

Mobile Authentication

Control which devices access your corporate networks

Mobile Devices in the Enterprise

Every day the number of Enterprises and employees relying on devices to conduct business is increasing, giving Enterprises and users flexibility to stay connected whether in the office or on the road. While this increased level of connectivity is beneficial for the Enterprise, opening sensitive business services to mobile device users creates serious security risks and vulnerabilities that must be addressed.



Securing Devices with Digital Certificates

Certificate-based authentication utilizing X.509 Digital Certificates are the perfect fit for the “bring your own device” era. Digital Certificates are an easy to implement and cost effective device authentication solution allowing organizations to balance employees desire to use their own mobile devices for work and the need to protect against unauthorized access to key business applications. Network Administrators can issue certificates to approved devices allowing users to access business services without relinquishing employee control of their mobile device.

Benefits to the Enterprise

- Streamlined business processes and decision making with device access anytime, anywhere (24 x 7 workforce)
- Mitigated risk associated with access to core business systems via mobile devices, no need to open up

Supported Mobile Devices

Digital Certificates are natively supported on various device platforms and can easily be imported onto devices controlling which users can access gated applications and networks while keeping rogue devices out. Whether your organization has all android devices or a mix of device types digital certificates allow users to securely access applications, cloud services and networks.



Certificate Management Made Easy- GlobalSign EPKI

GlobalSign digital certificates are available via a robust web-based management platform known as EPKI, allowing Enterprises to manage the full lifecycle of multiple digital certificates for the entire enterprise.

- Easy management of Certificate lifecycles (issuing, revoking, cancelling, reissuing, etc.)
- Simplified Certificate delivery with over-the-air enrollment

Below is a sample deployment of how GlobalSign digital certificates can be easily provisioned to devices.



Bulk Certificate Processing

GlobalSign’s EPKI platform allows the bulk upload of records, saving the administrator time when multiple employees require certificates. Bulk provisioning provides an alternative to bulk enrollment in that the enrollment steps performed by the end user are minimized or in some cases totally eliminated.

Bulk Provisioning Benefits:

- Easy method to provision a large number of certificates
- Single file PKCS12 delivery allows for easy back up
- Server side key generation eliminating local key generation
- Administrator can enroll on behalf of the end user allowing more control of the certificate provisioning and back up

Certificate Profiles for iOS Devices

iOS devices utilize configuration profiles which is a file that contains specific configures settings for iOS devices including password policies and policies for Wi-Fi, VPNs, Exchange Active Sync and applications. Configuration profiles quickly load settings and authorization information onto a device.

GlobalSign’s allows for streamlined distribution of configuration profiles via GlobalSign’s EPKI Platform which easily provisions the profiles to devices using digital certificates delivered via over the air enrollment..