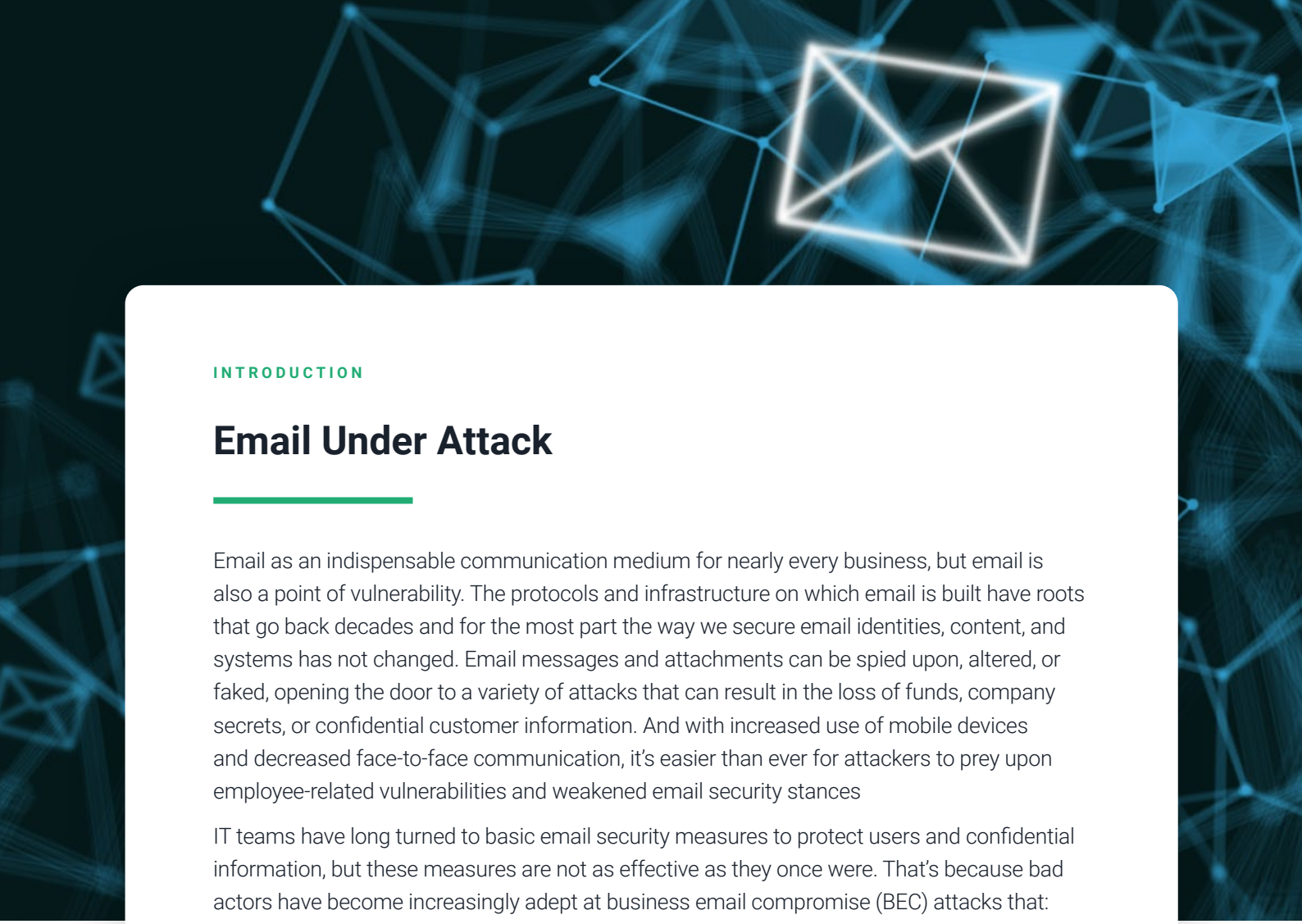
Protecting Enterprise Email With S/MIME Certificates

A WHITEPAPER BY SECTIGO

SECTIGO®



INTRODUCTION

Email Under Attack

Email as an indispensable communication medium for nearly every business, but email is also a point of vulnerability. The protocols and infrastructure on which email is built have roots that go back decades and for the most part the way we secure email identities, content, and systems has not changed. Email 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 funds, company secrets, or confidential customer information. And with increased use of mobile devices and decreased face-to-face communication, it's easier than ever for attackers to prey upon employee-related vulnerabilities and weakened email security stances

IT teams have long turned to basic email security measures to protect users and confidential information, but these measures are not as effective as they once were. That's because bad actors have become increasingly adept at business email compromise (BEC) attacks that:

Gain access to employee credentials, customer and employee personally identifiable information (PII), financial accounts, private conversations, and other non-public secrets.

