to your PC and add it to your CLASSPATH environment variable.

Figure 345 highlights the important statements to receive a client certificate that was sent by the client browser into the Java application.

```
public AuthenticatedUser(HttpServletRequest req, HttpServletResponse res,
        ClientCertificates cltCert, Database db) {

    //get the presented client certificate
    X509Certificate certChain[] = (X509Certificate[])
            req.getAttribute("javax.net.ssl.peer_certificates");
    if (certChain != null) {
        cert = certChain[0];
    } else {
        return;
    }

    //get the encoded certificate
    try {
        encodedCert = cert.getEncoded();
    } catch (CertificateEncodingException cee) {
        role = ROLE_UNKNOWN_USER;
        return;
    }

    //get the client account information if it exists
    try {
        certHandle = cltCert.getCertificateHandle(encodedCert);
        client = db.getClient(certHandle);
    } catch (Exception e) {
        certHandle = null;
        client = null;
    }
...
}
```

Figure 345. Receiving the client certificate sent by the user's browser

The constructor of the AuthenticatedUser class retrieves the certificate sent by the user's browser. The `doGet` and `doPost` of every servlet creates a `user` AuthenticatedUser object every time a request to the servlet is made and performs the entire authentication process.

The first step is the retrieval of the X.509 certificate. The first value of the returned X509Certificate array is the effective certificate of the user. From this value we get the ASN.1 encoded value of the certificate. This value is used by the AS/400 Toolbox for Java to access certificates in validation lists or user profiles.

9.3.2 Adding a certificate to a validation list

The com.ibm.as400.access.AS400CertificateVldlUtil class of the AS/400 Toolbox for Java provides the implementation of the methods for accessing certificates in an AS/400 validation list object.

```
public byte[] addCertificateToVLDL(byte[] cert , String validationList)
        throws ClientCertificatesException {

    byte certHandle[] = null;

    //create the validation list object
    AS400CertificateVldlUtil vldl = new
        AS400CertificateVldlUtil(as400,
        "/QSYS.LIB/" + library + ".LIB/" + validationList);

    try {
        //check if certificate exists in the validation list?
        if (vldl.checkCertificate(cert)) {
            //certificate already exists
        } else {
            //certificate does not exist: we add the certificate to the
            //validation list and get its handle
            vldl.addCertificate(cert);
        }
        certHandle = vldl.getCertificateHandle(cert);
    } catch (Exception e) {
            e.printStackTrace();
            throw new ClientCertificatesException("...");
    }

    //return the certificate handle
    return certHandle;
}
```

Figure 346. The addCertificateToVLDL method of ClientCertificates class

The addCertificateToVLDL method of the ClientCertificates class adds the `cert` ASN.1 encoded certificate to the `validationList` validation list.

The addCertificateToVLDL method:

- Creates the `vldl` AS400CertificateVldlUtil object by specifying the `as400` AS400 object and the fully qualified integrated file system path name of the validation list. The `as400` AS400 object represents an AS/400 sign-on and is created during the initialization of the servlets.

- Checks if the certificate already exists in the specified validation list.
- Adds the certificate to the validation list.
- Returns the AS/400 certificate handle of the certificate.

9.3.3 Deleting a certificate from a validation list

Figure 347 lists the statements that are required to delete a certificate from a validation list.

```
public boolean deleteCertificateFromVLDL(byte[] certHandle,
        String validationList) throws ClientCertificatesException {

    AS400Certificate[] certs;

    try {
        //create the validation list object
        String v = "/QSYS.LIB/" + library + ".LIB/" + validationList;
        AS400CertificateVldlUtil vldl =
               new AS400CertificateVldlUtil(as400, v);

        //delete the certificate
        vldl.deleteCertificateByHandle(certHandle);

    } catch (ExtendedIOException e) {
        //the certificate is not present: do nothing
    } catch (Exception e) {
        e.printStackTrace();
        throw new ClientCertificatesException("...");
    }
    return true;
}
```

Figure 347. The deleteCertificateFromVLDL method of ClientCertificates class

The deleteCertificateFromVLDL method of the ClientCertificates class deletes a certificate from the `validationList` validation list by specifying its AS/400 certificate handle.

The deleteCertificateFromVLDL method:

- Creates the `vldl` AS400CertificateVldlUtil object by specifying the `as400` AS400 object and the fully qualified integrated file system path name of the validation list.
- Deletes the certificate from the validation list by specifying its AS/400 certificate handle.

9.3.4 Check for a certificate in a validation list

Figure 348 shows the Java code to check if a certificate is in a validation list.

```
public byte[] checkForCertificateInVLDL(byte[] cert, String validationList)
        throws CertificateNotPresentException, ClientCertificatesException
{
    byte certHandle[] = null;

    //create the validation list object
    String v = "/QSYS.LIB/" + library + ".LIB/" + validationList;
    AS400CertificateVldlUtil vldl =
            new AS400CertificateVldlUtil(as400, v);

    //check if certificate exists in the validation list?
    boolean certificatePresent = false;
    try {
        certificatePresent = vldl.checkCertificate(cert);
    } catch (Exception e) {
        throw new ClientCertificatesException("...");
    }
    if (certificatePresent) {
        try {
            certHandle = vldl.getCertificateHandle(cert);
        } catch (Exception e) {
            e.printStackTrace();
            throw new ClientCertificatesException("...");
        }
    } else {
        throw new CertificateNotPresentException();
    }

    //return the certificate handle
    return certHandle;
}
```

Figure 348. The checkForCertificateInVLDL method of ClientCertificates class

The checkForCertificateInVLDL method of the ClientCertificates class checks if a client certificate is in the `validationList` validation list by specifying its AS/400 certificate handle.

The checkForCertificateInVLDL method:

- Creates the `vldl` AS400CertificateVldlUtil object by specifying the `as400` AS400 object and the fully qualified integrated file system path name of the validation list.
- Checks if the certificate is in the validation list by specifying its ASN.1 encoded value.
- Throws a `CertificateNotPresentException` if the certificate does not exist in the validation list.
- Returns the AS/400 certificate handle of the found certificate.

9.3.5 Getting a certificate from a validation list

To get a certificate from a validation list by specifying an AS/400 certificate handle, you have to browse the whole validation list and check for the matching AS/400 certificate handle.

Figure 349 shows the Java code to get a certificate from a validation list.

```
public byte[] getCertificateFromVLDL(byte[] certHandle,
        String validationList) {

    AS400Certificate[] certs;
    try {
        //create the validation list object
        String v = "/QSYS.LIB/" + library + ".LIB/" + validationList;
        AS400CertificateVldlUtil vldl =
                new AS400CertificateVldlUtil(as400, v);

        String usrspc =
            "/QSYS.LIB/" + library + ".LIB/CERTSPC.USRSPC");
        vldl.listCertificates(null,usrspc);

        // Start reading certificates from the user space into
        // AS400Certificate[].All complete certificates in the 8 Kbyte
        // buffer will be returned.
        certs = vldl.getCertificates(usrspc, 0, 8);

        // Continue to read the entire user space using 8 Kbyte buffer until
        // certificate match
        boolean matchingCertificate = false;
        while (null != certs) {
            // searching for the certificate
            for (int i = 0; i < certs.length; ++i) {
                byte[] tmpHandle =
                vldl.getCertificateHandle(certs[i].getEncoded());
                if (compareByteArray(tmpHandle, certHandle)) {
                    return certs[i].getEncoded();
                }
            }
            certs = vldl.getNextCertificates(8);
        }
    } catch (Exception e) {
    }
    return null;
}
```

Figure 349. The getCertificateFromVLDL method of ClientCertificates class

The getCertificateFromVLDL method of the ClientCertificates class returns a certificate from the `validationList` validation list by specifying its AS/400 certificate handle.

The getCertificateFromVLDL method:

- Creates the `vldl` AS400CertificateVldlUtil object by specifying the `as400` AS400 object and the fully qualified integrated file system path name of the validation list.
- Retrieves all the ASN.1 encoded certificates from the validation list and put them in the user space CERTSPC. The first parameter is the list of attributes the certificate should match. A value of `null` places all certificates from the validation list into the user space. The second parameter is the fully qualified integrated file system path name of the user space to put the list results.
- Gets the com.ibm.as400.access.AS400Certificate certificates from the user space using an 8 KB buffer and searches for a matching AS/400 certificate handle.
- Returns the ASN.1 encoded certificate found or a null value if the certificate could not be found.

9.3.6 Associating a certificate with a user profile

The Java code in Figure 350 is used to associate a client certificate with a user profile.

```
public byte[] addCertificateToUP(byte[] cert, String userProfileName)
        throws ClientCertificatesException {

    byte certHandle[] = null;

    AS400CertificateUserProfileUtil up = new
        AS400CertificateUserProfileUtil(as400,
            "/QSYS.LIB/" + userProfileName + ".USRPRF");

    try {
        certHandle = up.getCertificateHandle(cert);
        up.addCertificate(cert);
    } catch (ExtendedIOException eioe) {
        //the certificate already exists
    } catch (Exception e) {
        e.printStackTrace();
        throw new ClientCertificatesException("...");
    }

    //return the certificate handle
    return certHandle;
}
```

Figure 350. The addCertificateToUP method of ClientCertificates class

The addCertificateToUP method of the ClientCertificates class adds a certificate to a user profile by specifying its ASN.1 encoded certificate value and the user profile name.

The addCertificateToUP method:

- Creates the `up` AS400CertificateUserProfileUtil object by specifying the `as400` AS400 object and the fully qualified integrated file system path name of user profile.

- Retrieves the AS/400 certificate handle returned by the method.
- Adds the certificate to the user profile.
- Returns the AS/400 certificate handle of the added certificate.

9.3.7 Deleting a certificate from a user profile

Figure 351 lists the Java statements that are required to delete a client certificate from a user profile.

```
public boolean deleteCertificateFromUP(byte[] certHandle,
       String userProfileName) throws ClientCertificatesException {

    //create the AS400CertificateUserProfileUtil object
    AS400CertificateUserProfileUtil up = new
        AS400CertificateUserProfileUtil(as400,
            "/QSYS.LIB/" + userProfileName + ".USRPRF");

    try {
        up.deleteCertificateByHandle(certHandle);
    } catch (ExtendedIOException eioe) {
        //no certificate present
    } catch (Exception e) {
        e.printStackTrace();
        throw new ClientCertificatesException("...");
    }
    return true;
}
```

Figure 351. The deleteCertificateFromUP method of ClientCertificates class

The deleteCertificateFromUP method of the ClientCertificates class deletes a certificate from a user profile by specifying its AS/400 certificate handle and the user profile name.

The deleteCertificateFromUP method:

- Creates the `up` AS400CertificateUserProfileUtil object by specifying the `as400` AS400 object and the fully qualified integrated file system path name of user profile.
- Deletes the certificate by specifying its AS/400 certificate handle, if it is present in the user profile. If the certificate is not present the `deleteCertificateByHandle` method throws an `ExtendedIOException` exception. This exception is not handled.

9.3.8 Finding a user profile a certificate is associated with

Figure 352 shows the Java code that finds a user profile that a client certificate is associated with.

```
public String getUserProfile(byte[] certHandle)
        throws ClientCertificatesException {

    //create the AS400CertificateUserProfileUtil object
    AS400CertificateUserProfileUtil up = new
        AS400CertificateUserProfileUtil(as400,
            "/QSYS.LIB/QUSER.USRPRF");

    String userProfileName = null;
    try {
        userProfileName =
            up.findCertificateUserByHandle(certHandle);
    } catch (ExtendedIOException eioe) {
        //the certificate does not exist
        return ("");
    } catch (Exception e) {
        e.printStackTrace();
        throw new ClientCertificatesException("...");
    }
    return userProfileName;
}
```

Figure 352. The getUserProfile method of ClientCertificates class

The getUserProfile method of the ClientCertificates class retrieves the user profile name that a client certificate is associated with by specifying the client certificate AS/400 certificate handle.

The getUserProfile method:

- Creates the `up` AS400CertificateUserProfileUtil object by specifying the `as400` AS400 object and the fully qualified integrated file system path name of a valid user profile.

Note

When creating the `up` AS400CertificateUserProfileUtil object, we must specify a valid user profile although we do not access the user profile, because if we do not specify one, the `findCertificateUserByHandle` method throws an exception.

- Searches for a user profile name that contains the certificate by specifying its AS/400 certificate handle.
- Returns a blank string if the certificate is not found in any of the existing user profiles. In this case the `findCertificateUserByHandle` method throws an `ExtendedIOException` exception.
- Returns the name of the user profile the certificate is associated with.

9.3.9 Getting the AS/400 certificate handle

Figure 353 lists the Java statements that are required to get an AS/400 certificate handle.

```
public byte[] getCertificateHandle(byte[] cert)
        throws ClientCertificatesException {

    byte certHandle[] = null;

    //create a validation list object
    AS400CertificateVldlUtil vldl = new
        AS400CertificateVldlUtil(as400,
            "/QSYS.LIB/" + library + ".LIB/" + VLDL_PENDING);

    try {
        certHandle = vldl.getCertificateHandle(cert);
    } catch (Exception e) {
        e.printStackTrace();
        throw new ClientCertificatesException("...");
    }

    //return the certificate handle
    return certHandle;
}
```

Figure 353. The getCertificateHandle method of ClientCertificates class

The getCertificateHandle method of the ClientCertificates class retrieves the AS/400 certificate handle of a specified certificate.

The getCertificateHandle method:

- Creates the `vldl` AS400CertificateVldlUtil object by specifying the `as400` AS400 object and the fully qualified integrated file system path name of a valid validation list.

Note

The getCertificateHandle method of the AS400CertificateVldlUtil class always returns the AS/400 certificate handle of the specified certificate. The certificate need not be present in the validation list. Therefore you can specify any valid validation list.

- Retrieves the AS/400 certificate handle by specifying its ASN.1 encoded certificate value.
- Returns the AS/400 certificate handle.

9.3.10 Authentication process used by the servlets

The entire authentication process is based on the AuthenticatedUser class. The `doGet` and `doPost` of every servlet creates a `user` AuthenticatedUser object every time a request to the servlet is made

The AuthenticatedUser class represents the data of the authenticated user. It contains the user certificate, the corresponding certificate handle, its role (new user, an existing customer, an existing supplier) and the user account information.

