GlobalSign Enterprise Solutions

Enterprise PKI

Administrator Guide

Version 2.9

GlobalSign

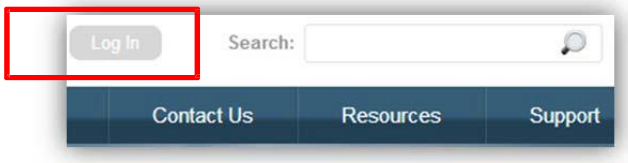
TABLE OF CONTENTS

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

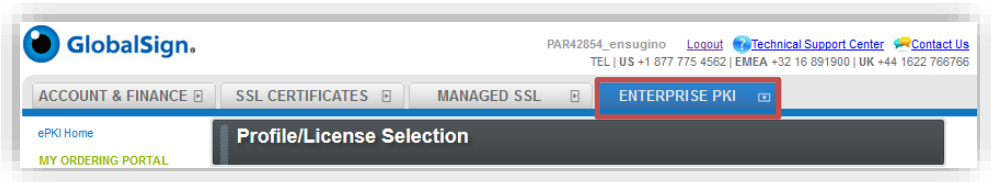


Enter your assigned **User ID** and **Password**. Your UserID is a combination of the CorporateID that GlobalSign assigns you and the username you specified during account signup (e.g. **PAR12345_UserID**). Your assigned UserID is provided at the end of the signup process and in the GCC Welcome Email.

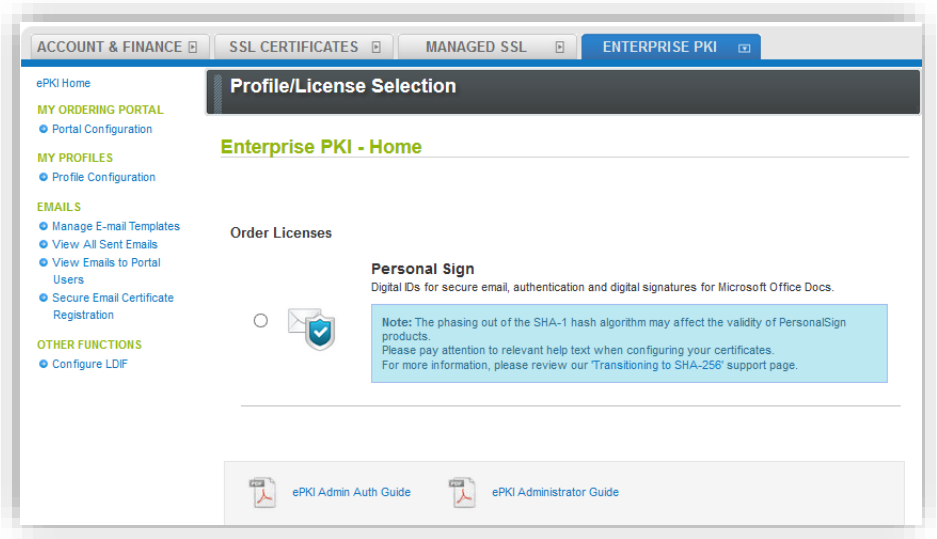
If you forget your password, you can click "Forgot your Password? Click here" on the login screen. If you have further difficulties logging in, please contact Support at: www.globalsign.com/support

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.



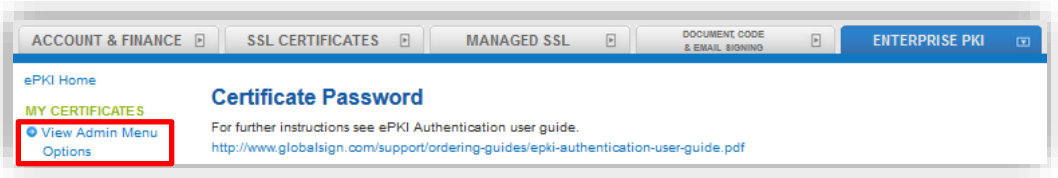
CLIENT AUTHENTICATION CERTIFICATE

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.