Trick employees to click links to malware sites to infect computers in the enterprise and possibly to perpetrate a ransomware attack.

Deceive employees into wiring money to accounts that appear to belong to suppliers or other partners but are really controlled by criminals.

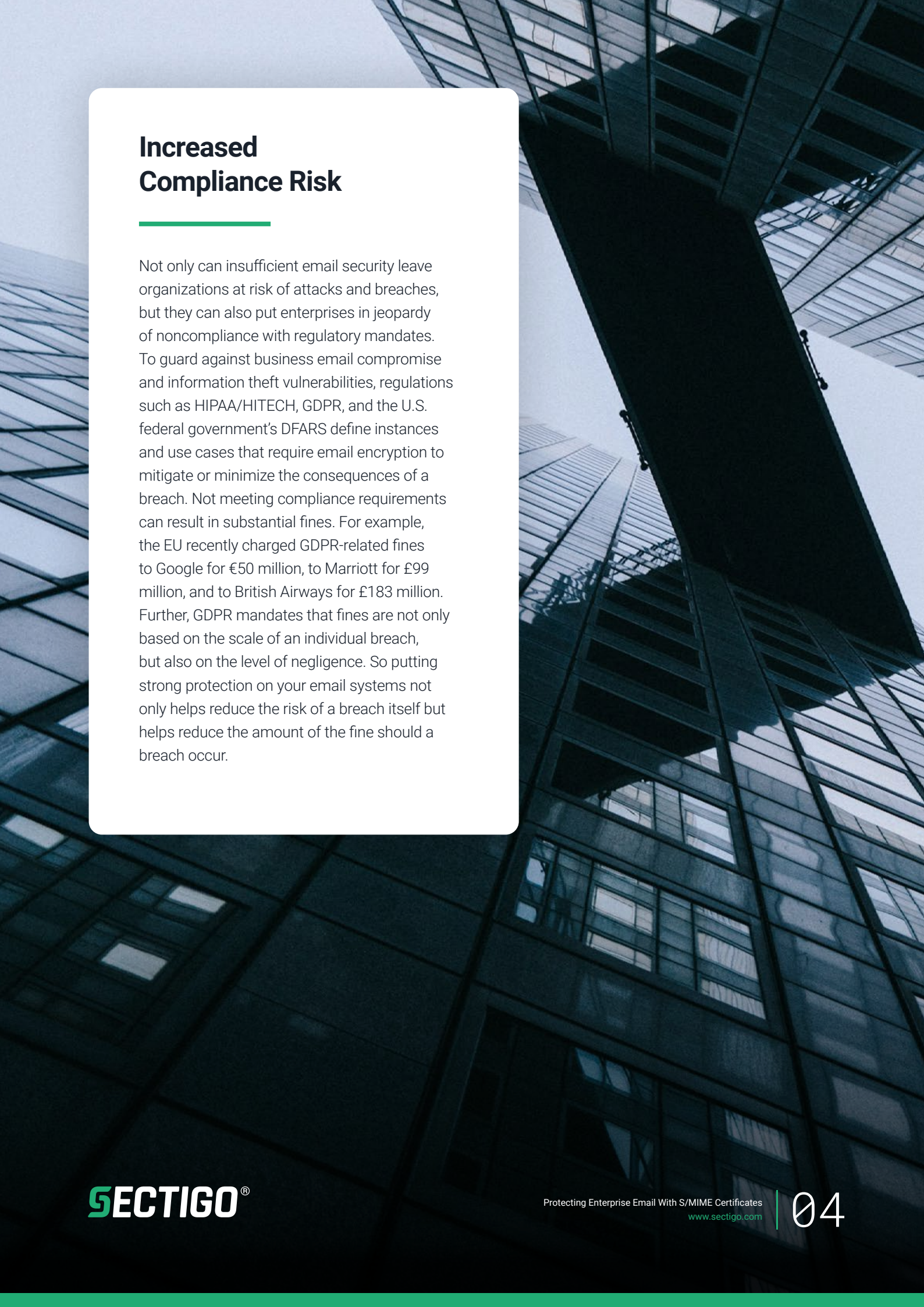
Social Engineering Preys on Human Nature

No longer do attacks consist of obviously fraudulent, scripted messages sent at high volume with low yield. Today, bad actors are social engineering experts using spear phishing emails to target high value opportunities. They are particularly effective when business operations change or are under duress. A recent study found that 62% of breaches that were not caused by error, misuse, or physical action involved phishing, stolen credentials, or brute force.

