SECTIGO

A WHITEPAPER FROM SECTIGO

Zero Touch Email Certificate Deployment

Improved S/MIME Installation and Management for the Enterprise

SECTIGO

Using Certificates as a Defense Against Email-Based Attacks

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 enterprises in jeopardy of noncompliance with mandatory regulatory requirements.

Attacks like Business Email Compromise (BEC) or other spear phishing schemes take advantage of the inherently spoofable nature of email to trick employees into taking action that the spear phishers can take advantage of – to the detriment of the company suffering the social engineering attack. These scams may aim at gaining access, employees' PII, or other secrets. They might offer links to malware sites to infect computers in the enterprise. They may even trick employees into wiring money to accounts that appear to belong to suppliers or other partners but are really controlled by criminals.

Because of these vulnerabilities, regulations such as HIPAA/HITECH, GDPR, and the U.S. federal government's DFARS may require email encryption to maintain compliance or to minimize the consequences of a breach.

S/MIME (Secure/Multipurpose Internet Mail Extension) using Sectigo certificates address these problems that are inherent to the email technology paradigm and improve protection against spying or social engineering attacks that depend on email.

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

- **ZDNet, September 2018**

S/MIME email certificates 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.

The Problem of Adoption

For the user the certificate-enabled email experience is exactly the same as sending and receiving email without certificates in place. That means email certificates can offer a strong security benefit with no real downside for work processes or employee productivity. Nonetheless, adoption of S/MIME certificates for email in the enterprise has been very low for many years.

The primary cause of this low adoption has been the difficult and confusing process of enabling these certificates on email clients. End users have needed to, on their own initiative, acquire a trusted S/MIME certificate from a public CA and install it on their own system. The ideas and process behind email certificates aren't widely understood by the average enterprise employee, and since email clients continue to function even when certificates are not in place, user compliance with company guidelines for S/MIME deployment has been lacking.

Without end user adoption, an S/MIME strategy fails to provide the protection or compliance benefits detailed above.

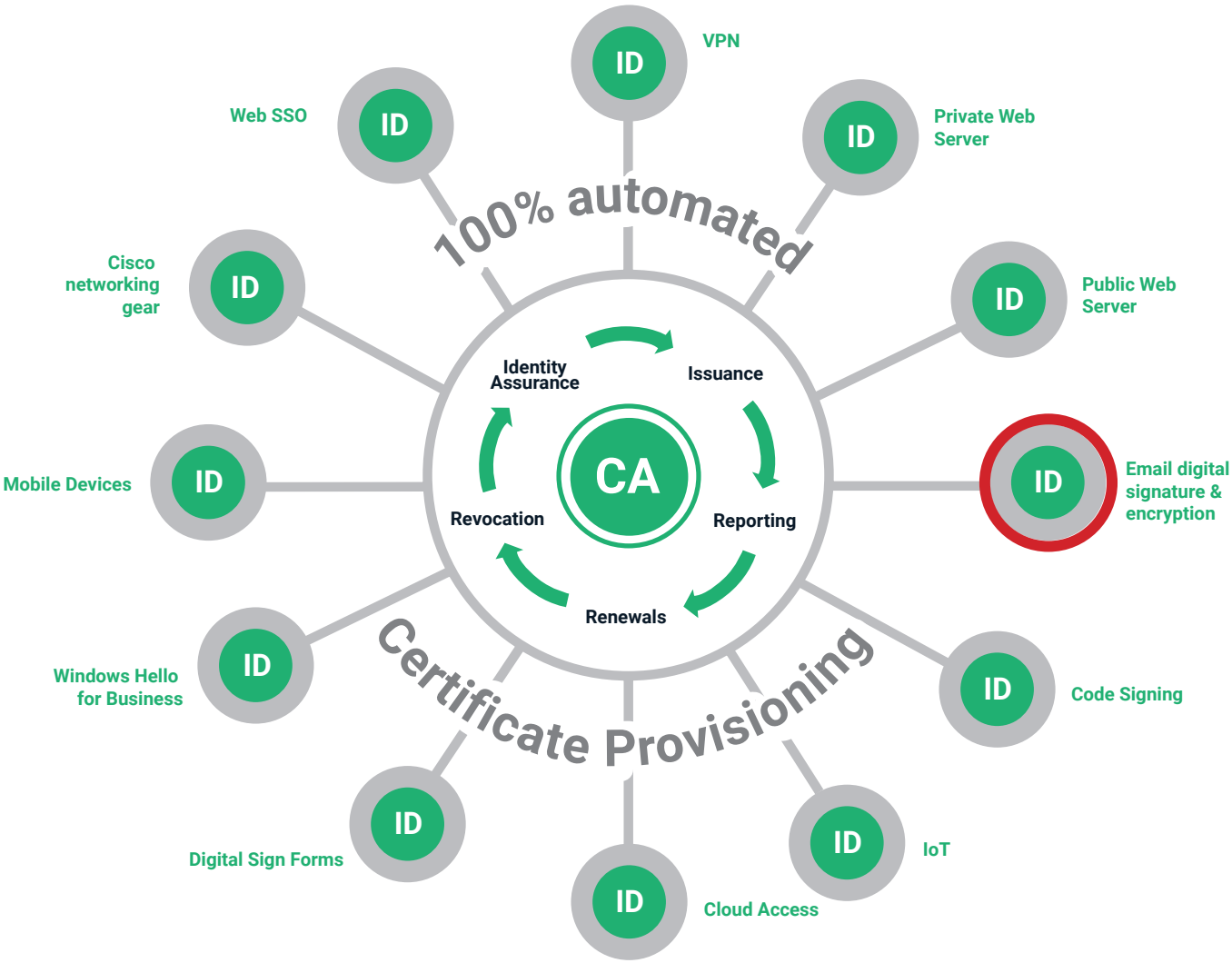
Sectigo has addressed this problem with the world's first zero-touch S/MIME adoption technology for enterprises. Zero-Touch