The constructor of the AuthenticatedUser class retrieves the certificate sent by the user’s browser and then searches for its account status.

```
public AuthenticatedUser(HttpServletRequest req, HttpServletResponse res,
ClientCertificates cltCert, Database db) {

    //get the presented client certificate
    refer to 9.3.1, “Receiving the client certificate sent by the user’s
browser” on page 361
    //get the encoded certificate
        refer to 9.3.1, “Receiving the client certificate sent by the user’s
browser” on page 361

    //get the client account information if it exists
    try {
        certHandle = cltCert.getCertificateHandle(encodedCert);
        client = db.getClient(certHandle);
    } catch (Exception e) {
        certHandle = null;
        client = null;
    }

    try {
        //a PENDING USER:
        certHandle = cltCert.checkForCertificateInVLDL(encodedCert,
                ClientCertificates.VLDL_PENDING);
        role = ROLE_PENDING_USER;
        return;
    } catch (CertificateNotPresentException certNotInPendingException)
{
        try {
            //an EXISTING USER: CUSTOMER or SUPPLIER
            certHandle =
                    cltCert.checkForCertificateInVLDL(encodedCert,
                        ClientCertificates.VLDL_ACCEPTED);
            if (client.getStatus().equals("U"))
                role = ROLE_ACCEPTED_SUPPLIER;
            else
                if (client.getStatus().equals("A"))
                    role = ROLE_ACCEPTED_CUSTOMER;
                else
                    role = ROLE_UNKNOWN_USER;
            return;
        } catch (CertificateNotPresentException certNotInAcceptedException)
        {
```

Figure 354. The constructor of the AuthenticatedUser class (part 1)

```
            //a NEW USER or a DECLINED USER:
            if (client == null) {
                //a NEW USER
                role = ROLE_NEW_USER;
                return;
            } else {
                //a DECLINED USER
                if (client.getStatus().equals("D")) {
                    role = ROLE_DECLINED_USER;
                    return;
                } else {
                    role = ROLE_UNKNOWN_USER;
                    return;
                }
            }
        } catch (ClientCertificatesException
                    acceptedValidationListException) {
            role = ROLE_UNKNOWN_USER;
            return;
        }
    } catch (ClientCertificatesException pendingValidationListException) {
        role = ROLE_UNKNOWN_USER;
        return;
    }
}
```

Figure 355. The constructor of the AuthenticatedUser class (part 2)

The constructor of the AuthenticatedUser class:

- Gets the client certificate presented by the browser (refer to 9.3.1, “Receiving the client certificate sent by the user’s browser” on page 361) and stores it in the `cert` private attribute. This `cert` attribute can be accessed by using the getCert method of this class.
- Gets the ASN.1 encoded certificate of the client certificate (refer to 9.3.1, “Receiving the client certificate sent by the user’s browser” on page 361) and stores it in the `encodedCert` private attribute. This `encodedCert` attribute can be accessed by the getEncodedCert method of this class.
- Gets the AS/400 certificate handle of the client certificate by using the getCertificateHandle method of the ClientCertificate class (refer to 9.3.9, “Getting the AS/400 certificate handle” on page 369) and stores it in the `certHandle` private attribute. The `certHandle` attribute can be accessed by the getCertHandle method of the AuthenticatedUser class.
- Retrieves the account record of the CLTMASP table associated with the presented certificate and stores it in the `client` attribute by using the getClient method of the Database class. The `client` attribute can be accessed by the getClient method of the AuthenticatedUser class.
- Checks if the user is a pending user by checking the PENDING validation list (refer to 9.3.4, “Check for a certificate in a validation list” on page 364). If yes, it sets the `role` attribute to the ROLE_PENDING_USER constant. The `role` attribute can be accessed by using the getRole method of the AuthenticatedUser class.

- If the user is not a pending user the `checkForCertificateInVLDL` method throws a CertificateNotPresentException. In this case the AuthenticatedUser class checks if the user is an accepted user by checking the ACCEPTED validation list. If yes, it sets the `role` attribute to the ROLE_ACCEPTED_SUPPLIER or ROLE_ACCEPTED_CUSTOMER constant by checking for the status of the `client` object.
- If the user is not an accepted user the `checkForCertificateInVLDL` method throws a CertificateNotPresentException. In this case AuthenticatedUser class sets the `role` attribute to the ROLE_NEW_USER if the `client` object is null (no account record available in the CLIMASP table for the user) or to the ROLE_DECLINED_USER constant by checking for the status of the `client` object.

9.4 The Administration Utility

The Java sample application also provides an administration utility. This utility runs, for example, on a PC. It is used to approve or decline user registration requests. It is also used to approve and register a supplier. When a supplier is registered, the utility prompts the administrator for a user profile name for the supplier. It then creates this user profile and an IFS directory for this particular supplier. The directory can only be accessed through the appropriate supplier.

This section shows you how to start the administration utility on a PC. The PC had the following software installed:

- Windows NT 4 plus Service Pack 4
- Java JDK 1.1.8
- Client Access Express
- Sample application administration utility classes (in directory D:\Projects\AS-9315)

It is assumed that you are familiar with the installation and operation of Windows NT, JDK 1.1.8 and Client Access Express.

The classpath used on the PC is as follows:

```
CLASSPATH=.;d:\Programs\IBM\Client
Access\jt400\lib\jt400.zip;d:\jdk1.1.8\lib\classes.zip;d:\jdk1.1.8\classes;d:\
jdk1.1.8\bin;d:\programs\ibm\client
access\jt400\lib\sslightx.zip;d:\programs\ibm\Client
Access\jt400\lib\SSLTools.zip;d:\projects\as-9315\adm\x509v1.jar
```

The directory structure of the administration utility is as follows:

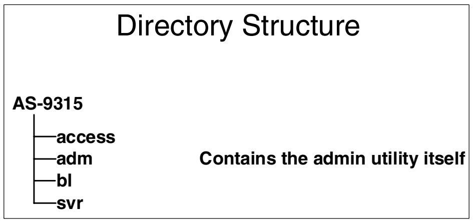
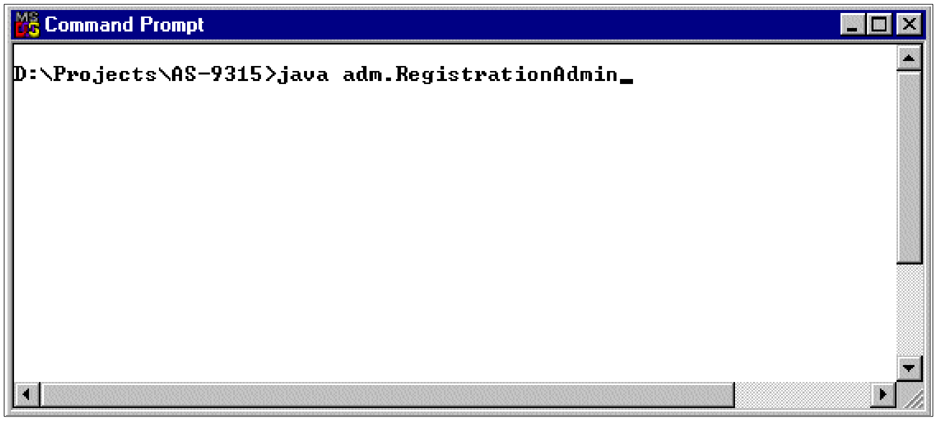


Figure 356. Administration utility directory structure

The following steps take you through the administration utility:

1. Start the administration utility through the following command:

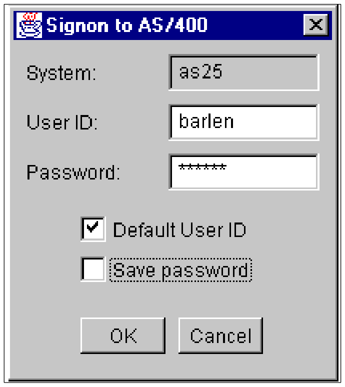
   ```
   java adm.RegistrationAdmin
   ```



```
D:\Projects\AS-9315>java adm.RegistrationAdmin_
```

Figure 357. Starting the administration utility

The user ID / password prompt is shown after the Java initialization.



System: as25

User ID: barlen

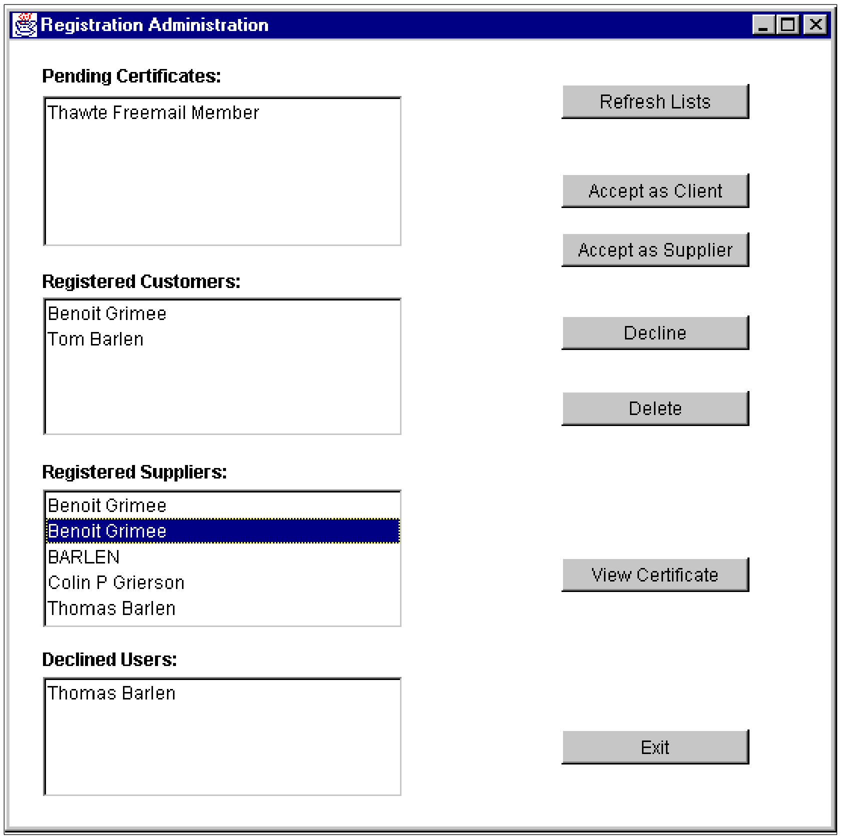
Password: ******

☑ Default User ID

□ Save password

Figure 358. User ID/Password prompt

2. Enter an AS/400 user profile and password that has *ALLOBJ and *SECADM authorities. These authorities are needed to create the user profiles, associate a client certificate with a user profile and access the validation lists.
3. Click **OK**. The administration utility interface is shown.



Pending Certificates:

Thawte Freemail Member

Registered Customers:

Benoit Grimee
Tom Barlen

Registered Suppliers:

Benoit Grimee
Benoit Grimee
BARLEN
Colin P Grierson
Thomas Barlen

Declined Users:

Thomas Barlen

Figure 359. Administration utility interface

The interface provides the following list windows:

Pending Certificates This window lists the common names of client certificates for which a registration request has been issued but not processed yet. It contains registration requests for customers and supplier.

Registered Customers The window lists the common names of client certificates that are registered as customers. Click **Accept as Client** was pressed to register a client as a customer.

Registered Suppliers The entries shown in this window represents the registered supplier. Click **Accept as Supplier** was pressed to register a client as a supplier.

Declined Users This window contains the common names of client certificates for which a registration request was declined. Click **Decline** was pressed to decline a request.

The utility provides the following functions through buttons:

Refresh List The interface does not refresh automatically. For example, when a new customer registers, the administrator has to click this button to see the new certificate in the Pending Certificates list.

Accept as Client This button is used to register a client from the Pending Certificates window as a customer. The desired certificate must first be selected.

Accept as Supplier This button is used to register a certificate from the Pending Certificates list as a supplier. After the certificate is selected and this button clicked, the administrator is prompted for a user profile name for the new supplier. The utility automatically creates the user profile and a supplier directory. It also grants the permissions for the new directory.

Decline Since the sample application's purpose is to show the principles and examples for working with client certificates, it does not provides all functions. For example, the decline function works only for pending certificates and registered customers. It does not work for registered suppliers.

Delete The Delete function deletes certificates from the Pending Certificates, Registered Customers and Declined Certificates lists. It does not delete registered suppliers.

View Certificate This option displays the client certificate attributes for pending certificates and registered customers only.

Exit Ends the administration utility.

Appendix A. Cryptographic product regulations

Due to regulations imposed by the United States and other governments, the cryptographic algorithms available and associated key lengths permissible vary by country. To avoid shipping separate versions of each product that uses cryptography, AS/400 employs a unique mechanism for controlling access to cryptographic functions.

A list of permitted algorithms and associated maximum key lengths is maintained for each cryptographic service provider. This SSL protocol engine queries the cryptographic service provider installed on the AS/400, to ensure only permitted algorithms are used and that maximum key lengths are not exceeded. IBM provides a collection of no-charge Cryptographic Access Provider products that specify the list of permitted algorithms and key lengths for the cryptographic service providers. The products are:

5769-AC1 Supports symmetric key algorithms with key lengths no greater than 40 bits. Available only in France.

5769-AC2 Supports DES and other symmetric key algorithms such as RC2 and RC4 with key lengths up to 56 bits. Available in most countries in which IBM does business with the exception of France, the United States and Canada. (Note: Recent changes in the encryption policy in France may allow this product to be available there in the future.)

5769-AC3 Supports DES and other symmetric key algorithms such as RC2 and RC4 with key lengths up to 128 bits. Available in the United States and Canada without restriction. With specific export approval by the U.S. government, it is also available to certain types of companies, such as financial institutions, in other countries.

The AS/400 cryptographic controls provide a number of unique advantages:

- Only one version of each SSL-enabled application needs to be shipped, which reduces software distribution and management complexity for multinational corporations.
- As government regulations change, either new Cryptographic Access Provider products will be created or the existing products will be modified. When these new or changed products are installed, the cryptographic capabilities of all applications on the AS/400 system are immediately effected.
- AS/400 applications written by customers and business partners that use SSL will automatically use these controls, which makes compliance with government regulations easier.

The SSL implementation for AS/400 is enabled for Global Server ID support. The Global Server ID support allows, with the proper government approvals, financial and other qualified companies residing outside the United States to use 128-bit symmetric keys for cryptographic operations. The company must obtain the proper United States Export Office approvals, install the 5769-AC3 product, and obtain a special certificate from VeriSign in order to use this support. Browsers from outside the United States will negotiate a 128-bit key instead of the typical 40- or 56-bit key when connecting to a server using this special certificate.

Appendix B. Enabling SSL for the *ADMIN HTTP server instance

Through the AS/400 Tasks page, you can configure, for example the HTTP Server for AS/400, the Digital Certificate Manager, and so on. The configuration of these applications requires that also sensitive and confidential data is sent between the administrator’s Web browser and the AS/400 system. To securely transmit this data, you have to enable SSL for the *ADMIN server instance of the HTTP Server for AS/400.

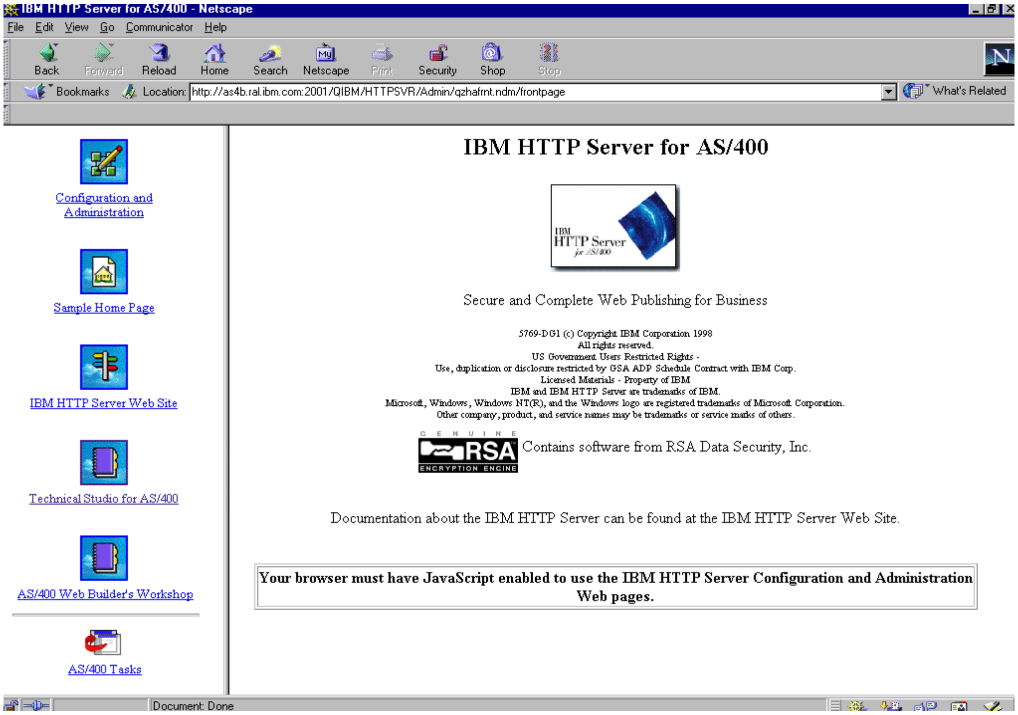
The tasks to enable SSL for the *ADMIN HTTP server instance are:

- Changing the *ADMIN HTTP configuration.
- Assign a server certificate to the *ADMIN server.
- Restarting the server to activate the configuration changes.