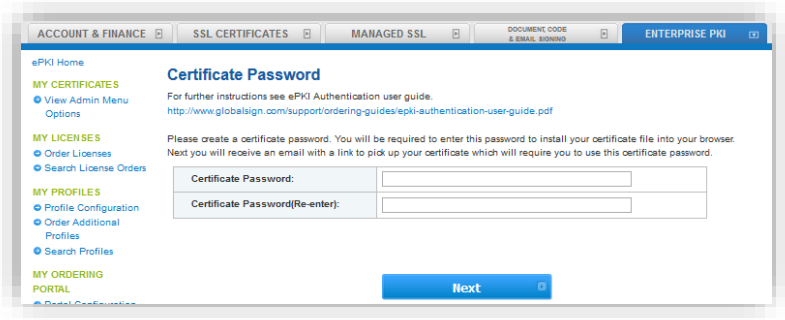
Note: If your account is not configured for Client Authentication, then you can skip to the next section.

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.

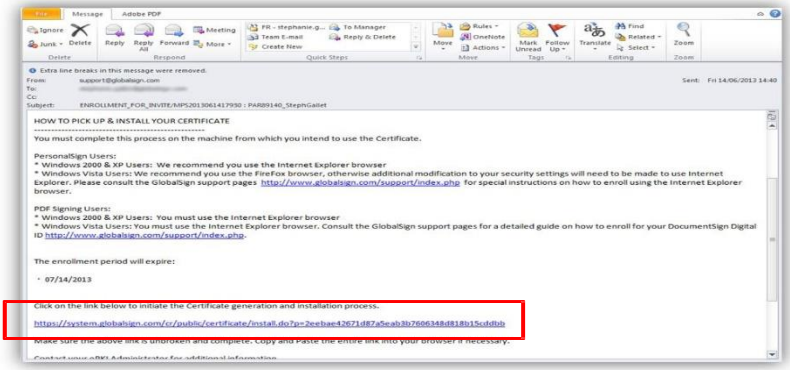


Follow the prompts to setup the Client Authentication Certificate, otherwise referred to as the Admin Certificate. You will have to create a **pick-up password** for your Admin Certificate. **It is important to remember this password**! You will need it to install the certificate into your computer(s)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



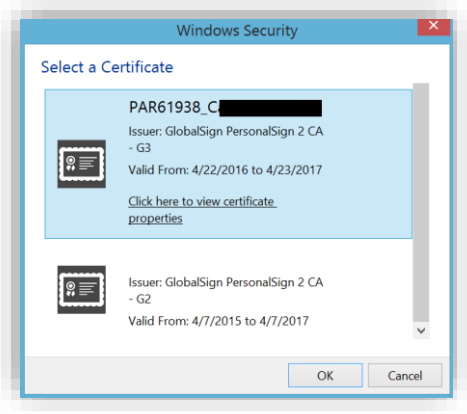
You will reach a confirmation page stating that your certificate registration is complete.

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.

