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.

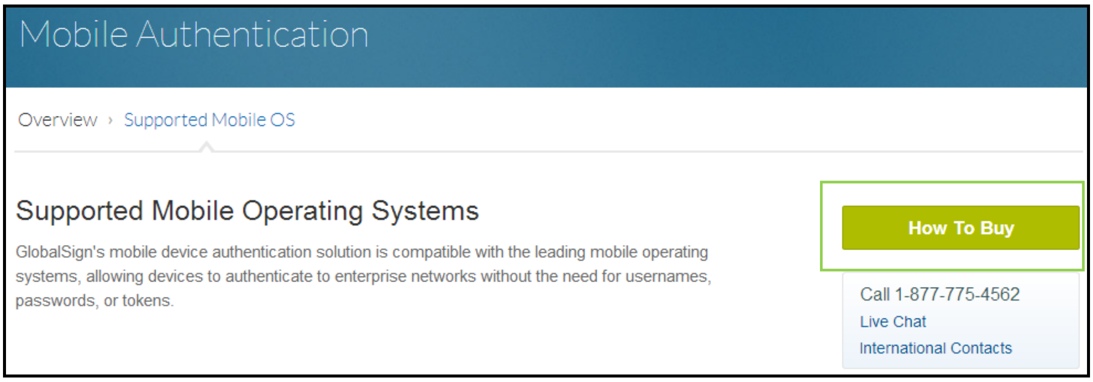
Step 1 - Establishing an EPKI Account

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:

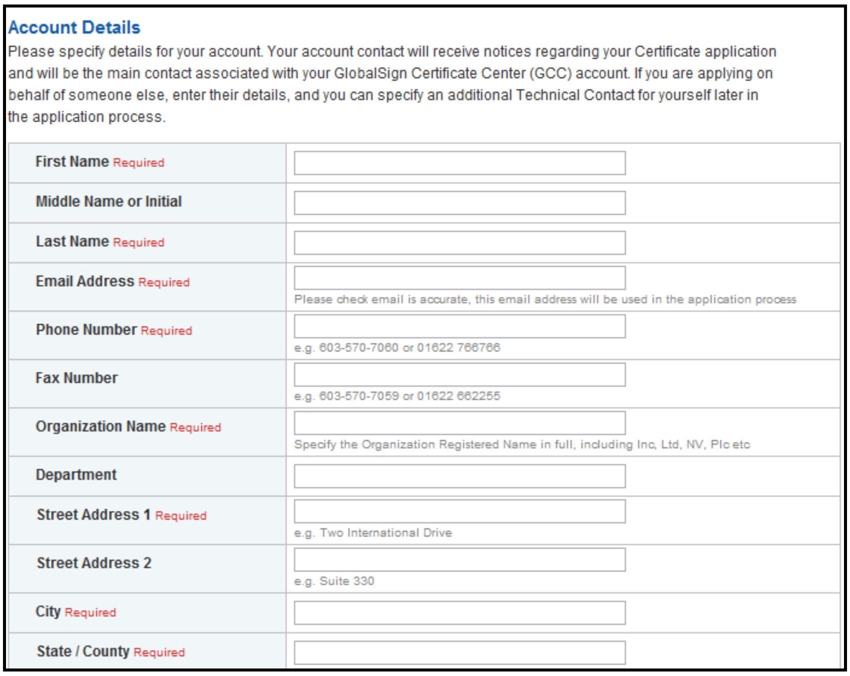
1. Navigate to https://www.globalsign.com/authentication/mobile/supported-os.html . Click **How To Buy**. An account representative will be in contact with you shortly to help you decide the best options for your EPKI account. The next step will be to register for an EPKI account.



Supported Mobile Operating Systems

GlobalSign's mobile device authentication solution is compatible with the leading mobile operating systems, allowing devices to authenticate to enterprise networks without the need for usernames, passwords, or tokens.

2. **Register** for an EPKI account by entering your account details. *Note: this is not the vetted profile information.*

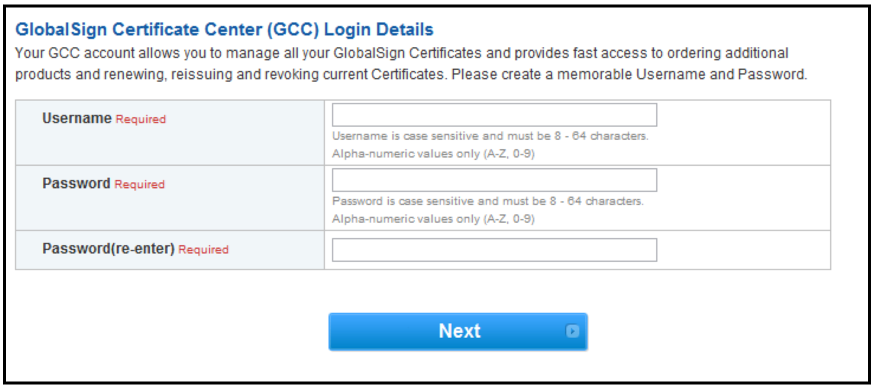


Account Details

Please specify details for your account. Your account contact will receive notices regarding your Certificate application and will be the main contact associated with your GlobalSign Certificate Center (GCC) account. If you are applying on behalf of someone else, enter their details, and you can specify an additional Technical Contact for yourself later in the application process.

First Name Required	
Middle Name or Initial	
Last Name Required	
Email Address Required	Please check email is accurate, this email address will be used in the application process
Phone Number Required	e.g. 603-570-7060 or 01622 766766
Fax Number	e.g. 603-570-7059 or 01622 662255
Organization Name Required	Specify the Organization Registered Name in full, including Inc, Ltd, NV, Plc etc
Department	
Street Address 1 Required	e.g. Two International Drive
Street Address 2	e.g. Suite 330
City Required	
State / County Required	

3. Choose a username and password. An account number (PAR####) will be appended to the username you choose. Click **Next** to continue.

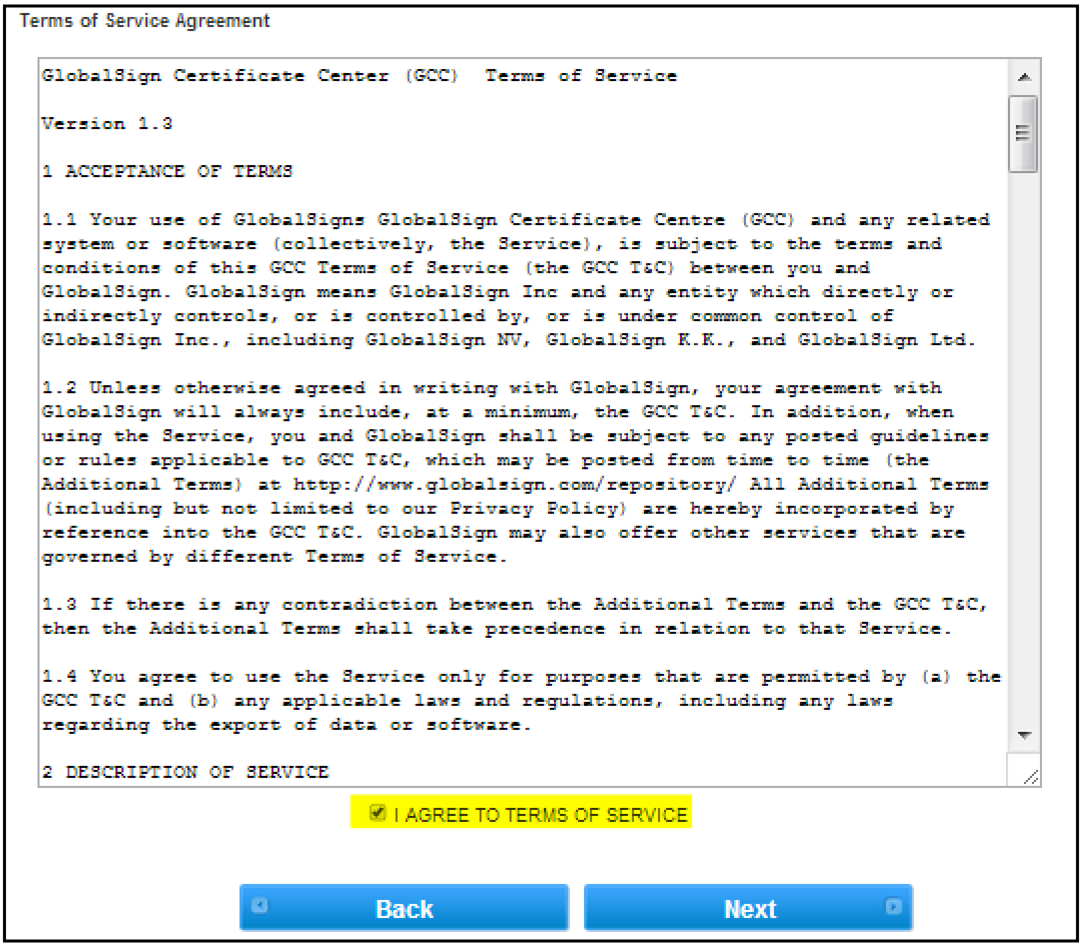


GlobalSign Certificate Center (GCC) Login Details

Your GCC account allows you to manage all your GlobalSign Certificates and provides fast access to ordering additional products and renewing, reissuing and revoking current Certificates. Please create a memorable Username and Password.

Username Required	Username is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9)
Password Required	Password is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9)
Password(re-enter) Required	

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.



Terms of Service Agreement

GlobalSign Certificate Center (GCC) Terms of Service

Version 1.3

1 ACCEPTANCE OF TERMS

1.1 Your use of GlobalSigns GlobalSign Certificate Centre (GCC) and any related system or software (collectively, the Service), is subject to the terms and conditions of this GCC Terms of Service (the GCC T&C) between you and GlobalSign. GlobalSign means GlobalSign Inc and any entity which directly or indirectly controls, or is controlled by, or is under common control of GlobalSign Inc., including GlobalSign NV, GlobalSign K.K., and GlobalSign Ltd.