B.1 Changing the *ADMIN server configuration

The following steps show how to enable SSL for the *ADMIN server:

1. Start a Web browser and go to the AS/400 Tasks page using the URL `http://your.system.domain:2001`.
2. Select **IBM HTTP Server for AS/400** from the AS/400 Tasks page. The main page of the IBM HTTP Server for AS/400 is displayed.


IBM HTTP Server for AS/400 - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location:
What's Related
Configuration and Administration
Sample Home Page
IBM HTTP Server Web Site
Technical Studio for AS/400
AS/400 Web Builder's Workshop
AS/400 Tasks
IBM HTTP Server for AS/400
GENUINE RSA ENCRYPTION ENGINE
Document: Done

Location: http://as4b.ral.ibm.com:2001/QIBM/HTTPSVR/Admin/qzhafrnt.ndm/frontpage

IBM HTTP Server for AS/400

Secure and Complete Web Publishing for Business

5769-DG1 (c) Copyright IBM Corporation 1998
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM
IBM and IBM HTTP Server are trademarks of IBM.
Microsoft, Windows, Windows NT(R), and the Windows logo are registered trademarks of Microsoft Corporation.
Other company, product, and service names may be trademarks or service marks of others.

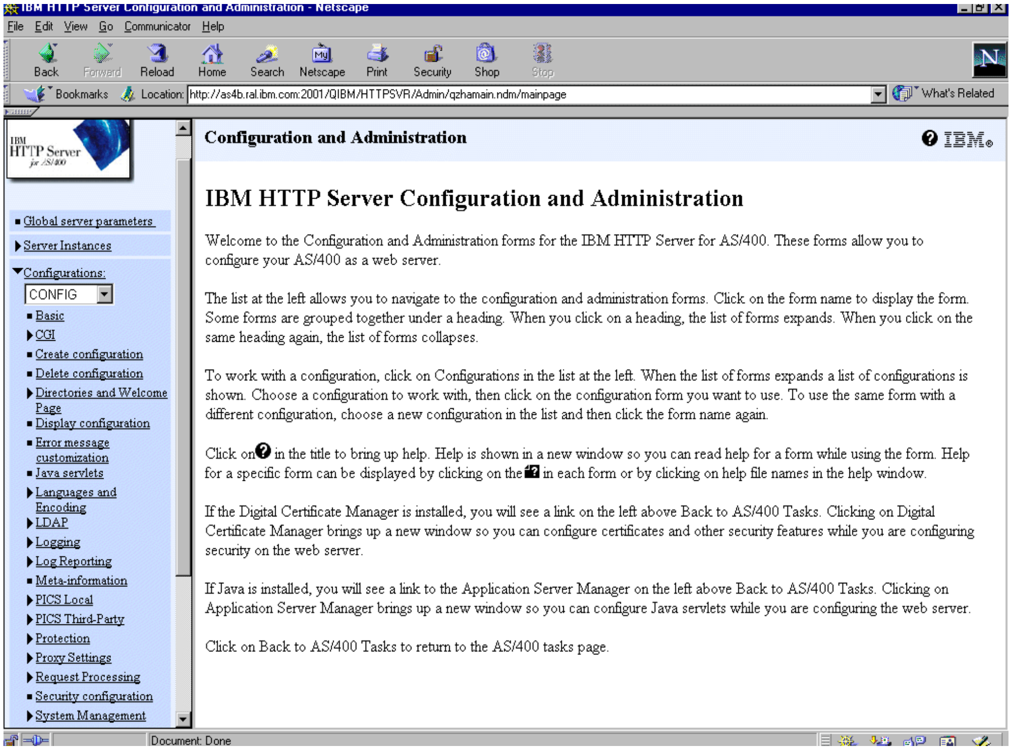
Contains software from RSA Data Security, Inc.

Documentation about the IBM HTTP Server can be found at the IBM HTTP Server Web Site.

Your browser must have JavaScript enabled to use the IBM HTTP Server Configuration and Administration Web pages.

Figure 360. IBM HTTP Server for AS/400 main page

3. Click **Configuration and Administration** on the left pane of the window to open the HTTP server configuration and administration tasks.
4. Expand the configurations options by clicking **Configurations**.



Configuration and Administration

IBM HTTP Server Configuration and Administration

Welcome to the Configuration and Administration forms for the IBM HTTP Server for AS/400. These forms allow you to configure your AS/400 as a web server.

The list at the left allows you to navigate to the configuration and administration forms. Click on the form name to display the form. Some forms are grouped together under a heading. When you click on a heading, the list of forms expands. When you click on the same heading again, the list of forms collapses.

To work with a configuration, click on Configurations in the list at the left. When the list of forms expands a list of configurations is shown. Choose a configuration to work with, then click on the configuration form you want to use. To use the same form with a different configuration, choose a new configuration in the list and then click the form name again.

Click on ❓ in the title to bring up help. Help is shown in a new window so you can read help for a form while using the form. Help for a specific form can be displayed by clicking on the ❓ in each form or by clicking on help file names in the help window.

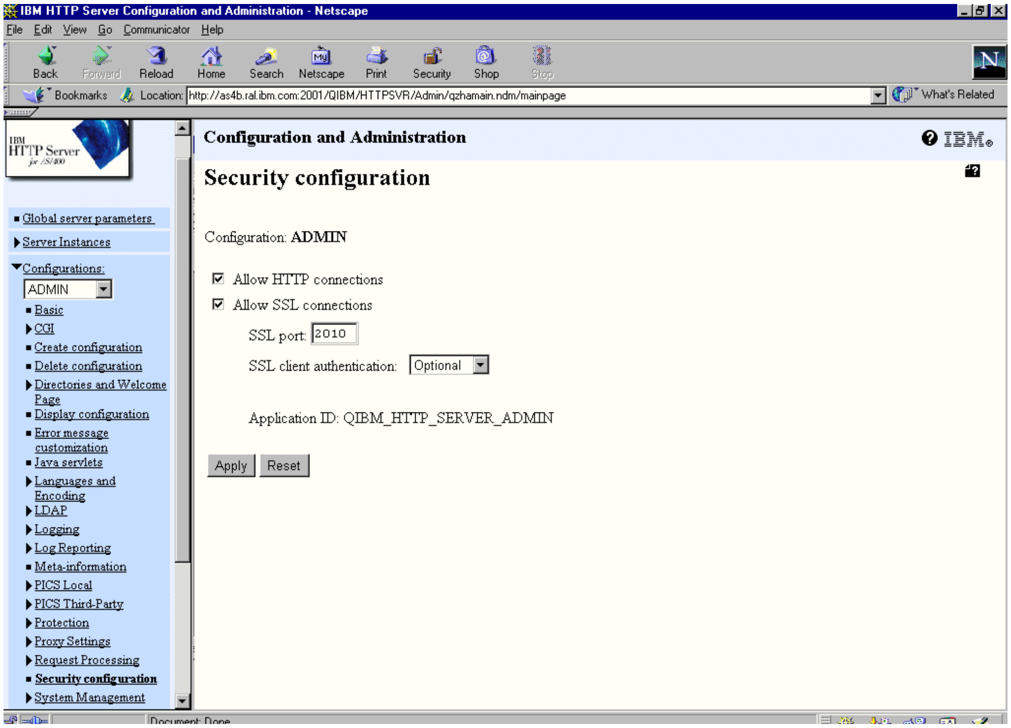
If the Digital Certificate Manager is installed, you will see a link on the left above Back to AS/400 Tasks. Clicking on Digital Certificate Manager brings up a new window so you can configure certificates and other security features while you are configuring security on the web server.

If Java is installed, you will see a link to the Application Server Manager on the left above Back to AS/400 Tasks. Clicking on Application Server Manager brings up a new window so you can configure Java servlets while you are configuring the web server.

Click on Back to AS/400 Tasks to return to the AS/400 tasks page.

Figure 361. HTTP Server for AS/400 - Configurations

5. To configure the *ADMIN server instance, select **ADMIN** from the drop-down list under Configurations. Then click **Security configuration** to display the security settings.



Configuration and Administration

Security configuration

Configuration: ADMIN

☑ Allow HTTP connections

☑ Allow SSL connections

SSL port: 2010

SSL client authentication: Optional

Application ID: QIBM_HTTP_SERVER_ADMIN

Apply Reset

Figure 362. Security configuration page

6. Fill in the Security configuration as follows:

   a. Be sure the **Allow HTTP connections** box is checked. This allows your server to handle non-secure HTTP connections.

   b. Click the **Allow SSL connections** check box. This allows your *ADMIN server to establish SSL connections with the client.

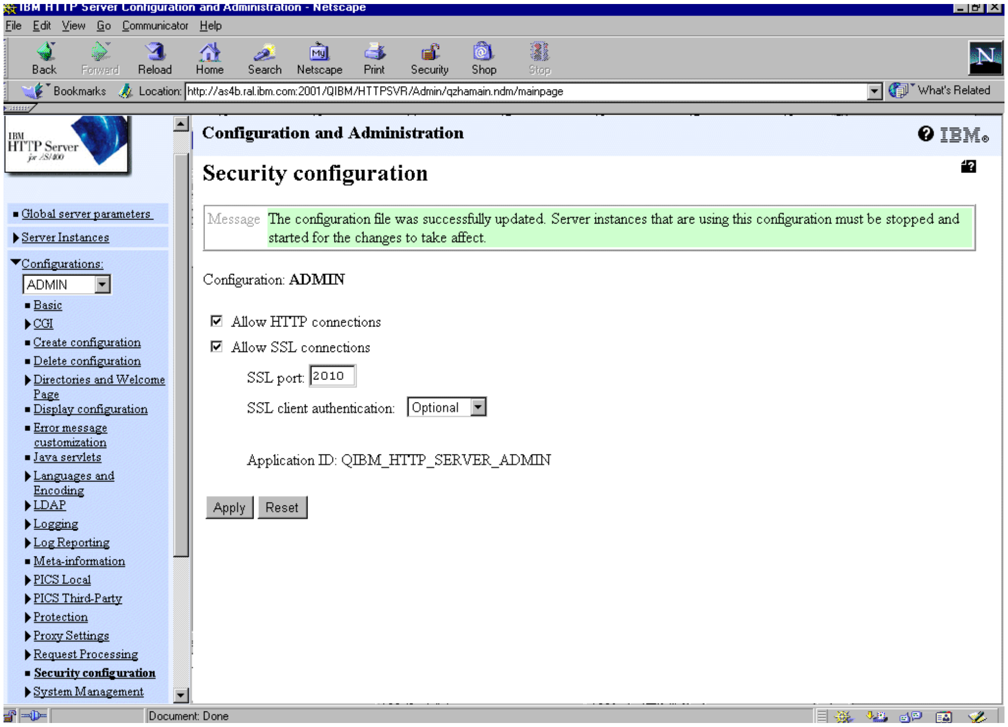
   c. Enter the port number 2010 into the SSL port parameter.

      In general, port number 443 is used as the well-known port for the SSL protocol. Since one port can only be assigned to one server instance at a given time, it is advisable to not use the well-known SSL port for the *ADMIN server. The commonly used SSL port for the *ADMIN server instance is 2010.

   d. Select **Optional** for the SSL client authentication.

> **Note**
>
> It would be sufficient to keep the parameter to its default None to use SSL protection for the *ADMIN server. But in order to register existing user certificates with AS/400 user profiles, the parameter has to be set to Optional.

7. Click **Apply**.



Configuration and Administration

Security configuration

Message The configuration file was successfully updated. Server instances that are using this configuration must be stopped and started for the changes to take affect.

Configuration: ADMIN

☑ Allow HTTP connections

☑ Allow SSL connections

SSL port: 2010

SSL client authentication: Optional

Application ID: QIBM_HTTP_SERVER_ADMIN

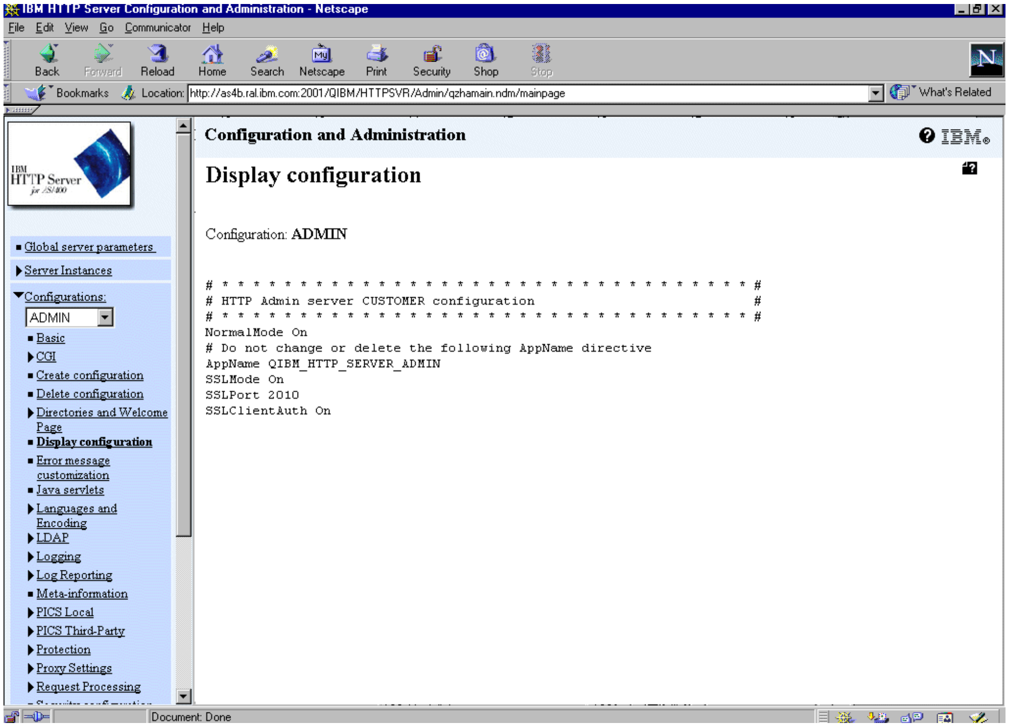
Apply Reset

Figure 363. Security configuration completion message

When you click **Apply** the ADMIN configuration is updated with the changes you made on these pages. An Application ID has been assigned to this configuration. This Application ID is used within DCM to assign a certificate to the *ADMIN server application.

The assigned application ID QIBM_HTTP_SERVER_ADMIN is displayed on the Security configuration page.

