S/MIME for Enterprise Email Security

WHITEPAPER

Contents

Introduction

Many organizations, both large and small, face difficult choices when considering secure communications and data transfer between stakeholder groups. Virtual teams made up of internal colleagues, outside partners, and even potential clients find a need to collaborate effectively and securely, requiring cost-effective ways to authenticate the integrity of messages they, receive but also the need to maintain confidentiality.

Now more than ever, email is one of the biggest concerns for CISOs and heads of security with solutions needed to cover the encryption of messages and data either at rest or during transmission to other parties. Within this white paper, we will be highlighting the use of S/MIME Certificates as a solution to provide a way to maintain confidentiality, as well as prove the integrity and origin of emails and their authors.

Email at the Core of Business

The average business user sends 122 emails per day, totaling 112.5B total business emails every day.

And it's not slowing down - 3% annual growth is expected through 2019.[1]

Risks of email communication

Email spoofing, phishing attacks, and Business Email Compromise

Phishing continues to be one of the largest threats facing enterprises today, both in terms of network security (95% of attacks are the result of successful spear phishing) [2] and financial loss (hackers have attempted to scam companies out of over $3B in the past three years)[3].

One of the most popular methods for carrying out a phishing attack is email spoofing, in which hackers forge the sender address to add a false sense of legitimacy to the email contents and mislead recipients into falling for the attack (e.g., downloading a malicious file, providing sensitive information or credentials, transmitting funds).

Trouble Spotting Phishing

94% of employees can't tell the difference between real and phishing emails.[4]

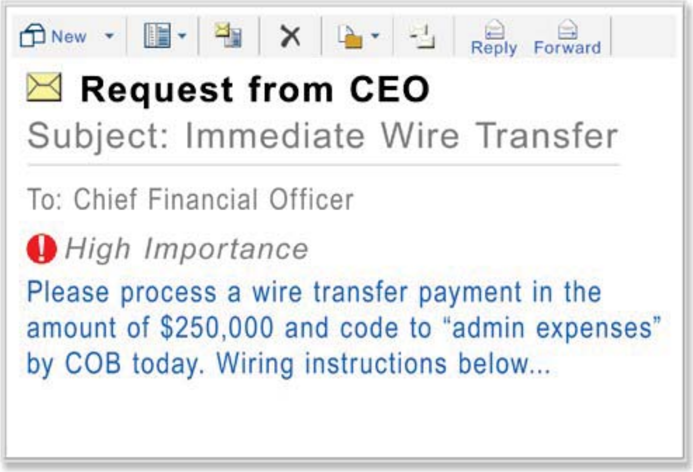
It is very easy to create these spoofed emails and they can be created for addresses already in use. Since core email protocols don't offer a way to authenticate email origin, there is generally no way for end users to identify a spoofed email versus a legitimate one.

Glossary

Phishing - large scale attack where a hacker will forge an email so it looks like it comes from a legitimate company (e.g. a bank), usually with the intention of tricking the unsuspecting recipient into downloading malware or entering confidential information into a phished website (a website pretending to be legitimate which in fact a fake website used to scam people into giving up their data), where it will be accessible to the hacker.

Spear phishing – type of phishing generally involving a dedicated attack against an individual or an organization. These types of attacks are generally well-researched, customized to the intended victim, and sent from a spoofed address of a known contact – making them appear very believable and "real."

Business Email Compromise – sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.[5]



Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

High Importance

Please process a wire transfer payment in the amount of $250,000 and code to "admin expenses" by COB today. Wiring instructions below...

Example spear phishing email. (Source: FBI)[5]

Data loss and leaks

Given the ubiquity of email, it's perhaps not a surprise that it's a leading weak point in enterprise security, with 22% of organizations experiencing data loss through email each year.[6] Industries that are traditionally highly regulated, such as healthcare and finance, among others, are no strangers to the need to protect email communications, but the past few years have seen high profile incidents (e.g., Sony megahack) put the impetus on other industries as well.

These recent incidents have also changed the conversation regarding the type of information that needs to be protected. In addition to personal identifying information (PII) and corporate financial information, enterprises need to consider proprietary information, including sales data, customer contracts, project plans, etc., and on a broader level, any content that, if released, could potentially harm the company's reputation.

