

GlobalSign Enterprise Solutions

Enterprise PKI Administrator Guide

Version 2.9

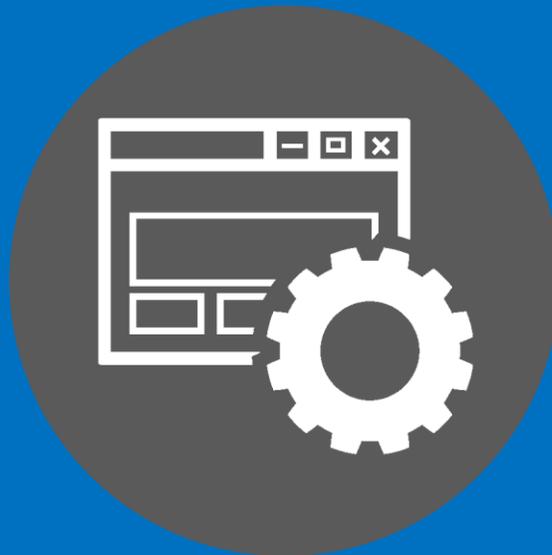


TABLE OF CONTENTS

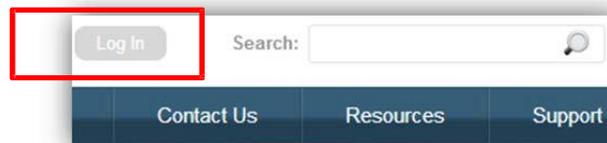
GETTING STARTED.....	3
ESTABLISHING EPKI SERVICE	3
CLIENT AUTHENTICATION CERTIFICATE.....	4
ESTABLISHING A PRE-VETTED CERTIFICATE PROFILE.....	6
TYPES OF PRE-VETTED IDENTITY PROFILES.....	7
ADDITIONAL PROFILE SPECIFIC CONFIGURATION OPTIONS.....	9
RENEWAL	11
PURCHASING CERTIFICATE LICENSE PACKS	12
CERTIFICATE TYPE	12
CERTIFICATE PACKS.....	12
PURCHASING PERMISSIONS.....	12
CERTIFICATE VALIDITY.....	13
CUSTOMIZING EMAIL TEMPLATES.....	14
CERTIFICATE ISSUANCE	16
USING THE PORTAL LINK.....	16
APPROVING REQUESTS (ORDERS).....	18
REGISTER USERS FOR CERTIFICATES VIA EPKI ADMINISTRATOR	18
INDIVIDUAL CERTIFICATE REGISTRATION	19
BULK ENROLLMENT.....	22
BULK PROVISIONING (PKCS#12)	24
EMAIL DOMAIN REGISTRATION.....	27
CERTIFICATE LIFECYCLE MANAGEMENT – REVOCATION, REISSUANCE, AND CANCELLATION.....	32
REPORTING	33
LDIF	34
CONFIGURING LDIF	34
GENERATING A LDIF REPORT	35
GCC ACCOUNT USERS	36
TYPES OF GCC ACCOUNT USERS	37
REGISTERING ADDITIONAL GCC ACCOUNT USERS.....	37
ADMINISTRATION DELEGATION	38
GETTING HELP	40

GETTING STARTED

LOGGING INTO YOUR GLOBALSIGN CERTIFICATE CENTER (GCC) ACCOUNT

Once your EPKI Account has been approved, you can log into the GlobalSign Certificate Center (GCC) straight away to start configuring and managing the lifecycle of your PersonalSign and PDF Signing for AATL Certificates.

Go to www.globalsign.com and click “Login” in the upper right hand corner or go to www.globalsign.com/login

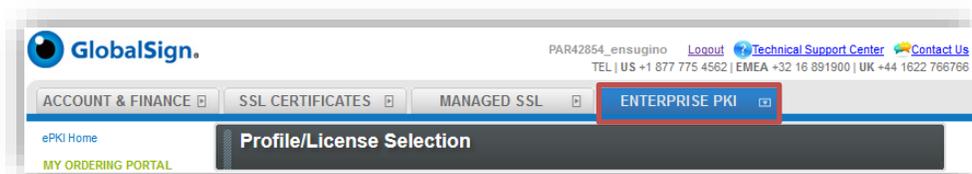


Enter your assigned **User ID** and **Password**. Your UserID is a combination of the CorporateID that GlobalSign assigns you and the username you specified during account signup (e.g. **PAR12345_UserID**). Your assigned UserID is provided at the end of the signup process and in the GCC Welcome Email.

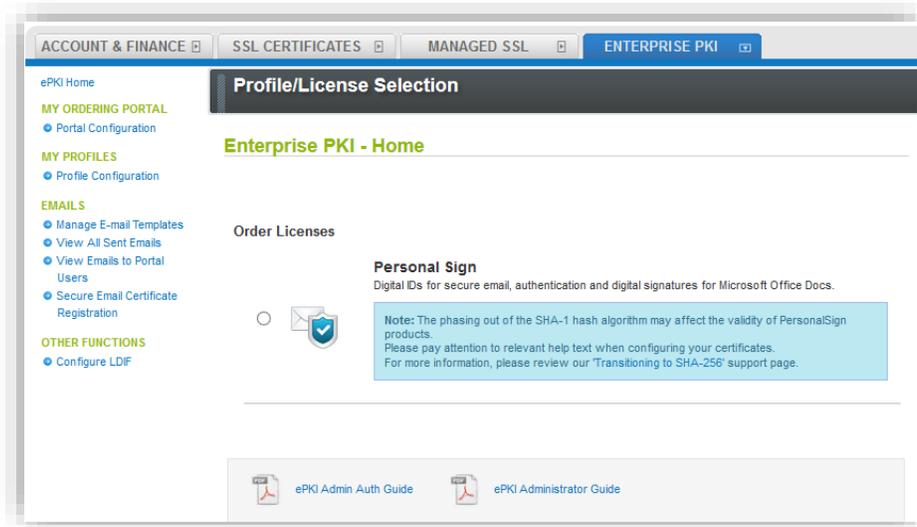
If you forget your password, you can click “[Forgot your Password? Click here](#)” on the login screen. If you have further difficulties logging in, please contact Support at: www.globalsign.com/support

ESTABLISHING EPKI SERVICE

The first time you log in, you will be prompted to choose which default tab you wish to land on every time you access your account. Select **Enterprise PKI**. In GCC there are four top tabs or sections for managing your Account and/or different types of Certificates. Select the upper tab labeled “**ENTERPRISE PKI**”.



You will land on the EPKI home page where you can find the types of certificates available for you to order: PersonalSign and PDF Signing Digital Certificates. All functions are accessed through the left hand menu system. You can also access the main features using the icons on the Enterprise PKI home page.



CLIENT AUTHENTICATION CERTIFICATE

You have the option to enable 2-Factor Authentication as an additional security feature when accessing your EPKI Account. Contact [GlobalSign Support](#) to enable (or disable) this setting for your Account. Once enabled, you will be required to install a client authentication certificate to gain access to the MY CERTIFICATES section for certificate lifecycle management.

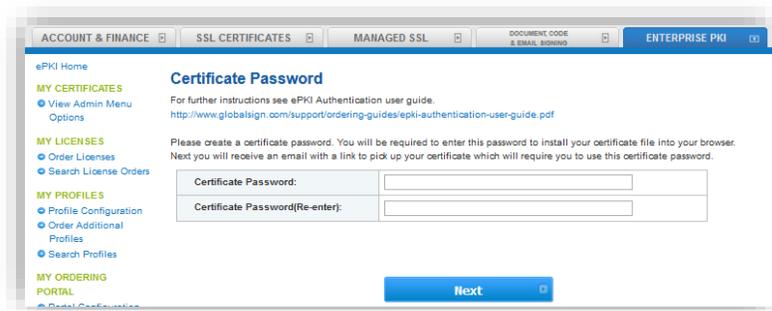
Note: If your account is not configured for Client Authentication, then you can skip to the next section.

INSTALLING YOUR CLIENT AUTHENTICATION CERTIFICATE

Login to your account, click on the **Enterprise PKI** tab and click on **View Admin Menu Options** under the **My Certificates** menu on the left side.

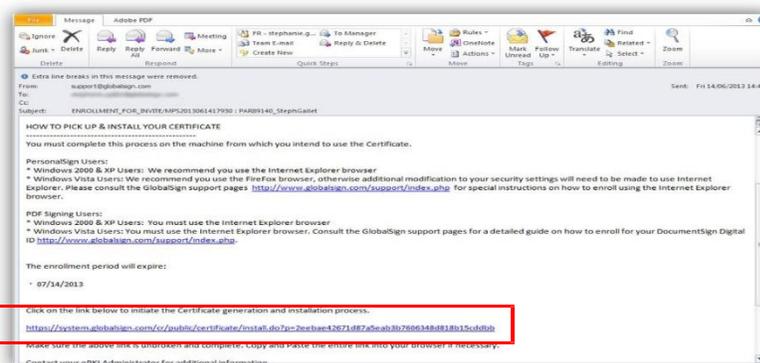


Follow the prompts to setup the Client Authentication Certificate, otherwise referred to as the Admin Certificate. You will have to create a **pick-up password** for your Admin Certificate. **It is important to remember this password!** You will need it to install the certificate into your computer(s) certificate store. Then click the **Next** button.



