How to Prepare Your Salesforce Service for Certificate Changes

Salesforce, Spring '16

@salesforcedocs

Last updated: April 27, 2016

CONTENTS

HOW TO PREPARE YOUR SALESFORCE SERVICE FOR CERTIFICATE CHANGES

Preface

We've created this document to explain the Salesforce certificate changes methodology, and to give you greater control over when and how you prepare for Salesforce certificate changes.

Since the official Summer '13 launch of Salesforce Communities, we have put all of our certificate changes in a single group, the Certificate Changes group, where we can communicate directly with you. This document, which you probably found by visiting that group, serves a similar purpose: It provides more transparency about certificate changes to maximize your success with our service.

Certificate Changes Overview

To secure the data that your organization sends over the Internet, Salesforce follows the industry best practice of encrypting connections to our service with SSL certificates.

When SSL certificates are correctly coupled with the root certificates issued by certificate authorities (CAs)—and any intermediate certificates needed to secure the SSL certificates—they serve the dual purpose of encrypting your user data, and presenting a *chain of trust* that browsers and intermediate applications can use to verify that you are connecting to the Salesforce servers directly and securely. A single chain of trust is formed from three types of certificates, in the following order: a root certificate, several intermediate certificates, and a Salesforce certificate.

Here's how those certificates are used with Salesforce.

1. Salesforce uses its own private key, which is available to only Salesforce, to generate a secret key for each connection that you make to the Salesforce servers.
2. This secret key is in turn used to generate a public key, or certificate, that is immediately available to any device or application connecting to the Salesforce infrastructure. Your connecting device or application can use the public certificate to negotiate per-session security tokens with the Salesforce servers, and compare the certificate with the Salesforce session credentials to verify that both the certificate and the credentials are generated using the same private Salesforce key.
3. The public certificate is then signed by a well-known CA's private key, allowing your application or device to verify both that the certificate is valid, and that your application or device is attempting to connect to what actually are the Salesforce servers. This initial, public certificate, which is also called a *Certificate Authority root certificate*, is distributed in almost all modern browsers and SSL implementations. By comparing the signatures in the Salesforce public certificate with those in the CA root certificate, your application or device can determine that the Salesforce certificate is generated from the CA's private key. If your client trusts the CA's public root certificate, you can know that the Salesforce certificate is issued through that CA and is valid property of Salesforce.
4. Because the CA must secure the root certificate, possibly add new functionality to it, and sometimes factor in additional considerations, it does not sign root certificates directly and with its own keys. Instead, it signs and creates intermediate certificates, a series of certificate-private key pairs that sign the next certificate in their chain, until finally signing the Salesforce certificate-private key pair.
5. To complete the chain of trust, Salesforce provides the intermediate CA certificates and gives each of them its own Salesforce certificate for each Salesforce session. The client browser or device verifies the chain of trust, going through the chain's certificates until it reaches the well-known and trusted CA root certificate credentials that are distributed with most browsers and SSL client implementations.

6. This chain of trust framework is generally referred to as the *public key infrastructure (PKI)*. By comparing the credentials of the certificate materials provided by Salesforce with the well-known and trusted CA root certificate credentials, the PKI can verify that it is connecting to your application or device directly and securely.

Why We Change Our Certificates

Salesforce changes its certificates for several reasons.

1. CA-provided SSL certificates are configured for a limited duration, and we must change these certificates before they expire.
2. Sometimes, we must change the certificates applied to Salesforce's instances to provide new product features and support new security technologies.
3. Although none of the following have occurred before, flaws discovered in the PKI, a suspicion of leaked PKI material, or similar issues that would compromise the security of customer data would require an immediate, emergency change of almost all Salesforce certificates. In these situations, we cannot guarantee that we would follow all of the guidelines presented in this document.

How Locally Cached Certificates Affect the Chain of Trust

Some of our customers have deployed infrastructure or middleware that inherently does not trust the Salesforce PKI, or its well-known and trusted root certificates.

