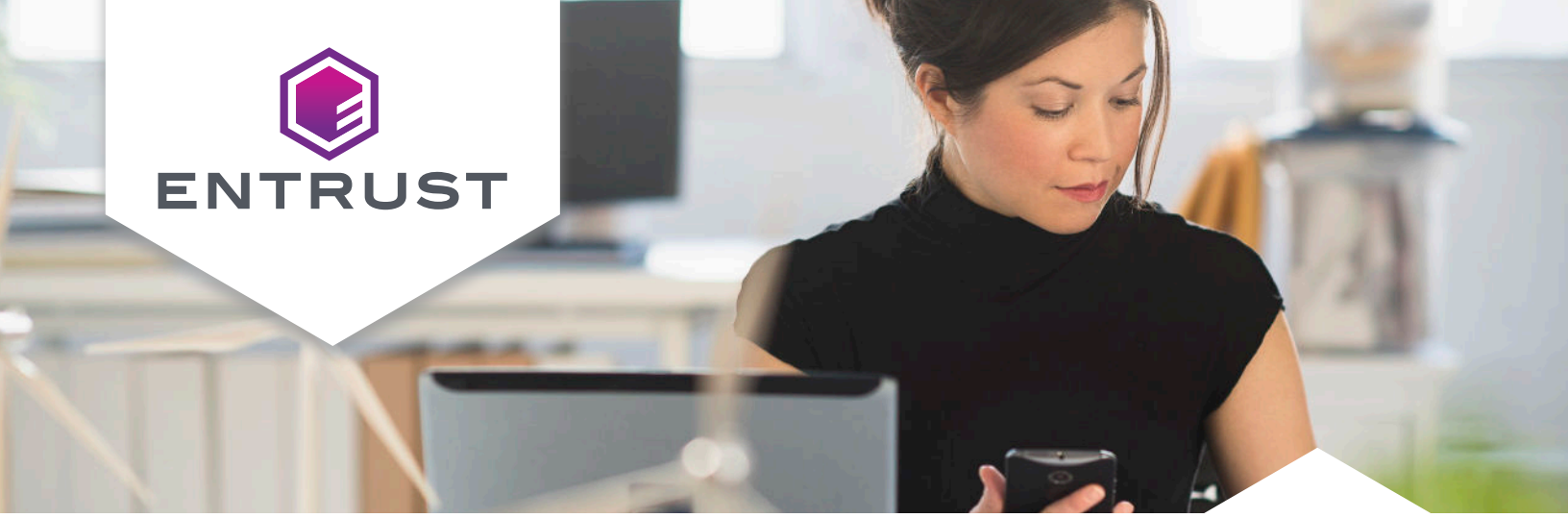

Entrust Secure Email Certificates for Enterprise

Fully automated S/MIME certificate deployment at scale

Market Challenge

Email hacking that results in theft of intellectual and capital property as well as damage to the business and brand is very common nowadays. Phishing tactics have become more sophisticated and effective at tricking their targets. So it's more critical than ever for organizations to adopt digitally signed and encrypted email technology to secure their email communications and protect their integrity.

New automation capabilities from Entrust remove the complexities that once hindered S/MIME deployment and adoption within enterprises.

Solution

Entrust Secure Email Certificates provide organizations with a capability to dramatically reduce the risk of company data loss originating from email. Entrust's identity and end-to-end encryption capabilities supported for internal and external emails, together with the deployment automation and lifecycle management capabilities, enable organizations to improve their compliance and security posture relative to other solutions.

BENEFITS

- For enterprise use and scalable in any industry
- Centralized and decentralized automated one-time deployment
- Automatic backup/restore with full key history and escrow, including MofN and HSM integrations
- Silent certificate renewal for set and-forget deployment and easy compliance
- Secure deployment to desktops and personal devices using the same key and certificate(s)
- Secure large file transfer using S/MIME technology
- Retrospective encryption of an organization's legacy emails
- S/MIME certificates that secure email, support large file transfer and the retrospective encryption use cases
- Separation of signing and encryption capabilities in an S/MIME certificate to support non-repudiation
- Seamless self-service platform for SaaS-based end-user enrollment
- Centralized management via Entrust Certificate Solutions platform
- Certificates can be issued from our public trust CA or our private cloud based CA, PKI as a Service

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

Entrust Secure Email Certificates

Features

Centralized and decentralized automated one-time deployment.
The network team can use Microsoft SCCM to deploy S/MIME certificates on behalf of end-users, and end-users can deploy S/MIME certificates on their personal devices through a self-service model through the receipt of a link from the network team.