Encrypting emails vs. mail servers

It is strongly recommended and considered a general best practice for enterprises to install a server (SSL/TLS) certificate on their mail server(s). This is because without one:

1. There's no way to identify that the mail server a user connects to is actually the correct mail server.

2. The connection between the user’s browser or email client and server isn’t encrypted, meaning any emails transmitted between the two could be intercepted.

Risky User Habits

53% of employees have received unencrypted, risky corporate data via email or email attachments. [7]

Without a certificate, enterprises are vulnerable to a man-in-the-middle (MITM) attack, whereby malicious parties could insert themselves between users and mail servers to intercept and access emails. Clearly, there’s no denying the need for a SSL certificate on the mail server, but unfortunately it can lead to a false sense of security.

While a SSL Certificate will protect emails in transit to and from the mail server, it does nothing to protect the emails as they pass through other servers, which may not have SSL. Additionally, securing the mail server doesn’t protect the emails at rest. For example, a hack where attackers gain access to email systems, like the aforementioned one at Sony in late 2014, would not be prevented by a server certificate. If enterprises want a solution that truly mitigates the risk of data loss via email, it’s essential that they consider options that protect emails both in transit *and at rest*.

Glossary

Public-key cryptography - aka asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key. It is computationally infeasible to compute the private key based on the public key.

Public key – half of a cryptographic keypair, used to encrypt data and verify digital signatures. Can be freely shared and is stored on a Digital Certificate for secure transport and sharing.

Private key – half of a cryptographic keypair, used to decrypt data and create digital signatures. Should be kept secret and is generally stored in the end user’s software or operating system or on cryptographic hardware.

A Practical Approach to Email Security: The S/MIME Protocol

S/MIME or Secure/Multipurpose Internet Mail Extensions is the industry standard for public-key encryption for MIME-based data. S/MIME provides message integrity and privacy via data encryption, as well as proving the origin of the message and ensuring non-repudiation via the addition of digital signatures.

S/MIME is a standard tracked by the Internet Engineering Task Force (IETF) and defined by multiple Requests for Comments (RFCs), including 5652, 5750, 5751, and 5754. S/MIME works by using a data envelope to surround the data ntity, which is inserted into a PKCS7 MIME Entity when encrypting. In real world terms, the S/MIME protocol is utilized through X.509 Digital Certificates.

Glossary

Digital Certificate – a small data file that digitally binds a user's identity to a cryptographic public key

Third party Certificate Authorities (CAs) – highly regulated entities that issue publicly trusted Digital Certificates

Internal Certificate Authorities (CAs) – internally owned and operated CA that issues Digital Certificates that generally aren't trusted outside of the internal networks

S/MIME Business Applications

S/MIME, and public-key cryptography in general, offers two main business applications:

- Digital signatures - content is digitally signed with an individual's private key and is verified by the individual's public key
- Encryption - content is encrypted using an individual's public key and can only be decrypted with the individual's private key

Why S/MIME?

Using S/MIME offers a number of security benefits, including addressing the risks discussed above, but also lends itself to some administration benefits, which can simplify deployment and decrease total cost of ownership.

Security Benefits

Assuming the private key has remained secret and the individual it was issued to is the only person with access to it, S/MIME offers the following security benefits:

Proof of message origin / sender authentication

As mentioned above, core email protocols have no way to authenticate message origin, but S/MIME offers this capability via digital signatures. Digitally signatures contain identity information about the sender (from their Digital Certificate), so recipients can verify and validate the sender's identity.

Message integrity

Part of decrypting a message or verifying a digital signature involves checking that the contents of the email match what was in there when the signature was applied. Even the slightest change to the original document would cause this check to fail and trigger a warning message to the recipient that the email has been tampered with.

Confidentiality – in transit and at rest

The cryptography technology underlying S/MIME means that only the intended recipient of emails can actually read them. This comes back to the key pair – a user's public key is used to encrypt the email and ONLY the corresponding private key can decrypt it. This means that whether a hacker, or any other unintended recipient, tries to intercept a message in transit or gains access to corporate email systems, they will not be able to read the contents.

