SECTIGO

Secure Email Certificates (S/MIME)

Overview

Posing as legitimate employees, servers, or devices, hackers can utilize email to infiltrate an organization's digital infrastructure and wreak havoc on its business — potentially resulting in theft of intellectual property and capital as well as damage to the business and brand. You can combat these potential attacks by signing email using **Sectigo S/MIME Email certificates**.

BUSINESS EMAIL COMPROMISE ATTACKS

78,000

Incidents of Fraud

$12B

in corporate losses

Hackers target weak points in an organization's email infrastructure using several common tactics. Business Email Compromise (BEC) is a sophisticated type of scam targeting companies that regularly perform wire transfer payments with suppliers. Hackers disguise themselves as known suppliers using spoofed email addresses in order to dupe companies into wiring funds to them instead of the real recipients. Between October 2013 and May 2018, there have been an estimated 78,000 fraud incidents of this type worldwide — causing upwards of $12 billion in corporate losses. By requiring email communication with suppliers and vendors to be certificate-signed from their true sources, companies can radically decrease their exposure to BEC attacks.

The interception of unencrypted email is another method hackers use to steal sensitive information. By sending essential documents and information unsecured through the internet, users expose these properties to interference by malicious actors — which can result in the loss of business secrets or employee personally identifiable information (PII), reputational damage to the company, and legal exposure.

Additionally, hackers can use the simple strategy of bombarding employee inboxes with malware and phishing attacks to infiltrate a company's digital infrastructure or gain access to assets. Without a Secure Email Gateway in place, it is easy to slip malicious messages into employees' mailboxes.

With Sectigo S/MIME (Secure/Multipurpose Internet Mail Extensions) Email certificates, companies can protect themselves against attacks by rogue actors. Automatically installed into all mail clients, the public S/MIME certificate adds a layer of defense by encrypting emails both in storage and in transit. The encryption key archive is accessible to the secure email gateway, signing, encrypting, and decrypting emails at the gateway. Utilizing publicly trusted digital signatures, Sectigo is the only company that delivers this capability.

Through a slew of sophisticated security features, Sectigo S/MIME Email certificates give users the confidence they need to trust their digital correspondence and help their companies thrive. S/MIME Email certificates:

- Automatically encrypt and decrypt emails.
- Display encryption via blue lock symbol in popular email programs.
- Tell users emails are authentic and unmodified via check mark icon.
- Decrypt incoming attachments.
- Automatically encrypt replies.
- Encrypt all sent attachments.
- Deliver the same experience as plain text email.
- Utilize the same email repository and search.

Throughout the fall of 2018, Sectigo SMIME Email certificates provide a seamless means of adding the digital signatures needed to fight Business Email Compromise fraud. By December 2018, Sectigo will implement updates that remove the need for users to back up their encryption key on a USB drive. And by March 2019, this tool will become compatible with all mobile devices and secure email gateways.

Consolidation of Certificate Management

Offering a single management console for all enterprise identities, Sectigo S/MIME Email certificates are available alongside public SSL, Code Signing, and private certificates. By scanning servers using an SSL handshake and searching the active directory for Microsoft CA issued certificates, Sectigo Certificate Management automatically discovers existing certificates.

With automated enrollment and renewals, certificates are renewed without the need to manually manage the task — reducing cost and the risk of outages due to human error. And with Sectigo's predictable fee and the ability to issue certificates for temporary projects, we can help your company grow. While other venders don't offer public and private certificates in the same console, Sectigo Certificate Management stands alone in offering an unlimited enterprise license.