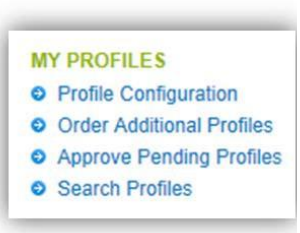
ESTABLISHING A PRE-VETTED CERTIFICATE PROFILE

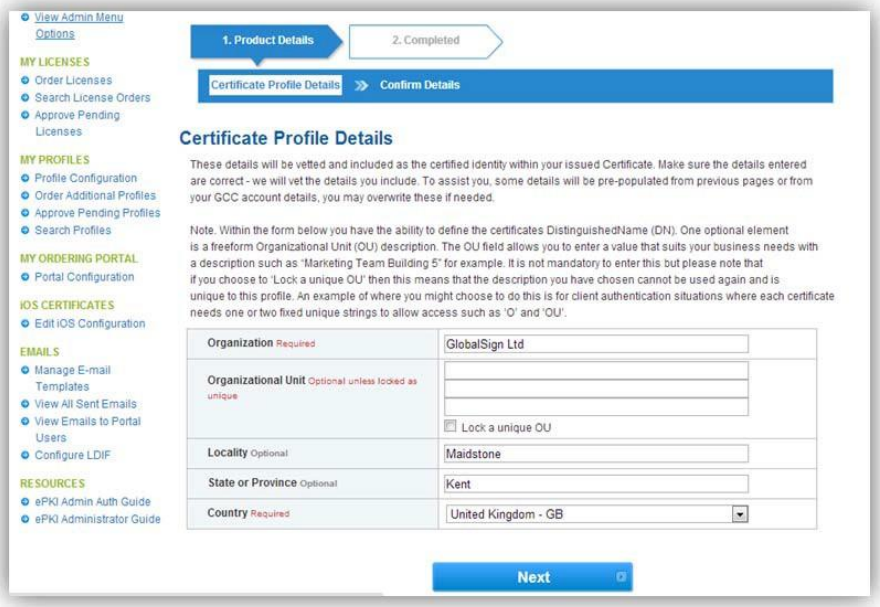
Certificate Profiles will be the content of the Digital Certificate as seen by anyone viewing and relying on the certificate, so it is important to ensure the Profile is accurate and representative of the certificate holder. You can create multiple profiles in a single EPKI account, should you have multiple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





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.

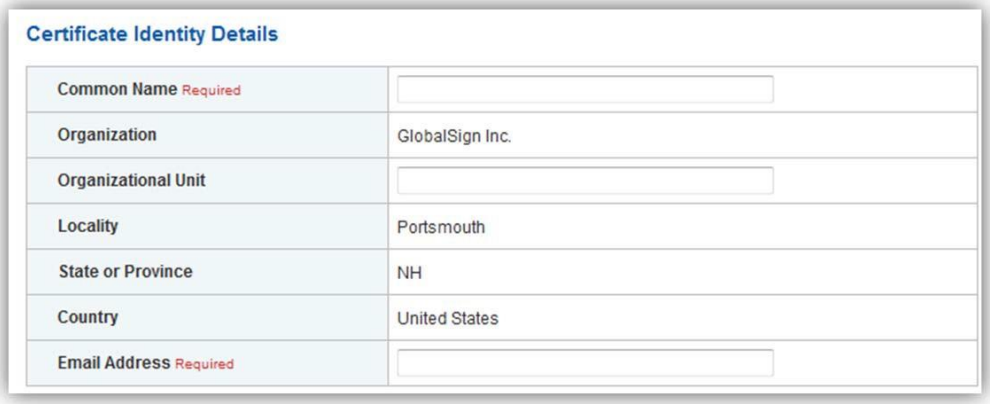
A pre-vetted identity has 1 of 3 main profile options:

- **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**:

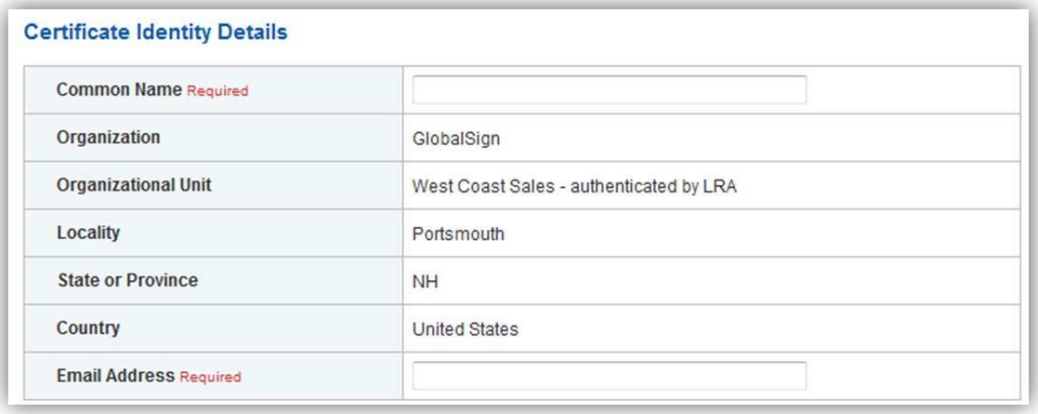


OPTION 2: FIXED ORGANIZATION NAME WITH A FIXED ORGANIZATION UNIT

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**

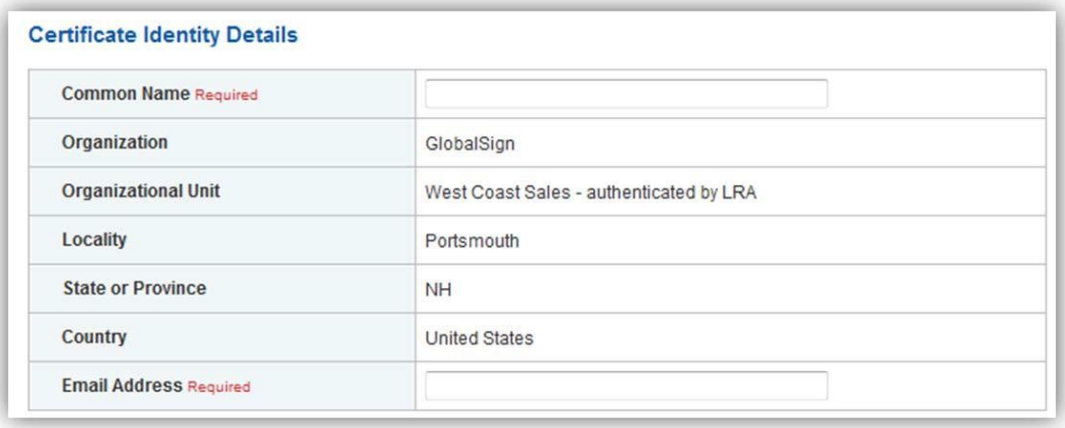


OPTION 3: FIXED ORGANIZATION NAME WITH A FIXED "RESERVED*" ORGANIZATION UNIT IN THE BASE DISTINGUISHED NAME (DN)

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**:



*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.

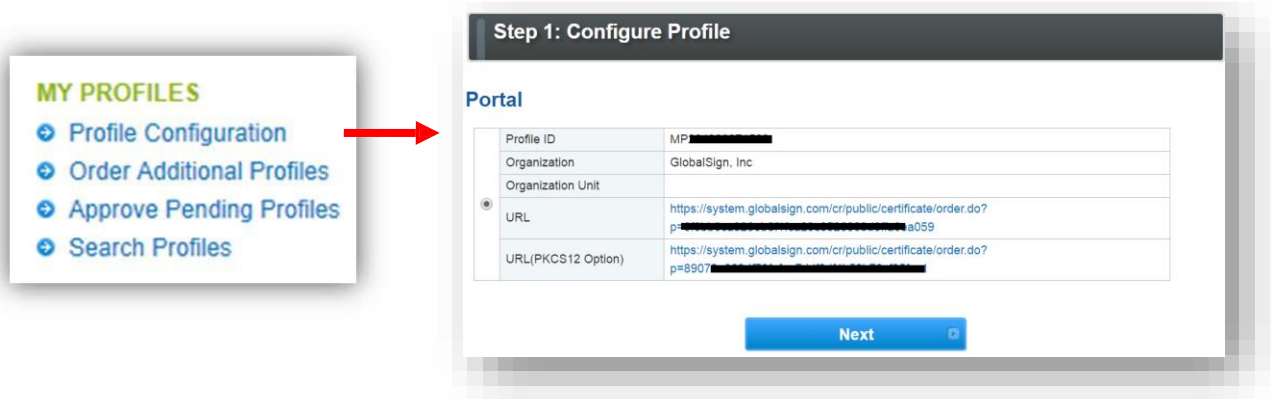
Once you have configured your profile(s) with the distinguished values, click the **Confirm** button and the vetting department will be notified of your request and begin the vetting process.

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.

