DATASHEET

S/MIME Certificates for Email Security

Encrypt Sensitive Internal Communications and Validate Email Sources to Counter Phishing

Malicious parties have become increasingly sophisticated at targeting organizations via email, including intercepting messages to view sensitive information and/or email spoofing with the intent of pushing to phishing sites or triggering malware downloads. Using S/MIME Certificates to digitally sign and encrypt emails help organizations protect themselves from these threats, by ensuring only intended recipients can access email content and also verifying the email origin to help distinguish between legitimate and malicious emails.

What is S/MIME?

S/MIME, or Secure/Multipurpose Internet Mail Extensions, is the industry standard for public key encryption for MIME-based (message-based) data. S/MIME Certificates offer two key email security functions:

- **Digital Signature** - proves authorship and prevents tampering, assuring the email recipient that the email came from you, not an imposter and that the content of the email has not been altered in transit
- **Encryption** - ensures a message can only be opened by the intended recipient and keeps sensitive information from falling into the wrong hands

KEY BENEFITS

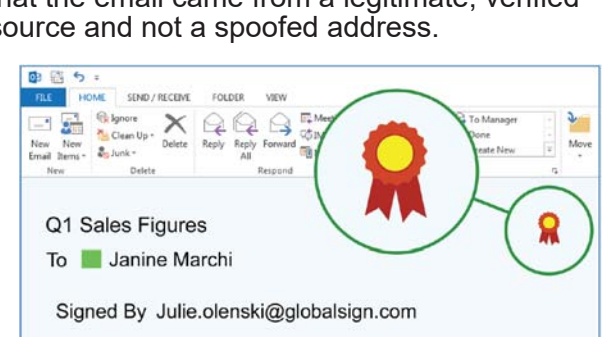
- PROVE MESSAGE ORIGIN
  Digitally signing emails verifies message origin, assuring recipients that the email is legitimate and not a spoofed email
- ENCRYPT MESSAGES IN TRANSIT AND AT REST
  Encrypting emails ensures only intended recipients can access email content, regardless of where the email resides
- CONTENT INTEGRITY
  Digital signing and/or encrypting emails creates a tamper-evident seal on message content, ensuring message integrity
- NATIVE COMPATIBILITY
  No additional software needed and compatible with leading enterprise email clients (Outlook, Thunderbird, Apple Mail, Lotus Notes, etc.)
- EASY FOR END USERS
  Requires minimal user training. For most clients, digitally signing and/or encrypting an email is as simple as clicking a button. Many clients also offer the option to automatically do this for all outgoing messages
- CHOOSE YOUR SIGNING ALGORITHM
  Select SHA256RSA or RSASSA-PSS (Managed PKI users only)

GlobalSign®
GMO INTERNET GROUP

Mitigate Phishing and Spoof Emails

Verify origin of emails and sender identity

Sending emails from a forged sender address, called email spoofing, is one of the most popular methods for carrying out a phishing attack. Digitally signing emails counters this threat by clearly presenting the email sender's verified identity information. Email recipients can be sure that the email came from a legitimate, verified source and not a spoofed address.



Example: Digitally signed email in Microsoft Outlook

Prevent Data Loss and Leaks

Protect email communications in transit and on mail servers

Encrypted emails can only be decrypted by the intended recipient. This is due to the cryptographic process that takes place during encryption. The email is encrypted with the recipient's public key and can only be decrypted with the corresponding private key.

This means that no one else can decrypt the email and read its contents, whether an outsider gains access to your company's mail server or if the email is obtained in transit.

Example: Encrypted email in Microsoft Outlook

Certificate Provisioning and Management

GlobalSign's S/MIME Certificates scale to accommodate businesses of all sizes, from individuals to small and mid-sized business to large enterprises, with certificate lifecycle management and automation technologies to simplify high volume deployments.

- **MANAGED PKI PLATFORM**
  Organizations requiring more than five certificates can benefit from GlobalSign's Managed PKI (MPKI) platform, which offers significant volume discounts compared to purchasing individual certificates, centralizes billing information and enables administrators to efficiently issue, renew and revoke certificates as needed.

- **ACTIVE DIRECTORY INTEGRATION**
  Automate deployments by leveraging existing Active Directory architecture and Group Policy to provision and silently install certificates for domain-joined Windows and Apple OSX endpoints.

- **INDIVIDUAL CERTIFICATES**
  For organizations that only require a few certificates (< 5), orders can be placed directly through the GlobalSign website. Renewal reminder emails are sent when each certificate is approaching expiration.

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