1.2 Unless otherwise agreed in writing with GlobalSign, your agreement with GlobalSign will always include, at a minimum, the GCC T&C. In addition, when using the Service, you and GlobalSign shall be subject to any posted guidelines or rules applicable to GCC T&C, which may be posted from time to time (the Additional Terms) at http://www.globalsign.com/repository/ All Additional Terms (including but not limited to our Privacy Policy) are hereby incorporated by reference into the GCC T&C. GlobalSign may also offer other services that are governed by different Terms of Service.

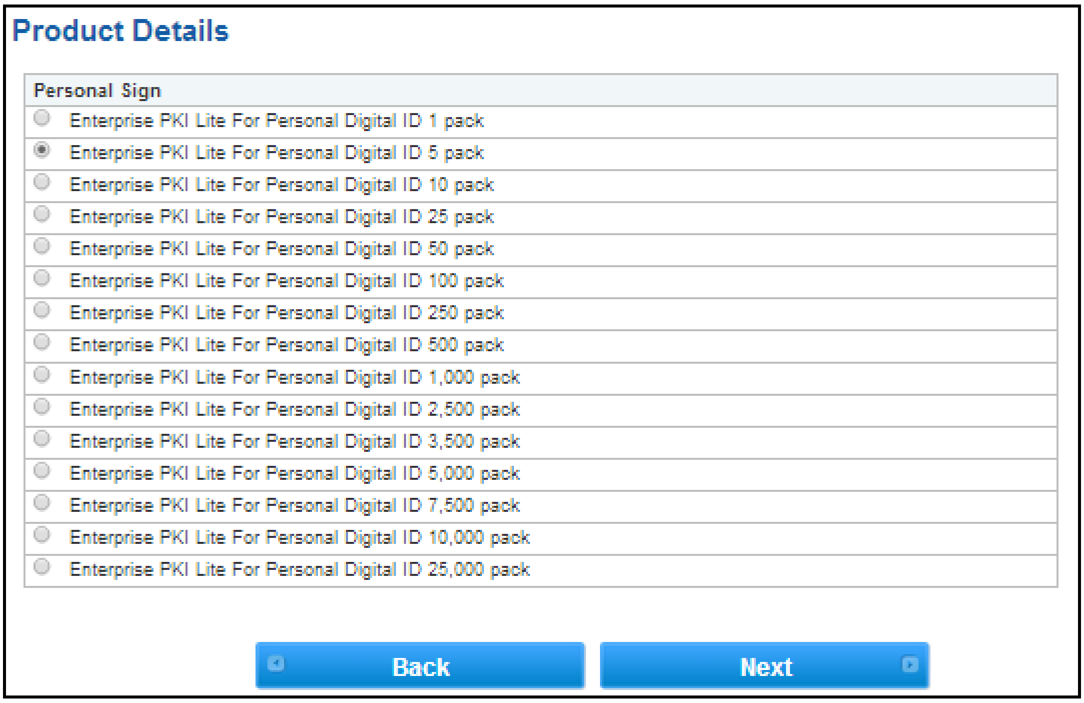
1.3 If there is any contradiction between the Additional Terms and the GCC T&C, then the Additional Terms shall take precedence in relation to that Service.

1.4 You agree to use the Service only for purposes that are permitted by (a) the GCC T&C and (b) any applicable laws and regulations, including any laws regarding the export of data or software.

2 DESCRIPTION OF SERVICE

☑ I AGREE TO TERMS OF SERVICE

5. Choose the license pack size of Identity Certificates you wish to purchase. Click **Next**.



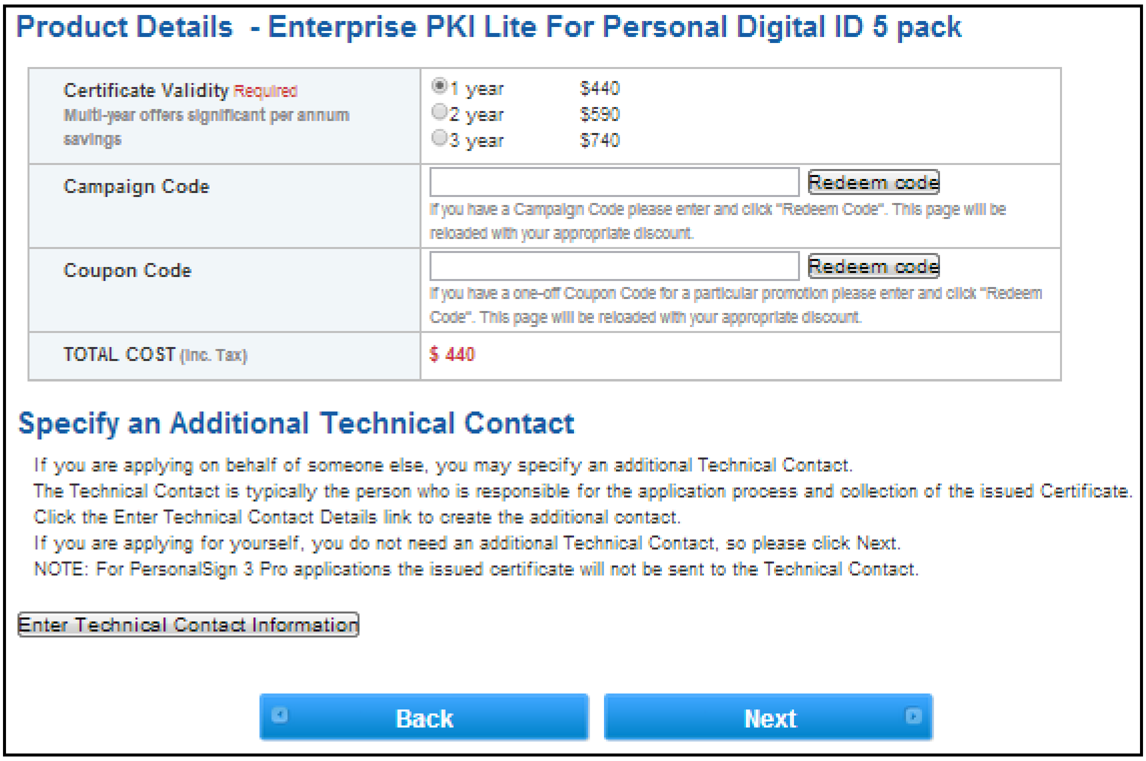
Product Details

Personal Sign

- ○ Enterprise PKI Lite For Personal Digital ID 1 pack
- ● Enterprise PKI Lite For Personal Digital ID 5 pack
- ○ Enterprise PKI Lite For Personal Digital ID 10 pack
- ○ Enterprise PKI Lite For Personal Digital ID 25 pack
- ○ Enterprise PKI Lite For Personal Digital ID 50 pack
- ○ Enterprise PKI Lite For Personal Digital ID 100 pack
- ○ Enterprise PKI Lite For Personal Digital ID 250 pack
- ○ Enterprise PKI Lite For Personal Digital ID 500 pack
- ○ Enterprise PKI Lite For Personal Digital ID 1,000 pack
- ○ Enterprise PKI Lite For Personal Digital ID 2,500 pack
- ○ Enterprise PKI Lite For Personal Digital ID 3,500 pack
- ○ Enterprise PKI Lite For Personal Digital ID 5,000 pack
- ○ Enterprise PKI Lite For Personal Digital ID 7,500 pack
- ○ Enterprise PKI Lite For Personal Digital ID 10,000 pack
- ○ Enterprise PKI Lite For Personal Digital ID 25,000 pack

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.



Product Details - Enterprise PKI Lite For Personal Digital ID 5 pack

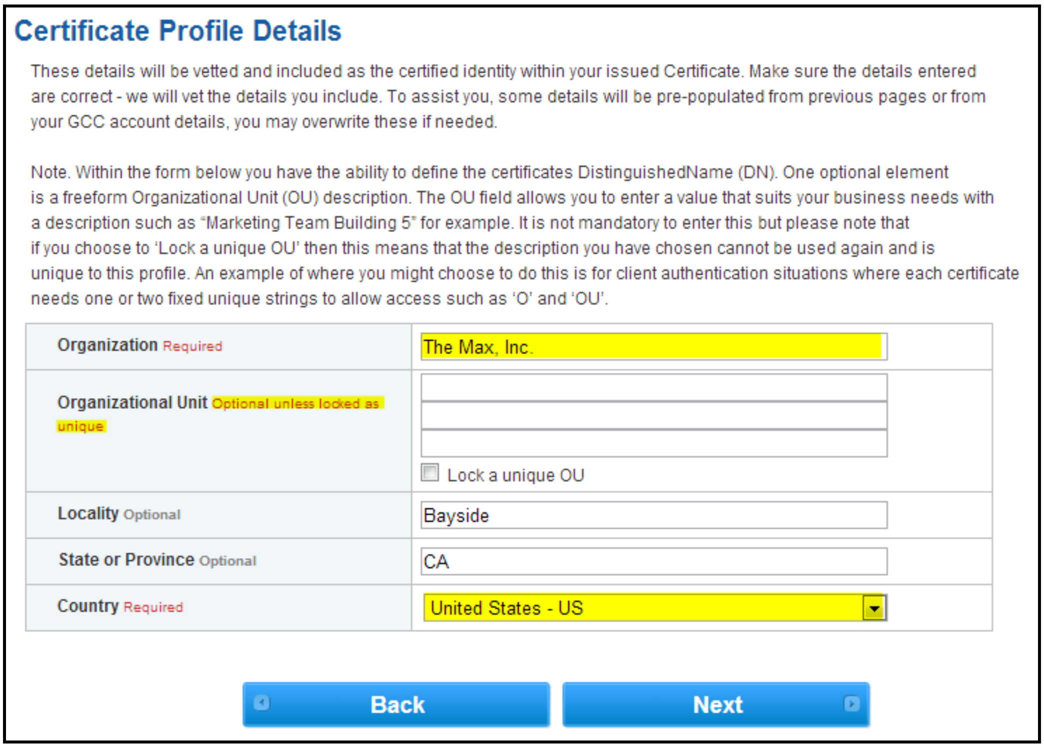
Certificate Validity Required Multi-year offers significant per annum savings	● 1 year $440 ○ 2 year $590 ○ 3 year $740
Campaign Code	If you have a Campaign Code please enter and click "Redeem Code". This page will be reloaded with your appropriate discount.
Coupon Code	If you have a one-off Coupon Code for a particular promotion please enter and click "Redeem Code". This page will be reloaded with your appropriate discount.
TOTAL COST (Inc. Tax)	$ 440

Specify an Additional Technical Contact

If you are applying on behalf of someone else, you may specify an additional Technical Contact.
The Technical Contact is typically the person who is responsible for the application process and collection of the issued Certificate.
Click the Enter Technical Contact Details link to create the additional contact.
If you are applying for yourself, you do not need an additional Technical Contact, so please click Next.
NOTE: For PersonalSign 3 Pro applications the issued certificate will not be sent to the Technical Contact.