Automatic backup/restore with full key history and escrow.
Maintains access to historical emails through automated, full-key history backup and restoration capabilities. Whether it is a forgotten password, destroyed private key, or a normal renewal process, a user can always restore their full key history with a single request managed by the organization's IT administrator.

Complete email protection in real time and retroactively. The Entrust S/MIME solution encrypts all organizational emails that were received or sent in the past, as well as future incoming or outgoing un-encrypted emails.

Real-time reporting and monitoring. Avoid expired S/MIME certificates. The solution monitors and manages S/MIME certificates and prompts users to renew when their certificates are close to expiry.

Seamlessly secure email on all user devices. Entrust provides integration points to major mobile device management solutions, which allows for delivery of keys and certificates to users' mobile devices.

Send encrypted large files to multiple recipients from any device. Simplify the user experience by enabling users to send large documents securely without the need for zip files or passwords. Automated recipients certificate selection and built-in file compression enables users to securely share large files and send to any number of internal or external recipients.

Organization validation. Entrust Secure Email Certificates for Enterprise confirm the name of the organization, name of the individual, and email address of the individual, enabling employee emails to be distinguished from SPAM or phishing attacks.

Certificate revocation. Entrust's enterprise certificates give administrators the ability to revoke employee digital IDs upon departure, ensuring they can no longer digitally sign as an employee – a key security feature for today's organization while still supporting access to encrypted email through key escrow.

Directory service integration. Compatible with most of the popular directory services – such as Active Directory, LDAP, and G-Suite Directory – to automatically synchronize the S/MIME certificates of your contacts.

Multiple platform support. Entrust's email security is seamless across multiple platforms and devices. Supports Microsoft Windows, Mac OS X, iOS, and Android platforms.

Private SMIME via PKI as a Service (PKIaaS). Issuing certificates through our private-cloud-based CA, PKIaaS, provides authentication and end-to-end encryption of private email communications, with a fully automated deployment of S/MIME certificates and lifecycle management at scale.

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

Entrust Secure Email Certificates

Features	Entrust Secure Email Certificates
Term length	1, 2, or 3 years
Validation	Name, email address, domain, organization
Centralized management to Entrust Certificate Solutions platform	✓
Automation capabilities	✓
One click to request and deploy S/MIME certificates	✓
Digitally signed and encrypted emails	✓
Support for Active Directory	✓
Support for desktop, mobile phones, and tablets	✓
Automated certificate renewal	✓
Plug-in for email clients	✓
Secure backup, recovery, and escrow	✓
Compliance-centric deployment	✓
Retrospective email encryption	✓
Prospective email protection	✓
Secure large file transfer	✓
Share files to multiple recipients	✓
Separate encryption and signing profiles	✓

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

Entrust Secure Email Certificates

Perfect for enterprise use cases

Based on proven industry standards, Entrust Secure Email Certificates are for organizations that require secure email encryption with historical access to emails. These certificates provide the capability to digitally sign emails to prove the attachments and content originated from the sender's email address and haven't been modified. They include validation of the organization, email domain, and end user, offering the higher ID assurance level that organizations require.

Help maintain compliance

Entrust S/MIME Email Certificates comply with various confidentiality regulations related to healthcare, education, government, military, financial, and other consumer sectors.

The Entrust advantage

Verified trust
Ensure email communication is secure with digital identities that include independent verification of organization and email domain – all completed on an organization's behalf by Entrust.

Industry-leading PKI
Our public certificate authority (CA) and PKI as a Service are based on industry-leading public key infrastructure (PKI), which was developed by Entrust's world-class cryptographers and software developers.

Centralized certificate management or cloud-based management
Regardless of the type of certificates in use, leverage Entrust Certificate Services to oversee your inventory of public and private TLS/SSL, and digital signing certificates.

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com