8. To verify the changes you made to the ADMIN server configuration, click **Display configuration.**


IBM HTTP Server Configuration and Administration - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://as4b.ral.ibm.com:2001/QIBM/HTTPSVR/Admin/qzhamain.ndm/mainpage
What's Related
IBM HTTP Server for AS/400
Global server parameters
Server Instances
Configurations:
ADMIN
Basic
CGI
Create configuration
Delete configuration
Directories and Welcome Page
Display configuration
Error message customization
Java servlets
Languages and Encoding
LDAP
Logging
Log Reporting
Meta-information
PICS Local
PICS Third-Party
Protection
Proxy Settings
Request Processing
Configuration and Administration
IBM
Document: Done

Display configuration

Configuration: ADMIN

```
# * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * #
# HTTP Admin server CUSTOMER configuration                             #
# * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * #
NormalMode On
# Do not change or delete the following AppName directive
AppName QIBM_HTTP_SERVER_ADMIN
SSLMode On
SSLPort 2010
SSLClientAuth On
```

Figure 364. Display configuration

Review the following directives in the configuration:

a. AppName: `QIBM_HTTP_SERVER_ADMIN`

b. SSL mode is enabled: `SSLMode On`

c. Port used for SSL: `SSLPort 2010`

d. Client authentication mode: `SSLClientAuth On` (corresponds to Optional)

This complete the steps to prepare the *ADMIN server instance to use SSL. The following steps are required to assign a server certificate to the *ADMIN HTTP server application.

> **Important**
>
> Do not restart the *ADMIN server yet. The server certificate must be assigned first; otherwise, the server will fail during restart.

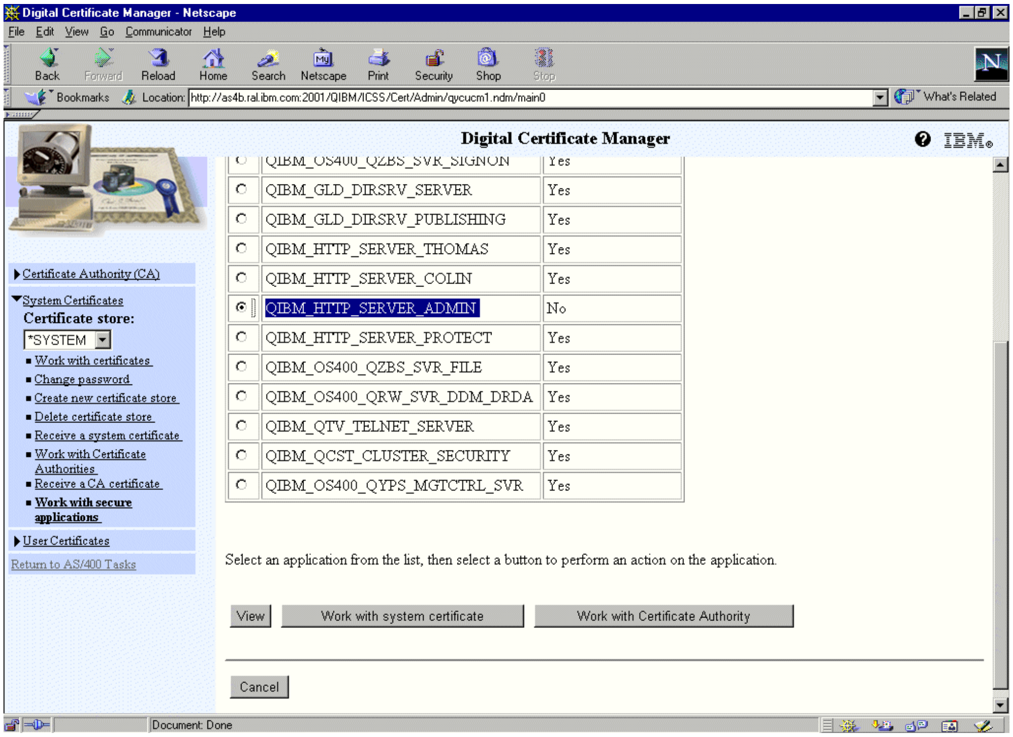
B.2 Assigning a server certificate to the *ADMIN server

Every SSL-enabled server application needs to have a digital server certificate assigned to it. To assign a server certificate to the *ADMIN HTTP server, perform the following steps:

1. From the AS/400 Tasks page click **Digital Certificate Manager**.

2. Expand the **System Certificates** and click **Work with secure applications**.

3. Select the *ADMIN server application ID QIBM_HTTP_SERVER_ADMIN. Note that there is currently no certificate assigned.



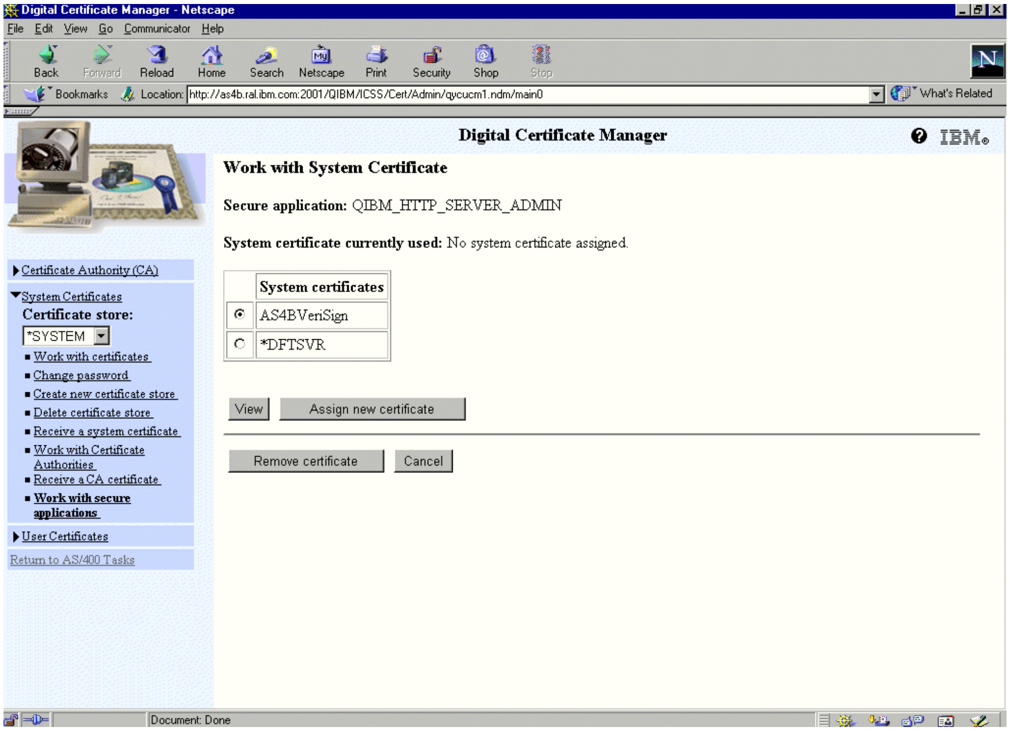
Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://as4b.ral.ibm.com:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Digital Certificate Manager
IBM.
Certificate Authority (CA)
System Certificates
Certificate store:
*SYSTEM
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Work with system certificate
Work with Certificate Authority
Cancel
Document: Done

○	QIBM_OS400_QZBS_SVR_SIGNON	Yes
○	QIBM_GLD_DIRSRV_SERVER	Yes
○	QIBM_GLD_DIRSRV_PUBLISHING	Yes
○	QIBM_HTTP_SERVER_THOMAS	Yes
○	QIBM_HTTP_SERVER_COLIN	Yes
●	QIBM_HTTP_SERVER_ADMIN	No
○	QIBM_HTTP_SERVER_PROTECT	Yes
○	QIBM_OS400_QZBS_SVR_FILE	Yes
○	QIBM_OS400_QRW_SVR_DDM_DRDA	Yes
○	QIBM_QTV_TELNET_SERVER	Yes
○	QIBM_QCST_CLUSTER_SECURITY	Yes
○	QIBM_OS400_QYPS_MGTCTRL_SVR	Yes

Select an application from the list, then select a button to perform an action on the application.

Figure 365. DCM - Assigning a server certificate - Application IDs

4. Click **Work with system certificate**. Select the server certificate you want to assign to the *ADMIN server.


Digital Certificate Manager - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://as4b.ral.ibm.com:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
What's Related
Certificate Authority (CA)
System Certificates
Work with certificates
Change password
Create new certificate store
Delete certificate store
Receive a system certificate
Work with Certificate Authorities
Receive a CA certificate
Work with secure applications
User Certificates
Return to AS/400 Tasks
View
Assign new certificate
Remove certificate
Cancel
Document: Done

Digital Certificate Manager

Work with System Certificate

Secure application: QIBM_HTTP_SERVER_ADMIN

System certificate currently used: No system certificate assigned.

Certificate store: *SYSTEM

	System certificates
●	AS4BVeriSign
○	*DFTSVR

Figure 366. DCM - Assigning a server certificate - Selecting a certificate

5. Click **Assign new certificate** to assign the selected server certificate to the *ADMIN server. A completion message confirms that the certificate was assigned successfully.

For more information on assigning certificates to an application refer to 5.6.1.5, “Associate the certificate with a secure application” on page 155.

B.3 Activating the configuration changes

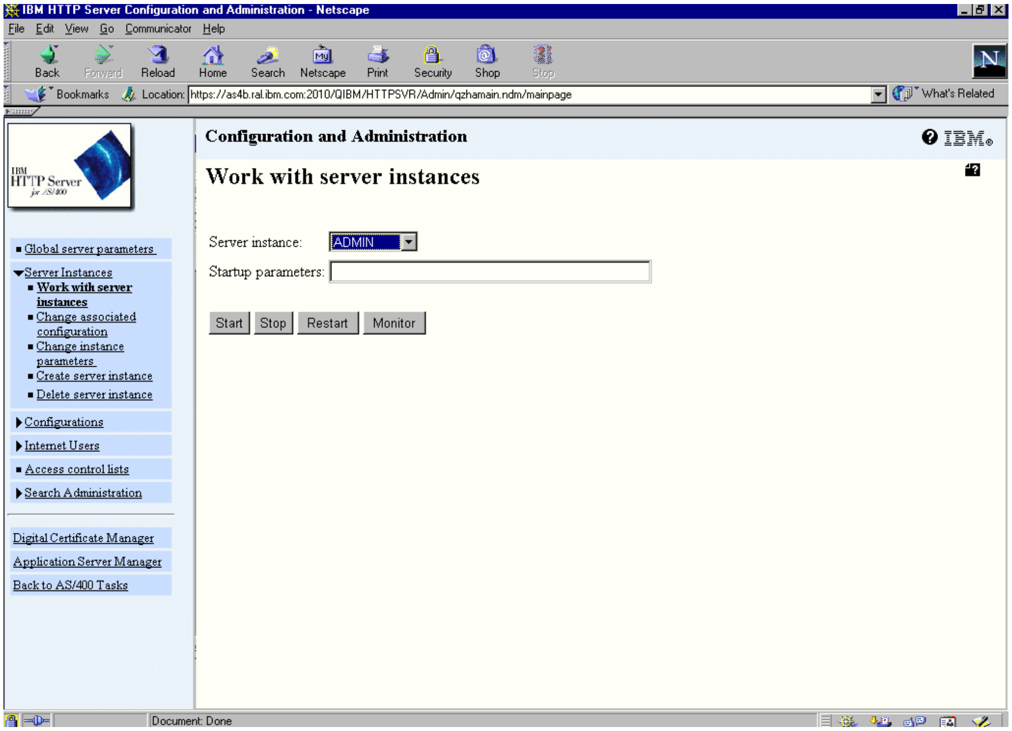
After the *ADMIN server instance is configured for SSL and a server certificate is assigned, the *ADMIN server needs to be stopped and started. Restarting the server instance will not activate the changes.

You can stop and start the server through the following methods:

