ENTRUST

Entrust S/MIME Solution FAQs

What is an S/MIME certificate?

Secure/Multipurpose Internet Mail Extension (S/MIME) certificates secure email communication through end-to-end encryption and identify the sender via a digital signature. They are a standard for public key encryption and signing of MIME data.

With S/MIME certificates, recipients of an email can identify where the email came from, so employees can verify that the email came from a CEO, CFO, or other member within the organization and can trust the "From" address of the email.

What is included in the Entrust S/MIME Certificate Solution?

When we refer to our S/MIME "solution," we are referring not just to our Entrust S/MIME certificates, but also integrated automation features from our technology partner, Sixscape Communications, including:

- **Secure Mail Module:** A security add-in for popular email clients for certificate-based digital signing and encryption of emails
- **Key Escrow Module:** Enables authorized third parties to recover stored keys to decrypt data and enable security and compliance requirements
- **Secure Large File Transfer:** Provides the end-user with the ability to securely transfer large files to intended recipients using S/MIME technology
- **Mobile Device Management Module:** Allows for delivery of keys and certificates to user's mobile device
- **Retrocrypt Module:** Provides the ability to globally or selectively encrypt legacy email in folders as well as new incoming email

Sixscape

Learn more about Entrust S/MIME certificates at entrust.com

What dangers can organizations experience from email attacks?

There are two types of email hacking activities:

- **Phishing:** When generic messages are delivered to a wider pool of potential victims
- **Spear phishing or business email compromise (BEC) attacks:** Specific and planned targeted attacks to an individual or a group; these attacks aim to:
    - Extract sensitive information
    - Install malware onto the network
    - Wire money to accounts that belong to the attackers

How big of a threat are business email compromise (BEC) attacks?

BEC attacks have been exploding in recent years, moving across geographies and business sectors. According to the most recent FBI Internet Crime Reports (ICRs), organizations in the U.S. lost $6.4 billion to BEC attacks from 2014 to 2020 – with $1.8 billion of that in 2020 alone.*

What are the risks/costs associated with NOT securing emails?

The biggest risk to an organization not securing their emails is that it leaves them vulnerable to email hacking activities (mentioned earlier), which can result in theft of their intellectual and capital property as well as damage to their brand and erosion of customer trust.

There are also certain compliance risks that organizations can face depending on their sector or jurisdiction in which they do business. For example, in the U.S., the Health Insurance Portability and Accountability Act (HIPAA) requires that organizations protect sensitive patient health information from being disclosed without a patient's knowledge or consent. According to the U.S. Department of Health and Human Services, HIPAA violation costs in 2020 alone were $13 million.

In the European Union, the General Data Protection Regulation (GDPR) guidelines state that personal data must be fully protected, and if it's not, organizations can be subjected to fines of up to 4% of their preceding year's revenue or up to 20 million euros.

* FBI Internet Crime Reports 2014-2020

Entrust S/MIME Solution FAQs

How can S/MIME certificates help reduce an enterprise's attack vector?

S/MIME certificates can help reduce an enterprise's attack vector by providing:

- **Identity:** Entrust S/MIME certificates provide identity by enabling employees to digitally sign emails so recipients know that the email is coming from an employee of the organization. Emails that are digitally signed by an employee can be trusted to come from the stated source and provide assurance that the content hasn't been modified during transit.
- **End-to-end encryption:** Entrust enables employees to encrypt emails, making the theft of encrypted emails without access to the private keys useless to an attacker. Entrust's end-to-end encryption is inherently a stronger form of security compared to gateway encryption.

Why has it been difficult for organizations to deploy S/MIME certificates?

Even though email is an essential business tool and S/MIME and PKI have been around for decades, S/MIME historically has had a very low adoption rate in an enterprise context.

Some of the biggest challenges have been that S/MIME certificates are often costly and time-consuming to deploy and manage because there are many manual steps that make it hard for enterprises to scale without significant IT and employee support. Plus, many employees have multiple devices and computers, and the same S/MIME certificate needs to be installed across all of them, making the IT and employee burden even higher.

If enterprises follow best practices by encrypting their emails to protect their data, employees will get locked out of their emails (just as a bad actor would) if their private key gets lost. This requires the retrieval of those keys in a secure way and reprovisioning the employee device.

Entrust has partnered with Sixscape to provide a solution that can provide both automation and private key escrow capabilities. It "checks all of the boxes" and allows organizations to deploy to a large enterprise within seconds, minutes, and hours as opposed to days, weeks, and months.

Are Entrust S/MIME certificates easy to install?

Yes. Our centralized and decentralized one-time deployment gives network teams the ability to deploy on behalf of end-users within minutes or support a self-service end-user model, regardless of the number of users.

Does the Entrust S/MIME solution provide protection across multiple devices?

Yes. It supports a scalable deployment of email encryption and identity within your organization – across multiple devices such as desktops, laptops, tablets, and mobile phones.

Entrust S/MIME Solution FAQs

Will the Entrust S/MIME solution protect our employees from phishing emails from third parties?

Yes. By enabling S/MIME internally and externally, phishing emails can be mitigated because emails exchanged between both parties will be digitally signed. Furthermore, the digitally signed email with an Entrust certificate can be trusted by any party.

As an employee, is it possible to get a solution that can be used for both email signing and email encryption?

Yes. When requesting an S/MIME certificate on your device, you can specify signing, encryption, or dual-purpose certificates. If you need to digitally sign to support non-repudiation, choose signing certificates.

As an IT administrator, can I recover an employee's private key if it becomes lost or the employee leaves the organization?

Yes. The Entrust S/MIME solution includes a Key Escrow Module that enables authorized third parties to recover stored keys to decrypt data and enable security and compliance requirements. The private key of each end-user remains on the device and is non-exportable. However, during the deployment process the private key is escrowed to an encrypted file format that can be integrated with an HSM if required. This also prevents employees from potentially extracting the private key from the system and saving it for their own use after leaving the organization.

As an IT administrator, can I deploy email encryption and identity across multiple devices for each employee?

Yes. The Entrust S/MIME solution deploys to desktops, laptops, and corporate-issued mobile devices seamlessly by leveraging popular mobile device management (MDM) solutions. For encrypted email, employees can have the same secure email credentials (digital identity) in each of their devices used for email. The user can access their encrypted email anytime, anywhere.

Entrust S/MIME Solution FAQs

As an IT administrator, can I encrypt legacy email that is currently in the clear or incoming email that is not encrypted?

Yes. The Entrust S/MIME solution can automatically encrypt users' old, unencrypted emails with the private keys of the user's respective S/MIME certificates at time of deployment. This ensures a stronger security posture because all previous/legacy emails are signed and/or encrypted with the new certificate and private key. Furthermore, with all emails in the email server encrypted, emails can no longer be read by unauthorized entities, reducing unnecessary access to confidential information in emails.

As an IT administrator, can I enable employees to exchange files securely without impacting file size limits?

Yes. We made secure large file transfer easy to reduce the risk of employees using unapproved software to send large files. With the Entrust S/MIME solution, users can send protected files without the need for Zip files or passwords. Automated recipients' certificate selection and built-in file compression enable users to securely share large files and send to any number of internal or external recipients.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223