These issues are compounded by the human factor. Spear phishing emails often take advantage of people's natural tendencies to be helpful and responsive. Spear phishing emails creatively spoof seemingly viable requests from executives, human resources, customers, or suppliers and reference realistic scenarios for added urgency. Bad actors often only need to ask in a seemingly normal way to get a response from someone in an organization. Employees are often quick to support executives and customers and unknowingly share sensitive information in response to the request or click on a link that plants malware.

The cost to business is high. The FBI reported a financial loss to businesses of $1.2 billion in 2018 due to business email compromise alone, an increase of 78% from the previous year. Additionally, high-profile email breaches can impact brand image and lead to senior executives' job losses. In 2015, Sony's CEO was forced to resign after hackers leaked the company's email store, releasing full versions of unreleased movies and damaging conversations. In 2016, the Democratic National Committee left unencrypted email content exposed on its server, making it easily accessible to bad actors.

Examples of spear phishing include sophisticated attacks that ask financial teams for the "aging accounts" list of companies that owe money. Then the bad actor sends those indebted companies an email pretending to be the receivables department and requests payment of their outstanding balance. Unsuspecting companies then send payment to accounts controlled by the criminals.



Increased Compliance Risk

Not only can insufficient email security leave organizations at risk of attacks and breaches, but they can also put enterprises in jeopardy of noncompliance with regulatory mandates. To guard against business email compromise and information theft vulnerabilities, regulations such as HIPAA/HITECH, GDPR, and the U.S. federal government's DFARS define instances and use cases that require email encryption to mitigate or minimize the consequences of a breach. Not meeting compliance requirements can result in substantial fines. For example, the EU recently charged GDPR-related fines to Google for €50 million, to Marriott for £99 million, and to British Airways for £183 million. Further, GDPR mandates that fines are not only based on the scale of an individual breach, but also on the level of negligence. So putting strong protection on your email systems not only helps reduce the risk of a breach itself but helps reduce the amount of the fine should a breach occur.

S/MIME Defends Against Email-Based Attacks

Clearly, IT professionals must rethink their strategies for securing email communications and systems. To truly protect email from today's sophisticated attacks, enterprises need a complete security approach that enables both email encryption and authentication of digital identities for all employees and devices.

Leveraging numerous sophisticated security features, S/MIME (Secure/Multipurpose Internet Mail Extension) email certificates give users the confidence to trust their digital correspondence and avoid many of today's attacks on enterprise email users and infrastructure. They are an indispensable part of the enterprise's complete email security strategy.

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

- Authentication of sender. Each S/MIME email certificate includes the sender's authenticated email address, giving receivers a mechanism to confirm that all communications are genuinely from authorized parties by displaying a check mark icon that identifies the email sender as authentic and the email as unmodified.
- Encryption of email content and attachments. Sending and receiving mail clients use the certificates to encrypt and decrypt email content, including attachments. This prevents attackers from intercepting email communication in transit and from reading email content stored on servers.
- 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.

S/MIME certificates protect employees against spear phishing attacks, even when they use smartphones and mobile devices to access email. By encrypting/decrypting email messages and attachments and by validating senders' identities, S/MIME email certificates assure users that emails are authentic and unmodified.

What You Need in an Enterprise S/MIME Solution

With S/MIME, the end user's certificate-enabled email experience is 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 low for many years. The primary cause of this low adoption has been the cumbersome and confusing process required for both IT administrators and employees to enable these certificates on email clients. Without broad end user adoption, enterprise S/MIME strategies often fail to provide protection or compliance benefits and generally result in more helpdesk calls.

When considering implementing S/MIME to provide certificate authentication, encryption, and identity assurance, enterprises need a solution that:

- Provisions certificates automatically through centralized enterprise management without requiring employees to issue and configure certificates
- Signs emails from a Certificate Authority (CA) trusted by all email applications worldwide
- Encrypts email in-transit and at rest stored on the mail server
- Vaults certificate keys that synchronize an enterprise's email applications and directories
- Integrates with Secure Email Gateways to sign and encrypt at the gateway
- Deploys a single certificate for a user to multiple devices used by that employee, including mobile devices
- Is easy not only for security teams to deploy, but also for employees to use

Sectigo can help. 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 across all their devices without requiring action from the end users.