- Through the command line interface using the following commands:

```
ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```

- Through the HTTP server configuration and administration function using the Web browser.


IBM HTTP Server Configuration and Administration - Netscape

Location: https://as4b.ral.ibm.com:2010/QIBM/HTTPSVR/Admin/qzhamain.ndm/mainpage

Configuration and Administration

Work with server instances

Server instance: ADMIN

Startup parameters:

Figure 367. Activating HTTP server configuration changes

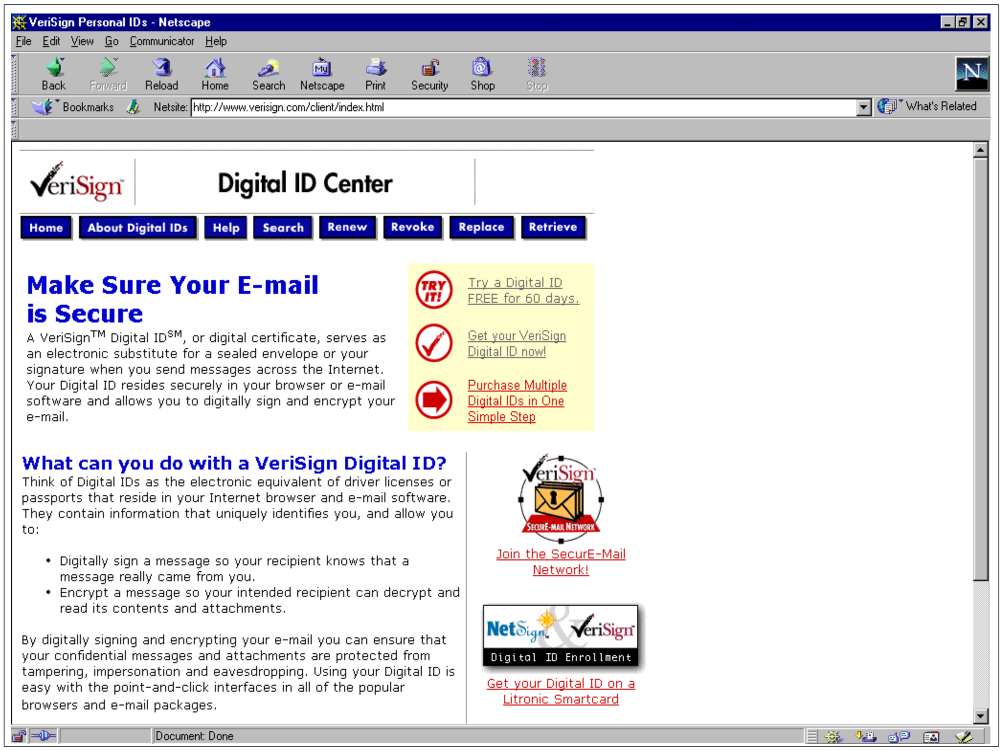
Do not select Restart. Instead click **Stop** and then **Start** for the ADMIN server.

Appendix C. Obtaining a digital certificate

The way to request a digital certificate depends on whether you are requesting a client or server certificate. It also varies from certificate authority to certificate authority. Usually server certificate requests are created on the server itself. The request is then being sent by e-mail to the certificate authority or copied and pasted to a Web form of the CA. Once the certificate is issued, it will be sent by e-mail to the institution that requested the certificate.

Opposed to server certificates, client certificates are usually used to authenticate the client to other entities or to sign and encrypt e-mail. Typically client certificates are stored on PCs. This appendix shows an example of how to request and install a client certificate using the Netscape Communicator 4.7. The certificate is requested from VeriSign.

1. To request the certificate, start the Netscape Communicator and enter the URL `http://www.verisign.com/client/index.html`.


VeriSign Personal IDs - Netscape
File Edit View Go Communicator Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Shop
Stop
Bookmarks
Netsite: http://www.verisign.com/client/index.html
What's Related
VeriSign
Digital ID Center
Home
About Digital IDs
Help
Search
Renew
Revoke
Replace
Retrieve
TRY IT!
Try a Digital ID FREE for 60 days.
Get your VeriSign Digital ID now!
Purchase Multiple Digital IDs in One Simple Step
SecurE-Mail Network
Join the SecurE-Mail Network!
NetSign & VeriSign
Digital ID Enrollment
Get your Digital ID on a Litronic Smartcard
Document: Done

Make Sure Your E-mail is Secure

A VeriSign™ Digital ID℠, or digital certificate, serves as an electronic substitute for a sealed envelope or your signature when you send messages across the Internet. Your Digital ID resides securely in your browser or e-mail software and allows you to digitally sign and encrypt your e-mail.

What can you do with a VeriSign Digital ID?

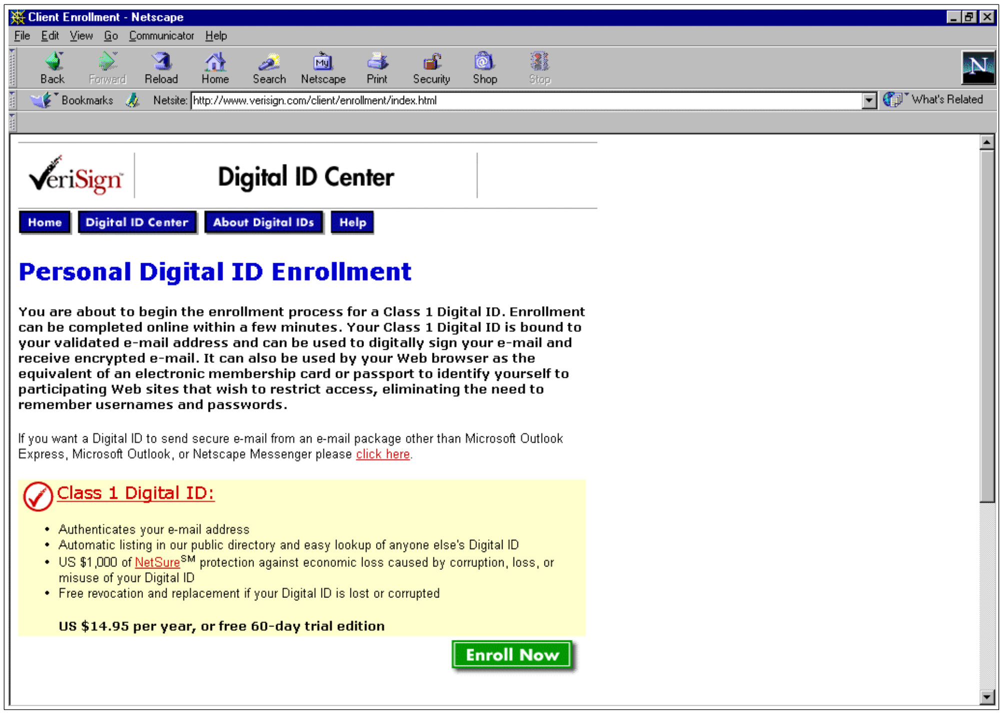
Think of Digital IDs as the electronic equivalent of driver licenses or passports that reside in your Internet browser and e-mail software. They contain information that uniquely identifies you, and allow you to:

- Digitally sign a message so your recipient knows that a message really came from you.
- Encrypt a message so your intended recipient can decrypt and read its contents and attachments.

By digitally signing and encrypting your e-mail you can ensure that your confidential messages and attachments are protected from tampering, impersonation and eavesdropping. Using your Digital ID is easy with the point-and-click interfaces in all of the popular browsers and e-mail packages.

Figure 368. Requesting a digital certificate from VeriSign

2. Select **Try a Digital ID FREE for 60 days**. Through this option you request a digital certificate without any cost.


Client Enrollment - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Netsite: http://www.verisign.com/client/enrollment/index.html What's Related
VeriSign
Digital ID Center
Home Digital ID Center About Digital IDs Help

Personal Digital ID Enrollment

You are about to begin the enrollment process for a Class 1 Digital ID. Enrollment can be completed online within a few minutes. Your Class 1 Digital ID is bound to your validated e-mail address and can be used to digitally sign your e-mail and receive encrypted e-mail. It can also be used by your Web browser as the equivalent of an electronic membership card or passport to identify yourself to participating Web sites that wish to restrict access, eliminating the need to remember usernames and passwords.

If you want a Digital ID to send secure e-mail from an e-mail package other than Microsoft Outlook Express, Microsoft Outlook, or Netscape Messenger please click here.

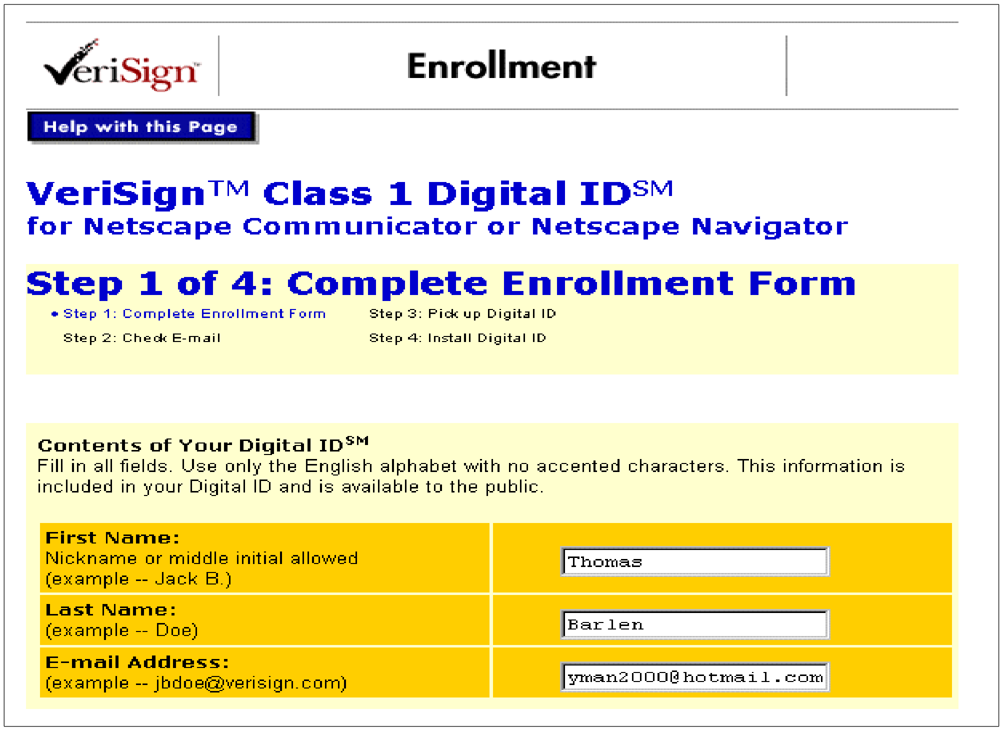
Class 1 Digital ID:

- Authenticates your e-mail address
- Automatic listing in our public directory and easy lookup of anyone else's Digital ID
- US $1,000 of NetSure^{SM} protection against economic loss caused by corruption, loss, or misuse of your Digital ID
- Free revocation and replacement if your Digital ID is lost or corrupted

US $14.95 per year, or free 60-day trial edition

Figure 369. Requesting a class 1 digital ID from VeriSign

3. Click **Enroll Now** to get the certificate request form.



VeriSign™ Class 1 Digital ID^{SM}
for Netscape Communicator or Netscape Navigator

Step 1 of 4: Complete Enrollment Form

- Step 1: Complete Enrollment Form
- Step 2: Check E-mail
- Step 3: Pick up Digital ID
- Step 4: Install Digital ID

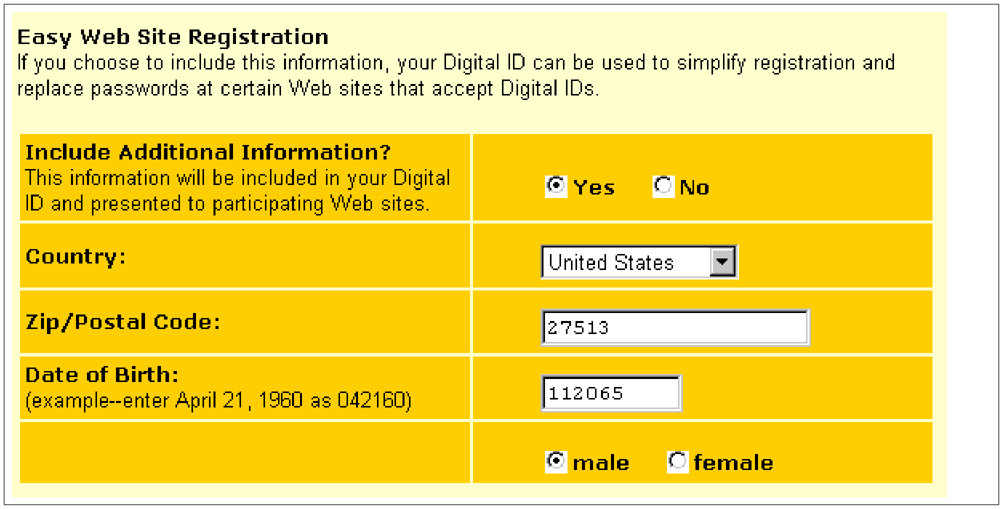
Contents of Your Digital ID^{SM}
Fill in all fields. Use only the English alphabet with no accented characters. This information is included in your Digital ID and is available to the public.

First Name: Nickname or middle initial allowed (example -- Jack B.)	Thomas
Last Name: (example -- Doe)	Barlen
E-mail Address: (example -- jbdoe@verisign.com)	yman2000@hotmail.com

Figure 370. Certificate enrollment form - section 1

The certificate enrollment form requires the user to enter information, such as the user's first and last name, e-mail ID, and so on.

4. Scroll through the enrollment form and fill out the required fields.



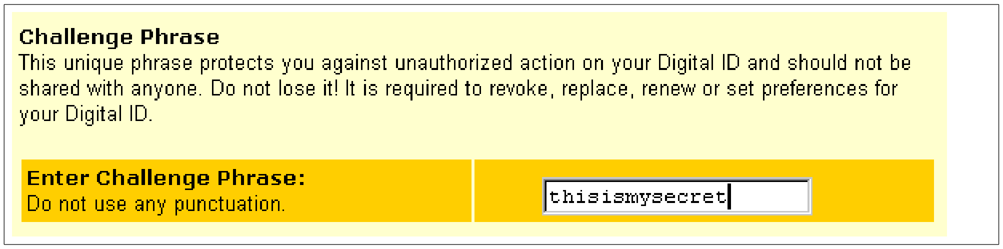
Easy Web Site Registration
If you choose to include this information, your Digital ID can be used to simplify registration and replace passwords at certain Web sites that accept Digital IDs.

Include Additional Information? This information will be included in your Digital ID and presented to participating Web sites.	● **Yes** ○ **No**
Country:	United States ▾
Zip/Postal Code:	27513
Date of Birth: (example--enter April 21, 1960 as 042160)	112065
	● **male** ○ **female**

Figure 371. Certificate enrollment form - section 2

The next section in the enrollment form is optional. If you want to include additional information, select the appropriate option and enter the data.

5. Scroll to the next section of the enrollment form.



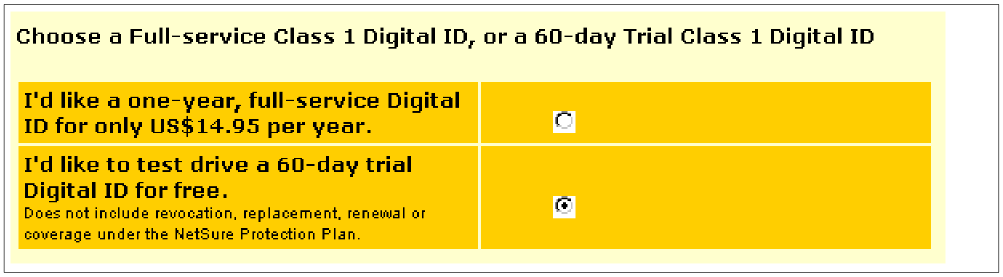
Challenge Phrase
This unique phrase protects you against unauthorized action on your Digital ID and should not be shared with anyone. Do not lose it! It is required to revoke, replace, renew or set preferences for your Digital ID.

Enter Challenge Phrase: Do not use any punctuation.	thisismysecret

Figure 372. Certificate enrollment form - section 3

Fill in the challenge phrase. Every time you request an action on this certificate, you will be requested to provide the challenge phrase specified in the certificate request. Note that some certificate authorities charge a fee in case you are requesting an action on your certificate and forgot your challenge phrase.

6. Scroll to the next section of the enrollment form.



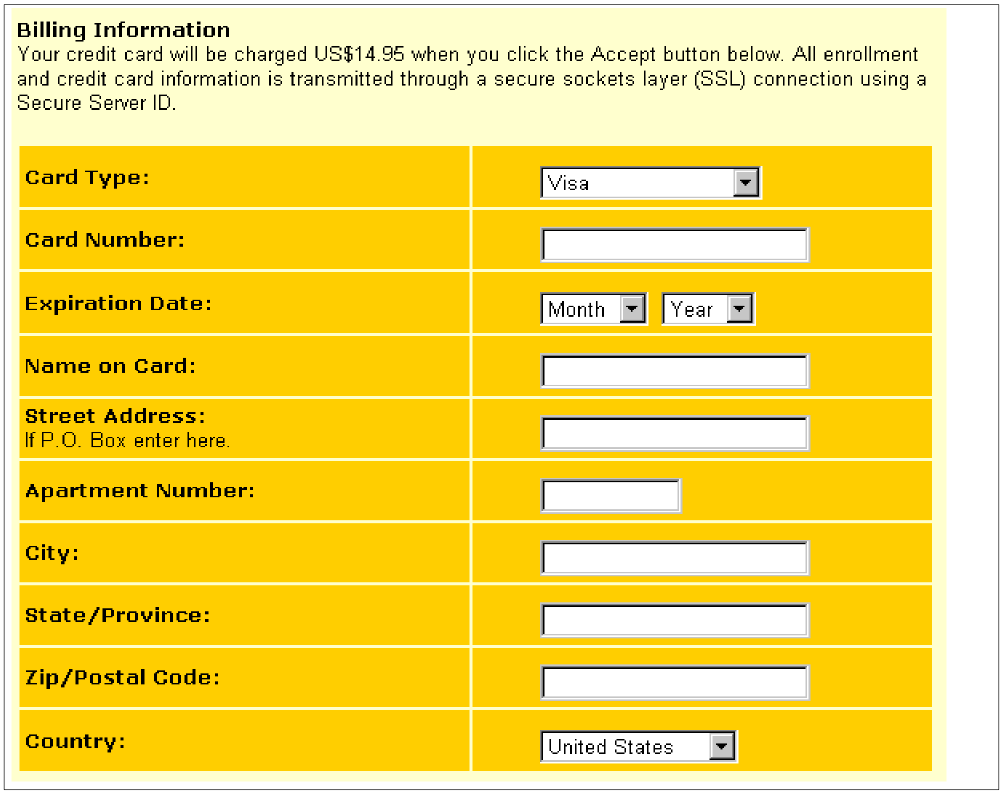
Choose a Full-service Class 1 Digital ID, or a 60-day Trial Class 1 Digital ID

I'd like a one-year, full-service Digital ID for only US$14.95 per year.	○
I'd like to test drive a 60-day trial Digital ID for free. Does not include revocation, replacement, renewal or coverage under the NetSure Protection Plan.	●

Figure 373. Certificate enrollment form - section 4

In this case, a free trial certificate is chosen. Beware that this certificate is not validated by the certificate authority and therefore likely not to be accepted by any server application. But it can be used to sign and encrypt e-mail. If the server application trusts also this particular certificate authority from VeriSign, then your trial certificate can also be used.

7. Scroll to the next section of the enrollment form.



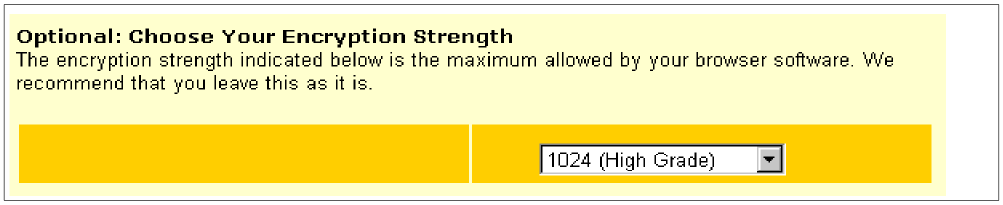
Billing Information
Your credit card will be charged US$14.95 when you click the Accept button below. All enrollment and credit card information is transmitted through a secure sockets layer (SSL) connection using a Secure Server ID.

Card Type:	Visa ▾
Card Number:	
Expiration Date:	Month ▾ Year ▾
Name on Card:	
Street Address: If P.O. Box enter here.	
Apartment Number:	
City:	
State/Province:	
Zip/Postal Code:	
Country:	United States ▾

Figure 374. Certificate enrollment form - section 5

Note that a free trial certificate has been chosen and therefore no billing information is needed.

8. Scroll to the next section of the enrollment form.



Optional: Choose Your Encryption Strength
The encryption strength indicated below is the maximum allowed by your browser software. We recommend that you leave this as it is.

1024 (High Grade) ▾

Figure 375. Certificate enrollment form - section 6

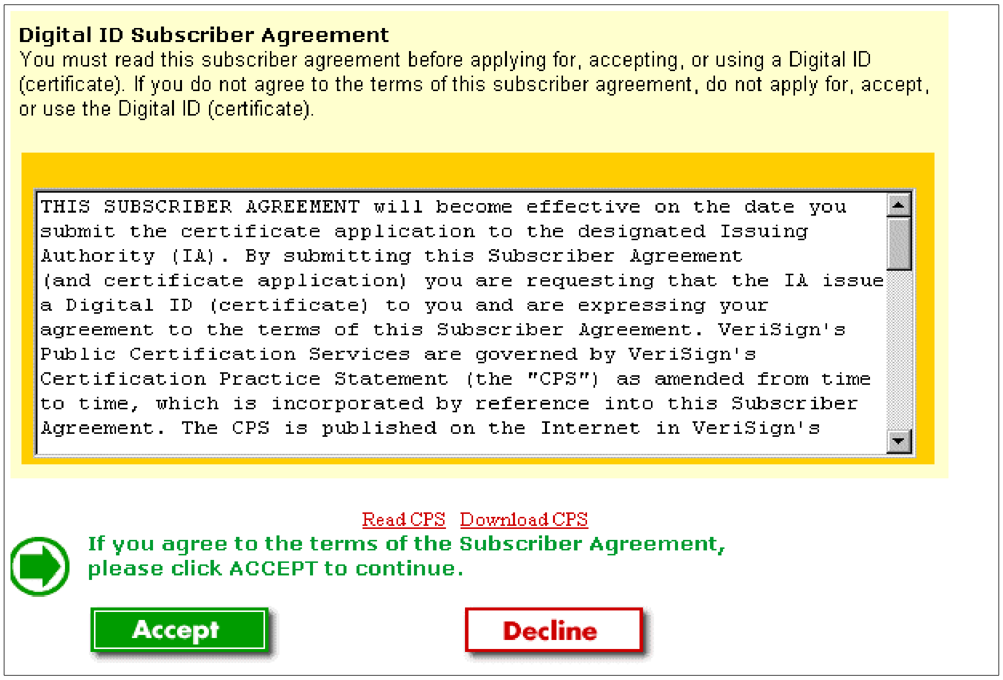
Select the encryption strength for the certificate. The key sizes available in the selection box vary according to the country in which your system is located. Some countries, such as France, restrict the size of keys that may be imported for use. The United States also has export restrictions on certain larger key sizes. Additionally, browser software has built-in support for a limited set of key sizes. As a result, the browser actually generates the selection box for user certificate key sizes based on both of these factors.

The key size that you select determines the size of the public key and private key that accompany your certificate. Because larger keys provide more secure encryption, choose the largest key size available to you.

Note

Not all browsers create a key size selection box when requesting a certificate. Netscape browsers do provide the selection box.

9. Scroll to the next section of the enrollment form.



Digital ID Subscriber Agreement

You must read this subscriber agreement before applying for, accepting, or using a Digital ID (certificate). If you do not agree to the terms of this subscriber agreement, do not apply for, accept, or use the Digital ID (certificate).

THIS SUBSCRIBER AGREEMENT will become effective on the date you submit the certificate application to the designated Issuing Authority (IA). By submitting this Subscriber Agreement (and certificate application) you are requesting that the IA issue a Digital ID (certificate) to you and are expressing your agreement to the terms of this Subscriber Agreement. VeriSign's Public Certification Services are governed by VeriSign's Certification Practice Statement (the "CPS") as amended from time to time, which is incorporated by reference into this Subscriber Agreement. The CPS is published on the Internet in VeriSign's

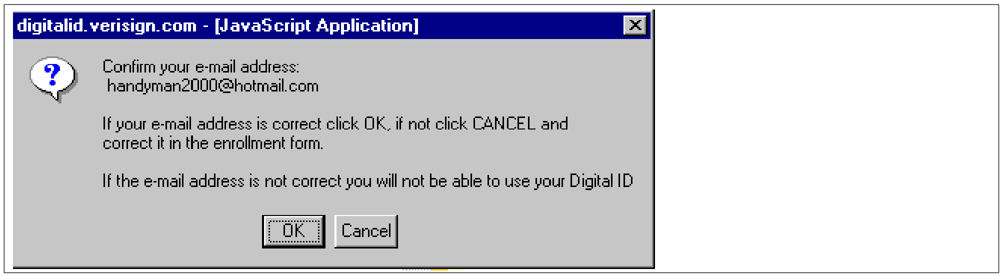
Read CPS Download CPS

If you agree to the terms of the Subscriber Agreement, please click ACCEPT to continue.

Figure 376. Certificate enrollment form - section 7

After the form has been filled out, you must read the Digital ID Subscriber Agreement. Select the appropriate button depending if you agree or not. From this form you can also click the link **Read CPS** for further information about the term and conditions of this CA.

10.Select **Accept** to submit the certificate request.



digitalid.verisign.com - [JavaScript Application]

Confirm your e-mail address:
handyman2000@hotmail.com

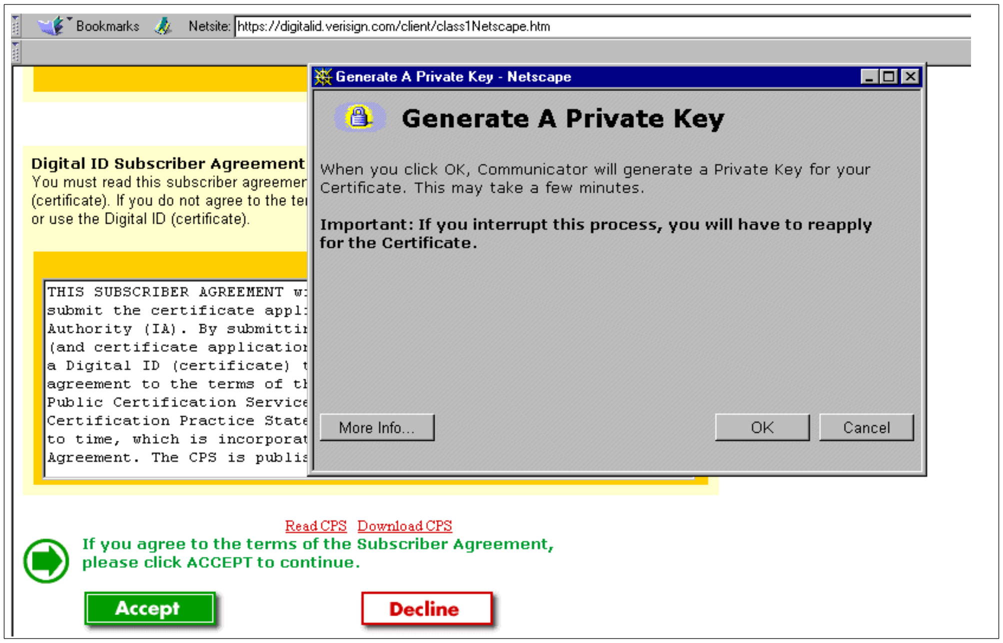
If your e-mail address is correct click OK, if not click CANCEL and correct it in the enrollment form.

If the e-mail address is not correct you will not be able to use your Digital ID

Figure 377. Certificate request - e-mail confirmation message

A confirmation message is shown to verify that the correct e-mail address was specified in the request. Check the e-mail address thoroughly because the certificate notification will be sent to this address.

11.Click **OK** if the address is correct. Otherwise go back, correct the address, and submit the request again.



Bookmarks
Netsite: https://digitalid.verisign.com/client/class1Netscape.htm
Generate A Private Key - Netscape
More Info...
OK
Cancel
Read CPS
Download CPS
Accept
Decline

Generate A Private Key

When you click OK, Communicator will generate a Private Key for your Certificate. This may take a few minutes.

Important: If you interrupt this process, you will have to reapply for the Certificate.

Digital ID Subscriber Agreement
You must read this subscriber agreemer
(certificate). If you do not agree to the ter
or use the Digital ID (certificate).

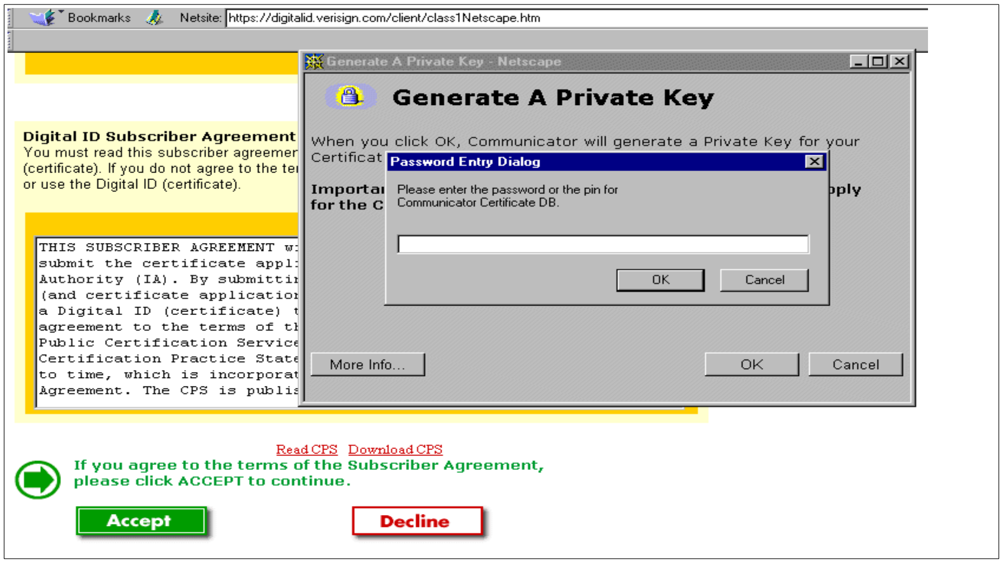
```
THIS SUBSCRIBER AGREEMENT w:
submit the certificate appl:
Authority (IA). By submittir
(and certificate applicatior
a Digital ID (certificate) t
agreement to the terms of tl
Public Certification Service
Certification Practice State
to time, which is incorporat
Agreement. The CPS is publis
```

If you agree to the terms of the Subscriber Agreement, please click ACCEPT to continue.

Figure 378. Certificate request - generating the private key

This message is issued from the Netscape browser and initiated through the VeriSign certificate request process.

12.Click **OK**. The browser will generate the key. Depending on whether the Netscape Communicator database is already protected by a password, the following password request is issued.



Bookmarks
Netsite: https://digitalid.verisign.com/client/class1Netscape.htm
Generate A Private Key - Netscape
Password Entry Dialog
OK
Cancel
More Info...
OK
Cancel
Read CPS
Download CPS
Accept
Decline

Generate A Private Key

When you click OK, Communicator will generate a Private Key for your Certificat

Importa ... pply
for the C

Please enter the password or the pin for Communicator Certificate DB.

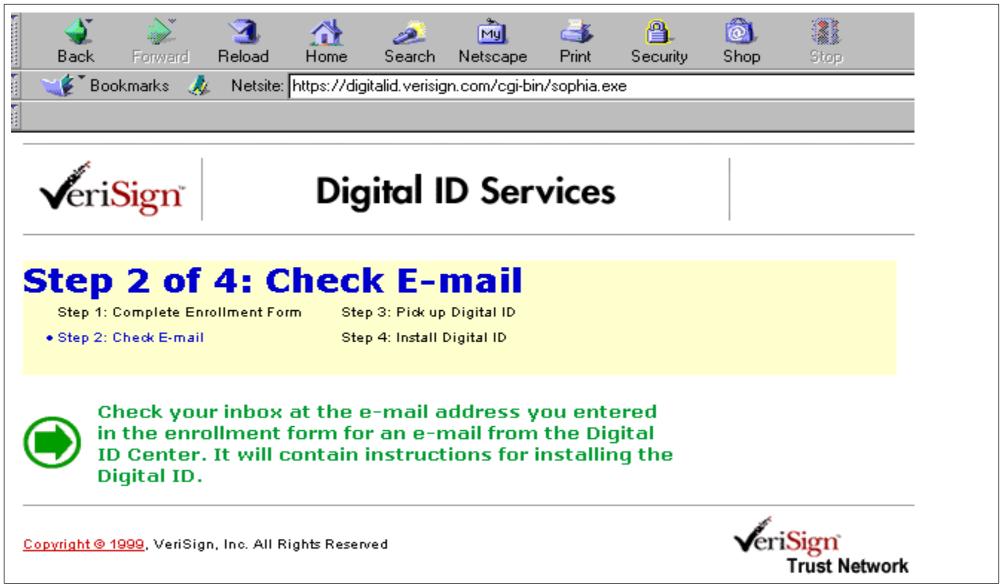
Digital ID Subscriber Agreement
You must read this subscriber agreemer
(certificate). If you do not agree to the ter
or use the Digital ID (certificate).