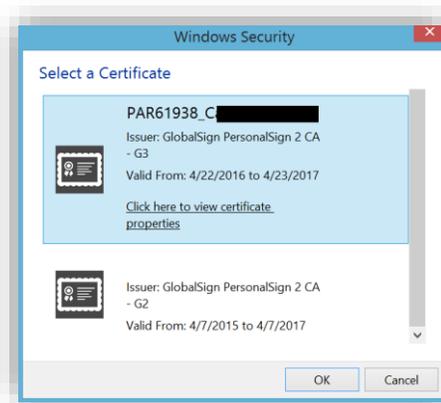
You will reach a confirmation page stating that your certificate registration is complete.

Then you will receive the certificate pick-up email within a few minutes. Click on the certificate pick-up URL in order to start installing your certificate.



Follow the remaining download and install steps listed in the [Support Article here](#).

After installation is complete, click on **View Admin Menu Options** again. You will be prompted to choose the Admin Certificate that you just installed. You can verify the correct certificate to choose, as the common name will be your **UserID** (ex. PAR10101_UserName).



You will then have full access to the MY CERTIFICATES section.

ESTABLISHING A PRE-VETTED CERTIFICATE PROFILE

Certificate Profiles will be the content of the Digital Certificate as seen by anyone viewing and relying on the certificate, so it is important to ensure the Profile is accurate and representative of the certificate holder. You can create multiple profiles in a single EPKI account, should you have multiple offices, parent or subsidiary companies that require certificates.

The EPKI Managed Service offers you the ability to use pre-vetted identity or Certificate profiles. Your company identity (as requested in Certificate Profiles) and your authorization to issue digital certificates will be vetted by third party independent checks performed by GlobalSign. Once the verification is complete, Administrators can instantly issue Certificates to end users against approved certificate profiles, without having to go through the individual validation process required when you buy a certificate outside the EPKI platform.

Note: If you setup a new GCC Account and purchased an EPKI license pack via an EPKI Ordering link, then you have already established your initial Certificate Profile. You do not need to order another certificate profile, unless you intend to specify additional or subsidiary organization details. To view your Profile(s) or to view the vetting status of a profile, click the “Search Profiles” menu option and then click the search button. Profile(s) with the Profile Status Order: VALIDATED have been vetted and you can refer to the REGISTERING USERS VIA EPKI ADMINISTRATOR section of this guide to begin issuing Certificates to end users.

To establish your initial Certificate Profile (if not previously setup), click the **Profile Configuration** menu option under **My Profiles**. Subsequent Profiles can be added after the initial Profile has been approved by clicking the **Order Additional Profiles** link.

The screenshot displays the EPKI Administrator interface. On the left, a sidebar menu titled 'MY PROFILES' is visible, with 'Profile Configuration' selected. The main content area shows a progress bar at the top with '1. Product Details' and '2. Completed' steps. Below the progress bar, there are two buttons: 'Certificate Profile Details' and 'Confirm Details'. The 'Certificate Profile Details' form is the primary focus, containing the following fields:

Organization <small>Required</small>	GlobalSign Ltd
Organizational Unit <small>Optional unless locked as unique</small>	<input type="text"/>
Locality <small>Optional</small>	Maidstone
State or Province <small>Optional</small>	Kent
Country <small>Required</small>	United Kingdom - GB

Below the form is a 'Next' button. A note above the form states: '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.' Another note below the form states: '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'.'

TYPES OF PRE-VETTED IDENTITY PROFILES

Certificate Profiles determine which fields in the end user’s Digital Certificate will be fixed values (verified by GlobalSign) or variable values for each end user registration. **Organization** and **Country Code** are required fields that GlobalSign must verify and these fields become fixed values in the Certificate profile. It is optional to provide values for **Organization Unit**, **Locality** and **State**. If these optional values are provided, they will be vetted and fixed for each Digital Certificate issued from the Profile. However, if left blank, they will be optional variable fields available to the EPKI Administrator at registration. Common Name and email are variable fields and unique to each application. Also, there is an option of pre-vetting email domain(s) associated with a profile (see the Email Domain Registration section). The end result of a submitted certificate profile is referred to as the Base Distinguished Name (DN). If you wish to ensure that a particular Organization and Organization Unit value is never used in another Certificate Profile, select “Lock Unique OU”, to “Reserve” the settings as illustrated in Option 3.

A pre-vetted identity has 1 of 3 main profile options:

- **Option 1: Fixed** Organization Name with an Optional Variable Organization Unit
- **Option 2: Fixed** Organization Name with a **Fixed** Organization Unit
- **Option 3: Fixed** Organization Name with a **Fixed** and “**Reserved**” Organization Unit in the Base Distinguished Name

OPTION 1: FIXED ORGANIZATION NAME WITH AN OPTIONAL VARIABLE ORGANIZATION UNIT

- Common Name: Required (John Doe or Jane Smith for example)
- Organization Name: Fixed during validation
- Organization Unit: Optional and Variable (“authenticated by LRA” appended)
- Locality: Fixed during validation
- State: Fixed during validation
- Country: Fixed during validation
- Email Address: Required (This is included in the certificate, but also the pickup link will be delivered to this e-mail address.)

The following is an example of an end user registration based on **Option 1**:

Certificate Identity Details	
Common Name <small>Required</small>	<input type="text"/>
Organization	GlobalSign Inc.
Organizational Unit	<input type="text"/>
Locality	Portsmouth
State or Province	NH
Country	United States
Email Address <small>Required</small>	<input type="text"/>

OPTION 2: FIXED ORGANIZATION NAME WITH A FIXED ORGANIZATION UNIT

With “Lock OU” not selected, but OU populated in the profile.

- Common Name: Required (John Doe or Jane Smith for example) Fixed
- Organization Name: during validation
- Organization Unit: Fixed during validation but variable (“authenticated by LRA” appended)
- Locality: Fixed during validation
- State: Fixed during validation
- Country: Fixed during validation
- Email Address: Required (This is included in the certificate, but also the pickup link will be delivered to this e-mail address.)

The following is an example of an end user registration based on **Option 2**

Certificate Identity Details	
Common Name <small>Required</small>	<input type="text"/>
Organization	GlobalSign
Organizational Unit	West Coast Sales - authenticated by LRA
Locality	Portsmouth
State or Province	NH
Country	United States
Email Address <small>Required</small>	<input type="text"/>

OPTION 3: FIXED ORGANIZATION NAME WITH A FIXED “RESERVED*” ORGANIZATION UNIT IN THE BASE DISTINGUISHED NAME (DN)

With “Lock OU” selected, the OU is fixed and unique within the profile.

- Common Name: Required (John Doe or Jane Smith for example) Fixed
- Organization Name: during validation
- Organization Unit: Fixed during validation (“authenticated by LRA” appended)
- Locality: Fixed during validation
- State: Fixed during validation
- Country: Fixed during validation
- Email Address: Required (This is included in the certificate, but also the pickup link will be delivered to this e-mail address.)

The following is an example of an end user registration based on **Option 3**:

Certificate Identity Details	
Common Name <small>Required</small>	<input type="text"/>
Organization	GlobalSign
Organizational Unit	West Coast Sales - authenticated by LRA
Locality	Portsmouth
State or Province	NH
Country	United States
Email Address <small>Required</small>	<input type="text"/>

*To address concerns surrounding secure web access, new / additional profiles cannot be established using a “Locked” Organization and Organization Unit combined value. By checking the ‘Lock OU’ selection box, you’ll prohibit this combination from being used in future Profiles.

Once you have configured your profile(s) with the distinguished values, click the **Confirm** button and the vetting department will be notified of your request and begin the vetting process.

After your Profile has been vetted, you will be able to order/issue certificates to end users against that pre-vetted profile information. Note: Certificates from within Certificate license packs can draw off as many pre-vetted Profiles as you establish.

Should you have any questions regarding the status of your Profile request, please open a Support ticket at <https://www.globalsign.com/help/>.

ADDITIONAL PROFILE SPECIFIC CONFIGURATION OPTIONS

By selecting **Profile Configuration**, the EPKI Administrator can enable support for additional PKI-enabled applications that require specific key usages. Additionally, key size restrictions can be enforced for PKCS12 delivery options.

The image shows a navigation menu on the left with the following options: MY PROFILES, Profile Configuration, Order Additional Profiles, Approve Pending Profiles, and Search Profiles. A red arrow points from 'Profile Configuration' to the main configuration window.

