DATASHEET

用于电子邮件安全的S / MIME证书

加密敏感的内部通信并验证电子邮件来源以阻止网络钓鱼

恶意方越来越擅长通过电子邮件锁定企业，包括拦截邮件以查看敏感信息或电子邮件欺骗，目的是推向钓鱼网站或触发恶意软件下载。使用S / MIME证书对电子邮件进行数字签名和加密，可以确保仅目标收件人可以访问电子邮件内容，还可以通过验证电子邮件来源来帮助区分合法电子邮件和恶意电子邮件，从而帮助组织保护自己免受这些威胁。

S/MIME是什么?

S / MIME或安全多用途Internet邮件扩展是针对基于MIME（基于消息）的数据进行公钥加密的行业标准。 S / MIME证书提供两个关键的电子邮件安全功能：

- 数字签名 – 可证明作者身份并防篡改,向电子邮件收件人保证电子邮件来自于您，而不是冒名顶替者，并且电子邮件的内容在传输过程中没有进行更改
- 加密 – 确保消息只能由预期的收件人打开，并防止敏感的消息落入坏人之手

主要特点

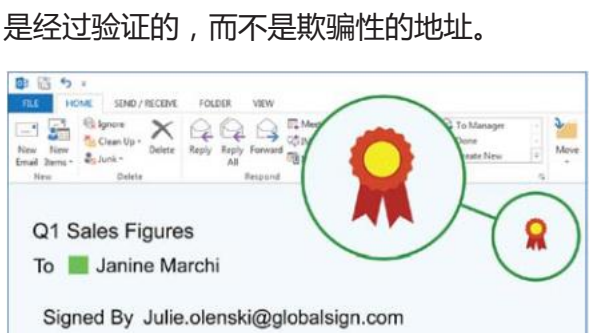
- **证明消息来源**
  对电子邮件进行数字签名可以验证邮件的来源，向收件人保证电子邮件是合法的，而不是伪造的
- **加密传输静态消息**
  加密电子邮件可确保只有预期的收件人才能访问电子邮件内容，无论电子邮件位于何处
- **内容的完整性**
  数字签名或加密电子邮件时会在邮件内容上创建一个防篡改的印章，从而确保邮件的完整性
- **兼容性**
  不需要其他软件，且与领先的企业电子邮件客户端（Outlook，Thunderbird，Apple Mail，Lotus Notes等）兼容。
- **方便终端用户**
  许多客户端还提供了针对所有传出邮件自动执行此操作的选项
- **选择你的签名算法**
  选择SHA256RSA或RSASSA-PSS（仅受管PKI用户）

GlobalSign
GMO INTERNET GROUP

减轻网络钓鱼和欺骗电子邮件

验证电子邮件的来源和发件人身份

从伪造的发件人地址发送电子邮件（称为电子邮件欺骗）是进行网络钓鱼攻击的最流行方法之一。通过对电子邮件进行数字签名，可以清楚地显示电子邮件发件人的已验证身份信息来应对这种威胁。电子邮件收件人可以确保电子邮件来自合法的，来源是经过验证的，而不是欺骗性的地址。



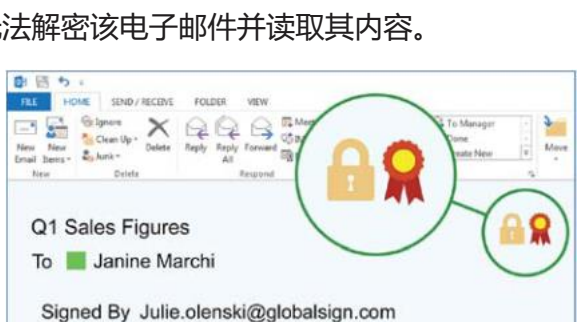
示例：微软 Outlook中经过数字签名的电子邮件

防止数据丢失和泄漏

保护传输中和邮件服务器上的电子邮件通信

加密的电子邮件只能由指定收件人解密。这是由于在加密期间发生的加密过程。电子邮件使用收件人的公钥加密，只能使用相应的私钥解密。

这意味着无论是外部人员是否可以访问您公司的邮件服务器，或者是否在传输途中获得了电子邮件，任何人都无法解密该电子邮件并读取其内容。



示例：微软 Outlook中的加密电子邮件

证书供应和管理

GlobalSign的S/MIME证书适用于各种规模的企业，从个人到中小型企业到大型企业，并具有证书生命周期管理和自动化技术来简化大批量部署。

- **PKI管理平台**

需要五个以上证书的企业可以从GlobalSign的Managed PKI（MPKI）平台中受益，该平台与购买单个证书相比提供大量折扣，集中计费信息，并使管理员能够根据需要有效地发行，续订和吊销证书

- **活动目录集成**

通过利用现有的Active Directory体系结构和组策略为加入域的Windows和Apple OSX端点设置和静默安装证书，从而自动执行部署

- **个人证书**

对于只需要少量几个证书（<5个）的企业，可以直接通过GlobalSign网站下订单。每个证书即将到期时，都会发送续订提醒电子邮件

关于GlobalSign

GlobalSign是全球领先的可信身份和安全解决方案提供商，致力于帮助全球的企业，大型企业，云服务提供商和物联网创新者保护在线通信，管理数百万个经过验证的数字身份，并自动进行身份验证和加密。 其高规格的公钥基础设施（ PKI ）和身份解决方案支持包括万物互联网IoE ）在内的数十亿服务，设备，人员和事物。

Tel: +86 021-60952260
www.globalsign.cn

GlobalSign
GMO INTERNET GROUP