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.



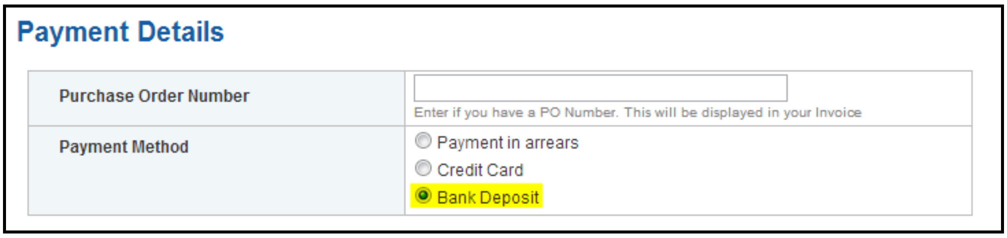
Certificate Profile Details

These details will be vetted and included as the certified identity within your issued Certificate. Make sure the details entered are correct - we will vet the details you include. To assist you, some details will be pre-populated from previous pages or from your GCC account details, you may overwrite these if needed.

Note. Within the form below you have the ability to define the certificates DistinguishedName (DN). One optional element is a freeform Organizational Unit (OU) description. The OU field allows you to enter a value that suits your business needs with a description such as "Marketing Team Building 5" for example. It is not mandatory to enter this but please note that if you choose to 'Lock a unique OU' then this means that the description you have chosen cannot be used again and is unique to this profile. An example of where you might choose to do this is for client authentication situations where each certificate needs one or two fixed unique strings to allow access such as 'O' and 'OU'.

Organization Required	The Max, Inc.
Organizational Unit Optional unless locked as unique	□ Lock a unique OU
Locality Optional	Bayside
State or Province Optional	CA
Country Required	United States - US

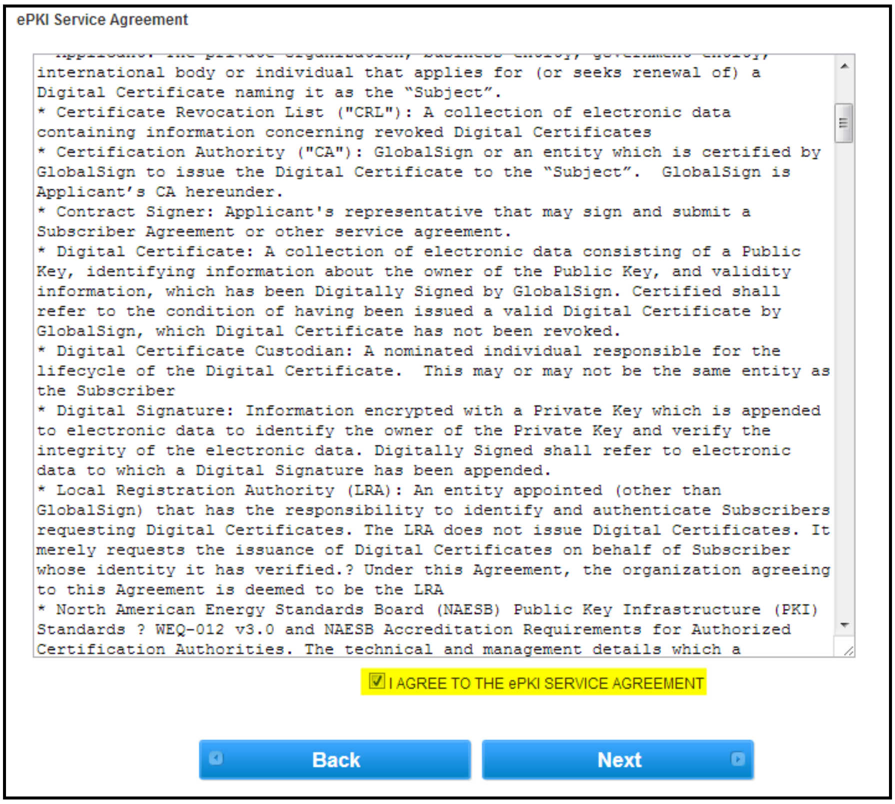
8. Complete the payment details.



Payment Details

Purchase Order Number	Enter if you have a PO Number. This will be displayed in your Invoice
Payment Method	○ Payment in arrears ○ Credit Card ● Bank Deposit

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

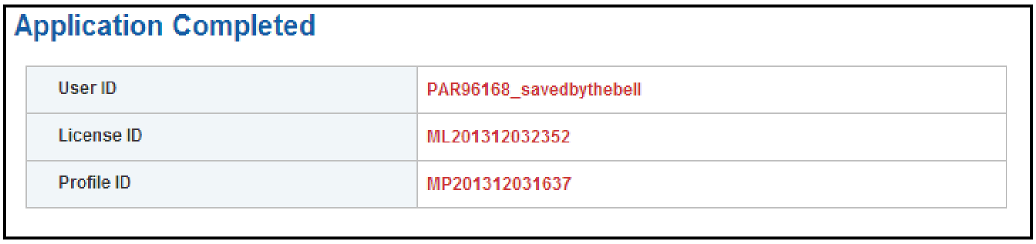


ePKI Service Agreement

```
Applicant: The private organization, business entity, government entity,
international body or individual that applies for (or seeks renewal of) a
Digital Certificate naming it as the “Subject”.
* Certificate Revocation List ("CRL"): A collection of electronic data
containing information concerning revoked Digital Certificates
* Certification Authority ("CA"): GlobalSign or an entity which is certified by
GlobalSign to issue the Digital Certificate to the “Subject”.  GlobalSign is
Applicant’s CA hereunder.
* Contract Signer: Applicant's representative that may sign and submit a
Subscriber Agreement or other service agreement.
* Digital Certificate: A collection of electronic data consisting of a Public
Key, identifying information about the owner of the Public Key, and validity
information, which has been Digitally Signed by GlobalSign. Certified shall
refer to the condition of having been issued a valid Digital Certificate by
GlobalSign, which Digital Certificate has not been revoked.
* Digital Certificate Custodian: A nominated individual responsible for the
lifecycle of the Digital Certificate.  This may or may not be the same entity as
the Subscriber
* Digital Signature: Information encrypted with a Private Key which is appended
to electronic data to identify the owner of the Private Key and verify the
integrity of the electronic data. Digitally Signed shall refer to electronic
data to which a Digital Signature has been appended.
* Local Registration Authority (LRA): An entity appointed (other than
GlobalSign) that has the responsibility to identify and authenticate Subscribers
requesting Digital Certificates. The LRA does not issue Digital Certificates. It
merely requests the issuance of Digital Certificates on behalf of Subscriber
whose identity it has verified.? Under this Agreement, the organization agreeing
to this Agreement is deemed to be the LRA
* North American Energy Standards Board (NAESB) Public Key Infrastructure (PKI)
Standards ? WEQ-012 v3.0 and NAESB Accreditation Requirements for Authorized
Certification Authorities. The technical and management details which a
```

☑ I AGREE TO THE ePKI SERVICE AGREEMENT

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



Application Completed

User ID	PAR96168_savedbythebell
License ID	ML201312032352
Profile ID	MP201312031637

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

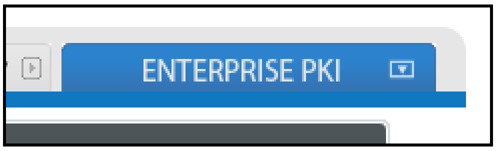
There are three options that the EPKI Administrator can use to “invite” users to apply for pre-approved digital certificates:

- 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/.

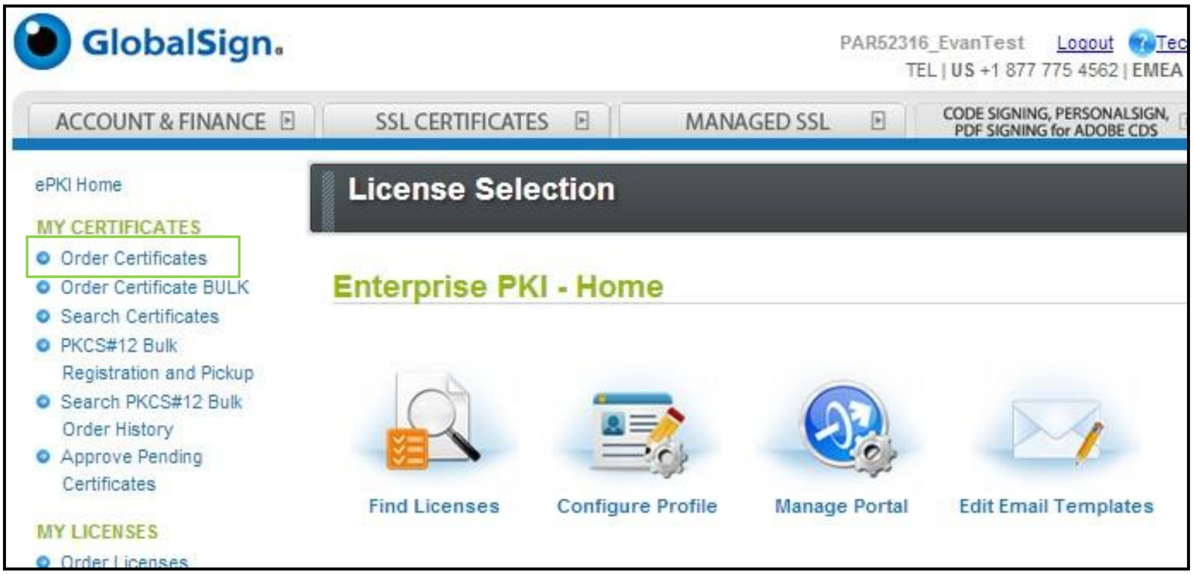
2. Select the **“Enterprise PKI”** tab found on the top menu bar.



