Support BYOD and Secure Corporate Devices with Mobile PKI

PKI is a known and trusted security technology that organizations have been using for decades to authenticate users, machines, and servers within their organizations. Expanding PKI to devices creates an easy to implement and cost effective identity management solution for both employee- and company-owned devices.

Digital certificates can be used on mobile devices for:

**Email Encryption and Signing**
Encrypt and digitally sign email communications sent via devices, ensuring privacy of sensitive information and proof of authorship/message origin.

**Email Authentication**
Enable email authentication for 24 x 7 email access without leaving email accounts vulnerable to intruders, only authorized devices will be able to access your corporate email servers.

**VPN and Wi-Fi Authentication**
Replace weak and vulnerable username and passwords with multi-factor authentication for corporate Wi-Fi and VPN connections, only approved devices will be able to access your enterprise connections.

Enable Convenient and Secure Mobile Access for Customers and Devices

OAuth 2.0 is one of the primary protocols behind secure identities on mobile devices. In simple terms, OAuth 2.0 enables a standard way of accessing protected resources using an existing identity. A typical use case would be using a Facebook credential to access another online service or an application.

GlobalSign’s identity and access management (IAM) solution supports OAuth 2.0 to deliver:

**Social Login from Mobile Users**
Enable mobile users to login to a third-party application, service, or the mobile app using their social (Facebook, Google, etc.) credentials – providing a convenient user experience.

**Email Authentication**
Enable email authentication for 24 x 7 email access without leaving email accounts vulnerable to intruders, only authorized devices will be able to access your corporate email servers.

**Strong Authentication for Mobile Devices**
Add ‘weak-to-strong’ authentication for mobile applications to conduct more secure transactions by supporting 20+ authentication methods.

**Authentication Services for Connected Devices**
Secure data communications between devices and applications with password grant and API protection using OAuth 2.0

**AirWatch MDM Integration**
GlobalSign's integration with AirWatch connects GlobalSign's Managed PKI solution directly to the AirWatch MDM platform allowing enterprises to streamline provisioning of digital certificates onto devices. The integration relieves IT staff from having to manually install certificates on each employee device. As soon as a new device is enrolled with AirWatch a GlobalSign digital certificate will be issued to the device.

**GlobalSign OAuth 2.0 Authorization Server**
GlobalSign SSO, the Identity Provider (IdP) of its IAM solution suite, has built-in support for OAuth 2.0 and acts as an authorization server. With support for 20+ out-of-the-box authentication methods, including multi-factor out-of-band mechanisms, developers of mobile apps, desktop applications and device manufacturers can provide the right method for identity verification and authentication.

Contact us for more information about mobile identity and authentication services.

www.globalsign.com | sales@globalsign.com