GlobalSign
GMO INTERNET GROUP

DATASHEET

基于证书的身份验证

保留合适的用户和设备; 不合适的则进行处理

密码不再是可靠的用户身份验证方法。恶意方和想要携带自己的设备（BYOD）的员工的恶意机器的威胁越来越大，因此产生了很多疑问，他们想知道如何控制哪些用户和机器可以访问和在其网络上运行。使用数字证书作为身份验证因素，它可以识别端点并将访问权限限制为仅允许批准的用户，机器和设备。

什么是基于证书的身份验证？

基于证书的身份验证是在授予对资源，网络，应用程序等的访问权限之前，使用数字证书来标识用户，机器或设备。对于用户身份验证，通常与传统方法（如用户名和密码）配合部署。基于证书的身份验证的一个区别是，与某些仅对用户有效的解决方案（例如生物识别和一次性密码（OTP））不同，该解决方案可以用于所有端点-用户，机器，设备，甚至是不断发展的物联网（IOT）。

优点

- **易于部署和管理**
  GlobalSign的基于云的证书管理平台以及可选的Active Directory和MDM集成使管理员可以根据需要轻松地颁发和吊销证书
- **关于端点的一种解决方案**
  证书可以颁发给所有端点，包括用户，机器和设备
- **没有额外的硬件**
  节省成本，减轻令牌管理的麻烦，更加易于用户使用（注意：对于更高保证的使用案例，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来启用基于角色的访问并控制哪些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，而无需在其本地计算机上安装额外的软件或进行广泛的培训

用例示范

用户身份验证

替换密码或添加第二个身份验证因素以控制对以下内容的访问：

- Windows登录
- 公司电子邮件，内部网络或内部网
- 基于云的服务和应用程序（例如Google，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进行通信的位置/现场机器（例如，位于便利店的付款亭）
- 在允许访问WiFi网络，VPN，网关，Web服务等之前，先确定所有员工笔记本电脑和移动设备
- 识别企业内的所有服务器以启用相互身份验证

证书供应和管理

GlobalSign的身份验证证书可以扩展，以适应从中小型企业到大型企业的各种规模的业务，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

GlobalSign的PKI管理（MPKI）平台简化了证书管理，与购买单个证书相比，提供了大量折扣，集中了计费信息，并使管理员能够根据需要有效地发行，更新和吊销证书。

Active Directory集成

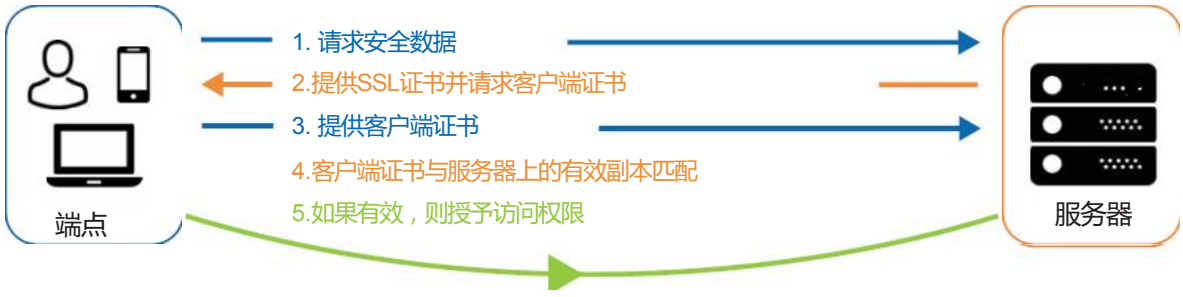
通过利用现有的Active Directory体系结构和组策略为加入域的Windows和Apple OSX端点设置和静默安装证书，从而自动执行部署。

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人员在每个员工设备上手动安装证书的需要。一旦将新设备注册到MDM平台，就会向该设备颁发GlobalSign数字证书。

运行原理

服务器从客户端请求数字证书，以验证他们是否是自己声称的那个人。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的证书列表对其进行检查，然后才会建立安全会话。



关于GlobalSign

GlobalSign是全球领先的可信身份和安全解决方案提供商，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。

021-60952260
www.globalsign.cn

GlobalSign GMO INTERNET GROUP