Zero-Touch deployment is designed to be invisible to the user, unlike traditional S/MIME certificate deployments, which place the burden on the user to participate in manual certificate and key management for desktop, mobile devices, and directory.

deployment is designed to be invisible to the user, unlike traditional S/MIME certificate deployments, which place the burden on the user to participate in manual certificate and key management for desktop, mobile devices, and directory.

The Sectigo S/MIME solution is a single application within the larger enterprise certificate management platform offered by Sectigo, providing a single pane of glass to all applications that consume certificates to enable their security features.

Solution Overview



S/MIME: Public or Private

Enterprises have the option to choose between publicly trusted or private S/MIME certificates.

- **Public S/MIME:** All certificates are issued from a common, shared issuing Certificate Authority. This common CA uses a root CA that Sectigo has embedded into all SMIME capable mail applications, meaning the mail application will trust the digital signature without any configuration change. Public S/MIME certificates are a great solution for sending email that allows any recipient in the world to verify that its true sender and that the email has not been tampered with. Automated controls within the Sectigo solution prevent one enterprise from being able to issue certificates in the name of another enterprise. The enterprise will also share in the responsibility to ensure its employee receive certificates for their specific email addresses. Sectigo is the first ever provider of Zero-Touch deployment for publicly trusted S/MIME.

- **Private S/MIME:** In this scenario the each enterprise receives a root that is unique to it, allowing all enterprise applications to trust any certificate issued from this CA without the need to configure or program the applications to exclude other companies based on fields within the certificate. This approach is ideal for when only encryption is required and the same certificate will be used for additional enterprise applications such as VPN. The private CA approach is not appropriate for cases when digitally signed emails need to be validated outside this particular enterprise. Sectigo also offers Zero-Touch deployment for privately trusted S/MIME.

Self-Service S/MIME Certificates

A traditional S/MIME offering depends on a web portal, where the user can enter the needed individual information and then request for the certificate be issued with that information. The certificate and private key will be download to the user's desktop as a P12 or PFX file. The user then has the responsibility to install that file on each of device or mail application intended to

