GlobalSign Enterprise Solutions

Secure Mobile Access User Guide

Android Identity Certificates EPKI for Network Authentication
# Table of Contents

Table of Contents ......................................................... 2
Introduction ........................................................................... 3
Device Configuration .......................................................... 3
Step 1 - Establishing an EPKI Account .................................. 3
Step 2 - Registering Users for Android Identity Certificates .......... 8
Step 3 - Certificate Installation ............................................ 11
Android Certificate Management .......................................... 18
Appendix A - Additional Certificate Management - EPKI Admin Guide ......................................................... 18
Appendix B – Certificate Installation for a CSP Certificate ..................... 18
GlobalSign Contact Information ............................................. 22
Introduction
With the adoption of digital certificate technology, Android devices (such as Nexus, Galaxy, and HTC) are proving to be a viable and secure method to remotely access internal networks via the Enterprise. GlobalSign’s PersonalSign digital certificates delivered through EPKI are designed to permit access from all sorts of end points including Android devices to corporate business services such as VPN, Wi-Fi, and email.

Device Configuration
Once the certificate is installed it will need to be configured to work with the VPN, Wi-Fi, applications, etc. that the administrator would like the device to have access to. At this point in time there are no easy configuration tools for Android. Each device will need to be manually configured and third-party applications will need to be used to connect to certain VPN clients, use S/MIME, etc.

It is recommended to have a strategy for what you are looking to provide access to and what sort of applications or native capabilities will need to be leveraged to do so. The following are two examples of device configuration guides for VPN and S/MIME:

- Cisco VPN Client
- Djigzo for S/MIME

A Mobile Device Management (MDM) solution is also recommended to help you with the configuration process.

Step 1 - Establishing an EPKI Account
If you do not already have a GlobalSign EPKI Account, you will need to register for an EPKI account and setup a Certificate Profile. A Certificate Profile will serve as a pre-vetted organization template containing the organization’s identity records (such as organization name, city, state, etc) that end user certificate requests will be issued from. Verifying the organization’s identity associated with a profile typically takes between 2 and 3 business days.

If you already have an EPKI Account, please proceed to Step 2 - Registering Users for Android Identity Certificates.

If you do not already have an EPKI Account, please follow the instructions below:

1. Navigate to https://www.globalsign.com/authentication/mobile/supported-os.html. Click How To Buy. An account representative will be in contact with you shortly to help you decide the best options for your EPKI account. The next step will be to register for an EPKI account.

2. Register for an EPKI account by entering your account details. Note: this is not the vetted profile information.
3. Choose a username and password. An account number (PAR####) will be appended to the username you choose. Click Next to continue.

4. Confirm your account information and review the Terms of Service Agreement. Be sure to double check that all information is entered correctly. Click Next to continue.
5. Choose the license pack size of Identity Certificates you wish to purchase. Click **Next**.
6. Choose a validity period to be applied to your license pack (1-3 years).

**Optional** - Add an additional technical contact (this is commonly used when you are applying on behalf of someone else). Click Next to complete.

7. Enter the Certificate Profile Details. These details will be vetted and included as the certified identity within your issued certificates. Click Next to continue.

**Important** - make sure the details entered are correct as GlobalSign will vet the details you include.
8. Complete the payment details.

9. Confirm your order details. Review and agree to the EPKI Service Agreement. Click Next when finished.

10. The next screen will display your username and information about your profile. Save this information for your records.

Once you have successfully created an EPKI account, your information will be sent to our vetting team. Vetting your organization details can take up to 2-3 business days. Once the vetting process is complete, you will receive an email notifying you of its completion.

Once your EPKI account is setup and established, please continue to Step 2 – Registering Users for Android Identity Certificates
Step 2 - Registering Users for Android Identity Certificates

There are three options that the EPKI Administrator can use to “invite” users to apply for pre-approved digital certificates:

- Single – New Certificate (Order Certificates)
- Multiple – New Certificate BULK (Order Certificate BULK)
- Multiple – New Certificate Registration and Pick-up PKCS#12 BULK (PKCS#12 Bulk Registration and Pickup)

The following steps will walk you through the single invite process using the Order Certificates function. If you are looking to invite multiple users please refer to the instructions found in the EPKI Administrator Guide: https://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf

1. Login to your GlobalSign Certificate Center (GCC) account at www.globalsign.com/login/.

2. Select the “Enterprise PKI” tab found on the top menu bar.

   ![Enterprise PKI Tab](image)

   Please note: if this is your first time logging in your menu options will be limited. For first time users, you will need to enroll for an “EPKI Administrator Certificate”, which is an authentication certificate needed to access secure areas of GCC such as the Certificate Management section. Please follow the steps below to enroll for your administrator certificate.

   a. Click the Get EPKI Administrator Certificate link in the left hand menu to start the enrollment process.
   b. Follow the prompted steps to enroll and install your certificate.
   c. If you need further assistance and detailed instructions on how to enroll for your EPKI Administrator Certificate, please see our administrator guide located at https://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf

3. In the left hand menu, select Order Certificates under My Certificates.

   ![Order Certificates Menu](image)

4. Next, select the Profile and License pack that you want to issue the certificate from. In most cases there will be only one option for each area. Click Next.
Next, complete the Certificate Identity Details. Note it is highly recommended that you select the PKCS12 option when ordering the certificate. This format is easily accepted by Android devices and will provide the simplest installation experience for the user. If you do not select this option the certificate will be issued in a CSP format.

