DATASHEET

基于移动设备

通过移动PKI支持BYOD和安全的企业设备

公钥基础结构（PKI）是一种已知且受信任的安全技术，企业数十年来一直使用该技术对企业中的用户，计算机和服务器进行身份验证。安装在移动设备上的证书可确保只有授权的设备和用户才能访问公司资源并启用移动电子邮件的安全和加密，从而使企业能够平衡员工在移动过程中访问电子邮件和公司数据的需求和防止未经授权访问关键业务应用程序的需求。

一个为移动和桌面的解决方案

PKI用于保护所有端点，无论是移动端还是桌面、外部还是内部。可以对设备本身进行标识和认证，以防止恶意设备访问，并且可以将基于桌面的用户身份转移到移动设备，以实现强大的用户认证以及S / MIME电子邮件加密和安全性。适用于所有端点的解决方案既可以为最终用户创建一个安全的，用户友好的环境，又可以创建健壮，高度可扩展且易于管理的基础架构。

优势

- **防止恶意设备访问**
  确保仅授权设备可以访问公司网络和资源(例如，电子邮件，WiFi，VPN）
- **支持BYOD或公司拥有的设备**
  证书与领先的移动操作系统本地兼容，可以部署到公司网络内部或外部的设备上
- **自动化部署**
  MDM / EMM集成可自动在设备上提供数字身份，而无需最终用户交互或采取手动操作
- **MDM / EMM集成**
  通过与AirWatch，MobileIron(思可信)和微软设备的集成轻松管理证书
- **方便最终用户**
  安装证书后，最终用户可以无缝地对资源进行身份验证并对电子邮件进行加密和签名
- **覆盖所有端点**
  一个针对桌面和移动终端的解决方案简化了部署并降低了成本
- **证书吊销**
  它可以轻松地远程撤消证书，以解决离开或丢失的设备

GlobalSign
GMO INTERNET GROUP

使用PKI解决三大移动设备安全挑战

确保用户通过移动设备对应用程序，服务和资源进行安全访问

从移动设备访问公司网络和资源可为员工提供更大的灵活性来开展业务，但是建议不要使用密码来保护这种访问。 与台式机一样，您需要考虑通过移动设备进行访问的多因素身份验证措施。

基于证书的身份验证可确保只有具有正确配置的证书的授权用户才能通过其移动设备访问公司资源。终端用户无需额外的应用程序或令牌，只需要为桌面和移动终端管理提供一个解决方案。

防止恶意设备访问

VPN，WiFi，电子邮件系统和其他网络是恶意方的常用入口点，一旦它们可以访问，就更容易窃听和拦截流量或传播恶意软件。确保只有经过授权的设备才能访问和操作您的网络是至关重要的。

通过为移动设备（BYOD或公司拥有的）提供证书，您可以识别和控制哪些设备可以访问哪些资源，并有助于防止恶意设备访问。

电子邮件加密和签名

电子邮件访问通常是希望使用移动设备进行工作的员工的最常见请求，但是在授予访问权限之前，必须像台式桌面邮件客户端一样采取安全预防措施。

电子邮件加密和数字签名的S/MIME证书可以添加到员工设备中，以帮助应对一些最大的安全威胁并满足法律的合规性。最终用户可以轻松地对电子邮件进行加密以保护内容，并对他们的消息进行数字签名以证明作者身份并与欺骗性电子邮件区分开。

通过MDM和EMM平台集成自动化部署

移动设备管理（MDM）和企业移动性管理（EMM）平台使企业可以轻松地将证书部署到移动设备上。通过直接连接到GlobalSign的托管证书服务，企业可以使用MDM和EMM平台实现完全自动化证书供应和管理，从而实现安全的BYOD并防止未经授权的访问。集成使IT人员不必在每个员工设备上手动安装和管理证书，从而减轻了管理负担并降低了总拥有成本。

GlobalSign 目前支持与AirWatch, MobileIron和微软设备集成：

airwatch mobile device management

MobileIron (Cloud and Core platforms)

Microsoft

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