GlobalSign
GMO INTERNET GROUP

DATASHEET

基于证书的认证

保留正确的用户和设备；把错误的人拒之门外

密码不再是一种可靠的用户身份验证方法。来自恶意团体和希望携带自己设备（BYOD）的员工的流氓机器的威胁越来越大，这让许多人想知道他们如何控制哪些用户和机器可以访问和操作他们的网络。使用数字证书作为身份验证因素允许它识别端点，并将访问限制为只有经过批准的用户、机器和设备。

什么是基于证书的认证？

基于证书的身份验证是在授予对资源、网络、应用程序等的访问之前，使用数字证书来识别用户、机器或设备。在用户身份验证的情况下，通常与用户名、密码等传统方法协同部署。基于证书的身份验证的一个区别在于，与生物特征识别和一次性密码（OTP）等仅适用于用户的解决方案不同，相同的解决方案可以用于所有端点——用户、机器、设备甚至不断增长的物联网（IoT）。

好处

- **易于部署和持续管理**
  GlobalSign基于云的证书管理平台和可选的活动目录和MDM集成使管理员可以根据需要轻松签发和吊销证书
- **所有端点的一个解决方案**
  证书可以颁发给所有终端，包括用户、机器和设备
- **无需额外硬件**
  节省了成本，减轻了令牌管理的痛苦，并且对用户来说很容易（注意：对于更高保障的用例，证书可以作为加密硬件的一部分）
- **相互认证**
  通信中涉及的所有各方（用户、机器、设备）都可以识别自己
- **利用现有的访问控制策略**
  使用现有的组策略和权限启用基于角色的访问和控制，使端点可以访问不同的应用程序和网络
- **扩展到外部用户**
  外部用户（例如合作伙伴、独立承包商、自由职业者）可以访问您的网络，而不需要在本地机器上安装额外的软件或进行广泛的培训

基于证书的认证

DATASHEET

示例

用户认证

替换密码或添加第二个身份验证因子来控制访问：

- Windows登录
- 企业电子邮件，内部网络或内部网
- 基于云的服务和应用程序（例如谷歌应用程序、Office 365、SharePoint、Salesforce）

机器和设备认证

通过以下方式防止恶意机器和设备访问：

- 识别需要与后端服务通信的现场/现场机器（例如，位于便利店的付款亭）
- 在允许员工访问WiFi网络、vpn、网关、网络服务等之前，识别所有员工的笔记本电脑和移动设备。
- 标识企业内的所有服务器以启用相互身份验证

证书发放与管理

GlobalSign的认证证书规模适用于各种规模的企业，从中小型企业到大型企业，证书生命周期管理和自动化技术简化了大规模部署。

托管PKI平台

GlobalSign的托管PKI（MPKI）平台简化了证书管理，与单独购买证书相比，提供了显著的批量折扣，集中了账单信息，并使管理员能够根据需要有效地签发、更新和吊销证书。

Active Directory集成

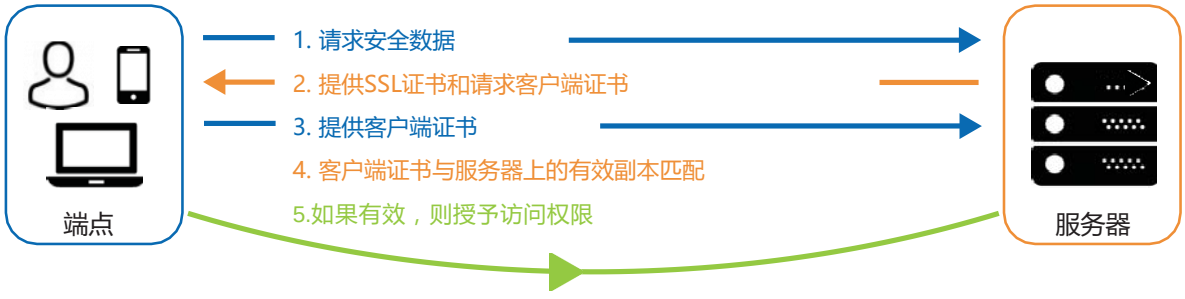
通过利用现有的Active Directory架构和组策略来自动化部署，为加入域的Windows和Apple OSX端点提供并静默安装证书。

移动设备管理（MDM）集成

GlobalSign与AirWatch和MobileIron等MDM平台的集成，消除了IT员工在每个员工设备上手动安装证书的需要。只要新设备在MDM平台注册，就会向该设备颁发GlobalSign数字证书。

如何运作

服务器向客户端请求数字证书，以验证客户端是否是他们声称的身份。该证书必须是X.509证书，并且必须由受信任的证书颁发机构（CA）签名，因为服务器将根据其受信任证书列表对其进行检查，只有这样才能建立安全会话。



关于GlobalSign

GlobalSign是全球领先的可信身份和安全解决方案提供商，使全球的企业、大型企业、云服务提供商和物联网创新者能够确保在线通信的安全，管理数百万已验证的数字身份以及自动化认证和加密。其大规模公钥基础设施（PKI）和身份解决方案支持数以亿计的服务、设备、人和物组成的万物互联（IoE）。

CN: +86 021 60952260

www.globalsign.cn

GlobalSign GMO INTERNET GROUP