

Cisco Registered Envelope Service

Simplified Messaging Security through a Cloud-Based Encryption Service

The Cisco® Registered Envelope Service is the most advanced cloud based-encryption key service available today. Whether you need to meet compliance requirements, secure customer and partner communications, or protect intellectual property, the Cisco Registered Envelope Service provides a flexible and scalable solution to help you support your secure messaging requirements without having to invest in additional infrastructure.

Although regular emails are not a secure communication medium, encryption and key management is often seen as too complex to be used in everyday communications. The Cisco Registered Envelope Service takes away the complexity behind encryption and makes it seamless for senders and recipients to exchange secure messages.

The Cisco IronPort Difference

Cisco IronPort® email and web security products are high-performance, easy-to-use, and technically innovative solutions, designed to secure organizations of all sizes. Purpose-built for security and deployed at the gateway to protect the world's most important networks, these products enable a powerful perimeter defense.

The Cisco IronPort line of appliances is smarter and faster in part because they take advantage of Cisco Security Intelligence Operations center and global threat correlation. This advanced technology enables organizations to improve their security and transparently protect users from the latest Internet threats.

Features

Secure Delivery Methods

The Cisco Registered Envelope Service offers a wide range of options for secure message delivery, and can support any email encryption requirement.

Cisco IronPort Encryption is a highly secure, envelope-based "push" technology that combines universal reach, ease of use, and the lowest total cost of ownership (TCO) of any email encryption technology. Encrypted messages can be received by any email user - independent of the email client, the operating system, or the device used - without the need to install any software or requiring the sender to preexchange encryption credentials with the recipients.

Business-Class Email

In addition to securing email content, Cisco IronPort Encryption technology enhances visibility and control over email.

Guaranteed read receipts enable users to know exactly when a message was viewed by each recipient.

Message expiration and recall prevents mistakenly sent messages from being opened and automatically secures old messages. The message may be recalled at any time, keeping the message from ever being opened again.

Authentication and key delivery typically occurs by identifying user credentials. When a recipient has been successfully authenticated, the key for that message is released and the recipient gets access to the message.

Enrollment management is enabled for first-time recipients as they are guided through a single-screen enrollment to create an account on the key server. This account may be used to receive any future messages.

Security Assertion Markup Language (SAML) 2.0 gateways integration is an advanced feature enabling organizations that have implemented an identity gateway to use their existing investment with Cisco Registered Envelope Service. Recipients of an encrypted envelope will be able to use their corporate credentials to authenticate with and decrypt the message automatically. This integration removes the need for first-time recipients to create a new account on the service and makes it very easy to access secure messages using their corporate username and password.

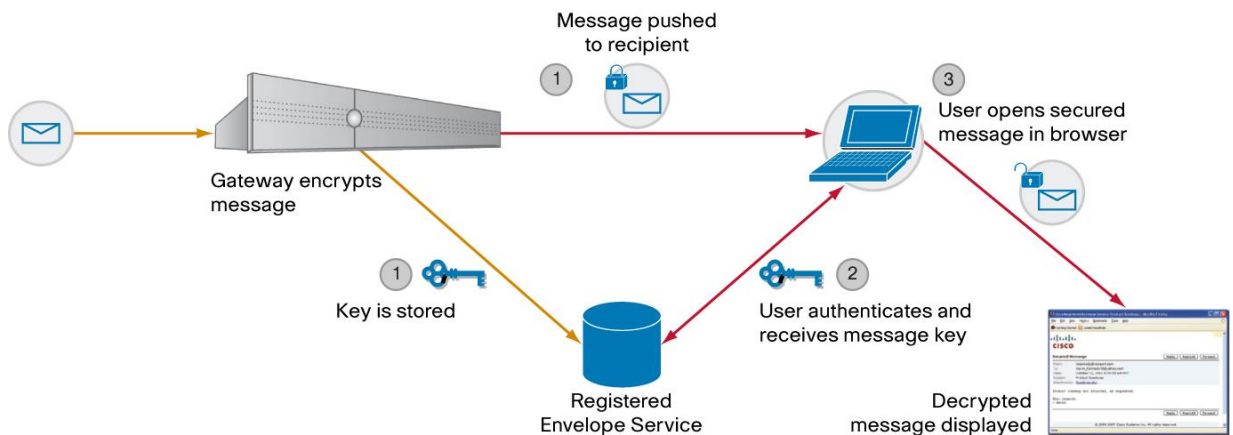
Universal device support guarantees that secure messages can be read by any recipient regardless of the device they use to open the message. Dedicated plug-in applications offer an enhanced user experience for Microsoft Outlook and on Apple iOS and Google Android smartphones.