The main window is titled 'Step 1: Configure Profile' and contains a 'Portal' section with the following details:

Profile ID	MP [REDACTED]
Organization	GlobalSign, Inc
Organization Unit	
URL	https://system.globalsign.com/cr/public/certificate/order.do? p=[REDACTED]a059
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do? p=8907 [REDACTED]

At the bottom of the configuration window is a blue 'Next' button.

Select the Profile and click **Next** to configure the additional options shown below:

Step 1: Configure Profile

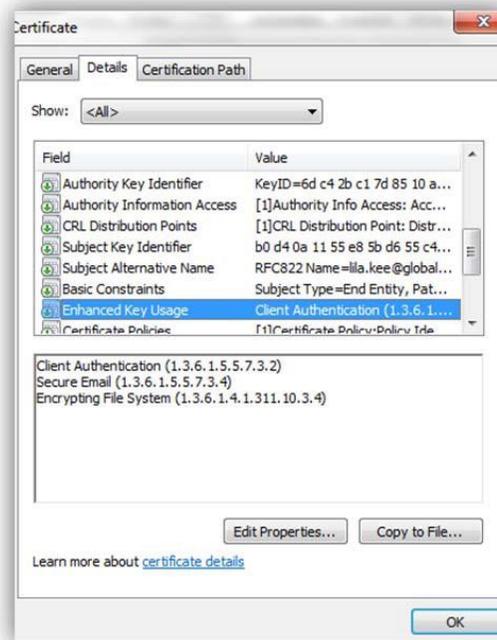
Profile Configuration

Profile ID	MP201800030818
Organization	
Organization Unit	
URL	
URL(PKCS12 Option)	
User Permission	Configure
Email Domains	Configure
1 Signature Algorithm	<input checked="" type="radio"/> sha256RSA <input type="radio"/> RSASSA-PSS (sha256) <small>Required for German Energy Sector email certificates</small>
2 Encrypting File System	<input type="radio"/> Disabled <input type="radio"/> Enabled
3 MS SmartCard Logon	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Renewal Type	<input type="radio"/> Manual <input checked="" type="radio"/> Auto <input type="radio"/> Quick
Non Exportable Option <small>Limited to only Internet Explorer.</small>	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
API IP Address range <small>IP Address is limited to only at the time of API e.g) 1.1.1.1-4.4.4.4 211.11.149.249,211.11.149.250</small>	*****

[Back](#) [Next](#)

1. Signature Algorithm: The default signature algorithm is **sha256RSA**. GlobalSign also offers **RSASSA-PSS (sha256)** which is required for secure email certificates used for the German Energy Sector ([see more information here](#)).

2. Encrypted File Systems (EFS): Enabling the EFS option will display EFS as an option at certificate registration. The issued certificate will include the enhanced key usage extension: Encrypting File System (1.3.6.1.4.1.311.10.3.4).



3. Microsoft (MS) SmartCard Logon: You can enable this feature at the profile level to allow for smartcard-based authentication.

RENEWAL

There are three main renewal configurations available to the EPKI Administrator:

1. **Manual** (Default setting) – Renewal reminder emails sent to subscriber at periodic intervals; Subscriber registers for renewed certificate and a notification email is sent to the EPKI Administrator alerting them of a pending request that requires review.
2. **Automatic** – Renewal reminder sent to subscriber at periodic intervals; successful client authentication will automatically generate a renewed certificate.
3. **Quick** – At 30 days before certificate expiration, active certificate holders are automatically sent an email to immediately install a renewed certificate.

Renewal reminder settings can be enabled or disabled in the **Manage Email Templates** link found under the **EMAIL** menu. In either case, renewed certificates will include the identical identity information included in the original certificate. Please note, that sufficient certificate inventory must be available for the renewal order to successfully be completed.

To enable Automatic or Quick Renewal options, go to **Profile Configuration**, click **Next** and select your preferred renewal option:

Step 1: Configure Profile

Profile Configuration

Profile ID	MP201808030818
Organization	View/Select
Organization Unit	
URL	View/Select
URL(PKCS12 Option)	View/Select
User Permission	Configure
Email Domains	Configure
Signature Algorithm	<input checked="" type="radio"/> sha256RSA <input type="radio"/> RSASSA-PSS (sha256) <small>Required for German Energy Sector email certificates</small>
Encrypting File System	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
MS SmartCard Logon	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Renewal Type	<input type="radio"/> Manual <input checked="" type="radio"/> Auto <input type="radio"/> Quick
Non Exportable Option	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled <small>Limited to only Internet Explorer.</small>
API IP Address range	<small>IP Address is limited to only at the time of API e.g) *.*.*.* e.g) 211.11.149.249,211.11.149.250</small> <input type="text"/>

[Back](#) [Next](#)

PURCHASING CERTIFICATE LICENSE PACKS

Certificate licenses may be purchased based on several certificate configurations, including:

CERTIFICATE TYPE

- PersonalSign & DepartmentSign for Windows trusted applications. For a detailed product description go to <https://www.globalsign.com/personalsign/>
- PDF, Microsoft Office, and Email Signing For AATL for a detailed product description go to: <https://www.globalsign.com/en/digital-signatures/>

CERTIFICATE PACKS

Depending on the Certificate Type, you may order certificate packs starting from as low as 1 up to and including 1,000. Note, that an additional 10% quantity of spare certificates will be added to address attrition due to employee turn-over or revocation.

PURCHASING PERMISSIONS

By default, the Account Administrator has the permission to purchase license packs. The Admin can choose to enable purchasing permissions for Managers and/or Staff. Managers can also enable purchasing permissions for Staff in Charge users. To do so, navigate to the "ACCOUNT & FINANCE" tab in GCC, click "Manage Users", then click "Edit" next to a user. Scroll to the bottom to "Deposit / Enterprise PKI license purchase privilege" and select either **Yes** or **No**, then click confirm.

■ Certificate approval permission	Yes <input checked="" type="radio"/> No <input type="radio"/>
■ Deposit / Enterprise PKI license purchase privilege	Yes <input checked="" type="radio"/> No <input type="radio"/>

[Back](#) [Confirm](#)

CERTIFICATE VALIDITY

Depending on the Certificate types, validities range from 1 to 3 years resulting in significant discounts the longer the validity. Licenses can be purchased by clicking **Order Licenses** found under the **My Licenses** tab. Select the Certificate validity you wish to apply and click **Next**.

ACCOUNT & FINANCE
SSL CERTIFICATES
MANAGED SSL
DOCUMENT CODE & EMAIL SIGNING
ENTERPRISE PKI

ePKI Home

MY CERTIFICATES

- Order Certificates
- Order Certificate BULK
- Search Certificates
- PKCS#12 Bulk Registration and Pickup
- Search PKCS#12 Bulk Order History
- Approve Pending Certificates

MY LICENSES

- Order Licenses
- Search License Orders

MY PROFILES

- Profile Configuration
- Order Additional Profiles
- Search Profiles

MY ORDERING

PORTAL

- Portal Configuration

EMAILS

- Manage E-mail Templates
- View All Sent Emails
- View Emails to Portal Users

OTHER FUNCTIONS

License Selection

1. Product Details

2. Completed

[Select Product](#) >> [Payment](#) >> [Confirm Details](#)

Product Details - Enterprise PKI Lite For Department Digital ID 1,000 pack

Certificate Validity Required <small>Multi-year offers significant per annum savings</small>	<input checked="" type="radio"/> 1 year \$0 <input type="radio"/> 2 year \$0 <input type="radio"/> 3 year \$0	
Campaign Code	<input type="text"/> <small>Redeem code</small> <small>If you have a Campaign Code please enter and click "Redeem Code". This page will be reloaded with your appropriate discount.</small>	
Coupon Code	<input type="text"/> <small>Redeem code</small> <small>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.</small>	
TOTAL COST (inc. Tax)	\$ 0	

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.

13



Select one of the following Payment methods:

- **Payment in arrears** – Select this option if you are paying by **Purchase Order** (which must be pre-arranged with your GlobalSign Account Manager) and supply the Purchase Order Number.
- **Bank Deposit** – Select this option to use existing **Account funds** that have been deposited into your account (via the Account and Finance Tab)
- **Credit Card** – Supply your credit card details as prompted.

The screenshot shows a two-step process: '1. Product Details' and '2. Completed'. Below this is a navigation bar with 'Select Product', 'Payment', and 'Confirm Details'. The 'Payment Details' section contains a form with the following fields:

Purchase Order Number	<input type="text"/> Enter if you have a PO Number. This will be displayed in your Invoice
Payment Method	<input type="radio"/> Payment in arrears <input checked="" type="radio"/> Credit Card <input type="radio"/> Bank Deposit

Below the form is the section 'Credit Card Details & Billing Address' with logos for VISA, MasterCard, and AMERICAN EXPRESS.