```
THIS SUBSCRIBER AGREEMENT w:
submit the certificate appl:
Authority (IA). By submittir
(and certificate applicatior
a Digital ID (certificate) t
agreement to the terms of tl
Public Certification Service
Certification Practice State
to time, which is incorporat
Agreement. The CPS is publis
```

If you agree to the terms of the Subscriber Agreement, please click ACCEPT to continue.

Figure 379. Certificate request - password entry display

13.Enter the password and click **OK**.



Digital ID Services

Step 2 of 4: Check E-mail

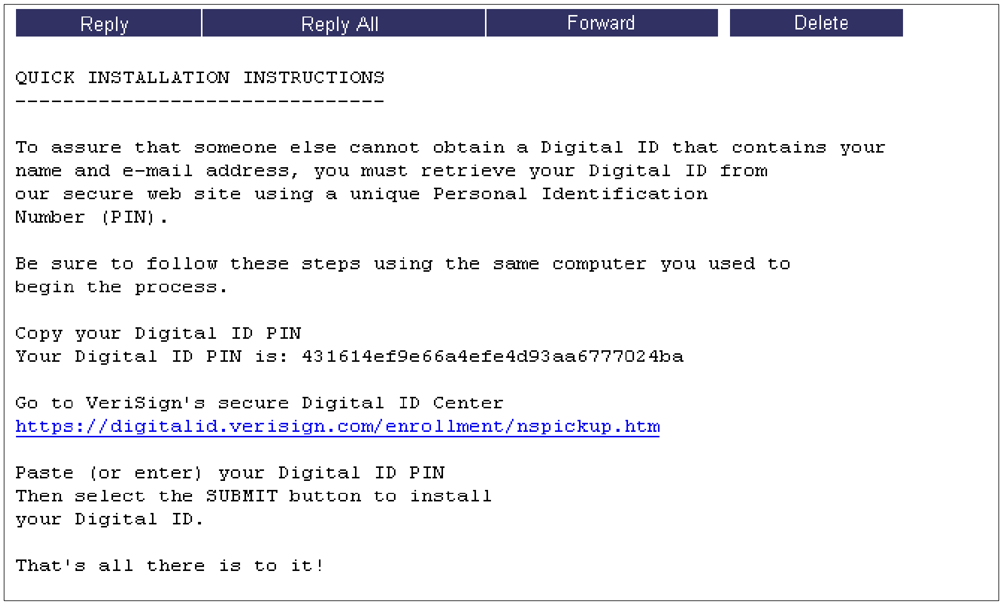
Step 1: Complete Enrollment Form
• Step 2: Check E-mail
Step 3: Pick up Digital ID
Step 4: Install Digital ID

Check your inbox at the e-mail address you entered in the enrollment form for an e-mail from the Digital ID Center. It will contain instructions for installing the Digital ID.

Copyright © 1999, VeriSign, Inc. All Rights Reserved

Figure 380. VeriSign step 2 of the certificate request

After a while an e-mail note arrives at the e-mail address specified in the certificate request containing instructions on how to install the certificate.

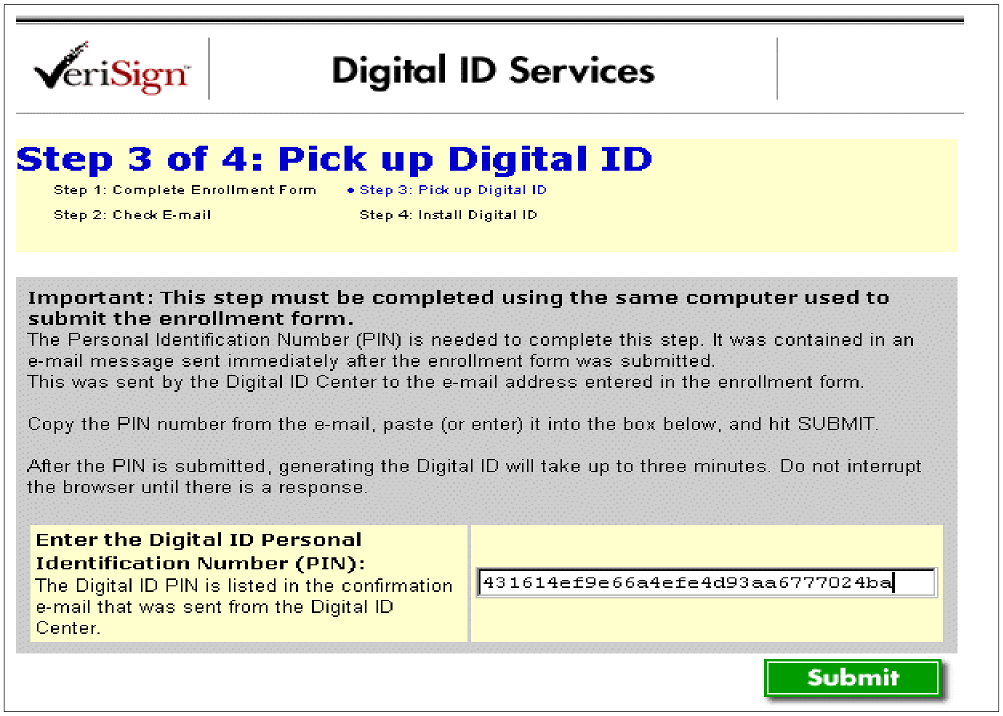