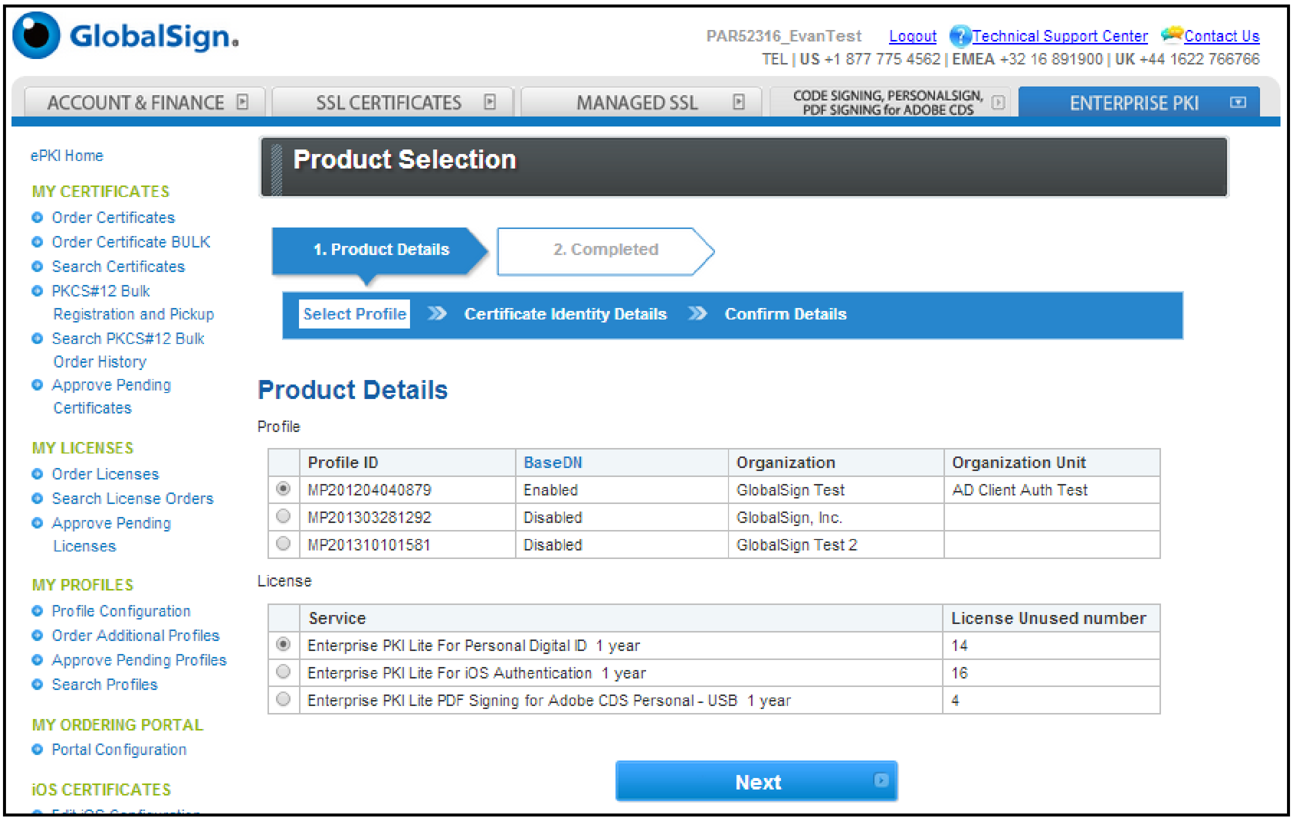
Please note: if this is your first time logging in your menu options will be limited. For first time users, you will need to enroll for an “EPKI Administrator Certificate”, which is an authentication certificate needed to access secure areas of GCC such as the Certificate Mangement section. Please follow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



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**.



Product Selection

Product Details

Profile

	Profile ID	BaseDN	Organization	Organization Unit
●	MP201204040879	Enabled	GlobalSign Test	AD Client Auth Test
○	MP201303281292	Disabled	GlobalSign, Inc.	
○	MP201310101581	Disabled	GlobalSign Test 2	

License

	Service	License Unused number
●	Enterprise PKI Lite For Personal Digital ID 1 year	14
○	Enterprise PKI Lite For iOS Authentication 1 year	16
○	Enterprise PKI Lite PDF Signing for Adobe CDS Personal - USB 1 year	4

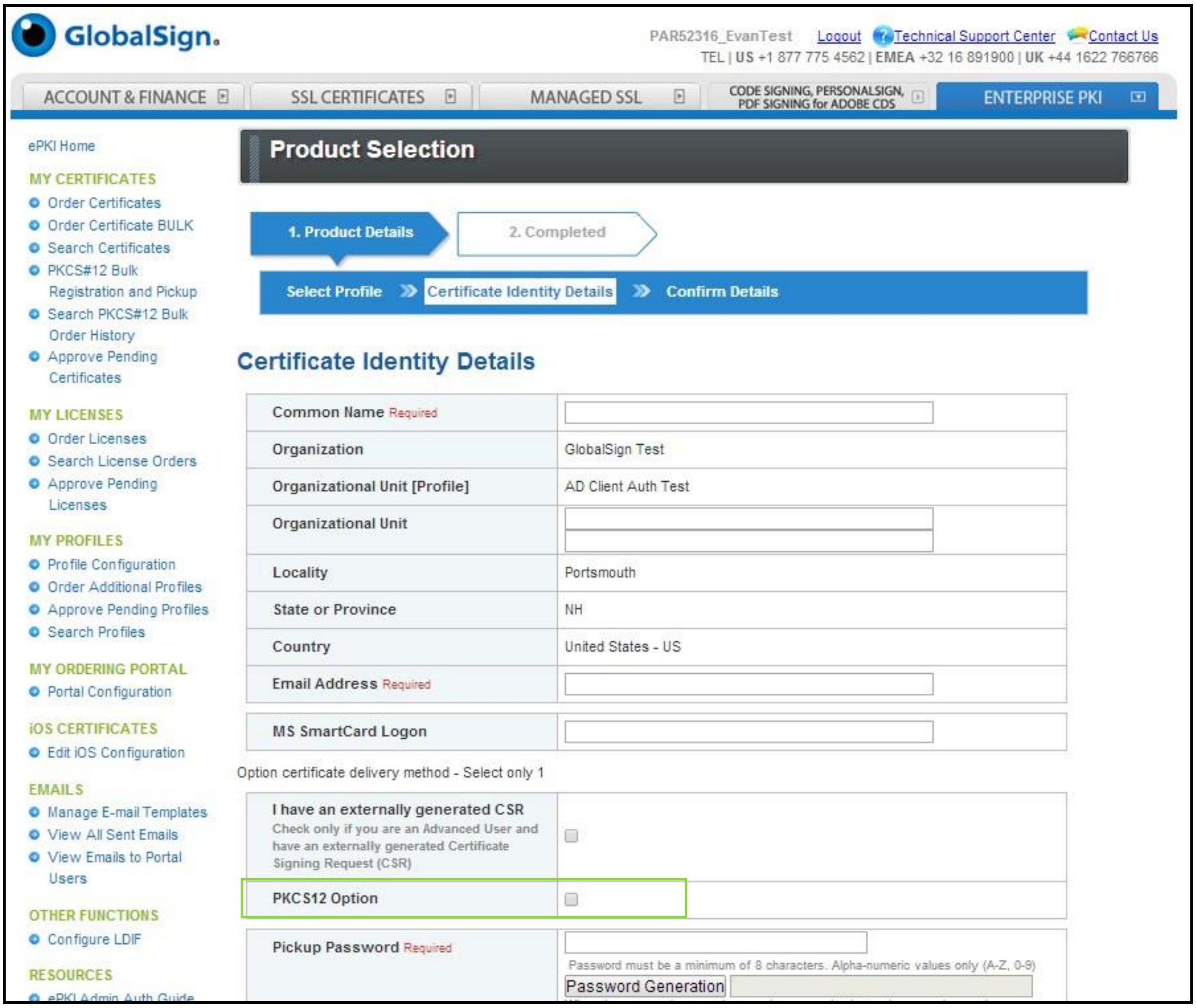
5. Next, complete the **Certificate Identity Details**. Note it is highly recommended that you **select the PKCS12 option** when ordering the certificate. This format is easily accepted by Android devices and will provide the simplest installation experience for the user. If you do not select this option 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.



Certificate Identity Details

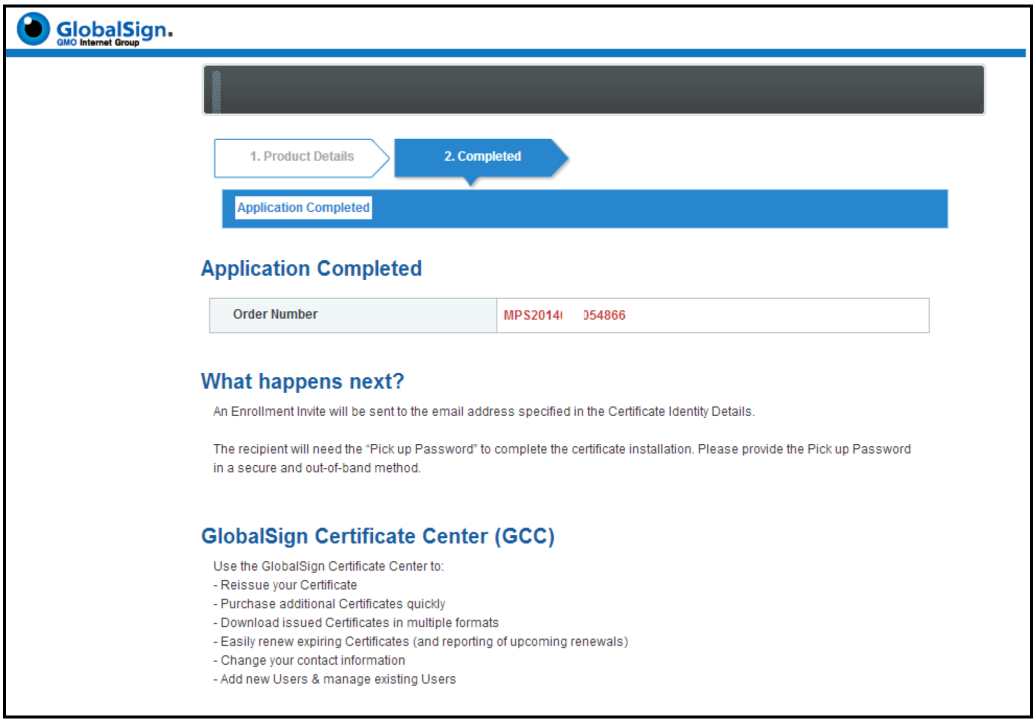
Common Name Required	
Organization	GlobalSign Test
Organizational Unit [Profile]	AD Client Auth Test
Organizational Unit	
Locality	Portsmouth
State or Province	NH
Country	United States - US
Email Address Required	
MS SmartCard Logon	

Option certificate delivery method - Select only 1

I have an externally generated CSR Check only if you are an Advanced User and have an externally generated Certificate Signing Request (CSR)	□
PKCS12 Option	□
Pickup Password Required	Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9) Password Generation

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.