Review and confirm the details of your order. You will need to accept the EPKI Service Agreement when placing your first order. Note, the EPKI Service Agreement binds you to the Local Registration Authority and other obligations as outlined in the GlobalSign Certificate Practice Statements found at <http://www.globalsign.com/repository>. Click Next. The certificate license pack order is now completed.

CUSTOMIZING EMAIL TEMPLATES

EPKI Administrators may use the standard email templates “out-of-the-box” or customize the messages for specific organization instructions. To customize your email templates, select **Manage E-mail Templates** found under the **EMAILS** menu.

ACCOUNT & FINANCE | SSL CERTIFICATES | MANAGED SSL | DOCUMENT, CODE & EMAIL SIGNING | ENTERPRISE PKI

ePKI Home

Edit Mail Template

This is where you manage the email that end-users of your certificates will receive.

English - EN (Default) Add a language

Selected Template: English - EN

mail type	Delivery	Contents
Bulk Order (Admin) Renewal Reminders in 30 days	true	Edit
Cancellation Completed	true	Edit
Enrollment(Invite)	true	Edit
Enrollment(Portal)	true	Edit
Enrollment(QUICK RENEW)	true	Edit
Enrollment(Reissue)	true	Edit
Enrollment Information 15 days	true	Edit
Enrollment Information 30 days	true	Edit
Enrollment Information 31 days	true	Edit
Issuance Completed	true	Edit
PKCS12 Issuance Completed	true	Edit
Cancellation Completed(Not consent)	true	Edit
Portal Order Received	true	Edit
Reissuance Completed	true	Edit
PKCS12 Reissuance Completed	true	Edit
Renewal Reminders Today	true	Edit
Renewal Reminders	true	Edit
Renewal Reminders in 7 days	true	Edit
Renewal Reminders in 14 days	true	Edit
Renewal Reminders in 21 days	true	Edit
Renewal Reminders in 30 days	true	Edit
Renewal Reminders in 60 days	true	Edit
Renewal Reminders in 90 days	true	Edit
Revocation Completed	true	Edit
Suspend completed	true	Edit
Unsuspend completed	true	Edit

Selected Template: English - EN

Click **Edit** next to the email you wish to customize. You can add additional email addresses for the carbon copy (CC) or blind copy (BCC) and modify the message details.

Please note that the items prefixed with \$\$ are variables that the EPKI system will replace with values as the email is sent out. They should not be modified, as they contain necessary information to complete the intended action.

ePKI Home

Edit Mail Template

Message Detail

Send timing: Cancellation Completed

Delivery Enable Disable

Mail Encoding: UTF-8 Reset Message

Message Header

From: \$\$[ContractUser!Email]

To: \$\$[CertAdminUser!Email]

Cc:

Bcc:

Message Details

Subject: CANCEL_COMPLETE/\$(OrderID) - \$\$[DefaultCommonName]

Please note that this e-mail is automatically sent from a noreply mailbox.

Dear: \$\$[OrderID]

Certificate Order Number
 Partner ID
 Profile ID
 License ID
 Product
 New/Renew
 Period
 Install Path
 Pickup Path
 Renewal Path
 Common Name
 Organization
 Organization Unit 1
 Organization Unit 2
 Organization Unit 3
 CountryCode
 CountyName
 State Or Province
 Locality
 Email Address
 Title

CERTIFICATE ISSUANCE

There are two main options for requesting certificates:

1. **End User Initiated/ Portal Enrollment process** – Where a Portal link (one per Profile) may be published for open enrollments.
2. **EPKI Administrator registration** – Where you, as the EPKI Administrator, register a user via the GCC EPKI Portal.

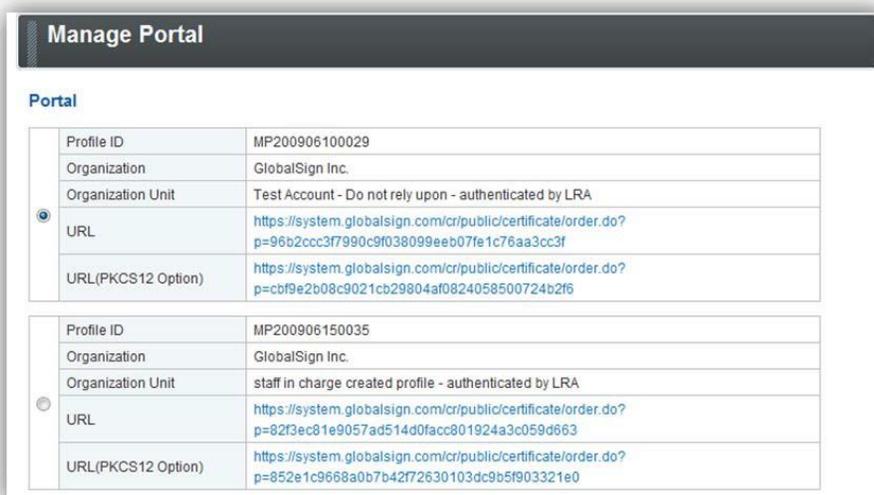
With the End User Initiated/Portal Enrollment process, end users set their own pickup password for the enrollment process; whereas with the EPKI Administrator registration process, the Administrator generates or creates the certificate pickup password which must be securely provided to the end user.

USING THE PORTAL LINK

The EPKI Managed Service offers the ability for organizations with dispersed offices or departments to centralize the Certificate ordering process. Administrators have the option of publishing a certificate enrollment page (Portal Link). Anybody within your organization will then be able to complete an application for a Certificate through the account by leveraging the Pre-vetted company information.

The Certificate will not be issued until the EPKI Administrator with Approval privileges logs into the account and approves the application. This ensures organizations issue Certificates only to legitimate applicants.

A unique Portal will be established for each Profile established. A separate Portal link or URL is provided to support both local and GlobalSign Server key generation, which you can find by clicking **Portal Configuration** under the **My Ordering Portal** menu section. Select the URL (PKCS12 Option) to enable the GlobalSign server key generation option that will create and distribute the public and private keys along with the digital certificate delivery.



The screenshot shows a 'Manage Portal' interface with two portal configurations. Each configuration is a table with fields for Profile ID, Organization, Organization Unit, URL, and URL(PKCS12 Option). The first configuration is selected with a radio button.

Manage Portal	
Portal	
Profile ID	MP200906100029
Organization	GlobalSign Inc.
Organization Unit	Test Account - Do not rely upon - authenticated by LRA
<input checked="" type="radio"/> URL	https://system.globalsign.com/cr/public/certificate/order.do?p=96b2ccc3f7990c9f038099eeb07fe1c76aa3cc3f
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=cbf9e2b08c9021cb29804af0824058500724b2f6
Profile ID	MP200906150035
Organization	GlobalSign Inc.
Organization Unit	staff in charge created profile - authenticated by LRA
<input type="radio"/> URL	https://system.globalsign.com/cr/public/certificate/order.do?p=82f3ec81e9057ad514d0facc801924a3c059d663
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=852e1c9668a0b7b42f72630103dc9b5f903321e0

Optionally, by clicking **Next** after selecting a particular profile, the EPKI Administrator may upload a logo to be displayed on the top banner of the end user enrollment page, as well as a GIF to be displayed at the footer of the page.

Portal

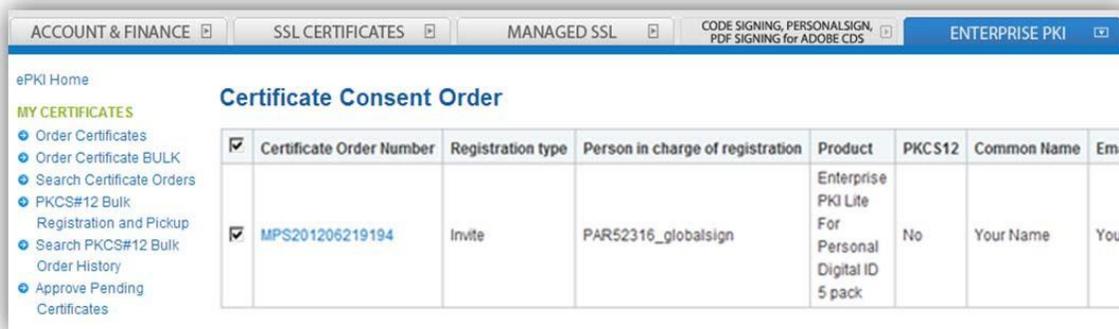
Profile ID	MP201306201398
Organization	GMO GlobalSign Ltd
Organization Unit	Marketing EMEA
URL	https://system.globalsign.com/cr/public/certificate/order.do?p=e83bf616dd9c1bd5de49178b7d5e5402c9bd6d9b
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=63d056a9ed3d81665cc0a406f0e2c719ecd441bb
Logo GIF	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/> Recommended size 176x37 pixel The maximum capacity 2MB Valid image types jpg,gif,png
Footer GIF	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/> Recommended size 950x7 pixel The maximum capacity 2MB Valid image types jpg,gif,png

Other Portal Configurable Options:

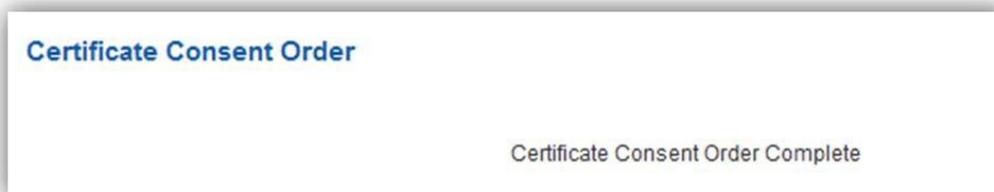
Modify Subscriber Agreement: You may add additional subscriber terms to the Mandatory GlobalSign Subscriber Agreement to capture unique or additional terms above and beyond the required GlobalSign terms. End users will be presented with the Subscriber Agreement and prompted to accept the terms prior to certificate installation.

