DATASHEET

加强电子邮件安全

验证发件人身份并加密敏感通信

功能 & 优势

证明信息来源
对电子邮件进行数字签名可验证发件人的身份，向收件人保证电子邮件的合法性

对传输中和静态信息进行加密
加密电子邮件可确保只有目标收件人才能访问电子邮件内容，无论电子邮件位于何处

内容完整性
对电子邮件进行数字签名可对信息内容进行防篡改密封，确保信息的完整性

本地兼容性
无需额外软件；与主流企业电子邮件客户端（Outlook、Thunderbird、Apple Mail、Lotus Notes 等）兼容

大规模自动化部署
使用证书自动化管理器 (CAM)，大规模高效管理 S/MIME 证书

选择您的签名算法
选择 SHA256RSA 或 RSASSA-PSS（仅限 PKI 托管用户）

监管合规
SMIME 通过确保敏感通信的安全，帮助企业遵守 GDPR 和 HIPAA

随着网络犯罪分子的日益猖獗，电子邮件仍然是最主要的攻击载体，**91%** 的安全漏洞都是由电子邮件造成的。假冒和网络钓鱼等常见攻击利用电子邮件漏洞，欺骗收件人共享敏感信息或转移资金。
S/MIME 证书通过对电子邮件进行数字签名来验证发件人的身份，并对信息进行加密以确保机密数据的安全，从而提供强有力的保护。

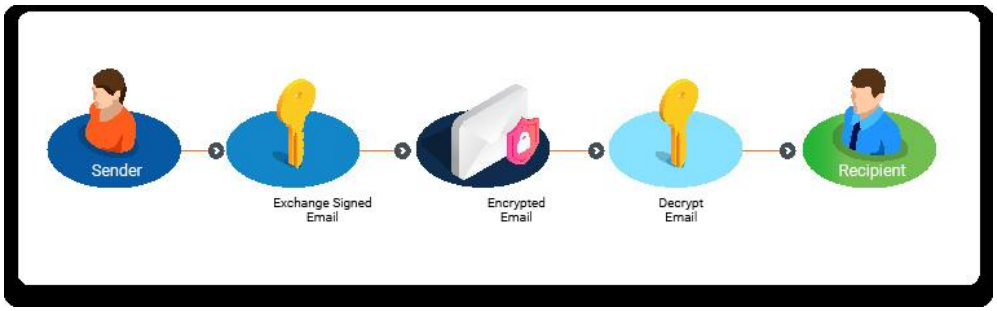
什么是 S/MIME？

S/MIME（Secure/Multipurpose Internet Mail Extensions，安全/多用途互联网邮件扩展）可确保电子邮件的完整性和保密性，防止拦截和冒充。S/MIME 是通过数字签名和加密确保电子邮件通信安全的公认行业标准。

S/MIME 证书提供两种基本加密功能：

- **数字签名** - 验证电子邮件的发件人身份，并创建一个唯一的数字指纹（或哈希值）以防止篡改，从而向收件人保证电子邮件来自可信来源，其内容在传输过程中未被篡改。
- **加密** - 以加密方式保护电子邮件，使其只能由预定收件人打开，没有相应私人密钥的任何人都无法阅读。

S/MIME 加密工作流程

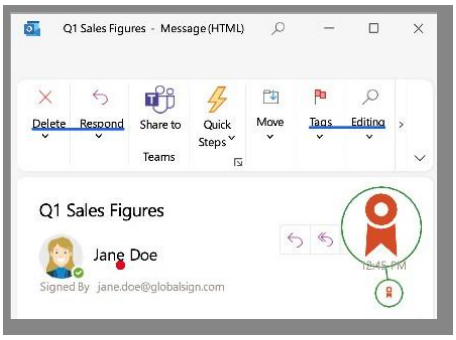


防范常见的电子邮件威胁

- 防止冒充攻击 - 数字签名可验证发件人身份，确保电子邮件来自可信来源，而不是冒充同事或高管的攻击者。
- 阻止网络钓鱼和恶意软件企图 - 经过验证的电子邮件更容易发现网络钓鱼计划和恶意附件，从而降低有害互动的风险。
- 防止数据泄露--加密可确保敏感信息受到保护，只有目标收件人才能访问电子邮件内容。
- 防止账户被接管 - 即使电子邮件账户被入侵，加密技术也能防止未经授权访问敏感信息。

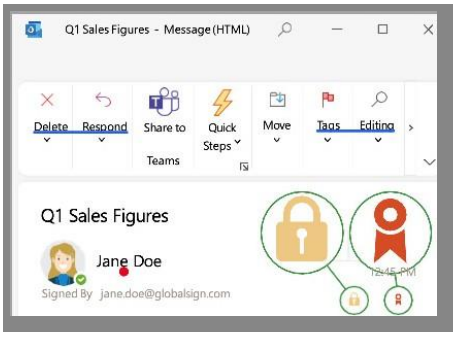
数字签名电子邮件

验证邮件来源和发件人身份



加密邮件

保护传输中和邮件服务器上的电子邮件通信



证书供应、管理和 Active Directory 集成

GlobalSign 的 S/MIME 证书可扩展以适应各种规模的企业，从个人、中小型企业到大型企业。利用 GlobalSign 的证书自动化管理器 (CAM) 等证书生命周期管理和自动化技术，可简化大批量部署。CAM 还与 Active Directory 集成，通过利用现有架构和组策略为域连接的 Windows 和 Apple OSX 端点提供和静默安装证书，从而实现自动化部署。

企业 PKI 平台

需要五张以上证书的组织可受益于 GlobalSign 的企业 PKI (EPKI) 平台。该平台可集中管理计费信息，使管理员能够根据需要有效地签发、更新和撤销证书，为需要更多证书的企业提供简化的管理解决方案。

个人证书

对于只需要少量证书（< 5 个）的组织，可直接通过 GlobalSign 网站下订单。当每张证书即将到期时，将发送续订提醒电子邮件。

与当地团队取得联系 - 访问

http://www.globalsign.cn/company/contact

关于 GlobalSign

作为世界上根基最牢固的证书颁发机构之一，GlobalSign 是可信身份和安全解决方案的领先提供商，可帮助全球组织、大型企业、基于云的服务提供商和物联网创新者进行安全的在线通信、管理数以百万计的经过验证的数字身份并自动进行身份验证和加密。该公司的大规模 PKI 和身份解决方案为物联网中的数十亿服务、设备、人和物提供支持。GMO GlobalSign 是日本 GMO Cloud KK 和 GMO Internet Group 的子公司，在美洲、欧洲和亚洲设有办事处。

GlobalSign® by GMO