```
QUICK INSTALLATION INSTRUCTIONS
-------------------------------

To assure that someone else cannot obtain a Digital ID that contains your
name and e-mail address, you must retrieve your Digital ID from
our secure web site using a unique Personal Identification
Number (PIN).

Be sure to follow these steps using the same computer you used to
begin the process.

Copy your Digital ID PIN
Your Digital ID PIN is: 431614ef9e66a4efe4d93aa6777024ba

Go to VeriSign's secure Digital ID Center
https://digitalid.verisign.com/enrollment/nspickup.htm

Paste (or enter) your Digital ID PIN
Then select the SUBMIT button to install
your Digital ID.

That's all there is to it!
```

Figure 381. Certificate request - e-mail with installation instructions

The e-mail sent by VeriSign contains the instructions how to proceed to install the certificate on your PC. VeriSign includes a digital ID PIN, which is used on the URL mentioned in this e-mail, to identify your certificate.

14.Click the URL `https://digitalid.verisign.com/enrollment/nspickup.htm`.



Step 3 of 4: Pick up Digital ID

Step 1: Complete Enrollment Form • Step 3: Pick up Digital ID
Step 2: Check E-mail Step 4: Install Digital ID

Important: This step must be completed using the same computer used to submit the enrollment form.
The Personal Identification Number (PIN) is needed to complete this step. It was contained in an e-mail message sent immediately after the enrollment form was submitted.
This was sent by the Digital ID Center to the e-mail address entered in the enrollment form.

Copy the PIN number from the e-mail, paste (or enter) it into the box below, and hit SUBMIT.

After the PIN is submitted, generating the Digital ID will take up to three minutes. Do not interrupt the browser until there is a response.

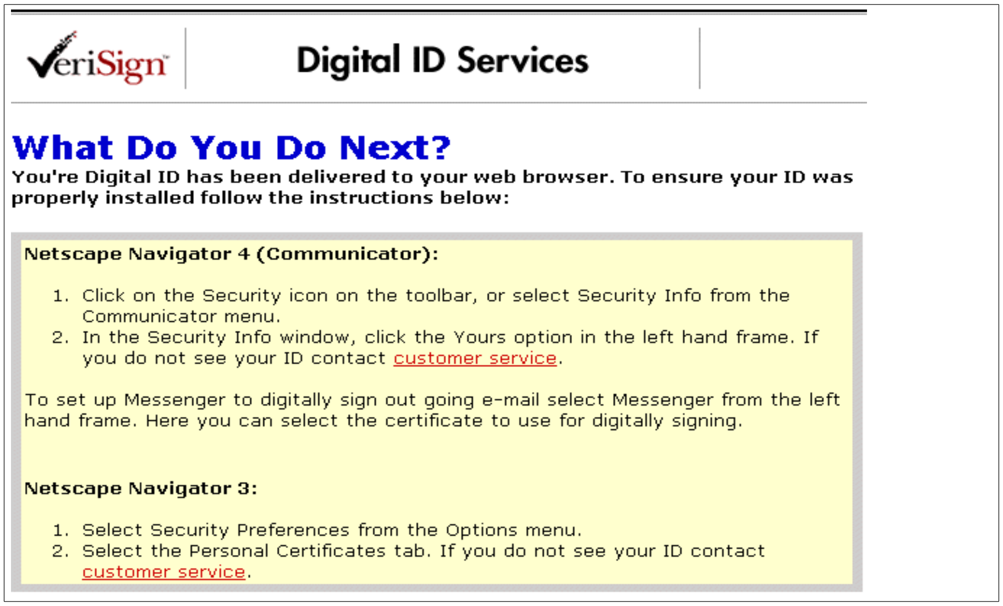
Enter the Digital ID Personal Identification Number (PIN):
The Digital ID PIN is listed in the confirmation e-mail that was sent from the Digital ID Center.

431614ef9e66a4efe4d93aa6777024ba

Figure 382. VeriSign step 3 of the certificate request

It is important to follow the instructions shown on the Web page. The reason why you have to perform the steps on the same computer used to request the certificate is that the certificate must be installed on the PC that possesses the private key.

15.Click **Submit** to receive the certificate into your browser database. The following information is displayed on the browser, indicating the successful installation.



What Do You Do Next?

You're Digital ID has been delivered to your web browser. To ensure your ID was properly installed follow the instructions below:

Netscape Navigator 4 (Communicator):

1. Click on the Security icon on the toolbar, or select Security Info from the Communicator menu.
2. In the Security Info window, click the Yours option in the left hand frame. If you do not see your ID contact customer service.

To set up Messenger to digitally sign out going e-mail select Messenger from the left hand frame. Here you can select the certificate to use for digitally signing.

Netscape Navigator 3:

1. Select Security Preferences from the Options menu.
2. Select the Personal Certificates tab. If you do not see your ID contact customer service.

Figure 383. VeriSign step 4 of the certificate request

16.From the Netscape browser click on the **Security** button.

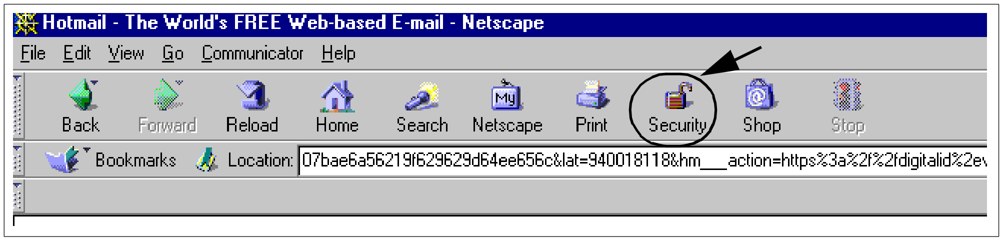
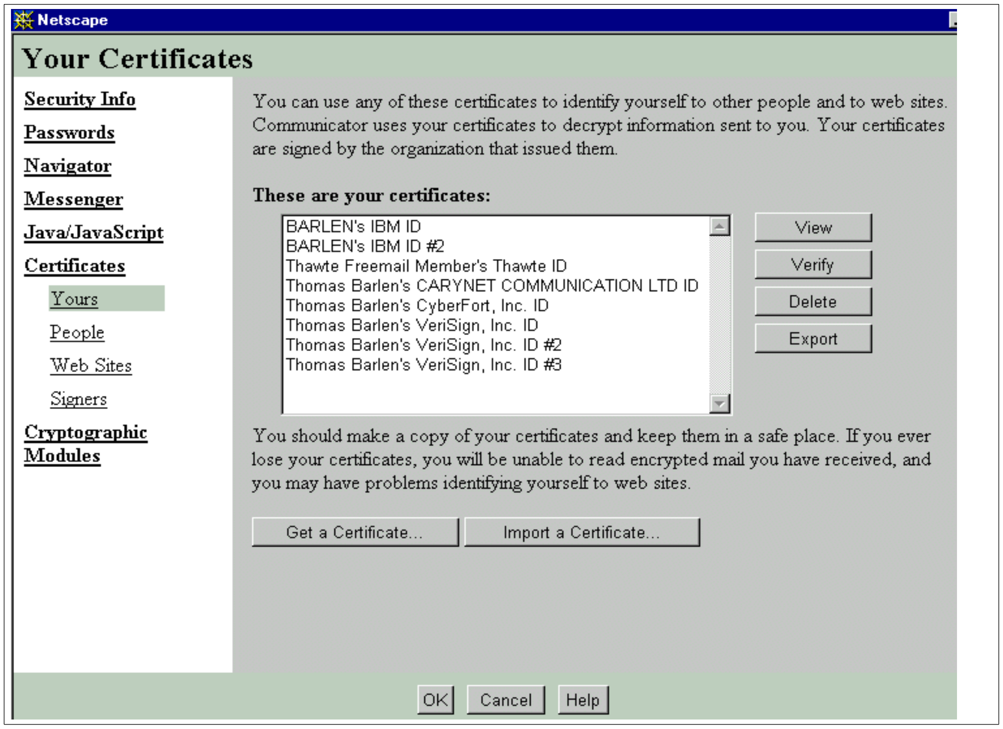

Hotmail - The World's FREE Web-based E-mail - Netscape
File Edit View Go Communicator Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Shop
Stop
Bookmarks
Location: 07bae6a56219f629629d64ee656c&lat=940018118&hm___action=https%3a%2f%2fdigitalid%2e

Figure 384. Netscape browser - select Security

The Security button opens the security information window of the Netscape browser. Select **Yours** under Certificates. All client certificates installed on this PC are displayed.



Your Certificates

You can use any of these certificates to identify yourself to other people and to web sites. Communicator uses your certificates to decrypt information sent to you. Your certificates are signed by the organization that issued them.

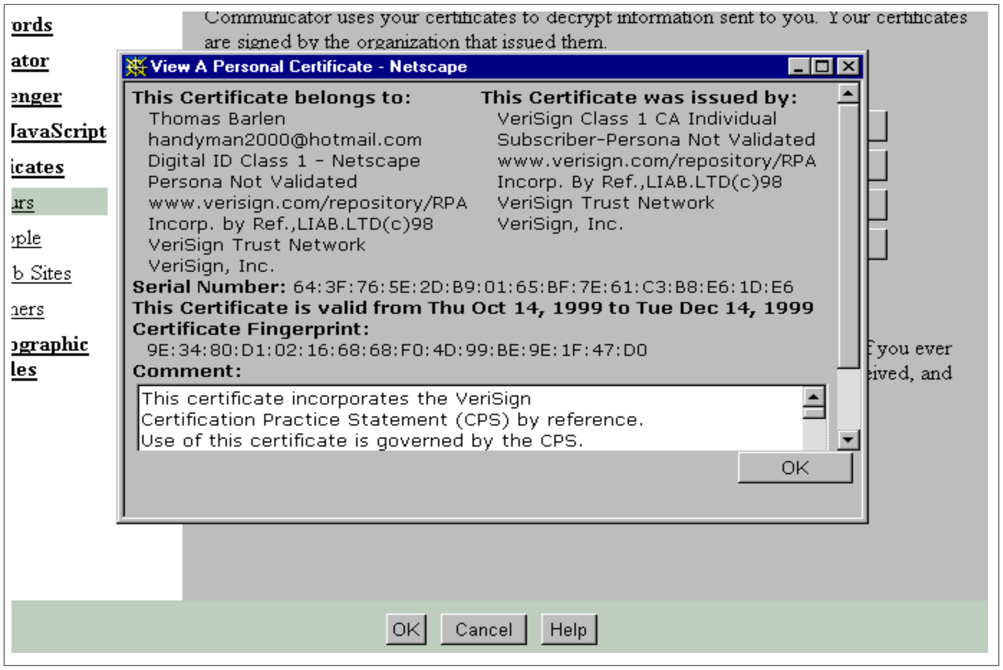
These are your certificates:

BARLEN's IBM ID
BARLEN's IBM ID #2
Thawte Freemail Member's Thawte ID
Thomas Barlen's CARYNET COMMUNICATION LTD ID
Thomas Barlen's CyberFort, Inc. ID
Thomas Barlen's VeriSign, Inc. ID
Thomas Barlen's VeriSign, Inc. ID #2
Thomas Barlen's VeriSign, Inc. ID #3

You should make a copy of your certificates and keep them in a safe place. If you ever lose your certificates, you will be unable to read encrypted mail you have received, and you may have problems identifying yourself to web sites.

Figure 385. Netscape browser - client certificates

17.Click your new certificate and select **View**.



Communicator uses your certificates to decrypt information sent to you. Your certificates are signed by the organization that issued them.

This Certificate belongs to:
Thomas Barlen
handyman2000@hotmail.com
Digital ID Class 1 - Netscape
Persona Not Validated
www.verisign.com/repository/RPA
Incorp. by Ref.,LIAB.LTD(c)98
VeriSign Trust Network
VeriSign, Inc.

This Certificate was issued by:
VeriSign Class 1 CA Individual
Subscriber-Persona Not Validated
www.verisign.com/repository/RPA
Incorp. By Ref.,LIAB.LTD(c)98
VeriSign Trust Network
VeriSign, Inc.

Serial Number: 64:3F:76:5E:2D:B9:01:65:BF:7E:61:C3:B8:E6:1D:E6
This Certificate is valid from Thu Oct 14, 1999 to Tue Dec 14, 1999
Certificate Fingerprint:
9E:34:80:D1:02:16:68:68:F0:4D:99:BE:9E:1F:47:D0
Comment:
This certificate incorporates the VeriSign
Certification Practice Statement (CPS) by reference.
Use of this certificate is governed by the CPS.

Figure 386. Netscape browser - Personal Certificate view

The new certificate is shown. As you can see, VeriSign has its own certificate authority instance to issue trial certificates. This is also shown in the certificate issuer information of the certificate.

Appendix D. Sample Java program using SSL

The sample code shown in this appendix was downloaded from the IBM publication library at the following URL:

http://publib.boulder.ibm.com/pubs/html/as400/v4r4/ic2924/info/java/rzahh/toolbox.htm

Many of the code samples on this URL use the AS/400 Toolbox for Java. But none of them contains information on how to enable Java for secure communications with SSL. Therefore, the following sample code is modified to use SSL. Basically only minor changes are needed to enable a Java application for SSL.

In general, except for JDBC calls, you need to change the object AS400() to SecureAS400() in the code.

For JDBC you need to add the security property secure=true in the connection object**.**

In the following sample code, characters shown in bold indicate the modifications for the SSL connection.

D.1 Secure command call