APPROVING REQUESTS (ORDERS)

Applications completed by Users / Departments using the Portal must be approved by an EPKI Administrator. When such applications are completed, an email alert will be sent to the EPKI Administrator(s) and the appropriate Administrator must log into the account and click the **Approve Pending Certificates** link under the **My Certificates** menu. Check the request and click **Next**. Review the order and after appropriate identity verification is completed, click **Next**.



The following screen will display at confirmation and an email will be sent to the end user with a link to install the digital certificate. Note, the end user will need the “Pick Up Password” they established at registration in order to install the certificate.

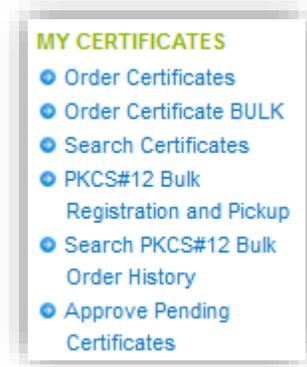


REGISTER USERS FOR CERTIFICATES VIA EPKI ADMINISTRATOR

There are **three** options that the EPKI Administrators can use to register users for digital certificates or essentially issue certificates to end users:

1. Individual – New Certificate (**Order Certificates**)
2. Multiple – New Certificate BULK Issuance (**Order Certificate BULK**)
3. Multiple – New Certificate BULK Registration and Pickup (**PKCS#12 Bulk Registration and Pickup**)

These links are found under the **My Certificates** menu.



INDIVIDUAL CERTIFICATE REGISTRATION

For individual registrations, click **Order Certificates** under the **My Certificates** menu and then select the Certificate Profile and License you wish to apply the certificate request to.

Product Selection

1. Product Details | 2. Completed

Select Profile >> Certificate Identity Details >> Confirm Details

Product Details

Profile

	Profile ID	BaseDN	Organization	Organization Unit
<input checked="" type="radio"/>	MP201306201398	Disabled	GMO GlobalSign Ltd	Marketing EMEA

License

	Service	License Unused number
<input checked="" type="radio"/>	Enterprise PKI Lite For Personal Digital ID 2 year	11

Next

Click **Next** and complete the certificate identity details for the end user/ subscriber. Note: Certain pre-vetted fields will be hardcoded.

Optionally, the EPKI Administrator may select an alternative certificate delivery method, other than the default PKCS7 method, where key generation is performed locally via the Subscriber’s browser:

1. Certificate Signing Request (CSR) – in this case, the Subscriber is expected to provide a CSR created either from a different system (e.g. Hardware security Module) or outside the browser session used to enroll for the digital certificate. This is typically for advanced users.
2. P12 – PKCS12 – in this case, GlobalSign will create the public and private key pair centrally and deliver a P12 file (including the public and private keys) that the Subscriber will install into their local system via the browser certificate import tool. GlobalSign has implemented the following security precautions surrounding P12 delivery:
 - a. The establishment of a strong certificate password by the subscriber (with a minimum of 12 characters) in order to install the P12 file. (Note, this is different than the “Pick up password” which is used to authenticate certificate pick-up requests regardless of enrollment method selected).

- b. P12 file purge. Note, GlobalSign will purge all P12 files. Therefore, it is recommended that Subscribers import the P12 file by marking the private key as exportable and then make a back-up. (See GlobalSign Support for additional details).

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)	<input type="checkbox"/>
PKCS12 Option	<input type="checkbox"/>
Pickup Password Required	<input type="text"/> Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9) Password Generation <input type="button" value="Generate"/> When the password automatic operation generation button is pressed, a random password automatic construction is set.
Pickup Password (re-enter) Required	<input type="text"/>
Memo	<input type="text"/>

Additionally, the EPKI Administrator will need to establish a “Pickup Password”, or use the “Password Generation” tool, that you are required to deliver to the Subscriber in an “Out of Band” secure method. As a security precaution, the certificate cannot be installed unless the user has received the System generated certificate pick up email. This provides the challenge response which is necessary to prove control of the email address. Confirm details, and if correct, click **Next**.

1. Product Details | 2. Completed

Select Profile > Certificate Identity Details > Confirm Details

Confirm Details

Product Details

Profile ID	MP201306201398
License ID	ML201306201396

Certificate Identity Details

Common Name	YourName
Organization	GMO GlobalSign Ltd
Organizational Unit	Marketing EMEA
Locality	Maldstone
State or Province	Kent
Country	United Kingdom - GB
Email Address	your.email@yourcompany.com
Encrypting File System	Disabled
MS SmartCard Logon	
I have an externally generated CSR	Disabled
PKCS12 Option	Disabled
Memo	

1. Product Details | 2. Completed

Application Completed

Order Number: **MP52013062118838**

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:

- Release 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

BULK ENROLLMENT

For multiple user registrations, click **Order Certificate BULK** under the **My Certificates** menu then select the appropriate Certificate Profile and License pack you wish to apply the certificate requests to. Click **Next** to continue.

Product Selection

1. Product Details 2. Completed

Product Details >> File specification >> Edit Details >> Confirm Details

Product Details

Profile

Profile ID	BaseDN	Organization	Organization Unit
<input checked="" type="radio"/> MP201306201398	Disabled	GMO GlobalSign Ltd	Marketing EMEA

License

Service	License Unused number
<input checked="" type="radio"/> Enterprise PKI Lite For Personal Digital ID 2 year	10

Next

You will then be instructed to browse for a Comma Separated Value (CSV) file, typically created in Notepad, which includes the records you wish to upload. Please note, depending upon the Profile selected, Organization Unit may or may not be a value supplied in the CSV. This is especially true for Organization Unit values that have been pre-established as part of a “Locked O and OU Profile”.

Item	Explanation	Limitation
CommonName	Common name	Up to 64 alphanumeric characters
OrganizationUnit	Organization Unit 2	Up to 64 alphanumeric characters
OrganizationUnit	Organization Unit 3	Up to 64 alphanumeric characters
Email	Email Address	Email Address
PickupPassword	Pickup Password	Enter 8 to 64 alphanumeric characters. Alternatively, enter "AUTOGEN" for system generated passwords
haveCSR	Preparing CSR in the test with HSM etc. sets "true"	true/false
PKCS12	if PKCS12, sets "true"	true/false

CSV file No file chosen

Below is an example of a CSV created for a Profile that allows for an Optional Variable Organization Unit. Note, for the records, where OU is desired “blank”, a space was created in the second value of the record.

```

bulk upload test3.txt - Notepad
File Edit Format View Help
CommonName,OrganizationUnit,Email,PickupPassword,
Mary Smith, ,mary.smith@globalsign.com,$&^(S2334
John Jones, ,john.jones@globalsign.com,jfo2n&nd98
Kate Habib, ,kate.habib@globalsign.com,$JKGJ23dhg
Jennifer Yee,Accounting,jennifer.yee@globalsign.com,947892jj#2
George Maloof,west Coast Sales,george.maloof@globalsign.com,kh95jg$%@r

```

As a reminder, Profiles with pre-established OU values will result in a common and required value for all users, regardless of what is specified for OU in the CSV.

After uploading the CSV, you may specify optional delivery methods discussed previously in this guide by checking either “haveCSR” or “PKCS12”. Leave both options unchecked if you wish to proceed with the default delivery method.

No	CommonName <small>Required</small>	OrganizationUnit	Email Address <small>Required</small>	Pickup Password <small>Required</small>	haveCSR	PKCS12
1	Mary Smith	staff in charge created profile - authenticated by LRA	mary.smith@globalsign.com	\$&^(S2334	<input type="checkbox"/>	<input type="checkbox"/>
2	John Jones	staff in charge created profile - authenticated by LRA	john.jones@globalsign.com	jfo2n&nd98	<input type="checkbox"/>	<input type="checkbox"/>
3	Kate Habib	staff in charge created profile - authenticated by LRA	kate.habib@globalsign.com	\$JKGJ23dhg	<input type="checkbox"/>	<input type="checkbox"/>
4	Jennifer Yee	staff in charge created profile - authenticated by LRA	jennifer.yee@globalsign.com	947892jj#2	<input type="checkbox"/>	<input type="checkbox"/>
5	George Maloof	staff in charge created profile - authenticated by LRA	george.maloof@globalsign.com	kh95jg\$%@r	<input type="checkbox"/>	<input type="checkbox"/>

To complete the process, click **Next** and securely distribute the Certificate pick-up passwords to the Users.