Application Completed

Order Number	MPS2014[redacted]54866

What happens next?

An Enrollment Invite will be sent to the email address specified in the Certificate Identity Details.

The recipient will need the "Pick up Password" to complete the certificate installation. Please provide the Pick up Password in a secure and out-of-band method.

GlobalSign Certificate Center (GCC)

Use the GlobalSign Certificate Center to:
- Reissue your Certificate
- Purchase additional Certificates quickly
- Download issued Certificates in multiple formats
- Easily renew expiring Certificates (and reporting of upcoming renewals)
- Change your contact information
- Add new Users & manage existing Users

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.

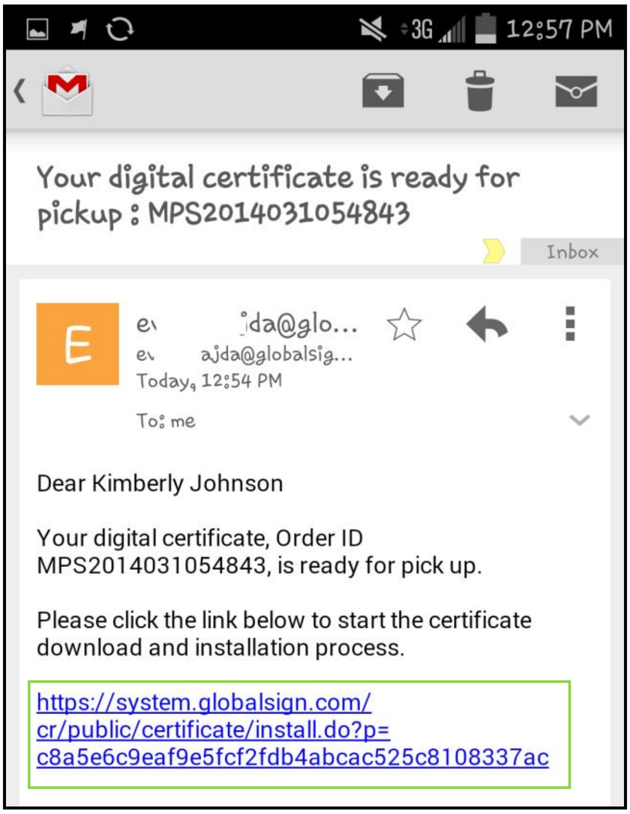
Android supports DER-encoded X.509 certificates, saved in files with a .crt or .cer file extension. Android also supports X.509 certificates saved in PKCS#12 key store files with a .p12 or .pfx extension. If your file is in some other extension is it important to change it to a compatible extension.

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.



Your digital certificate is ready for pickup : MPS2014031054843

e ida@glo…
e ajda@globalsig…
Today, 12:54 PM
To: me

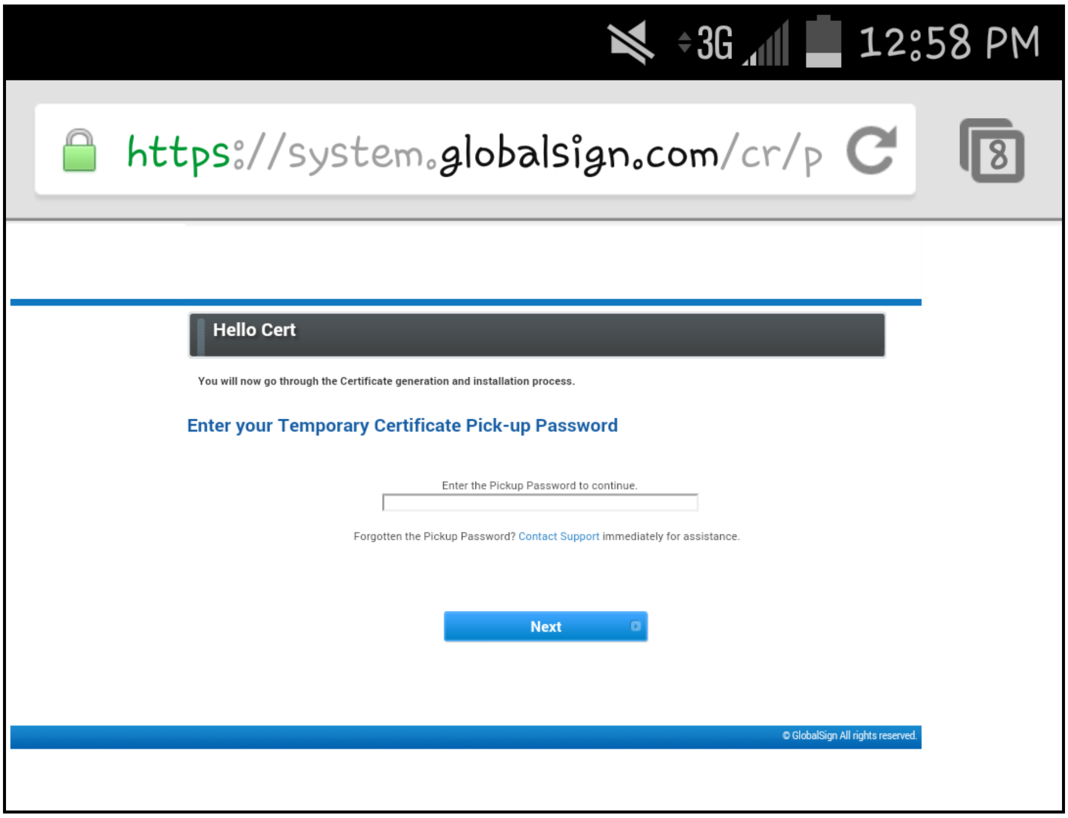
Dear Kimberly Johnson

Your digital certificate, Order ID MPS2014031054843, is ready for pick up.

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

https://system.globalsign.com/cr/public/certificate/install.do?p=c8a5e6c9eaf9e5fcf2fdb4abcac525c8108337ac

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.



12:58 PM
https://system.globalsign.com/cr/p

Hello Cert

You will now go through the Certificate generation and installation process.

Enter your Temporary Certificate Pick-up Password

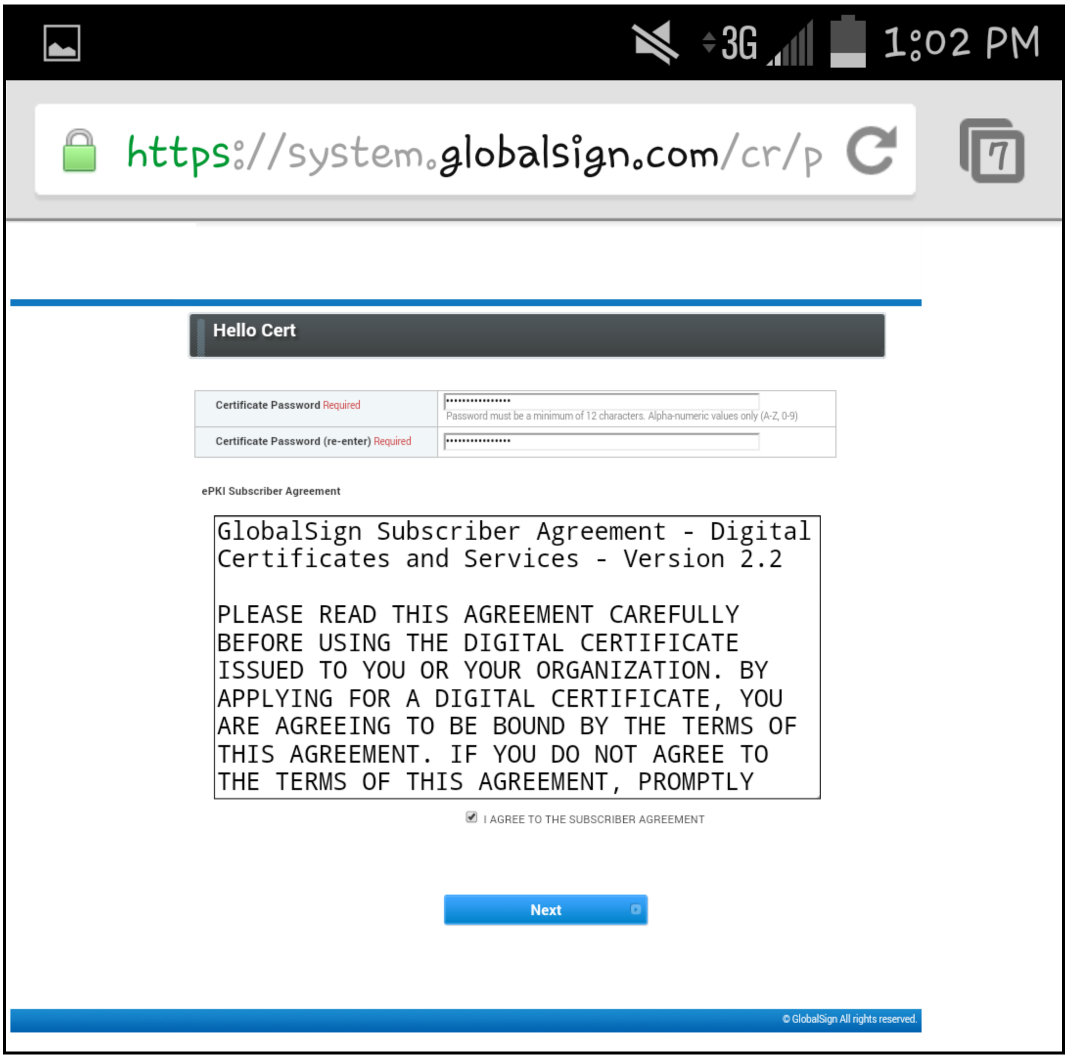
Enter the Pickup Password to continue.