```
//////////////////////////////////////////////////////////////////////////////////
//
// SecureCommand call example.  This program prompts the user
// for the name of the AS/400 and the command to run, then
// prints the result of the command.
// 1999/11/10
// How to excute: c:\java secureCommandCall
//////////////////////////////////////////////////////////////////////////////////

import java.io.*;
import java.util.*;
import com.ibm.as400.access.*;

public class secureCommandCall extends Object
{
   public static void main(String[] parmeters)
   {

      // Created a reader to get input from the user
      BufferedReader inputStream = new BufferedReader(new InputStreamReader(System.in),1);


      // Declare variables to hold the system name and the command to run
      String systemString  = null;
      String commandString = null;

      System.out.println( " " );


      // Get the system name and the command to run from the user
      try
      {
         System.out.print("System name: ");
         systemString = inputStream.readLine();

         System.out.print("Command: ");
         commandString = inputStream.readLine();
      }
      catch (Exception e) {};

      System.out.println( "connection start!" );
      // Create a secure AS400 object.  This is the system we send the command to
      AS400 as400 = new SecureAS400(systemString);
         System.out.println( "secure AS400 object creation OK!" );
      // Create an AS400 object.  This is the system we send the command to
      //AS400 as400 = new SecureAS400(systemString);
      // System.out.println( "non-secure AS400 object creation OK!" );



      // Create a command call object specifying the AS/400 that will
      // recieve the command.
      CommandCall command = new CommandCall( as400 );
      System.out.println( "commandcall object creation OK!" );


      try
      {
         // Run the command.
         if (command.run(commandString))
             System.out.print( "Command successful" );
         else
             System.out.print( "Command failed" );


         // If messages were produced from the command, print them
         AS400Message[] messagelist = command.getMessageList();

         if (messagelist.length > 0)
         {
             System.out.println( ", messages from the command:" );
             System.out.println( " " );
         }

         for (int i=0; i < messagelist.length; i++)
         {
            System.out.print  ( messagelist[i].getID() );
            System.out.print  ( ": " );
            System.out.println( messagelist[i].getText() );
         }
      }
      catch (Exception e)
      {
         System.out.println( "Command " + command.getCommand() + " did not run" );
      }

      System.exit(0);
   }
}
```

D.2 Secure JDBC call

```
//////////////////////////////////////////////////////////////////////////////////
//
// JDBCQuery example.  This program uses the AS/400 JDBC driver to
// query a table and output its contents.
//
// Command syntax:
//    secureJDBCQuery system collectionName tableName
//
// For example,
//    secureJDBCQuery MySystem qiws qcustcdt
//
//////////////////////////////////////////////////////////////////////////////////

import java.sql.*;

public class secureJDBCQuery
{



    // Format a string so that it has the specified width.
    private static String format (String s, int width)
    {
        String formattedString;
        // The string is shorter than specified width,
        // so we need to pad with blanks.
        if (s.length() < width) {
            StringBuffer buffer = new StringBuffer (s);
            for (int i = s.length(); i < width; ++i)
                buffer.append (" ");
            formattedString = buffer.toString();
        }

        // Otherwise, we need to truncate the string.
        else
            formattedString = s.substring (0, width);

        return formattedString;
    }

public static void main (String[] parameters)
    {
        // Check the input parameters.
        if (parameters.length != 3) {
            System.out.println("");
            System.out.println("Usage:");
            System.out.println("");
            System.out.println("   JDBCQuery system collectionName tableName");
            System.out.println("");
            System.out.println("");
            System.out.println("For example:");
            System.out.println("");
            System.out.println("");
            System.out.println("   JDBCQuery mySystem qiws qcustcdt");
            System.out.println("");
            return;
        }

        String system           = parameters[0];
        String collectionName   = parameters[1];
        String tableName        = parameters[2];

        Connection connection   = null;

        try {


            // Load the AS/400 Toolbox for Java JDBC driver.
            DriverManager.registerDriver(new com.ibm.as400.access.AS400JDBCDriver());

// Get a secure connection to the database.  Since we do not
// provide a user id or password, a prompt will appear. The JDBC property "secure" must
// be set as 'true'. The default value is false. It means only the password is encrypted.
connection = DriverManager.getConnection ("jdbc:as400://" + system + ";secure = true");
            DatabaseMetaData dmd = connection.getMetaData ();

            // Execute the query.
            Statement select = connection.createStatement ();
            ResultSet rs = select.executeQuery ("SELECT * FROM "
                + collectionName + dmd.getCatalogSeparator() + tableName);

            // Get information about the result set.  Set the column
            // width to whichever is longer: the length of the label
            // or the length of the data.
            ResultSetMetaData rsmd = rs.getMetaData ();
            int columnCount = rsmd.getColumnCount ();
            String[] columnLabels = new String[columnCount];
            int[] columnWidths = new int[columnCount];
            for (int i = 1; i <= columnCount; ++i) {
                columnLabels[i-1] = rsmd.getColumnLabel (i);
                columnWidths[i-1] = Math.max (columnLabels[i-1].length(),
                    rsmd.getColumnDisplaySize (i));
            }

            // Output the column headings.
            for (int i = 1; i <= columnCount; ++i) {
                System.out.print (format (rsmd.getColumnLabel(i), columnWidths[i-1]));
                System.out.print (" ");
            }
            System.out.println ();

            // Output a dashed line.
            StringBuffer dashedLine;
            for (int i = 1; i <= columnCount; ++i) {
                for (int j = 1; j <= columnWidths[i-1]; ++j)
                    System.out.print ("-");
                System.out.print (" ");
            }
            System.out.println ();

            // Iterate throught the rows in the result set and output
            // the columns for each row.
            while (rs.next ()) {
                for (int i = 1; i <= columnCount; ++i) {
                    String value = rs.getString (i);
                    if (rs.wasNull ())
                        value = "<null>";
                    System.out.print (format (value, columnWidths[i-1]));
                    System.out.print (" ");
                }
                System.out.println ();
            }

        }

        catch (Exception e) {
            System.out.println ();
            System.out.println ("ERROR: " + e.getMessage());
        }

        finally {

            // Clean up.
            try {
                if (connection != null)
                    connection.close ();
            }
            catch (SQLException e) {
                // Ignore.
            }
        }

        System.exit (0);
    }


}
```

Appendix E. Using the additional material

This redbook also contains additional material available on the Web. See the appropriate section below for instructions on using or downloading this type of material.

E.1 Locating the additional material on the Internet

The material associated with this redbook is also available in softcopy on the Internet from the IBM Redbooks Web server. Point your Web browser to:

ftp://www.redbooks.ibm.com/redbooks/SG245659

Alternatively, you can go to the IBM Redbooks Web site at:

http://www.redbooks.ibm.com/

Select **Additional materials** and open the directory that corresponds with the redbook form number.

E.2 Using the Web material

The additional Web material that accompanies this redbook includes the following:

File name	*Description*
README.HTML	Instructions on how to use the material

Important

The material consists of several files that contain the sample application code covered in this redbook. Detailed information about the downloadable files are documented in the README.HTML file.

E.2.1 System requirements for downloading the Web material

The following system configuration is recommended for downloading the additional Web material:

Hard disk space:	30 MB minimum
Operating System:	OS/400 V4R4 or higher

E.2.2 How to use the Web material

Create a subdirectory (folder) on your workstation and download the contents of the Web material into this folder.

Follow the instructions in the README.HTML file for further information on how to restore and use the material.

Appendix F. Special notices

This publication is intended to help AS/400 programmers, network administrators, consultants and IBM specialists to establish secure internet and intranet connections using the SSL protocol and digital certificates. The information in this publication is not intended as the specification of any programming interfaces that are provided by the IBM Operating System/400. See the PUBLICATIONS section of the IBM Programming Announcement for OS/400 V4R4 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

This document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AS/400 ®
AS/400e
C/400 ®
IBM ®
OS/400 ®
Operating System/400 ®
Integrated Language Environment
Net.Data
SP
WebSphere
XT
RPG/400 ®
AT
CT
DB2
Distributed Relational Database Architecture
DRDA
Language Environment
SecureWay
VisualAge
World Registry

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Netscape, Netscape Navigator, and the Netscape logo are trademarks of Netscape Communications Corporation in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and/or other countries licensed exclusively through X/Open Company Limited.

SET and the SET logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix G. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

G.1 IBM Redbooks

For information on ordering these ITSO publications see “How to get IBM Redbooks” on page 407.

- *AS/400 Internet Security: Implementing AS/400 VPNs*, SG24-5404
- *A Comprehensive Guide to Virtual Private Networks, Volume III: IBM Cross-Platform and Key Management Solutions*, SG24-5309
- *Management Central: A Smart Way to Manage AS/400 Systems,* SG24-5407
- *Deploying a Public Key Infrastructure*, SG24-5512
- *TCP/IP Tutorial and Technical Overview*, GG24-3376
- *Host On-Demand 4.0*, SG24-2149
- *Building AS/400 Client/Server Applications with Java*, SG24-2152
- *Building AS/400 Applications for IBM WebSphere Standard Edition 2.0*, SG24-5635

G.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at http://www.redbooks.ibm.com/ for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	**Collection Kit Number**
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046
RS/6000 Redbooks Collection (BkMgr Format)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

G.3 Other resources

The following publications may be found at
http://publib.boulder.ibm.com/pubs/html/as400/online/v4r4eng.htm:

- *HTTP Server for AS/400 Webmaster's Guide V4R4*, GC41-5434
- *OS/400 Security APIs V4R4*, SC41-5872
- *OS/400 UNIX-Type APIs V4R4*, SC41-5875
- *OS/400 TCP/IP Configuration and Reference V4R4*, SC41-5420
- *Web Programming Guide V4R4*, GC41-5435

These publications are also relevant as further information sources:

- *Java Servlet Programming,* O'Reilly, ISBN 1-56592-391-X
- *Java Cryptography,* by Jonathan Knudsen, O'Reilly, ISBN 1-56592-402-9

G.4 Referenced Web sites

These Web sites are also relevant as further information sources:

- `http://www.as400.ibm.com/tstudio/secure1/whitepapers/Cert.htm`
  Contains an article about digital certificates from Mark McKelvey
- `http://www.as400.ibm.com/tstudio/websphere/docs/as400v202/index.html`
  WebSphere Application Server online documentation
- `http://www.as400.ibm.com/clientaccess/cwbcossz.htm`
  Link to the key database update utility
- `http://www.software.ibm.com/network/hostondemand/library`
  IBM SecureWay Host On-Demand product information

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** http://www.redbooks.ibm.com/

  Search for, view, download, or order hardcopy/CD-ROM redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

IBM Redbooks fax order form

Please send me the following:

Title	Order Number	Quantity

First name | Last name

Company

Address

City | Postal code | Country

Telephone number | Telefax number | VAT number

□ Invoice to customer number

□ Credit card number

Credit card expiration date | Card issued to | Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

List of abbreviations

API	Application Programming Interface
AS/400	IBM Application System/400
CA	Certificate Authority
CCSID	Coded Character Set Identifier
CGI	Common Gateway Interface
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRMF	Certificate Request Message Format
DCM/400	Digital Certificate Manager/400
DDM	Distributed Data Management
DN	Distinguished Name
DNS	Domain Name Services
DRDA	Distributed Relational Database Architecture
DSS	Digital Signature Standard
EBCDIC	Extended Binary Communication Data Interchange Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines Corporation
IETF	Internet Engineering Task Force
ILE	Integrated Language Environment
IP	Internet Protocol
ITSO	International Technical Support Organization
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
ODBC	Open Database Connectivity
OPM	Original Program Model
OS/400	IBM Operating System/400
PKI	Public Key Infrastructure
PKCS	Public Key Cryptosystem
RA	Registration Authority
RFC	Request for Comments
SSL	Secured Socket Layer
TCP/IP	Transmission Control Protocol / Internet Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Networking
X.500	ITU and ISO Directory Service Standard
X.509	ITU and ISO Digital Certificate Standard

Index

IBM Redbooks evaluation

AS/400 Internet Security: Developing a Digital Certificate Infrastructure
SG24-5659-00

Your feedback is very important to help us maintain the quality of IBM Redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.ibm.com/
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?
_ Customer _ Business Partner _ Solution Developer _ IBM employee
_ None of the above

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction __________

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

____

____

____

____

What other Redbooks would you like to see published?

____

____

____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

____

____

____

____

____

SG24-5659-00

Printed in the U.S.A.

AS/400 Internet Security: Developing a Digital Certificate Infrastructure

SG24-5659-00