BULK PROVISIONING (PKCS#12)

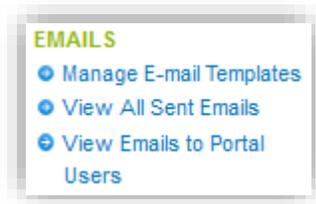
Bulk provisioning provides an alternative to bulk enrollment in that the enrollment steps performed by the end user are minimized or in some cases totally eliminated. The bulk provisioning feature provides the following benefits:

- Easy method to provision large number of certificates
- GlobalSign server-side key generation eliminates the need for local key generation
- Single file PKCS12 delivery allows for easy back up
- Administrator enrolls “on behalf” of end user allowing more control of certificate provisioning and back-up

NOTE: By default, the Bulk PKCS12 registration option will only support user registration that do not include email addresses in the certificate subject name. To include email addresses in Certificates when using the Bulk PKCS12 method, Email Domain Registration is required prior to ordering certificates. Please see Email Domain Registration section below.

BEFORE YOU BEGIN

1. There is a 200 record limit (3.2M) and depending on key size selected, the ZipFile containing PKCS12s may take up to 40 minutes to process.
2. Disable all renewal reminders, as follows, to prevent system generated email reminders from going directly to your end user:
 - a. Disable Renewal reminders by clicking on **Manage E-mail Templates** under the EMAILS Menu



- b. Click “Edit” for any template that is marked “true”.

Renewal Reminders Today	true	Edit
Renewal Reminders	true	Edit
Renewal Reminders in 7 days	true	Edit
Renewal Reminders in 14 days	true	Edit
Renewal Reminders in 21 days	true	Edit
Renewal Reminders in 30 days	true	Edit
Renewal Reminders in 60 days	true	Edit
Renewal Reminders in 90 days	true	Edit

c. Change Delivery from “Enable” to “Disable” as shown below

Delivery	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Mail Encoding	UTF-8 <input type="button" value="v"/>

d. Click “Next” and then “Complete”.

USING THE BULK PROVISIONING (PKCS#12) METHOD

1. From the **My Certificates** menu, select PKCS#12 BULK Registration and Pickup
2. Select the appropriate profile and license pack and click **Next**

Product Selection

1. Product Details

2. Completed

Product Details >>
 File specification >>
 Edit Details >>
 Confirm Details

Product Details

Profile

Profile ID	BaseDN	Organization	Organization Unit
<input checked="" type="radio"/> MP201306201398	Disabled	GMO GlobalSign Ltd	Marketing EMEA

License

Service	License Unused number
<input checked="" type="radio"/> Enterprise PKI Lite For Personal Digital ID 2 year	10

Next

- Browse and Upload a CSV file, formatted based on your certificate profile selection. Note, the CSV file format guidance will be based on the Profile settings associated with the selected profile. To include the email field, you must pre-register email domain(s) prior to ordering (refer to the Email Domain Registration section).

Product Selection

1. Product Details

2. Completed

Product Details >>
File specification
>> Edit Details
>> Confirm Details

File format

Bulk Upload provides the capability to pre-register multiple Subscribers. This is accomplished by uploading a file that contains information about the certificate and enrollment method. The file must have a Comma Separated Value (CSV)-format based on the Profile selected. The following is an example of file content that is properly formatted. Be sure to include the first line header as depicted below

```
CommonName ,OrganizationUnit2 ,OrganizationUnit3 ,PickupPassword
Kate Jones , ,9o7I9ghsa3YZ
Jennifer Jones ,Jennifer Jones ,Research and Dev ,9o7I9ghsa3YZ
George Jones ,Accounting ,9o7I9ghsa3YZ
```

CSV file

No file chosen

Back

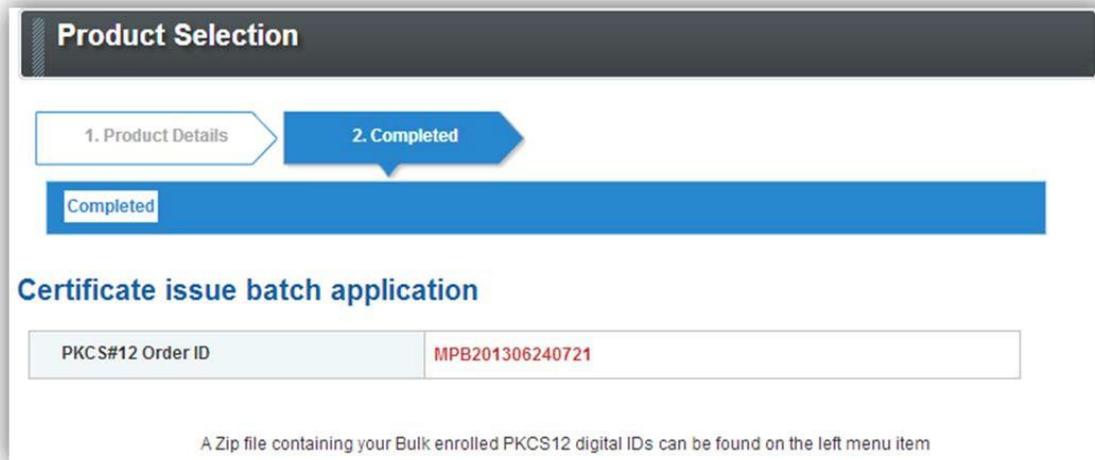
Next

- Review the certificate details pulled from the CSV file and make changes as necessary. Click “Next” to continue.

Edit Details

No	CommonName <small>Required</small>	OrganizationUnit	PKCS#12 Password <small>Required</small>
1	<input type="text" value="Test1"/>	<input type="text" value="C02731"/>	<input type="text" value="jfgt23966bCew"/>
2	<input type="text" value="Test2"/>	<input type="text" value="C02727"/>	<input type="text" value="ngfgtansgouetj"/>
3	<input type="text" value="Test3"/>	<input type="text" value="C02728"/>	<input type="text" value="nga9540bcd3#"/>
4	<input type="text" value="Test4"/>	<input type="text" value="C02713"/>	<input type="text" value="nglajd9ye2000@a"/>

5. You will reach a confirmation page which means the certificate generation is complete.



6. After receiving confirmation, a zip file containing the PKCS12 files can be found in the “**PKCS#12 Bulk order history Report**” located on the left hand menu pane. Click on the link and search for Order ID then click, “Download”. The zip file will be purged from your EPKI account 1 month after creation, therefore it is important to download the file within 30 days. Local Key recovery can be implemented by securely storing the zip file containing the PKCS12 files, while also securely storing the csv file that includes the passwords to the PKCS12 (sometimes referred to as private key passwords).

EMAIL DOMAIN REGISTRATION

The Email Domain Registration feature allows organizations to register the domain(s), which they own or are approved to use, and link the registered domains to an EPKI Profile. By registering email domain names to a Profile, you can then order certificates containing corresponding email addresses when using the Bulk Provisioning (PKCS#12) method. Once a domain name has been registered and vetted, the email address input field for Bulk Provisioning will be turned on for the EPKI Profile. The Email Domain Registration feature provides the following capabilities:

- Ability to add email domain(s) to EPKI Profile and submit the email domains to the RA to be vetted
- Ability to include email addresses (matching the registered email domains) in certificates when using the Bulk Provisioning (PKCS#12) method
- Assists end users with inputting their email address on the EPKI portal screen by providing a drop down menu containing registered domain(s)

HOW TO REGISTER EMAIL DOMAINS

1. Click **Profile Configuration** in the left menu pane
2. Select a Profile and click **Next**
3. Click the **Configure** button next to Email Domains

Profile Configuration

Profile ID	MP201609151177
Organization	GlobalSign
Organization Unit	
URL	https://dev-gcc.globalsign.com/cr/public/certificate/order.do?p=bd46ef624ccf76a14008c7bdc8b6aeddaf6afeb5
URL(PKCS12 Option)	https://dev-gcc.globalsign.com/cr/public/certificate/order.do?p=702b821fdb157b083d748ea1e800701b24242af2
User Permission	<input type="button" value="Configure"/>
Email Domains	<input type="button" value="Configure"/>
Hash Algorithm	<input checked="" type="radio"/> SHA-256 (Recommended) <small>SHA-256 certificates provide the highest level of security, but may not be compatible with older environments or applications. To ensure application compatibility, we strongly encourage testing PKI-dependent components before using SHA-256 certificates.</small> <input type="radio"/> SHA-1
Encrypting File System	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

Email Domains

This item is optional, and can be registered afterward. In order to include Email address by means of "PKCS#12 BULK Registration and Pickup" provisioning, the Email domain needs to be registered and approved. Please refer to EPKI Administrator Guide for more detail.