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 manually execute certificate and key management for their desktop, mobile devices, and directory.

Sectigo Zero-Touch S/MIME Automates Deployment

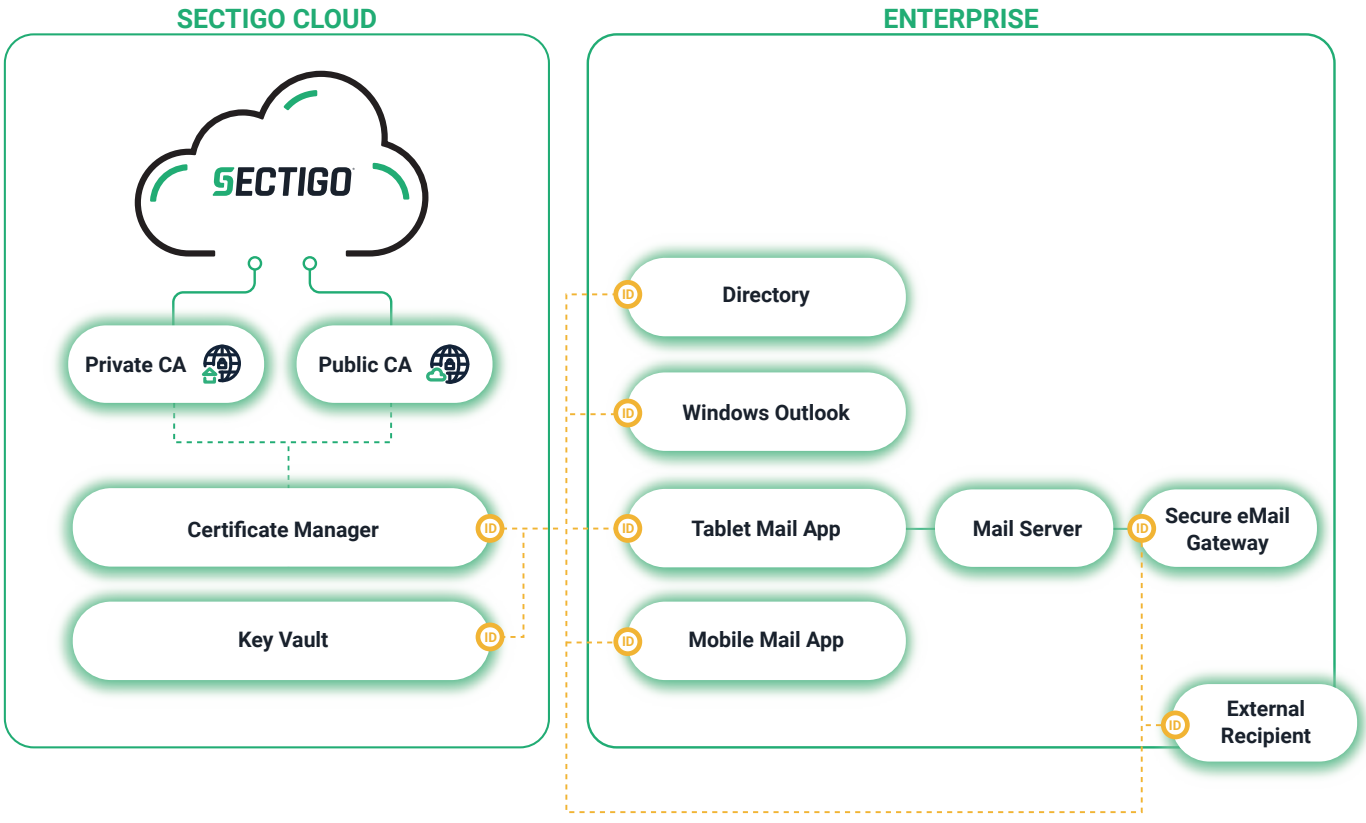
Traditionally, S/MIME solutions have required end users to acquire a trusted S/MIME certificate from a public CA and install it on their own systems, all on their own initiative. But the steps required to manually issue and configure S/MIME email certificates are exceedingly difficult for the average enterprise employee. 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.

Unlike traditional S/MIME certificate deployments, Sectigo Zero-Touch S/MIME is designed to be invisible to the user. This approach enables broad employee adoption as IT professionals can seamlessly deploy and maintain email certificates for employees without requiring action from them. By automating configuration and issuance of S/MIME certificates using a management console, you are reducing the risk of noncompliance while simplifying deployment of certificates across a large number of computer and mobile devices and reducing help desk calls.

