



## DATASHEET

# Securing Mobile Devices

## Support BYOD and Secure Corporate Devices with Mobile PKI

Public Key Infrastructure (PKI) is a known and trusted security technology that organizations have been using for decades to authenticate users, machines and servers within their organizations. Certificates installed on mobile devices ensure only authorized devices and users can access corporate resources and enable mobile email security and encryption, allowing organizations to balance employee desire to access email and corporate data on the go with the need to protect against unauthorized access to key business applications.

### One Solution for Both Mobile and Desktop

PKI is a powerful option for securing all endpoints whether mobile or desktop, external or internal. The devices themselves can be identified and authenticated to prevent rogue device access and desktop-based user identities can be transferred to mobile devices to enable strong user authentication and S/MIME email encryption and security. One solution for all endpoints creates both a secure, user friendly environment for end users and a robust, highly scalable and easy to manage infrastructure for IT.

## BENEFITS

- **PREVENT ROGUE DEVICE ACCESS**  
Ensure only authorized devices can access corporate networks and resources (e.g. email, WiFi, VPN)
- **SUPPORT BYOD OR CORPORATE-OWNED DEVICES**  
Certificates are natively compatible with leading mobile operating systems and can be deployed to devices within or outside the corporate network
- **AUTOMATE DEPLOYMENTS**  
MDM/EMM integrations automatically provision digital identities on devices without end user interaction or manual steps from IT
- **MDM/EMM INTEGRATIONS**  
Easily manage certificates utilizing AirWatch or MobileIron or GlobalSign's Cloud PKI service
- **EASY FOR END USERS**  
Once certificates are installed, end users can seamlessly authenticate to resources and encrypt or sign emails
- **COVER ALL ENDPOINTS**  
One solution for both desktop and mobile endpoints simplifies deployments and decreases costs for IT
- **CERTIFICATE REVOCATION**  
IT can easily and remotely revoke certificates to address departures or lost devices

## Solve 3 Major Mobile Device Security Challenges with PKI

### Secure User Access to Apps, Services and Resources via Mobile Device

Accessing company networks and resources from mobile devices offers employees greater flexibility to conduct business, but relying on passwords to secure this access is ill-advised. You need to consider multi-factor authentication measures for access via mobile device, just as you would for desktops.

Certificate-based authentication ensures only authorized users with correctly configured certificates can access corporate resources via their mobile device. End users aren't burdened with additional apps or tokens and IT only has to manage one solution for both desktop and mobile endpoints.

### Prevent Rogue Device Access

VPNs, WiFi, email systems and other networks are common entry points for malicious parties and once they have access, it's easier to eavesdrop and intercept traffic or spread malware. Ensuring only authorized devices can access and operate on your networks is critical.

By provisioning certificates to mobile devices (either BYOD or corporate-owned), you can identify and control which devices can access which resources and help prevent rogue device access.

### Email Encryption and Signing

Access to email is generally the most common request from employees who want to use their mobile devices for work, but security precautions must be taken, just as they are with desktop email clients, before access can be granted.

S/MIME Certificates for email encryption and digital signatures can be added to employee devices to help counter some of the biggest security threats and meet compliance. End users can easily encrypt email to protect contents and digitally sign their messages to prove authorship and differentiate from spoofed emails.

## Automate Deployments with MDM and EMM Platform Integrations

Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) platforms make it easy for organizations to deploy certificates to mobile devices. By connecting directly to GlobalSign's hosted certificate services, organizations can use the MDM and EMM platforms to completely automate certificate provisioning and management enabling secure BYOD and preventing unauthorized access. The integrations relieve IT staff from having to manually install and manage certificates on each employee device, removing administration burdens and decreasing total cost of ownership.

GlobalSign currently supports integration with:



### About NSS

NSS is an international Value Added Distributor of leading edge IT solutions, covering technology areas including information security, networking, unified communications, data storage, virtualization and data centre infrastructure systems. Through high technology and deep knowledge of the marketplace, NSS executes the due diligence to select leading edge strategic partnerships with superior vendors and leading technologies that give our channel an opportunity to differentiate from the competition in a crowded market through first class proven solutions.



NSS  
330 Iera Odos Ave. & 1 Koritsas St.  
12243 Egaleo  
Athens, Greece  
T: +30 210-5914326  
E: [info@nss.gr](mailto:info@nss.gr)

For additional information please visit:  
[www.nss.gr](http://www.nss.gr)