Add Email Domains

Email Domains
A comma-separated list of Email domain names (without the @ symbol) to approve.
Ex: globalsign.com
Ex: example.com, globalsign.com

4. Enter domain name(s) into the Email Domains field.
5. Submit the email domain(s) and GlobalSign vetting will verify that the email domain is owned/controlled by your organization. As part of the verification process, GlobalSign will contact you or the owner of the Domain name to confirm ownership which may take a few business days.
6. You can view the registered Email Domains/ check the status of registered domains by clicking on the Email Domain List menu option.
7. After your registered domains are approved, the email address input field will be turned ON in the Bulk Provisioning (PKCS#12) menu allowing you to include Email addresses in certificate orders.

ePKI Home

Profile Email Domain Search

Show:

1 - 4 / 4

< 1 >

Profile ID	Email Domain	Status	
MP201609151177	sample2.com	Pending	
MP201609151177	sample.com	Pending	
MP201609151177	example.com	Approved	<input type="button" value="Suspend"/>
MP201609151177	globalsign.com	Approved	<input type="button" value="Suspend"/>

MY CERTIFICATES
 Order Certificates
 Order Certificate BULK
 Search Certificates
 PKCS#12 Bulk
 Registration and Pickup
 Search PKCS#12 Bulk
 Order History
 Approve Pending Certificates

MY LICENSES
 Order Licenses
 Search License Orders

MY PROFILES
 Profile Configuration
 Order Additional Profiles
 Search Profiles
 Email Domain List

HOW TO SUSPEND/UNSUSPEND EMAIL DOMAINS

1. Registered Email Domains can be suspended temporarily, by clicking **Suspend** in the Email Domain List menu.
2. Suspended domains cannot be included in the certificate orders. Also, Portal users cannot select suspended domains.
3. Suspended Email Domains can be unsuspected, by clicking **Unsuspend** in the Email Domain List menu.

EMAIL DOMAIN OPTIONS FOR EPKI PORTAL USERS

The EPKI Portal has two option for portal users to input their email address/domain:

1. Portal users can manually input their full email address.
2. Or portal users can select: "Choose Email Domain". Then the user will enter the prefix of their email address and select their email domain from a drop down menu of pre-vetted email domains.

ePKI Portal

1. Product Details 2. Completed

Certificate Identity Details >> Confirm Details

Certificate Identity Details

Common Name <i>Required</i>	<input type="text"/>
Organization	GlobalSign
Organizational Unit	<input type="text"/> <input type="text"/>
Locality	Shibuya
State or Province	Tokyo
Country	United States - US
Email Address <i>Required</i>	Input Full Email Address or partial Email Address with domain list. <input checked="" type="radio"/> Full Email address <input type="radio"/> Choose Email domain Full Email address <input type="text"/>
I have an externally generated CSR Check only if you are an Advanced User and <input type="checkbox"/>	

Certificate Identity Details

Common Name <i>Required</i>	<input type="text"/>
Organization	GlobalSign
Organizational Unit	<input type="text"/> <input type="text"/>
Locality	Shibuya
State or Province	Tokyo
Country	United States - US
Email Address <i>Required</i>	Input Full Email Address or partial Email Address with domain list. <input type="radio"/> Full Email address <input checked="" type="radio"/> Choose Email domain Enter an email prefix and select a domain <small>※ Select an Email domain from the list, and complete your Email address. The @ symbol is required.</small> <input type="text" value="j.smith@hr"/> . <input type="text" value="globalsign.com"/> Email address preview j.smith@hr.globalsign.com
I have an externally generated CSR <input type="checkbox"/>	

- The EPKI Admin can restrict portal users and only allow the “choose email domain” option by checking the box: **“Require Registered Email Domains”** under **Portal Configurations**.

MY PROFILES Profile Configuration Order Additional Profiles Search Profiles Email Domain List MY ORDERING PORTAL Portal Configuration EMAILS Manage E-mail Templates	Portal	
	Profile ID	MP201609151177
	Organization	GlobalSign
	Require Registered Email Domains	<input checked="" type="checkbox"/>

4. This option will hide the full email address entry field for portal users.

Certificate Identity Details	
Common Name <i>Required</i>	<input type="text"/>
Organization	GlobalSign
Organizational Unit	<input type="text"/> <input type="text"/> <input type="text"/>
Locality	Shibuya
State or Province	Tokyo
Country	United States - US
Email Address <i>Required</i>	<p>Enter an email prefix and select a domain ※ Select an Email domain from the list, and complete your Email address. The @ symbol is required.</p> <p><input type="text"/> . <input type="button" value="Select Email domain"/></p> <p>Email address preview Enter your Email Address above.</p>
I have an externally generated CSR	<input type="checkbox"/>

CERTIFICATE LIFECYCLE MANAGEMENT – REVOCATION, REISSUANCE, AND CANCELLATION

To revoke, cancel or reissue a certificate, please navigate to **Search Certificate Orders** under **My Certificates** in the left menu pane. Search for a particular certificate using the search bar, Advanced Search functions or simply click the **Search** button to populate all certificate orders. Click on the **Application** button next to the certificate order you wish to access. At the bottom of the report, you can choose to revoke, cancel or reissue the certificate.

Various application	Certificate Order Number	Organization Name	Common Name	Product	Period	Email Address	Person in charge of registration	Order Status	Certificate Status	Date of application
Application	MPS2013062118838	GMO GlobalSign Ltd	YourName	Enterprise PKI Lite For Personal Digital ID 10 pack	2 year	your.email@yourcompany.com	PAR89496_SGMtg2013	ISSUE_WAIT	NONE	06/21/2013 16:41(GMT+00:00)

Certificate action information

Action details	Action date	Result
ORDER_REQUEST	2009/06/09(GMT+00:00)	SUCCESS
CERT_ISSUE_WAIT	2009/06/09(GMT+00:00)	SUCCESS
CERT_ISSUE	2009/06/09(GMT+00:00)	SUCCESS

[Mail History](#)

Notes:

1. Revoked certificates will be put on the Certificate Revocation List within 24 hours, making the certificate unusable by most applications.
2. The cancellation request option will be available for 7 days after initial issuance of the certificate. Choose this to completely cancel your order and have the funds credited to you (via the original payment method).
1. Reissued certificates will be issued with an expiration date equal to the original certificate expiration date. Note, a new private key will be generated, therefore, a reissued certificate will not allow decryption of the emails that were encrypted using the original certificate.

History	Order Number	Subject	To	Date Sent	Status
333430	MPS2013062118838	ENROLLMENT_FOR_INVITE/MPS2013062118838 : YourName	your.email@yourcompany.com	06/21/2013 16:44(GMT+00:00)	Sent

Click **Mail History** to review or resend system generated emails.

REPORTING

EPKI Administrators can manage the full lifecycle of Digital Certificates issued from GCC. Locating a particular order/certificate is simple. First, ensure that you are authenticated to the portal using your Admin Certificate. Then click the **Search Certificate Orders** link found under the **My Certificates** menu pane. You can leave the field blank and click **Search** to locate all orders. Or click on **Show Advanced Search** and search by order, date, product etc.

The screenshot shows the 'ePKI Home' interface with a 'Certificate List' search section. On the left, there is a navigation menu under 'MY CERTIFICATES' with options like 'Order Certificates', 'Order Certificate BULK', 'Search Certificate Orders', 'PKCS#12 Bulk: Registration and Pickup', 'Search PKCS#12 Bulk Order History', and 'Approve Pending Certificates'. Below that is 'MY LICENSES' with 'Order Licenses' and 'Search License Orders'. The main search area has a text input field with the placeholder 'e.g. ML201207030574 OR John Smith' and a 'Hide Advanced Search' link. Below the input field are several search filters: 'Application Date is' with a dropdown, 'between' with a dropdown, and two date input fields with a 'i.e. mm/dd/yyyy' example; 'Any Product' with a dropdown; 'Any Order State' with a dropdown; 'Any Certificate Status' with a dropdown; 'Profile ID...' with an input field; 'License ID...' with an input field; 'User in Charge...' with an input field; 'Organization Unit...' with an input field; and 'Email address...' with an input field. A 'Search' button is located at the bottom right of the filter area. At the bottom left of the search area, there is a 'Display Number:' label and a dropdown menu set to '10'.

Then click the Application button next to the order you wish to review.