Sectigo issues a single certificate for a user for deployment to multiple devices used by that employee, including their computer/laptop, tablet, or mobile device. Plus, certificates can be provisioned to mobile devices using an MDM like Microsoft Intune or Apple.

A visual representation of Sectigo's Zero-Touch email solution and how it interfaces with the enterprise's email system is provided in Figure 1.

Sectigo S/MIME Solution Overview



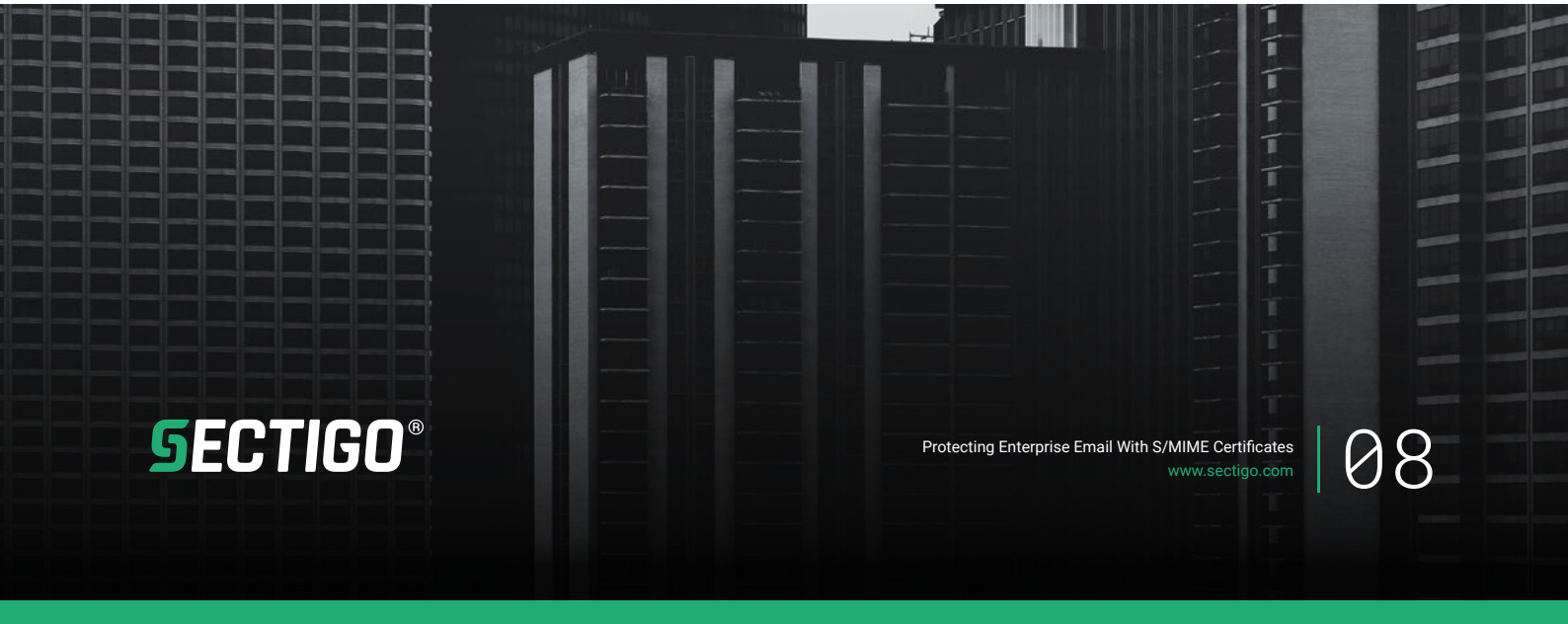
Sectigo Offers Multiple S/MIME Deployment Options

With Sectigo S/MIME certificates, enterprises have the option to choose between publicly trusted, private, or self-service S/MIME certificates:

Public S/MIME certificates: Public S/MIME certificates are a great solution for sending email that allows any recipient in the world to verify its true sender and that the email has not been tampered with. All certificates are issued from a common, shared issuing Certificate Authority. This common CA uses a root CA that Sectigo has embedded into all S/MIME capable mail applications, meaning the mail application will trust the digital signature without any configuration change. 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 the responsibility to ensure its employees receive certificates for their specific email addresses.

Private S/MIME certificates: The private CA approach is ideal for businesses that require only encryption (not identity) and the same certificate will be used for additional enterprise applications such as VPN and Wi-Fi. The private CA approach is not appropriate for cases when digitally signed emails need to be validated outside the enterprise. The 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.