Forgotten the Pickup Password? Contact Support immediately for assistance.

Next
© GlobalSign All rights reserved.

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.



Hello Cert

Certificate Password Required	•••••••••••••••• Password must be a minimum of 12 characters. Alpha-numeric values only (A-Z, 0-9)
Certificate Password (re-enter) Required	••••••••••••••••

ePKI Subscriber Agreement

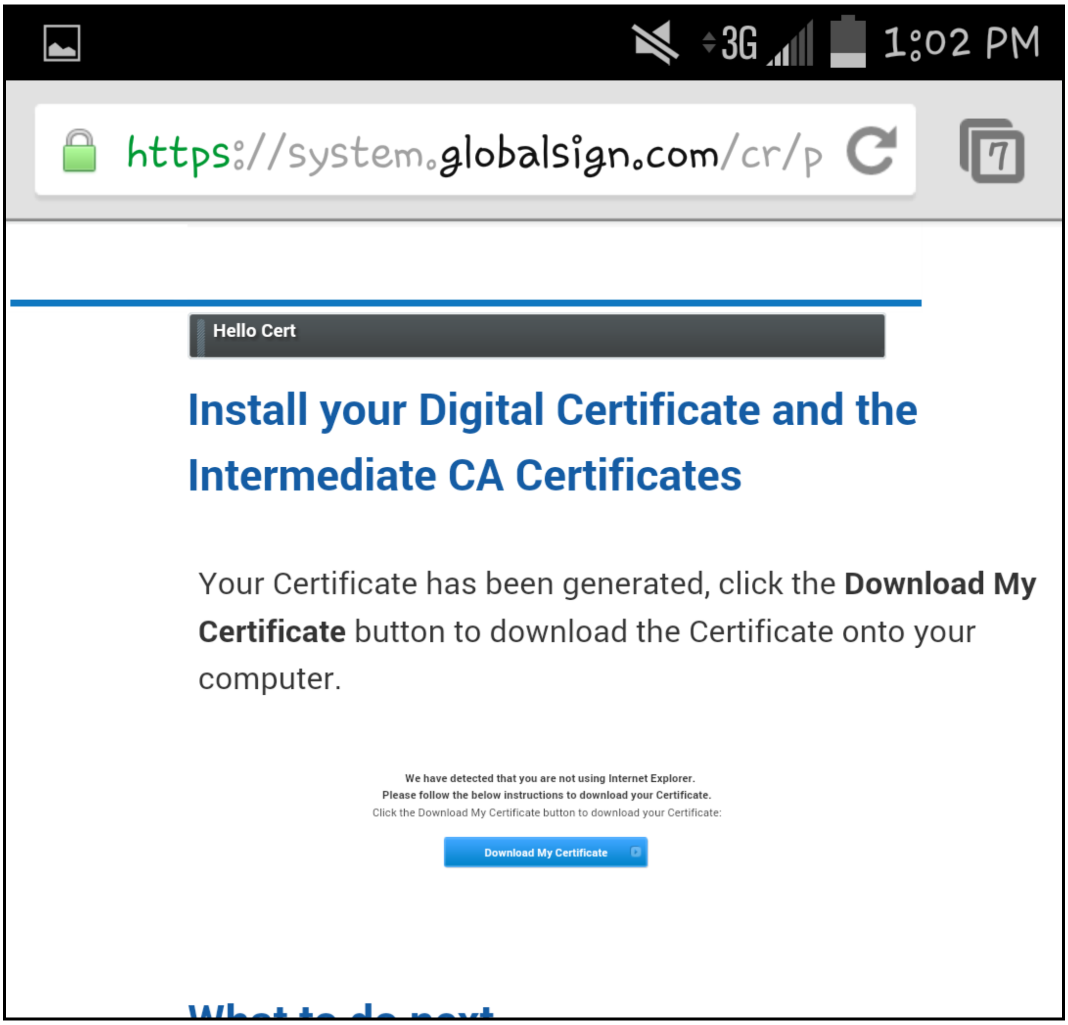
GlobalSign Subscriber Agreement - Digital Certificates and Services - Version 2.2

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A DIGITAL CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY

☑ I AGREE TO THE SUBSCRIBER AGREEMENT

© GlobalSign All rights reserved.

5. The certificate is now ready to be downloaded to the device. The user clicks **Download My Certificate** to finish installing the certificate.



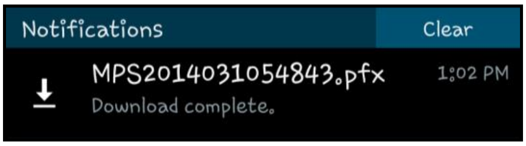
Hello Cert

Install your Digital Certificate and the Intermediate CA Certificates

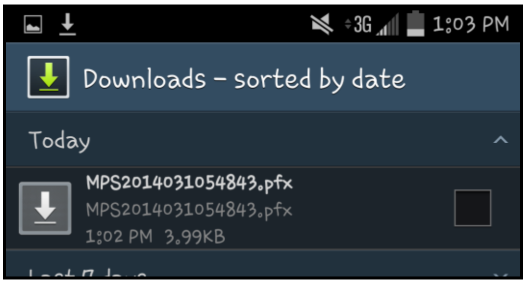
Your Certificate has been generated, click the **Download My Certificate** button to download the Certificate onto your computer.

We have detected that you are not using Internet Explorer.
Please follow the below instructions to download your Certificate.
Click the Download My Certificate button to download your Certificate:

The certificate will now appear in the **Downloads** on the device.

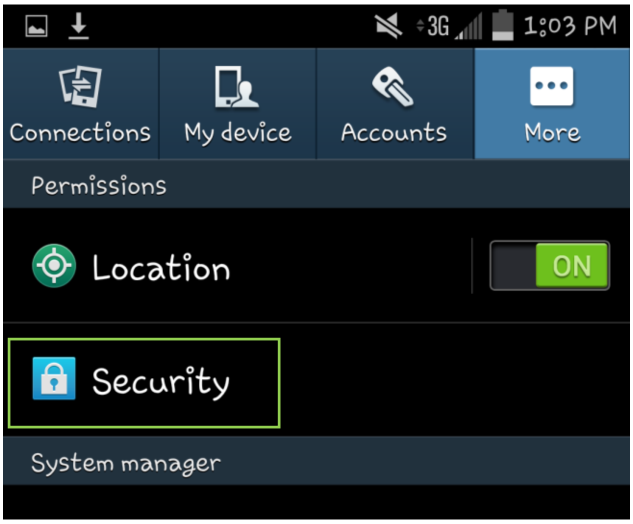


MPS2014031054843.pfx 1:02 PM
Download complete.



MPS2014031054843.pfx
MPS2014031054843.pfx
1:02 PM 3.99KB

6. To complete the install, the user will need to go to the device **Settings** and navigate to the **Security** settings on the device.



1:03 PM

Connections | My device | Accounts | More

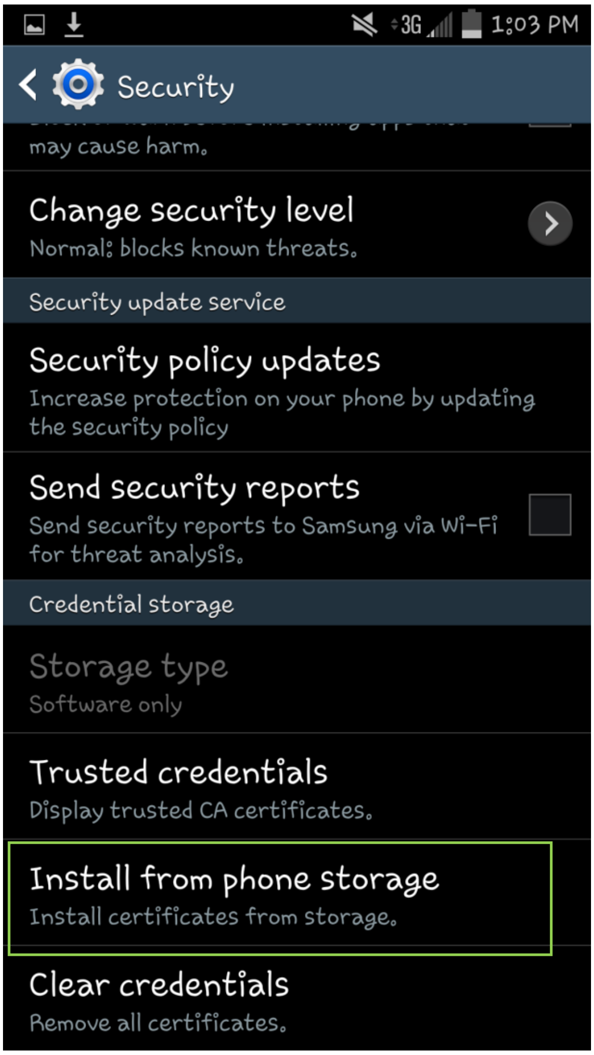
Permissions

Location ON

Security

System manager

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



1:03 PM

Security

may cause harm.

Change security level
Normal: blocks known threats.

Security update service

Security policy updates
Increase protection on your phone by updating the security policy

Send security reports
Send security reports to Samsung via Wi-Fi for threat analysis. □

Credential storage

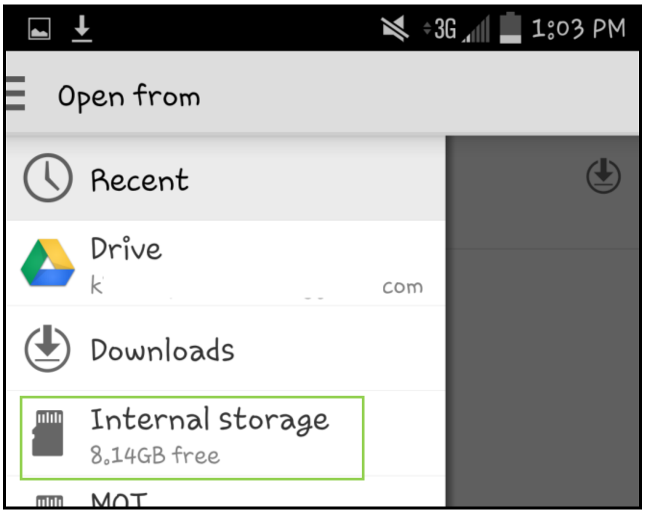
Storage type
Software only

Trusted credentials
Display trusted CA certificates.

