SECTIGO

Email Certificates for GDPR Compliance

Enable Encryption and Identity Authentication for Greater Email Security with S/MIME Certificates

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.

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 higher.

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.

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 GDPR 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.

To solve this problem Sectigo developed the industry's first zero touch, X.509 certificate management system. This system provisions digital identities automatically to any application using traditional windows devices or mobile devices. Many popular mail apps support S/MIME, so there is no need to change what you do.

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. The console enables crypto-agility using renewal on demand, including the ability to increase the cryptographic strength of the identity.

The console automatically adopts all previously issued certificates to dramatically improve deployment, with the most popular being the certificates issued by the corporation's Active Directory Certificate Service. These certificates can then be automatically replaced by publicly trusted S/MIME certificates. Public S/MIME allows for any S/MIME capable mail application to validate the sender's identity and also that the email and its attachments have not been altered in transit. This is in addition to encrypting both the email body and its attachments, with no change to the unencrypted email experience.

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

- **Sending the entire encryption key history to all mails apps so even older emails can be decrypted**
- **Encryption key archiving so the employee can recover accidentally destroyed keys**
- **Interoperation with the secure email gateways so that the enterprise may still use mail scanners to perform their functions on encrypted and signed emails**

To learn more about how zero-touch S/MIME certificates can help you protect your business and meet federal compliance requirements, contact Sectigo today.