Instead, this infrastructure or middleware requires that all intermediate certificates and the CA's root certificates be stored locally on the customers' own devices, and that the chain of trust presented by Salesforce match the customers' locally cached certificates. Other implementations might cache the well-known and trusted root certificates on a runtime basis, storing them and all intermediate certificates in memory so that a new chain of trust does not need to be presented for each new connection. In these cases, the device or application makes its certificate comparisons using the cached certificates from its initial connection to Salesforce.

This practice of caching certificate information locally creates problems when the Salesforce infrastructure certificates change. Because the Salesforce infrastructure certificates check the connections against a locally cached chain of certificates instead of against the live PKI, a change in the certificate credentials offered by Salesforce makes the connection seem insecure and invalid, even though the certificate chain itself might be valid.

In order to accommodate the needs of customers who do locally cache certificates, we attempt to provide as much advance notification of upcoming certificate changes as possible. This document gives customers whose infrastructure or middleware cannot use—or is deliberately configured not to use—the conventional SSL PKI greater control over how they prepare for Salesforce certificate changes.

When We Change Our Certificates

We try to keep certificates for a given security application valid for the longest reasonable time period, which is usually three or four years.

Because the SSL public key infrastructure is mostly transparent, and because Salesforce certificate changes are generally seamless, we hadn't originally scheduled certificate changes during maintenance windows or announced our certificate changes in advance.

As the use of middleware and API implementations has made Salesforce certificates changes more difficult for customers, we have tried to provide as much advance notice about these changes as possible. We aim to tie certificate changes that are more likely to affect customers with these implementations to Salesforce's major release cycle, which we also use for certificate changes to the primary instances and changes to outbound proxy (proxy.salesforce.com) certificates. This scheduling helps us give you the most seamless Salesforce experience possible.

In the past, we had been scheduling primary certificate changes independently of intermediate certificate changes, which had been causing bugs in certain OS-browser combinations. From now on, we will we be making both types of certificate changes at the same time.

Whenever possible, we roll certificate changes out to sandbox instances before rolling them out to production instances, especially when those changes accompany major changes to product functionality or certificate structure. So that you have time to test and prepare for changes that might appear in your production environment, we aim both to give you a minimum of 30 days' notice before the production rollout and to schedule that rollout at least 10 days after the sandbox rollout. With bigger certificate changes, we try to give even more than 30 days' notice before the production rollout.

How We Announce Certificate Changes

Our new notification process is simple: We aim to publish new certificates to the Salesforce Community's Certificate Changes group 30 days before your certificates need to be renewed.

If you have a Salesforce login, you can join the Certificate Changes group and subscribe to email notifications for it.

How to Prepare for Certificate Changes

You can find your current certificate information by looking at the connection settings in your browser or by using the command line in the OpenSSL toolkit.

If you use pre-placed certificate implementations, you probably used one of these methods initially to obtain the copies of the certificates that you used in your implementations. We recognize that the people who originally set up these implementations might not be available to manage certificate changes, or even identify if their company is using pre-placed certificate implementations, which is part of why we're improving our certificate changes notification process.

If you connect to Salesforce using standard Internet browsers, you will most likely never notice certificate changes or need to verify that you have the current Salesforce certificates. However, if you use certain types of middleware or API configurations, you might need to plan ahead to avoid service disruptions.

Middleware and the API

If you use middleware or an API implementation that depends on pre-placed keys, you might experience service disruptions when Salesforce certificates change.

The TIBCO® middleware products are an example of this middleware. In most cases, when TIBCO users both receive advance notice of Salesforce certificate changes and pre-publish the new certificates, they can pre-place the new certificates in the trusted certificates store and avoid service disruptions.

Note: The TIBCO middleware requires that the entire certificate chain of trust, including the CA root certificate, be installed in the trusted certificate store.

If you use certain Java API implementations, you might experience similar issues because of the caching associated with certain versions of Java. In most cases, reloading the API integration also re-caches the new certificate chain of trust and solves the problem.

Integration Considerations

When setting up a new integration, try to identify—or have your integrator identify—if your implementation requires pre-placed or cached certificates.

If your implementation does require pre-placed or cached certificates, you might need to add the new Salesforce certificates before the existing certificates change or prepare to restart your environment after they change, depending on your implementation.

To ensure a consistent Salesforce experience, we recommend avoiding integrations that cache certificates.