SECTIGO

AN E-BOOK ON THE VALUE OF S/MIME

Ensuring Compliance Through Email Certificates

SECTIGO

Table of Contents

Introduction

Email is a must. But email is a vulnerability.

Businesses across all industries depend on email as an indispensable communication medium. However, mail messages and attachments can be spied upon, altered, or faked, opening the door to a variety of attacks that can result in the loss of industries secrets, confidential customer information, or money from the company's accounts. This exposure can furthermore put your enterprise in jeopardy of noncompliance with mandatory regulatory requirements.

Fortunately, you can combat these attacks and enable compliance by protecting email communication with digital certificates. S/MIME (Secure/Multipurpose Internet Mail Extension) certificates address these problems inherent in the email technology paradigm and improve your institution's protection against spying or social engineering attacks that depend on email.

S/MIME email certificates improve the security profile of your email communications in three ways:

- **Authentication of sender.** Each S/MIME email certificate includes the sender's authenticated email address, giving receivers a mechanism to confirm that requests for information, wire transfers, or other actions are genuinely from authorized parties.

- **Encryption of email content and attachments.** Sending and receiving mail clients are enabled for encryption and decryption of email content (including attachments) if certificates are in place. That prevents malicious software from intercepting email communication in transit and reading its contents.

- **Assurance of integrity.** If a signed email or its attachments are altered in any way, it will fail validation and the user will be warned by the email client.

"One in every 100 emails is a hack attempt."

- **ZDNet, September 2018**

In this eBook you will learn:

- What Business Email Compromise is and how S/MIME email certificates can help defend against BEC and related spear phishing attacks

- How email certificates contribute to compliance with key regulatory requirements including,
  - HIPAA/HITECH
  - GDPR
  - DFARS (Defense Federal Acquisition Regulation Supplement)

Defending Against Business Email Compromise and Other Spear Phishing Attacks

Recent years have seen the rapid rise of spear phishing attacks aimed at corporate or government entities. These attacks depend on the use of counterfeit emails to trick employees into divulging sensitive information or taking other actions that benefit the spear phisher at the company's expense, including wire transfer of money to criminal accounts.

One basic attack involves sending an email to an employee of the organization with the ability to take the action the phishers ultimately want to occur. This email contains a spoofed header that creates the appearance it originated from someone inside the organization with the authority to require such an action. Phishers typically choose to imitate the CEO or President or another C-level executive and aim the communication at a lower-level employee asking for this action to take place. The content and layout of the email will reflect the look of ordinary email messages to the fullest degree possible.

Oftentimes the receiving employee will comply, believing the request to be a legitimate one from a senior member of the company who has the authority to make such a request. Common targets for spear phishing attacks include:

- Customer credit card numbers
- Employee W2 information
- Wire transfers to accounts controlled by phishers
- Industrial secrets

Another basic attack involves the installation of malware by following links to poisoned sites. In this attack emails pretending to be from trusted sources contain these links, and because employees trust the supposed senders, they wind up clicking on links and being exposed to the malware payload.

Business Email Compromise (BEC) is a specific flavor of spear phishing attack aimed at causing the target company to make a wire transfer of a large sum to a bank account controlled by the attackers. Typically BEC attacks come into a member of the finance department who has the ability to transfer money, such as someone in accounts payable. The message usually pretends to come from the CEO, the CFO, or another senior member of the finance department and instructs for this transfer to be made right away, with an emphasis on the request's urgency. Once the wire transfer occurs, the phishers quickly transfer the money to another account in a jurisdiction where it is difficult for the company or its local law enforcement to recover.

Using S/MIME email certificates across your organization defends against these spear phishing attacks by giving recipients the ability to confirm the true sender of an email. Employees are able to double check the origin of mail messages that seem suspicious or that request sensitive information.

"Health-related email requires end-to-end encryption."

HIPAA/HITECH Compliance

As in any industry, email is a critical communication medium for healthcare professionals. Left on its own, however, email is fundamentally insecure for transmitting Personal Health Information (PHI). Email containing PHI must be protected with digital certificates for institutions to successfully guard patients' privacy and maintain compliance with the HIPAA and HITECH regulations.

In particular, all health-related email traveling beyond the firewall requires end-to-end encryption, meaning that email is encrypted in the sending mail server, in all receiving mail servers, and in transit. This encryption prevents any party except the sender and receiver from viewing the content of the email, including the operator of the mail server or any malicious software that circumvents the established email controls. This approach works even with mail servers running in third-party cloud services.

Furthermore, encrypting email is a cost-effective method of meeting HIPAA's email retention requirements without compromising security. Since email content is encrypted prior to archiving, it is protected from disclosure regardless of the manner it is stored. And mail header information is still searchable within the mail application even for encrypted email, making it practical to retrieve emails according to specific criteria.

U.S. Federal Secure Email Requirements (DFARS) Compliance

S/MIME email certificates are a necessary part of compliance with DFARS (Defense Federal Acquisition Regulation Supplement) - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

For many years the United States government has been under constant cyberattack to steal intellectual property such as the designs of America's best military assets. As government agencies have improved their cyber defense, attackers have increasingly shifted focus U.S. defense contractors to gain access to information of strategic national importance. These attacks include stealing the weak credentials of employees to access contractor systems remotely and stealing the intellectual property stored in email, either in transit or stored on the mail server.

To remedy this situation, the government added section **252.204-7012** to the Defense Federal Acquisition Regulation. This regulation requires compliance with **NIST SP800-171** Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The regulation requires the encryption of all data at rest and in transit.

