

利用证书自动化管理 器将网络钓鱼风险降 至最低

为 Microsoft Outlook 部署
S/MIME 证书的更简便方法



客户利益

- 直接挂钩 Active Directory 和 Entra ID，使新设备和端点的注册、验证和配置变得简单
- 恢复密钥，以便在员工离职时轻松存档
- 验证组织内发送的每封电子邮件
- 利用 GlobalSign 强大的加密功能为每封邮件加密
- 通过单一界面管理各种使用情况下的证书--从 SSL/TLS 证书到 S/MIME 再到数字签名证书等等
- 体验对组织证书的全面控制-
-定期轮换或临时撤销证书
- 设置政策，然后让证书自动化管理器接管并完成其余工作

挑战

电子邮件仍然是企业首选的通信媒介。它也是黑客的主要切入点，黑客不断发现针对易受攻击员工的网络钓鱼和鱼叉式网络钓鱼诈骗以及商业电子邮件破坏攻击的成功案例。

最佳实践表明，您需要采取某些预防措施来确保 Microsoft Office 365 的安全，包括客户端身份验证和电子邮件加密。S/MIME 证书既能对电子邮件进行数字签名，也能对电子邮件进行加密，但由于采用 S/MIME 证书的历史障碍，企业通常不会部署 S/MIME 证书。由于必须为每个收件人管理证书和密钥，因此大规模部署尤其困难。

使用 S/MIME 证书的好处包括对发件人身份、信息完整性和身份验证进行加密验证，这使其成为希望降低网络攻击或数据泄露风险的企业的一个值得选择的方案。然而，S/MIME 传统上只用于需要更高水平保证和合规性的邮箱子集。目前的挑战是找到一种方法，使 S/MIME 能够被广泛采用，让所有员工都能享受到一目了然识别合法电子邮件的好处，并知道敏感或机密信息在传输和静止时都已加密。

背景介绍

随着远程工作者和电子邮件通信比以往任何时候都多，网络钓鱼威胁也达到了前所未有的高度。虽然社交媒体和即时通讯平台的发展和重要性日益凸显，但电子邮件仍然是日常生活中不可或缺的一部分。全球电子邮件用户数量已超过 42 亿，预计到 2026 年将继续增长到 47 亿以上（Statistica）。

这也就难怪，邪恶的黑客会利用我们对电子邮件的依赖，发送诈骗信息并窃取个人数据，这些数据可能会被用来勒索赎金，或在暗网上出售以获取高额利润。根据 SlashNext 的“网络钓鱼现状”报告，到 2023 年年中，网络钓鱼威胁达到峰值，每天 31,000 起，比 2020 年增加了 24%。

主要在人工智能等新技术的帮助下，制造更复杂攻击的障碍已经降低。因此，黑客不仅没有放慢脚步，他们制造更有说服力的欺诈或恶意电子邮件的能力还在增强。企业不能仅仅依靠网络安全培训，而是要寻找能够积极应对电子邮件安全的解决方案。



解决方案

GlobalSign 的证书自动化管理器在公司的 Active Directory 和我们的数字身份平台 Atlas 之间提供了一个直接网关，使 S/MIME 证书的注册和撤销变得简单高效。

Windows Active Directory 一直是企业简化 Windows 服务器、桌面和 SharePoint 等微软业务应用程序之间访问的主要方法。事实上，据 Frost & Sullivan 公司称，“AD 的使用非常普遍，全球《财富》1000 强企业中有 90% 都在使用它”。

“The use of AD is so common that approximately 90% of the Global Fortune 1000 companies use it.”

Frost &
Sullivan

对于已经使用活动目录的企业来说，证书自动化管理器是一个自然的解决方案，它允许 IT 管理员高效地向大量终端用户分发 S/MIME 证书。一旦安装了证书，终端用户的体验将是无缝的：数字签名电子邮件加密可自动应用于所有通信。

使用 S/MIME 证书对电子邮件进行数字签名有许多好处，包括：

- 将发件人经第三方验证的身份与电子邮件联系起来
- 明确标示经过验证的电子邮件，以帮助区分伪造邮件
- 支持不可抵赖性，防止邮件内容在发送后被更改

对于管理员来说，证书自动化管理器通过直观的用户界面提供了对 S/MIME 证书的简化管理。此外，它还具有可扩展性，使 IT 团队可以随着时间的推移，轻松将解决方案扩展到新的证书类型和用例。

使用案例

在大型大学系统中，终端用户的多样性和不断变化使得组织特别容易受到网络钓鱼欺诈的影响。近年来，网络钓鱼和鱼叉式网络钓鱼攻击的质量不断提高，忙碌的学术型员工越来越难以识别并向 IT 部门报告这些情况。鉴于学生信息的个人性质，一次数据泄露就可能引发公关灾难和长期经济损失。虽然管理层过去曾考虑过 S/MIME，但由于证书数量过多，以及建立新系统以帮助管理和跟踪所需的时间和资金等原因，S/MIME 一直没有得到推广。

使用 GlobalSign 的证书自动化管理器是一个简单的决定。它是一个直接连接到 Active Directory 的自动化解决方案，这意味着 IT 经理可以快速配置新的用户证书。IT 团队决定实施证书自动化管理器的另一个关键因素是它的跨平台代理支持在 Windows、Mac 和 Linux 机器和应用程序上注册。

S/MIME 证书不仅赢得了技术团队的青睐，而且还赢得了最终用户的青睐，因为合法发送的电子邮件中会出现易于识别的证书图标。由于需求量大，IT 管理员对证书自动化管理器和 GlobalSign 的基础架构能够承受极高的证书签发量表示赞赏，因此大学可以确信该解决方案将随着时间的推移而扩展。最重要的是，校领导们对拥有一个防止网络钓鱼诈骗、保护敏感电子邮件和其他数据安全的保障措施充满信心。

与当地团队取得联系 - 访问

<https://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。