Provide the end-user identity details.

a. **Important** - Establish a one-time Pickup Password. The user will need this password to install the certificate onto their device; you must deliver this Pickup Password in an out-of-band method.

b. **Optional** - enter a reason or note associated with the registration. This note will appear in the Order History section of EPKI and may be useful for audit purposes.

Click **Next** to continue.
6. Review and confirm registration details. If satisfied, click **Next** to complete the registration.

The registration is now complete and as indicated the Enrollment Invite will be sent to the email address specified in the Certificate Identity Details. Please continue to **Step 3 – Certificate Installation** to see how the user will complete the certificate pick-up and installation.
Step 3 - Certificate Installation

Certificate delivery can be completed using an over-the-air enrollment method, where the certificate enrollment is sent directly to the user’s Android device and is picked up via an email that will be delivered to the email address specified during registration. As mentioned, in order for the certificate to install correctly the certificate must be in the proper format.

Android supports DER-encoded X.509 certificates, saved in files with a .crt or .cer file extension. Android also supports X.509 certificates saved in PKCS#12 key store files with a .p12 or .pfx extension. If your file is in some other extension it is important to change it to a compatible extension.

The following process will walk the user through installing a PKCS#12 format certificate. If you issued the certificate in a CSP format please refer to Appendix B: Certificate Installation for a CSP Certificate for the correct installation steps. If you would like to issue the certificate as a PKCS#12 certificate please review the steps outlined in Step 2 - Registering Users for Android Identity Certificates.

To pick up a certificate via an Android Device:

1. The user will receive an email on their Android device containing instructions on how to install their new Certificate. This enrollment email can be customized for your users. Please view the Customizing Email Templates section of the EPKI Administrator Guide for instructions: https://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf
2. The user will be instructed to click the installation link provided in the email.

3. With the link open in the browser, the user will be prompted to enter their one-time certificate Pick-up password previously provided by the EPKI Administrator in an out-of-band method. The user enters their Pick-up Password and clicks Next to continue.

4. The user will then be prompted to create a PKCS12 Passphrase and agree to the GlobalSign Subscriber Agreement. The password must be a minimum of 12 characters and only alpha-numeric values (A-Z, 0-9) are accepted. Once complete
they click **Next** to continue.
5. The certificate is now ready to be downloaded to the device. The user clicks **Download My Certificate** to finish installing the certificate.

The certificate will now appear in the **Downloads** on the device.
6. To complete the install, the user will need to go to the device **Settings** and navigate to the **Security** settings on the device.

![Security Settings](image)

7. In the Security settings, the user scrolls down to the bottom of the list to select **Install from phone storage**.

![Security Settings](image)
8. From the available device storage locations the user selects **Internal Storage**.

9. The user navigates to the **Download** folder.

10. The user selects the downloaded certificate .pfx file from the list of available files.
11. The device will now prompt the user to enter in the PKCS12 Passphrase which was created during the certificate enrollment process (step 4). Once entered the user clicks **OK** to continue.

12. The device will now allow the user to set the **Certificate Name** and the **Credential Use**. The Credential Use can be set to either VPN and Apps or Wi-Fi depending on the certificate’s purpose. You can also see here the certificate package contains the user key, user certificate, and the CA certificate. The user clicks **OK** to continue.
13. The certificate is now successfully installed on the user’s device.

Android Certificate Management
The EPKI platform provides several methods to manage the lifecycle of your Android Identity Certificates.

- **Reissuance**: Allows certificates to be reissued with exact same identity details and expiration date at no extra cost.

- **Revocation**: Certificates may be revoked placing the serial number of the revoked certificate on the GlobalSign Certificate Revocation List (CRL).

- **Renewal**: Allows certificates to be renewed to avoid expiration.

For further details on how to reissue and revoke certificates please see our administrator guide located at https://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf

Unsupported:
Please note that EPKI for Android does not support the following EPKI functions that are applicable to standard EPKI PersonalSign users:

- Encrypted File System (EFS) extended key usage
- Smartcard logon extended key usage
- Private key un-exportability

Appendix A - Additional Certificate Management - EPKI Admin Guide
For further instructions on managing your GlobalSign Certificate Center (GCC) Account, please see our EPKI Admin Guide http://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf

Appendix B – Certificate Installation for a CSP Certificate
Certificate delivery can be completed using an over-the-air enrollment method, where the certificate enrollment is sent directly to the user’s Android device and is picked up via an email that will be delivered to the email address specified during registration. As mentioned, in order for the certificate to install correctly the certificate must be in the proper format.