Message management is provided as part of the business-class email features and includes message recall and expiration and guaranteed read-receipt. These features can be accessed through the Cisco Registered Envelope Service web interface or directly from the email client by installing dedicated plug-ins.

Hosted Key Server

The Cisco Registered Envelope Service manages recipient registration, authentication and per-message encryption keys. Figure 1 shows how the Cisco IronPort Email Security Appliance and Cisco Registered Envelope Service interact. The Cisco Registered Envelope Service works with Cisco IronPort C-Series email security appliances, encrypting and decrypting messages based on policies defined on the Cisco IronPort C-Series.

Figure 1. Cisco Ironport Encryption Business Class Email Path



Benefits

Helps Ensure Compliance

Sensitive messages are handled in compliance with regulatory legislation, such as Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Personal Information Protection and Electronic Documents Act (PIPEDA), and the European Union Data Directive.

Uses a Federated Identity Gateway

Compatibility with SAML 2.0 gateways removes the need for new-recipient registration and enables users to use their corporate identity to decrypt secure messages.

Provides Business-Class Email

The powerful features enable a new class of email, with unprecedented visibility and control.

Fosters Customer and Partner Trust

Encryption raises the levels of service to customers and partners, exemplifying Cisco's commitment to keep business transactions and communications confidential.

Protects Intellectual Property

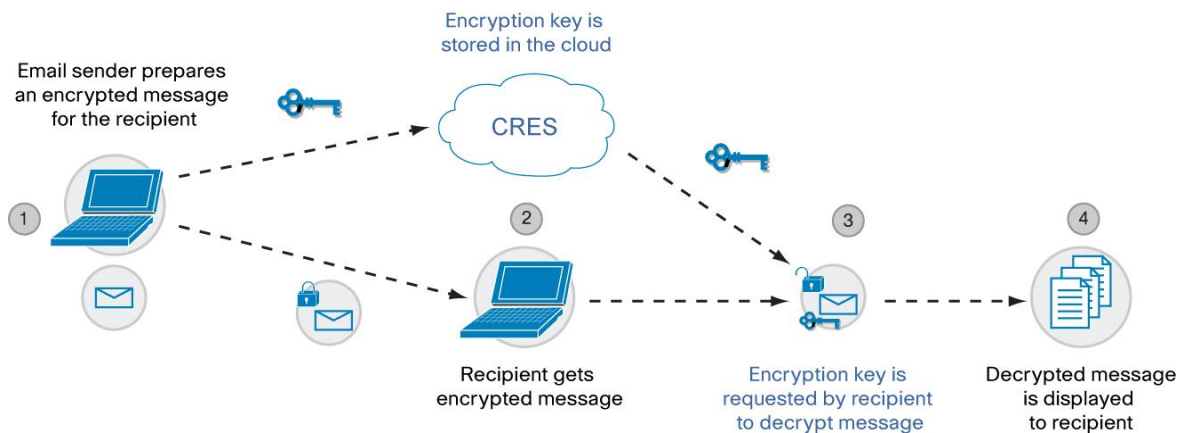
This solution safeguards sensitive business information and intellectual property contained in email outside the firewall - both in transit on the Internet and in storage on destination email servers.

Improves Customer Service

Organizations can communicate securely with customers using the channels that they prefer.

The Cisco Registered Envelope Service provides a turnkey, enterprise-class email encryption solution without the need to deploy new hardware. Multiple secure delivery methods offer the flexibility to meet diverse business needs, while integrated management and authentication simplify deployment. Figure 2 shows how simple it is for users to send and receive an encrypted e-mail.

Figure 2. Cisco Registered Envelope Service: Turnkey Email Encryption Solution



Deployment

The Cisco Registered Envelope Service works with Cisco IronPort C-Series email security appliances, encrypting and decrypting messages based on policies defined on the Cisco IronPort C-Series.

Summary

As demonstrated by many success stories, the Cisco Registered Envelope Service is the only cloud-based encryption key server flexible enough to meet the evolving secure-communications requirements of businesses today. Universal reach, flexible delivery methods, enterprise-class scalability, and business-class email features enable expanded use of the Internet as an efficient, reliable, and low-cost channel of secure communication.

For more information: [Supporting Multiple Brands on the Cisco Registered Envelope Service \(CRES\) Datasheet](#)



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)