Certificate-protected email remains encrypted from the time it leaves the sender's machine until the time it is opened in the receiver's inbox, encrypting the data in transit across both

the internet and mail servers within the sending and receiving organizations. Furthermore, email messages and attachments that are stored on mail servers will also be encrypted while at rest.

GDPR Compliance

In 2016, the European Union adopted the General Data Protection Regulation (GDPR) to replace its 1995 Data Protection Directive with stronger and more modern data protection requirements. The GDPR is now recognized as law across the EU.

"GDPR penalities could cost organizations €20 million or more."

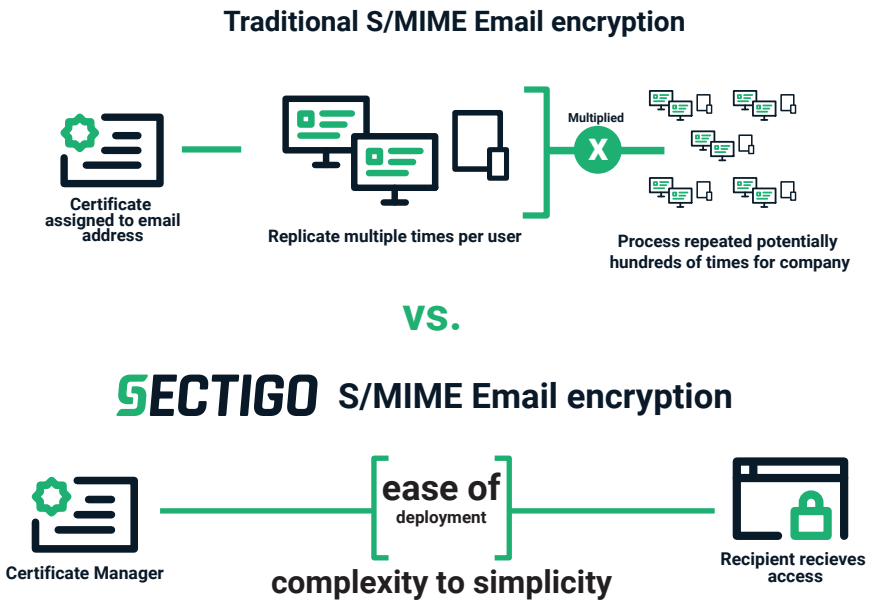
Article 25 of the GDPR requires data protection "by design and by default" for all business (IT) processes involving personal data. It is widely considered a best practice in most European nations to encrypt email containing sensitive personal data as a measure in following GDPR guidelines. Furthermore, as of January 1, 2019, Denmark will require businesses to encrypt all emails containing sensitive personal information. In determining the severity of the penalty for GDPR violations, authorities consider the degree to which offending companies took action to try to protect personal data. By taking action such as encrypting email, companies not only reduce the risk of data breaches in the first place, but in the event of a breach they also may mitigate their penalties by showing they implemented appropriate security measures to prevent data theft.

Under the GDPR penalties for loss, alteration, or unauthorized disclosure of data can range as high as four percent of global annual revenue or €20 million, whichever is greater. Because unencrypted email is readable by a number of parties including the enterprise IT administrator, the internet service

provider, and the cloud mail server provider, sending unencrypted email with individuals' personal or sensitive information may be illegal under GDPR.

Introducing S/MIME Email Certificates from Sectigo

Sectigo is the leading provider of strong digital identities using public key technology. These identities are valuable for a wide range of applications in the enterprise, from mobile device authentication in wireless networks to encrypting and digitally signing emails using the popular S/MIME standard. For effective compliance, email encryption must be invisible, easy for the administrator to deploy, and easy for the employee to use. Unfortunately, previous S/MIME solutions have been quite difficult, with the result that employees routinely fail to encrypt their email. This situation can lead to non-compliance even when a solution is in place.



This system provisions digital identities automatically to any application using traditional Windows or mobile devices. Many popular mail applications support S/MIME, so there is no need to change your systems or methods of working. Employees will have the ability to exploit the convenience of their tablets and mobile devices using the same mail applications they use today.

A single administrator console allows for the provisioning of both publicly trusted S/MIME certificates and private certificates dedicated to the exclusive use of the enterprise. The console allows for control over employee, server, and device enrollment. It effortlessly provides discovery, reporting, automated renewal without employee involvement, and revocation when the employee leaves.

For enterprises the console automatically adopts all previously issued certificates to dramatically improve deployment. The administrator can choose to replace these certificates automatically with publicly trusted S/MIME certificates. Public S/MIME allows for any S/MIME-capable mail application to validate both the sender's identity and the fact that the email and its attachments have not been altered in transit. Furthermore, the email certificate enables the encryption of both the email body and its attachments, all with no change to the end user's email experience.

To truly enable nearly 100% of emails to be encrypted, the solution adds these important features unavailable in previous S/MIME solutions:

- **Email certificate installation across the enterprise for multiple devices per user**
- **Sending the entire encryption key history to all mails applications so even older emails can be decrypted**
- **Hosting of an LDAP directory to aid compliance**
- **Encryption key archiving so employees can recover accidentally destroyed keys**
- **Interoperation with the secure email gateways (SEGs) so that the enterprise may still use mail scanners to perform their functions on encrypted and signed emails**

About Sectigo

Sectigo provides web security products that help customers protect, monitor, recover, and manage their web presence and connected devices. As the largest commercial Certificate Authority trusted by enterprises globally for more than 20 years, with more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs for securing today's digital landscape.
For more information, visit **www.sectigo.com.**