Android supports DER-encoded X.509 certificates, saved in files with a .crt or .cer file extension. Android also supports X.509 certificates saved in PKCS#12 key store files with a .p12 or .pfx extension. If your file is in some other extension it is important to change it to a compatible extension.

The following process will walk the user through installing a CSP format certificate. If you issued the certificate in a PKCS#12 format please refer to Step 3 – Certificate Installation for the correct installation steps. If you would like to issue the certificate as a PKCS#12 certificate please review the steps outlined in Step 2 - Registering Users for Android Identity Certificates.

To pick up a certificate via an Android Device:

1. The user will receive an email on their Android device containing instructions on how to install their new Certificate.
   This enrollment email can be customized for your users. Please view the Customizing Email Templates section of the EPKI Administrator Guide for instructions: https://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf
2. The user will be instructed to click the installation link provided in the email.

![Email message showing the installation link](image1)

Dear Kimberly Johnson

Your digital certificate, Order ID MPS2014031455546, is ready for pickup.

Please click the link below to start the certificate download and installation process.

https://system.globalsign.com/cr/public/certificate/install.do?pn=eb47fcb358e48b1be33c9a3812e9ca888813d29

3. When prompted the user will need to select Google Chrome as the browser to complete the installation, as this is the only browser which supports key creation.

![Select browser prompt](image2)
4. With the link open in the browser, the user will be prompted to enter their Pick-up password. The user enters their Pick-up Password and clicks Next to continue.

5. The user will then be prompted to select the Cryptographic Service Provider (CSP). The 2048 (High Grade) option is recommended. The user will need to agree to the GlobalSign Subscriber Agreement and click Next to continue.
6. The certificate has now been generated and is ready to be installed. The user can now click on **Install My Certificate** to complete the installation to the device.

![Install your Digital Certificate and the Intermediate CA Certificates](image1)

Your Certificate has been generated, click the **Install My Certificate** button to install the Certificate onto your computer.

![Install My Certificate](image2)

We have detected that you are not using Internet Explorer. Please follow the below instructions to install your Certificate.

Click the **Install My Certificate** button to install your Certificate.

Also click the below buttons to install the Intermediate CA Certificates. 

Installing the CA Certificates will ensure that your Certificate will be trusted by your computer, and by others.

![Install CA Certificate](image3)

7. The device will now allow the user to set the **Certificate Name** and the **Credential Use**. The Credential Use can be set to either VPN and Apps or Wi-Fi depending on the certificate’s purpose. You can also see here the certificate package contains the user key and user certificate. The user clicks **OK** to continue.

![Intermediate CA Certificates](image4)

![Name the certificate](image5)

Certificate name:

CSP Test Cert

Credential use:

VPN and apps

The package contains:

- one user key
- one user certificate

![Cancel OK](image6)

Guide support pages for instructions on the Certificate.

> Go to Product Guide pages
8. The certificate is now successfully installed on the user’s device.

GlobalSign Contact Information

<table>
<thead>
<tr>
<th>GlobalSign Americas</th>
<th>GlobalSign EU</th>
<th>GlobalSign UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tel: 1-877-775-4562</td>
<td>Tel: +32 16 891900</td>
<td>Tel: +44 1622 766766</td>
</tr>
<tr>
<td><a href="http://www.globalsign.com">www.globalsign.com</a></td>
<td><a href="http://www.globalsign.eu">www.globalsign.eu</a></td>
<td><a href="http://www.globalsign.co.uk">www.globalsign.co.uk</a></td>
</tr>
<tr>
<td><a href="mailto:sales-us@globalsign.com">sales-us@globalsign.com</a></td>
<td><a href="mailto:sales@globalsign.com">sales@globalsign.com</a></td>
<td><a href="mailto:sales@globalsign.com">sales@globalsign.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GlobalSign FR</th>
<th>GlobalSign DE</th>
<th>GlobalSign NL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tel: +33 1 82 88 01 24</td>
<td>Tel: +49 30 8878 9310</td>
<td>Tel: +31 20 8908021</td>
</tr>
<tr>
<td><a href="http://www.globalsign.fr">www.globalsign.fr</a></td>
<td><a href="http://www.globalsign.de">www.globalsign.de</a></td>
<td><a href="http://www.globalsign.nl">www.globalsign.nl</a></td>
</tr>
<tr>
<td><a href="mailto:ventes@globalsign.com">ventes@globalsign.com</a></td>
<td><a href="mailto:verkauf@globalsign.com">verkauf@globalsign.com</a></td>
<td><a href="mailto:verkoop@globalsign.com">verkoop@globalsign.com</a></td>
</tr>
</tbody>
</table>