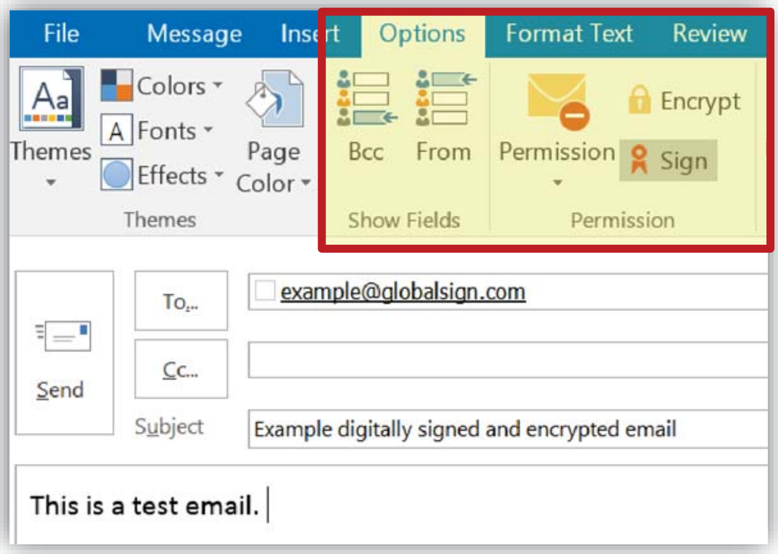
Non-repudiation

Since digital signatures are applied using an individual's private key, which is supposed to be in the sole possession of the individual, he cannot later claim that it wasn't he who applied the signature.

Administration Considerations

End user transparency / ease of use

Using S/MIME is typically straightforward and transparent to the end user. There is generally minimal user training needed, which also helps streamline deployment and minimizes any burden on IT. For most email clients, digitally signing and/or encrypting a message is as simple as clicking a button. Many also offer the option to automatically do this for all outgoing emails.



example@globalsign.com

Example digitally signed and encrypted email

This is a test email.

Signing and encrypting an outgoing email in Outlook 2016

S/MIME Functions

Digitally signing an email provides:

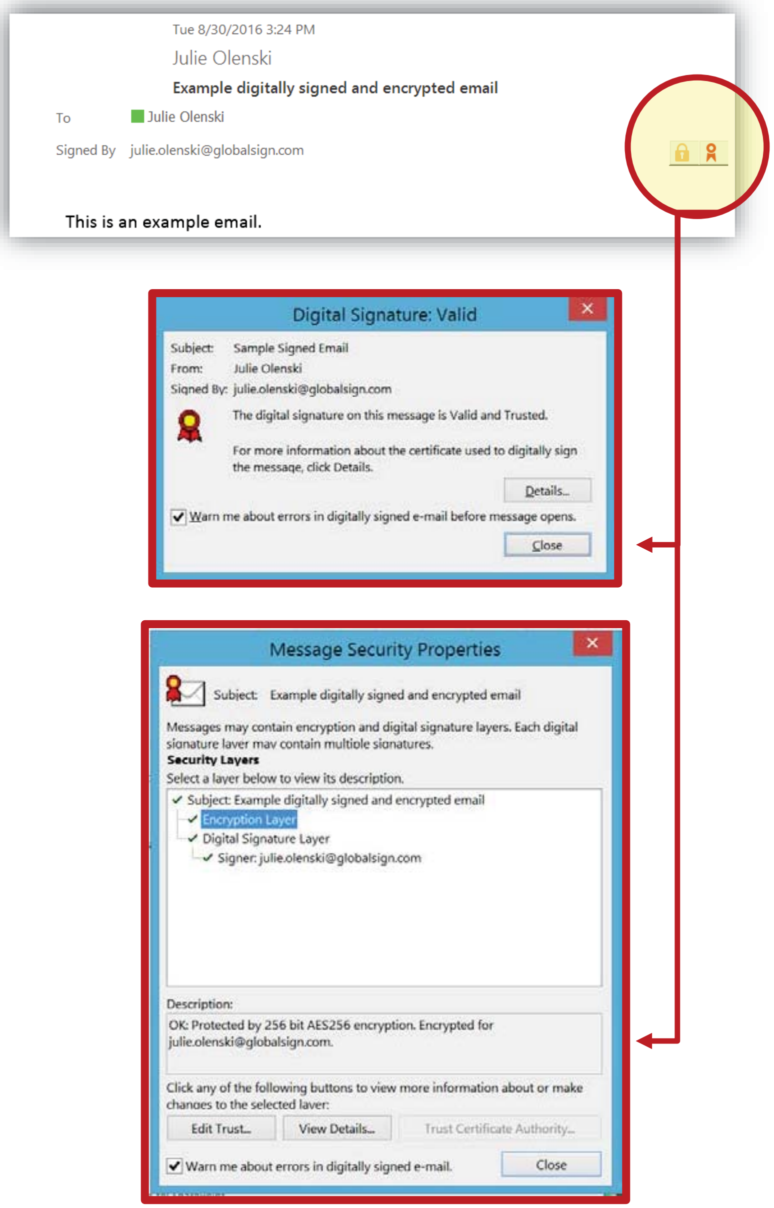
- Authentication of the email sender
- Non-repudiation
- Message integrity

Encrypting an email provides:

- Confidentiality (in transit and at rest)
- Message integrity

Note: Encryption alone does not provide any information about the sender of the message. Best practice is to always include a digital signature when encrypting to authenticate the identity of the sender.