Various application	Certificate Order Number	Organization Name	Common Name	Product	Period	Email Address	Person in charge of registration	Order Status	Certificate Status	Date of application
Application	MPS2013062118838	GMO GlobalSign Ltd	YourName	Enterprise PKI Lite For Personal Digital ID 10 pack	2 year	your.email@yourcompany.com	PAR89496_SGMIktg2013	ISSUE_WAIT	NONE	06/21/2013 16:41(GMT+00:00)

LDIF

EPKI Administrators may wish to upload the public certificates associated with their EPKI account to a directory. EPKI provides a method to generate a LDIF (Lightweight Directory Access Protocol) report for upload to a [LDAP](#) directory.

CONFIGURING LDIF

LDIF reports can be formatted by the EPKI Administrator via the **Configure LDIF** link found under the **Other Functions** menu section.



The LDIF message format can be modified by clicking on a variety of substitution variables available in the right side panel. To save changes click **Next** and then **Complete**.

Please note the initial LDIF default format has been established by GlobalSign. The EPKI Administrator must modify the LDIF Template based on the "Profile" the LDIF query will run against. You can reset the format back to the default values anytime by clicking **Reset Message** as illustrated below.

Reset Message

Header	#LDIF made by GlobalSign GCC	Certificate Order Number Common Name Organization Organization Unit CountryCode State Or Province Locality Email Address Starting certificate validity date Closing certificate validity date Certificate-SerialNo Certificate-PEM Certificate-PKCS7 Memo
Message	<pre> dn: CN=\${Dn!CommonName},CN=Users,DC=edit here changetype: modify replace: userCertificate userCertificate:: \${Certificate!Pem} - </pre>	
Footer		

GENERATING A LDIF REPORT

LDIF reports are generated from the **Search Certificates** link under the **My Certificates** menu pane.

Click **Show Advanced Search** and select the appropriate date range, the Profile and set the Order State to **ISSUED** via the drop down menu. Note: If a certificate has been “re-issued”, the replacement certificate will have a status = Issued and be included in the LDIF report. The original, “replaced” certificate will not be included in the query since its status will change to “reissued”. Only non-revoked and unexpired certificates will be included. Then click on the **LDIF** Button.

Certificate List

e.g. ML201207030574 OR John Smith Hide Advanced Search

Application Date is between i.e. mm/dd/yyyy and i.e. mm/dd/yyyy

Any Product **ISSUED** Any Certificate Status

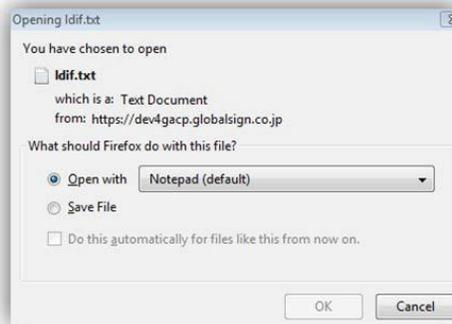
Profile ID... License ID... User in Charge...

Organization Unit... Email address...

Display Number:

1 - 3 / 3

Open the file with your preferred application.



Below, is an example of an LDIF Report opened in Notepad.



Upload the file to the LDAP directory according to your product specific instructions.

GCC ACCOUNT USERS

A list of active GCC Account users can be found by selecting the **ACCOUNT & FINANCE** top tab and then clicking **Manage Users** under **My Account**. New users can also be added by clicking the **New registration** button on this screen.



Note, all EPKI Users have equal access to established Profiles and licenses pack, however, user rights vary based on the assigned role. There are three main User Roles:

1. GCC Account Administrator – One per GCC account
2. Manager - unlimited per account
3. Staff in charge – unlimited per account

TYPES OF GCC ACCOUNT USERS

GCC ACCOUNT ADMINISTRATORS

GCC Account Administrators may add other Managers or Staff in charge and are provided full rights and access to the GCC product suite.

MANAGER

Managers may add other Staff in Charge user registrations, establish certificate profiles and approve orders if the GCC Administrator has set their **Certificate approval permission** option to **True**.

STAFF IN CHARGE

Staff in charge may initiate orders, resulting in **Pending Certificates** that the GCC Administrator or Managers with Certificate Approval Rights must review and approve.

Note, under the “**Search Certificates**” section, you can view the Administrator associated the issued Certificate, under the “Person in charge of registration” heading.

Various application	Certificate Order Number	Organization Name	Common Name	Product	Period	Email Address	Person in charge of registration
				Enterprise PKI AATL Signing			

REGISTERING ADDITIONAL GCC ACCOUNT USERS

To create either “Managers” or “Staff in charge”, select the **ACCOUNT & FINANCE** top tab. Select **Manage Users** under **MY ACCOUNT** and then click the **New registration** button. Begin by assigning a **User ID** and **Password** that will need to be distributed out-of-band to the appointed user. Complete the registration by entering the required fields, including user information and user type – either “Manager” or “Staff in

charge”. Set **Certificate Approval Permission** to **True**, to grant certificate approval and profile creation rights to a “Manager”. Note, “Staff in charge” will be unable to approve certificates or establish new profiles.

The screenshot shows the 'New user registration page' with the following fields and values:

- User ID: PAR89140_ (with a note: *Enter under 10 characters)
- Password: [Redacted]
- Password(confirmation): [Redacted]
- Organization Name: e.g. GlobalSign Inc
- Department: e.g. Marketing
- First Name: [Redacted]
- Middle Name: [Redacted]
- Last Name: [Redacted]
- Job Title: e.g. Web Administrator
- Street Address 1: e.g. Tech International Court

The screenshot shows the continuation of the registration form with the following fields and values:

- Street Address 2: e.g. Suite 330
- City: e.g. Portsmouth
- State or County: e.g. New Hampshire
- Zip Code / Postal Code: e.g. 03801
- Country: Germany (dropdown menu)
- Other address info: [Redacted]
- Telephone (inc. region code): e.g. +44 (0) 1622 766766
- Fax (inc. region code): e.g. +44 (0) 1622 662255
- Email Address: [Redacted] (with a note: *Please be careful when providing email address)
- User permissions: Manager (dropdown menu, highlighted with a red box)
- Language: [Redacted] (dropdown menu)
- Hoping for guide from this company:
- Certificate approval permission: true false (highlighted with a red box)
- Deposit purchase authority: true false

Buttons: Back, Confirm

ADMINISTRATION DELEGATION

Shared administration can be established. Under the Enterprise PKI tab, click on the **Profile Configuration** link under **My Profiles**. Select the profile and click **Next**. Click on the **Configure** button next to **User Permission**.

Profile Configuration

Profile ID	MP200906100029
Organization	GlobalSign Inc.
Organization Unit	Test Account - Do not rely upon - authenticated by LRA
URL	https://system.globalsign.com/cr/public/certificate/order.do?p=96b2ccc3f799c9f038099eeb071e1c76aa3cc3f
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?picbf9e2b28c9021cb29804af0824058500724b29f
User Permission	Configure
Hash Algorithm	<input checked="" type="radio"/> SHA-1 <input type="radio"/> SHA-256
Encrypting File System	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
MS SmartCard Logon	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Renewal Type	<input type="radio"/> Manual <input checked="" type="radio"/> Auto <input type="radio"/> Quick
Non Exportable Option <small>Limited to only Internet Explorer.</small>	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
API IP Address range <small>IP Address is limited to only at the time of API e.g. 1.1.1.1 - 1.1.1.1</small>	211.11.149.249,211.11.149.250

You can now select the permissions you wish to give to each user (provided you have previously added them as a **Staff in charge** or **Manager** by clicking the **Manage Users** link under the **Accounts & Finance** tab.)

User Permission

User Permission

User ID	User Name	User Permission		
		Place Order	Approve Order	Revoke Certificate
PAR12694_adminadmin	lbackup Kne	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PAR12694_eric	Eric Sprague	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PAR12694_evanecki	Evan wajda	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PAR12694_matt	Matthew Greene	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PAR12694_sean33	Sean Rogers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PAR12694_sic	staff in charge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PAR12694_staffnoa	Staff No approval	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

To extend a user's permissions and administrative rights, tick off the appropriate permission boxes next to the username/ User ID. Extended permissions allow users in Manager (or Staff in Charge) roles, to place orders, approve orders and revoke certificates for a given Account. Confirm your selection by clicking **Next**.

GETTING HELP

Although EPKI Administrators are responsible for providing first tier support to end users within their organization, every GlobalSign Enterprise EPKI customer has a dedicated Account Manager who is on hand to help with any commercial or technical queries you may have about the EPKI service. GlobalSign also provides best in class technical support through our Client Service departments around the world. www.globalsign.com/support/

GlobalSign encourages EPKI Administrators to browse the [GlobalSign Support pages](#) for Product specific guidance ranging from end user guides to FAQs. If you can't find the answer to your questions, please open a Support ticket at www.globalsign.com/help/.

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 9 75 1832 00 www.globalsign.fr ventes@globalsign.com	GlobalSign DE Tel: +49 30 8878 9310 www.globalsign.de verkauf@globalsign.com	GlobalSign NL Tel: +31 85 888 2424 www.globalsign.nl verkoop@globalsign.com