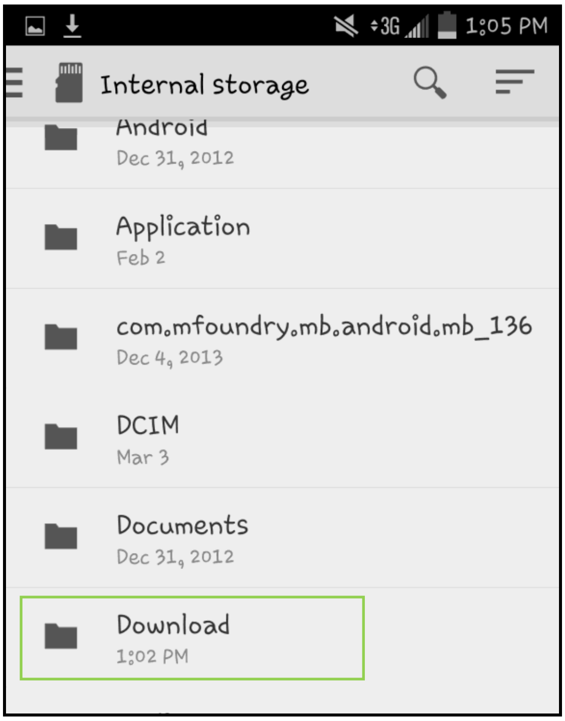
Install from phone storage
Install certificates from storage.

Clear credentials
Remove all certificates.

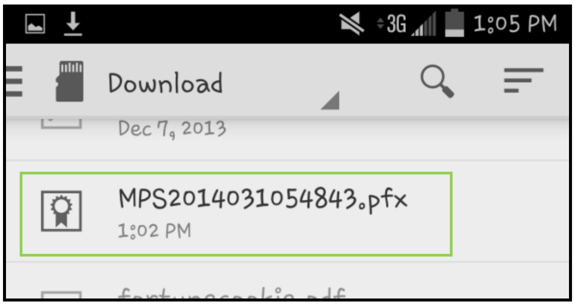
8. From the available device storage locations the user selects **Internal Storage**.



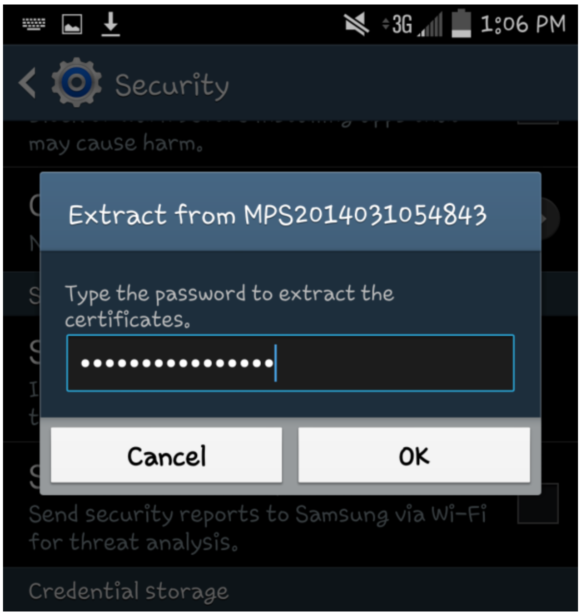
9. The user navigates to the **Download** folder.



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.

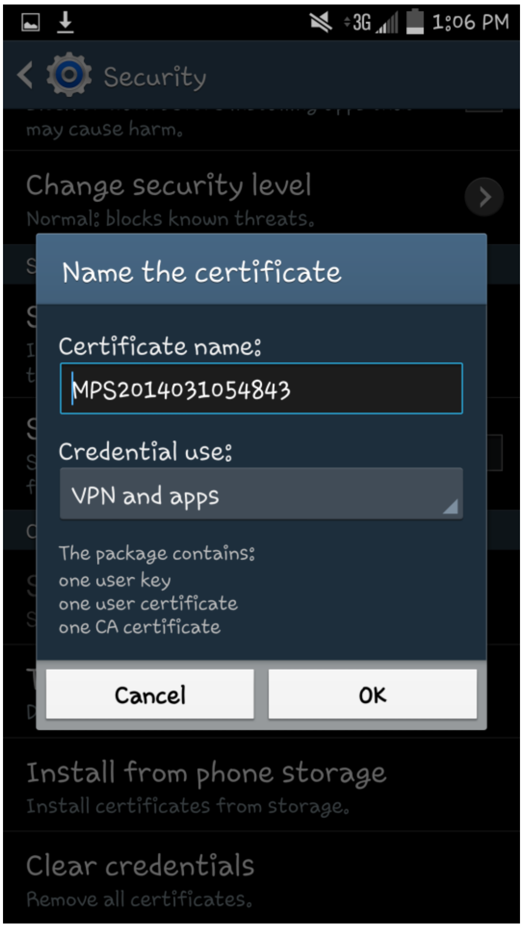


Extract from MPS2014031054843

Type the password to extract the certificates.

1:06 PM
Security
may cause harm.
Cancel
OK
Send security reports to Samsung via Wi-Fi for threat analysis.
Credential storage

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.



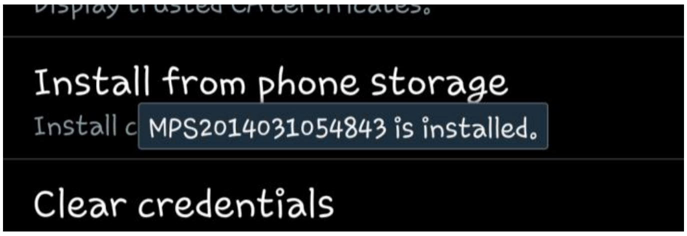
Name the certificate

Certificate name: MPS2014031054843

Credential use: VPN and apps

The package contains:
one user key
one user certificate
one CA certificate

13. The certificate is now successfully installed on the user’s device.



Install from phone storage

MPS2014031054843 is installed.

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.

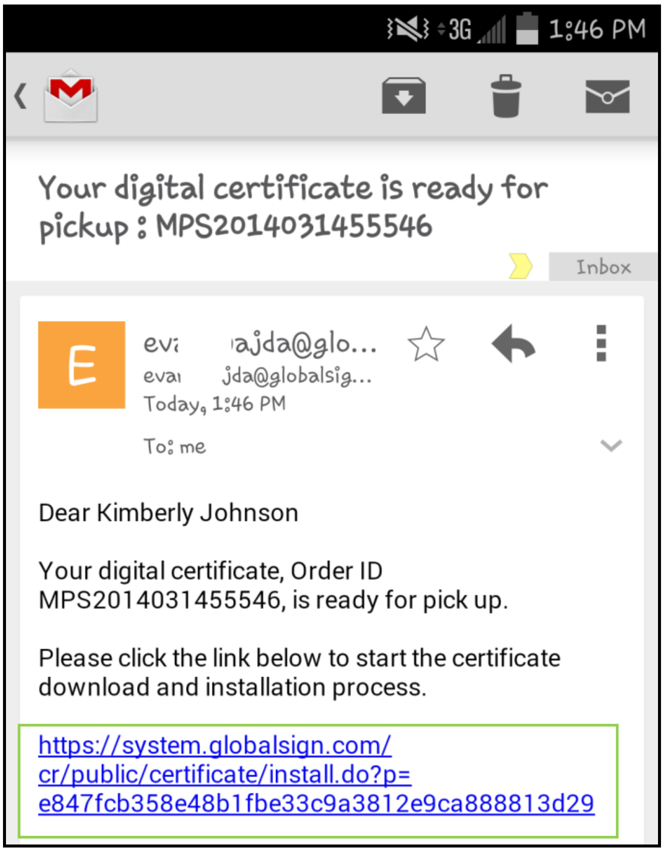
Android supports DER-encoded X.509 certificates, saved in files with a .crt or .cer file extension. Android also supports X.509 certificates saved in PKCS#12 key store files with a .p12 or .pfx extension. If your file is in some other extension is it important to change it to a compatible extension.

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.



Your digital certificate is ready for pickup : MPS2014031455546

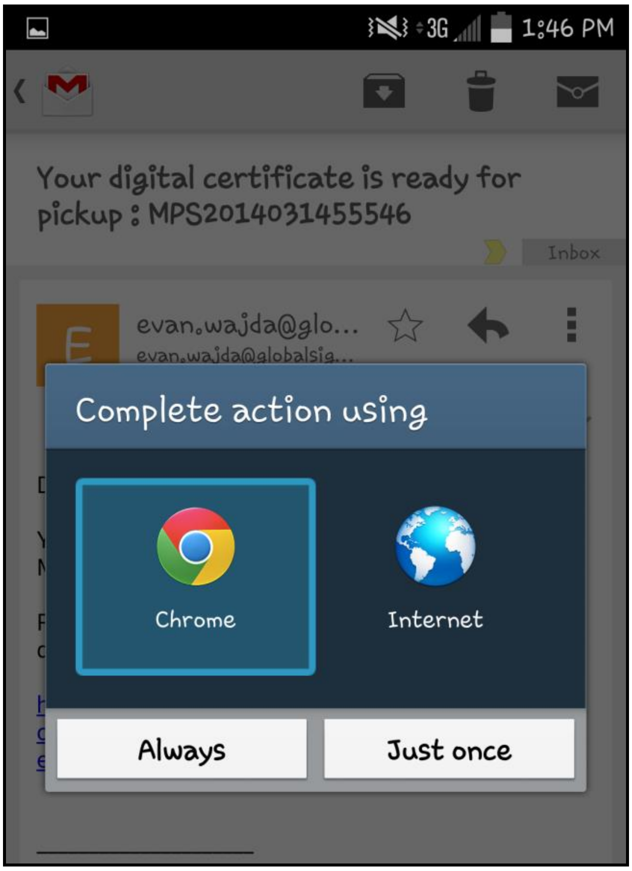
Dear Kimberly Johnson

Your digital certificate, Order ID MPS2014031455546, is ready for pick up.