Clear symbols make it easy for recipients to see when an email has been encrypted and/or digitally signed, with details readily available to confirm the integrity of the signature and the origin.



Tue 8/30/2016 3:24 PM

Julie Olenski

Example digitally signed and encrypted email

To 🟩 Julie Olenski

Signed By julie.olenski@globalsign.com

This is an example email.

Digital Signature: Valid

Subject: Sample Signed Email

From: Julie Olenski

Signed By: julie.olenski@globalsign.com

The digital signature on this message is Valid and Trusted.

For more information about the certificate used to digitally sign the message, click Details.

☑ Warn me about errors in digitally signed e-mail before message opens.

Message Security Properties

Subject: Example digitally signed and encrypted email

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

Security Layers

Select a layer below to view its description.

✓ Subject: Example digitally signed and encrypted email
  ✓ Encryption Layer
  ✓ Digital Signature Layer
    ✓ Signer: julie.olenski@globalsign.com

Description:

OK: Protected by 256 bit AES256 encryption. Encrypted for julie.olenski@globalsign.com.

Click any of the following buttons to view more information about or make changes to the selected layer:

☑ Warn me about errors in digitally signed e-mail.

Example encrypted and digitally signed email with click-through details in Outlook 2016.

Native compatibility with leading mail clients

Most leading enterprise email clients (Outlook, Thunderbird, Apple Mail, Lotus Notes etc.) are natively compatible with S/MIME so there is no need for additional software, appliances, or gateways. Compatibility with web-based email platforms is more mixed - Outlook 365 started supporting S/MIME in 2014, while Gmail requires the use of an additional plug-in or add-on. Several mobile email clients can also be configured for S/MIME (e.g., Windows 10 Mail app, Samsung native email app, iOS native email app); the user's certificate just needs to be installed on the device.

Leverage Active Directory and Group Policy

Since S/MIME is PKI-based, it can be integrated with existing Active Directory environments. Whether using an internal CA deployment or a third party CA service, enterprises can leverage the existing user identity information from Active Directory to streamline certificate registration and use Group Policy to determine which users require S/MIME Certificates. Certificates can then be automatically issued and installed on the appropriate users' machines, without any intervention needed from IT or the users themselves.

One solution for both mobile and desktop

S/MIME Certificates can be installed on both mobile devices and desktops, enabling users to digitally sign and encrypt emails no matter which device they use. A unified solution can also simplify deployments and decrease costs for IT. Integrations with Mobile Device Management (MDM) platforms automate certificate provisioning and management.

Conclusion

When it comes to email security, enterprises need a cost-effective solution that will not only protect the enterprise from growing threats, such as phishing and Business Email Compromise, and risks, such as data loss and breach, but that will also be embraced by end users and not burden IT. S/MIME strikes the balance between security and usability, addressing the leading email attack vectors without requiring extensive user training or IT resources to deploy and manage.

About GlobalSign

GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers and IoT innovators around the world to secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale Public Key Infrastructure (PKI) and identity solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE).

US: +1 877 775 4562
UK: +44 1622 766766
EU: +32 16 89 19 00

sales@globalsign.com
www.globalsign.com

GlobalSign®
GMO INTERNET GROUP

References

1 http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

2 https://www.bromium.com/resources/threat-information/spear-phishing.html

3 https://www.ic3.gov/media/2016/160614.aspx

4 https://kapost-files-prod.s3.amazonaws.com/published/55402a53952bde97e70000d1/harpooning-executives-how-phishing-evolved-into-the-c-suite.pdf

5 https://www.fbi.gov/news/stories/business-e-mail-compromise

6 Best Practices in Email, Web, and Social Media Security, Osterman Research, Inc., January 2014

7 SilverSky Email Security Habits Survey Report, SilverSky, 2013