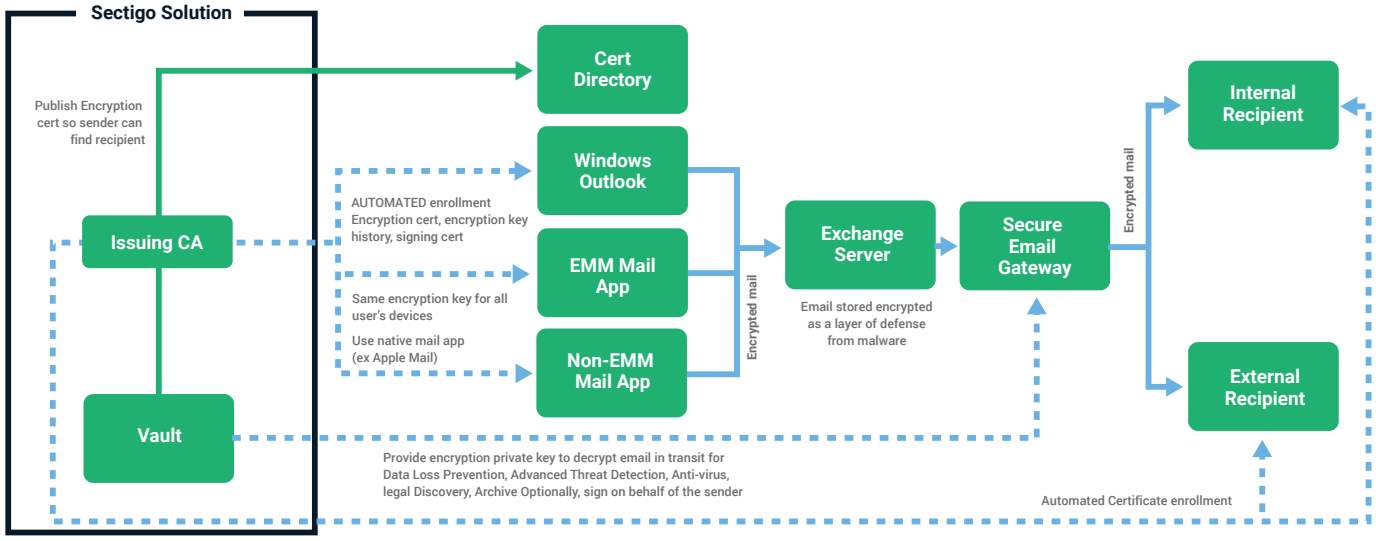
use signed and encrypted email. Each P12 file is limited to one email address controlled by the end user. Windows, iOS, and Android automatically install P12 files when opened.

Users must repeat this process when their certificates expire. They must manually publish their certificates to their directories so that senders can encrypt for them. Alternatively, users may send signed email to each person they wish to communicate with so that the other person may extract the user's certificate from the signed email. Finally, user must configure their email application to utilize the certificate and key from the P12 they recently installed.

This entire certificate lifecycle depends on end users who may not be savvy about computers to successfully execute on a series of particular and non-intuitive steps to deploy and maintain S/MIME email certificates.

Introducing Zero-Touch Email Certificate Deployment

To overcome these problems, Sectigo has developed the world's first Zero-Touch deployment capability for S/MIME email certificates. Sectigo's innovative architecture makes it possible for IT professionals to deploy and maintain email certificates for employees without requiring action from the end users.



Vault

The Sectigo solution starts the process by generating a cryptographic key pair, as defined by the policy set by the enterprise administrator. The public key can create either a public or private S/MIME certificate.

The private key is automatically stored encrypted in the vault, removing the responsibility for users to securely store backups of their own private keys for recovery in the event of accidental loss or deletion. Vaulting private keys radically reduces the risk that emails will be incapable of decryption due to lost keys. The system provides the same encryption key for all email applications used for a single email address, including desktops, tablets, and phones.

The vault also opens the door to additional capabilities such as allowing the email gateway to encrypt, decrypt, and sign emails on the users' behalf. Vaulted keys aid enterprises in complying with email retention and discovery requirements that may stem from legal action or court orders.

It provides access to emails in many circumstances where otherwise recovery would be difficult or impossible, including:

- An employee has left the company and no key can be found
- An employee has accidentally destroyed the private key, perhaps from a hard drive crash
- An employee is not available to provide the access to the private key

The vault even includes the ability to decrypt older emails which would have used prior keys by returning the entire key history and not simply the most recent key.

Vaulting private keys radically reduces the risk that emails will be incapable of decryption due to lost keys.

Sectigo Certificate Manager offers key vaulting as a standard capability, eliminating the need for enterprises to set up and configure their own vaults integrated with Active Directory. Vaulted keys can be located in Sectigo's cloud infrastructure or on the customer's premises.

Windows Desktop Email Application

The Sectigo solution issues certificates for desktop users without requiring action on their part. Sectigo offers an agent for deployment on the customer's network, which can receive requests from Windows desktops and translate them into action in Sectigo Certificate Manager.