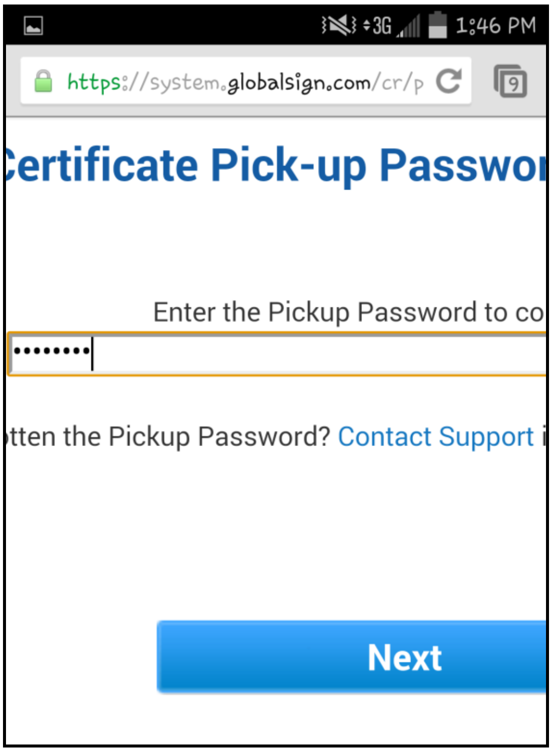
Please click the link below to start the certificate download and installation process.

https://system.globalsign.com/cr/public/certificate/install.do?p=e847fcb358e48b1fbe33c9a3812e9ca888813d29

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.



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.



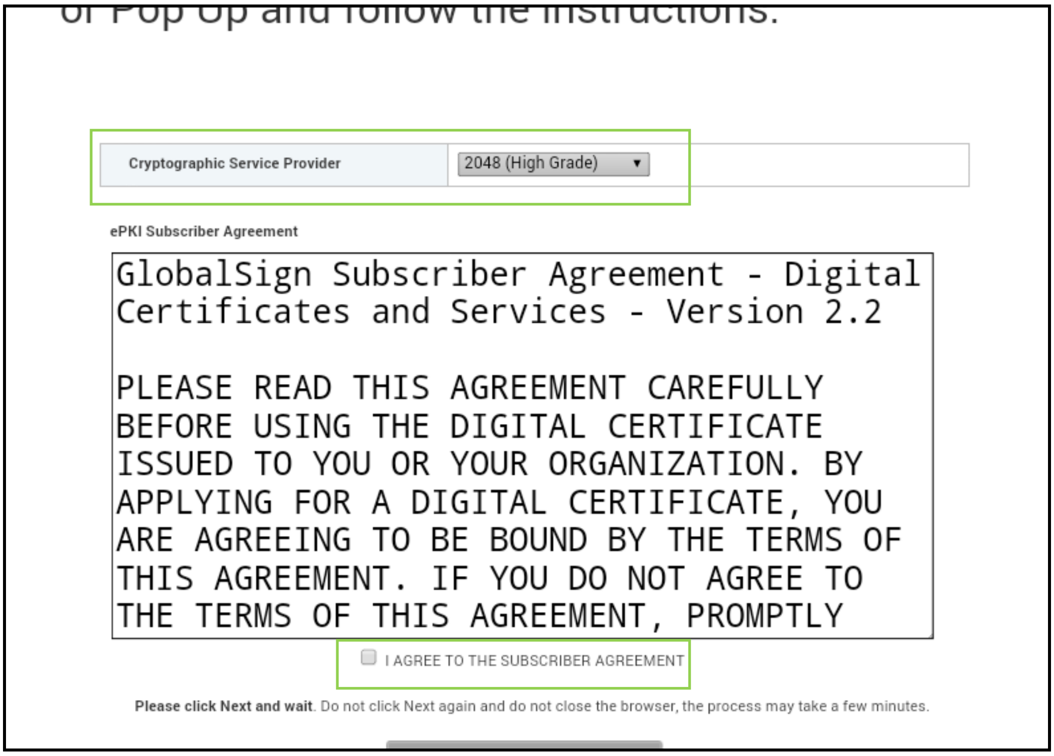
ertificate Pick-up Passwor

Enter the Pickup Password to co

••••••••

tten the Pickup Password? Contact Support i

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.



of Pop Up and follow the instructions.

Cryptographic Service Provider	2048 (High Grade) ▾

ePKI Subscriber Agreement

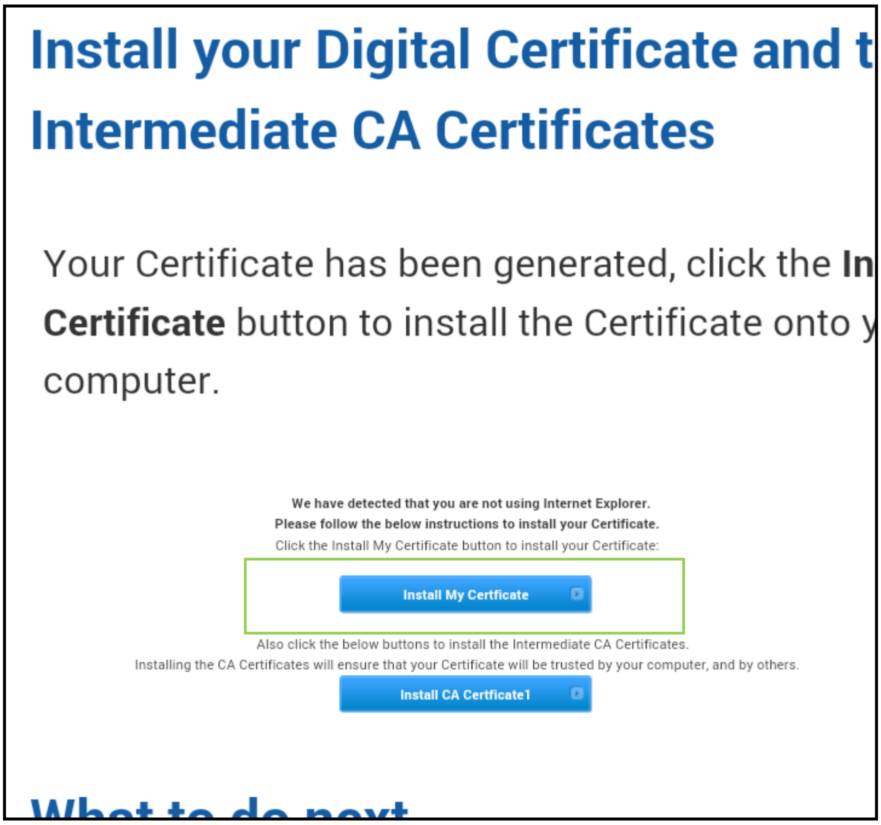
GlobalSign Subscriber Agreement - Digital Certificates and Services - Version 2.2

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A DIGITAL CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY

□ I AGREE TO THE SUBSCRIBER AGREEMENT

Please click Next and wait. Do not click Next again and do not close the browser, the process may take a few minutes.

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 t
Intermediate CA Certificates

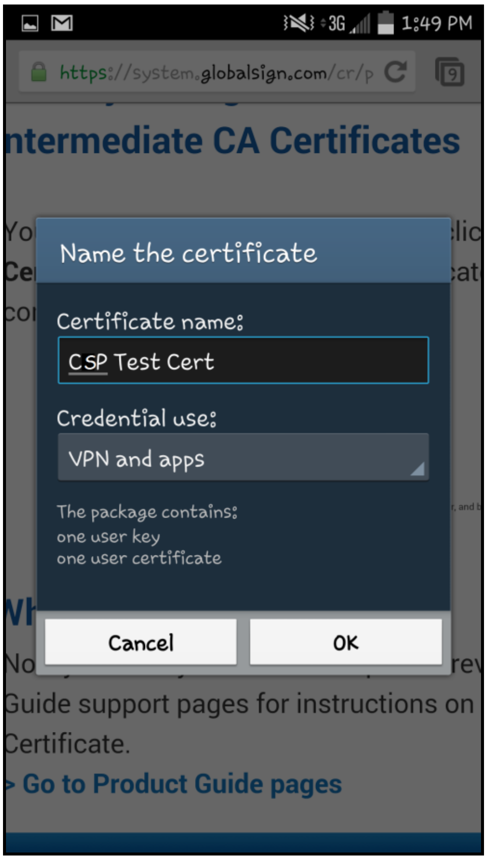
Your Certificate has been generated, click the **In**
Certificate button to install the Certificate onto y
computer.

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.

What to do next

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.



https://system.globalsign.com/cr/p

Name the certificate

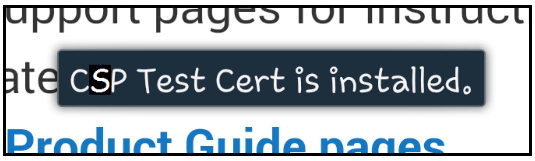
Certificate name: CSP Test Cert

Credential use: VPN and apps

The package contains:
one user key
one user certificate

3G
1:49 PM
ntermediate CA Certificates
Cancel
OK
Guide support pages for instructions on
ertificate.
Go to Product Guide pages

8. The certificate is now successfully installed on the user's device.



upport pages for instruct

ate CSP Test Cert is installed.

Product Guide pages

GlobalSign Contact Information

GlobalSign Americas Tel: 1-877-775-4562 www.globalsign.com sales-us@globalsign.com	**GlobalSign EU** Tel: +32 16 891900 www.globalsign.eu sales@globalsign.com	**GlobalSign UK** Tel: +44 1622 766766 www.globalsign.co.uk sales@globalsign.com
GlobalSign FR Tel: +33 1 82 88 01 24 www.globalsign.fr ventes@globalsign.com	**GlobalSign DE** Tel: +49 30 8878 9310 www.globalsign.de verkauf@globalsign.com	**GlobalSign NL** Tel: +31 20 8908021 www.globalsign.nl verkoop@globalsign.com