Self-Service S/MIME certificates: Self-service S/MIME is a more traditional approach to S/MIME and is implemented via a web portal, where users can enter the required information and then request a certificate be issued with that information. The certificate and private key are then downloaded 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.



Encryption Provides an Important Layer of Defense

With S/MIME certificates, both the sending and receiving email clients encrypt all email content and attachments for all locally-housed, certificate-signed email. This provides an additional layer of defense for stored, or at-rest emails. In addition, all email content and attachments are sent encrypted, preventing attackers from intercepting email communication in transit. As cloud-based mail servers such as Office 365 become more popular, encrypting emails prevents parties outside your enterprise from viewing sensitive content. In the event an attacker successfully steals a mail server password, no sensitive information will be lost since the email content and attachments stored on the server are encrypted. And the advantage of Sectigo Zero-Touch installation is that employees send encrypted email by default, removing the need for them to choose which emails to encrypt and which to leave unencrypted on a case-by-case basis.

Vault Certificate Keys for Any Email Environment

Sectigo's S/MIME certificate solution also includes a certificate vault which offers secure storage of users' private keys and removes the responsibility of secure private key backups from end users. Vaulting private keys radically reduces the risk that emails would be incapable of decryption when private key are lost. 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.

Sectigo offers key vaulting as a standard capability, eliminating the need for enterprises to set up and configure separate vaults using technologies such as Active Directory. You can locate vaulted keys in Sectigo's cloud infrastructure or on your own premises.

The Sectigo vault 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 in the event of accidental loss or deletion.

Keys vaulted with Sectigo also aid enterprises by:

Maintaining a key history that enables decryption of older emails which would have used prior keys.

Complying with email retention and discovery requirements that may stem from legal action or court orders.

Mitigating risk of lost private keys which make it impossible to then decrypt and access emails if an employee has left the company or cannot find or has accidentally destroyed the private key.

Augment Security with Secure Email Gateway Integration

Enterprises commonly use a secure email gateway (SEG) to provide basic email security. SEGs are essentially firewalls for email that scan and filter inbound and outbound email messages based on simple rules. Unfortunately, SEGs can be defeated by social engineering attacks, and when email content is not encrypted, confidential information sent by employees over email may be easily stolen. While helpful, basic security provided by your SEG is not sufficient to protect your business and users from all attacks.

Traditional S/MIME products interfere with the success of SEGs because:

- Email encryption prevents scanning of email bodies and attachments.
- Gateways can change the contents of the emails, invalidating digital signatures.

Sectigo's S/MIME solution provides a REST API to the secure email gateway, which permits the gateway to decrypt, encrypt, or sign emails, allowing it to continue delivering on its valuable function. Sectigo's S/MIME solution also provides the recipient better delivery choice, using the native mail application to decrypt the email without leaving the application.

Conclusion: Gain Peace of Mind With Sectigo Zero-Touch S/MIME Certificates

S/MIME certificates are an indispensable part of the enterprise's complete email security strategy. To protect the company from spear phishing attacks and other vulnerabilities, and to better ensure regulatory compliance, companies need to deploy S/MIME certificates.

S/MIME email certificates give users the confidence to trust their digital correspondence by displaying a check mark icon that identifies emails as authentic and unmodified. S/MIME certificates add a layer of defense by encrypting emails both in storage and in transit.

Sectigo addresses the common deployment and management problems that have kept S/MIME from achieving widescale adoption, with the industry's first truly usable enterprise email certificate solution. The Sectigo Zero-Touch S/MIME solution offers a seamless certificate deployment and user experience through:

- Automated deployment invisible to end users
- Key vaulting to prevent unencryptable email content through lost keys
- Secure Email Gateway integration
- The same end user email sending and receiving experience as email without certificates

About Sectigo

Sectigo is a cybersecurity technology leader providing digital identity solutions, including TLS/SSL certificates, web security, DevOps, IoT, and enterprise-grade PKI management. As the world's largest commercial Certificate Authority, with more than 700,000 customers worldwide and 20 years of experience delivering online trust solutions, Sectigo provides proven public and private trust solutions for securing web servers, digital identities, connected devices, and applications. Recognized for its award-winning innovations and best-in-class global customer support, Sectigo delivers the technologies required to secure the digital landscapes of today, as well as tomorrow. For more information, visit www.sectigo.com and follow @SectigoHQ.

SECTIGO®