Sectigo offers an agent for deployment on the customer's network, which can receive requests from Windows desktops and translate them into action in Sectigo Certificate Manager.

The Windows administrator can initiate certificate deployment by setting a policy for all employees to possess S/MIME certificates. At this point each desktop will automatically reach out to Sectigo Certificate Manager for an S/MIME certificate, with the private key being stored in Certificate Manager's key vault. The Windows desktops will receive and deploy these certificates without intervention from end users. The certificates are published in the corporate AD so the end users are immediately able to encrypt and sign emails, either on a case by case basis or by default, depending on the mail client's configuration.

EMM Mail Applications

When an EMM (Enterprise Mobility Management) vendor is in use, Sectigo collaborates with that vendor to provide the S/MIME certificate to the EMM's mail application. These EMM mobile mail applications will use their own certificates and key stores, within their containers, to offer another level of security.

Non-EMM Mail Applications

When no EMM vendor is available, Sectigo utilizes the native MDM capability within the iOS and Android operating systems to deliver certificates and private keys to the operating systems' key

stores. This allows native (non- EMM) mail applications to be used for S/MIME. This approach maintains the zero-touch capability delivered by third party MDMs.

As an option, the enterprise may set the solution to also configure the mail application to utilize the certificate and private key, avoiding the need for the user to navigate this mobile mail setup and minimizing help desk calls.

The S/MIME keys and certificates can be shared with the mobile browser to provide client-side SSL authentication to web server applications from the web browser. To permit exchanging secured emails with external recipients, users may access Sectigo's self-service web portal to download their certificates and private keys.

Encryption as Another Layer of Defense

The mail application will encrypt email content and attachments for all certificate-signed emails, providing an additional layer of defense for stored emails. As cloud-based mail servers such as Office 365 become more popular, encrypting emails prevents parties outside your enterprise from viewing sensitive emails as part of their normal operation. And in the event an attacker successfully steals a mail server password, no sensitive information will be lost since the email content and attachments will be encrypted. This encryption defends against attacks like the one from November 2014 in which unencrypted emails were stolen from Sony Pictures and published publicly.

The advantage of Zero Touch installation is that employees will default to encrypting all emails, removing the need to choose which emails to encrypt on a case-by-case basis. Sectigo's encryption key vault provides the entire S/MIME key history to the mail application, so even emails using older keys can still be decrypted.

Directory to Store Encryption Certificates

One challenge for SMIME encryption is finding recipients' certificates so senders can encrypt for them. Zero-Touch deployment takes care of this need by automatically placing the certificate into the enterprise's chosen directory, whether that's internal Active Directory or an external directory hosted by Sectigo and reachable worldwide by customers and partners.

Secure Email Gateways
Secure mail gateways can prevent malicious code from entering and intellectual property from leaving enterprise. Traditional S/MIME products interfere with these gateways success because:

- Email encryption prevented scanning of email bodies and attachments.
- Gateways can change the contents of the emails, invalidated digital signatures. This signature is important not only because it ensures the sender's the true identity but it also because it ensures the email body and attachment have not been altered in any way.

Some gateways have attempted to get around these problems by offering a web portal for recipients to retrieve encrypted email. This approach presents a poor user experience for the recipient, who is being asked to click a link in an unsolicited email and enter login credentials into an unfamiliar web page as opposed to simply accessing email in the standard way.

The Sectigo solution provides a REST API to the secure email gateway, which allows the gateway to decrypt, encrypt, or sign so that it can continue to deliver on its valuable function. It provides the recipient better delivery choice, using the native mail application to decrypt the email without leaving the application.

Conclusion

S/MIME certificates are an indispensable part of the enterprise's complete email security strategy. Unfortunately, low end user adoption of certificates can undermine the effectiveness of this defense. Sectigo has addressed the common problems associated with S/MIME certificates to provide the industry's first truly usable enterprise certificate solution. Sectigo Certificate Manager offers a best-possible certificate experience through:

- Zero Touch deployment for maximum employee adoption
- Key vaulting to prevent unencryptable email content through lost keys
- Secure Email Gateway integration

All these capabilities, combined with Sectigo's industry-leading Sectigo Certificate Manager, make Sectigo's S/MIME certificate solution the best solution for deploying and managing email certificates for the enterprise.