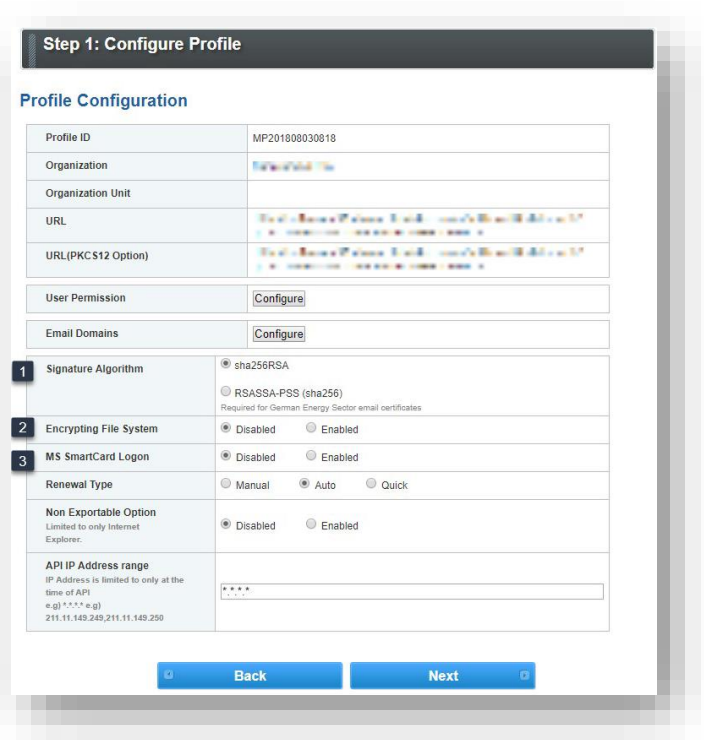
Should you have any questions regarding the status of your Profile request, please open a Support ticket at https://www.globalsign.com/help/ .

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.

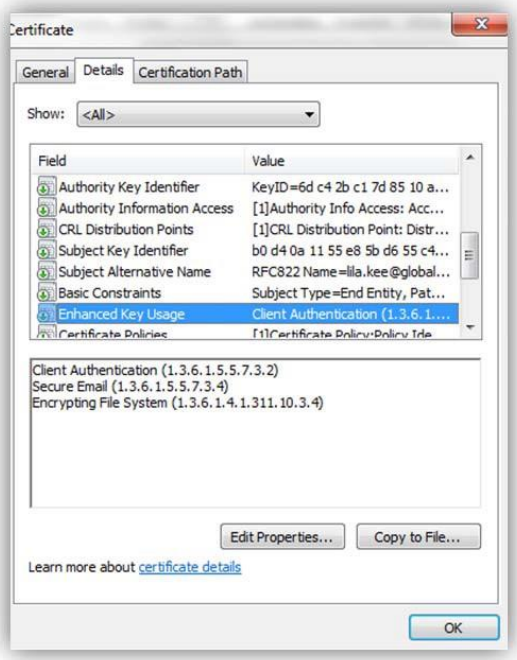


Select the Profile and click **Next** to configure the additional options shown below:



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.

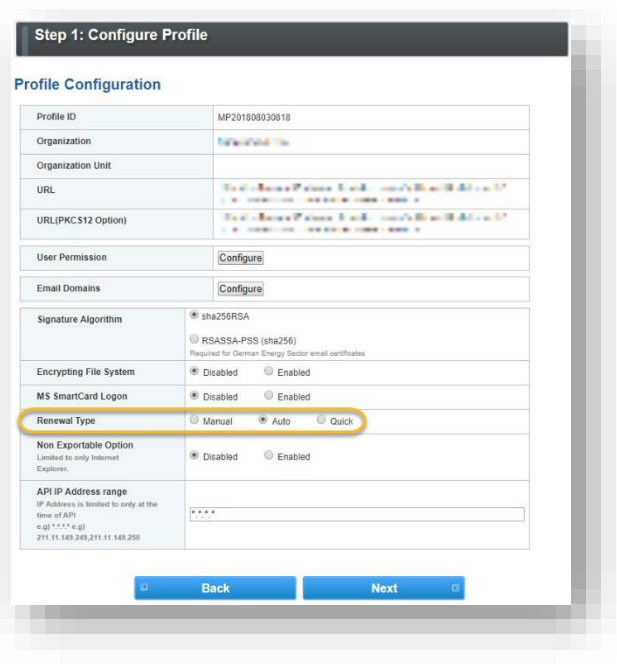
RENEWAL

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:



PURCHASING CERTIFICATE LICENSE PACKS

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

CERTIFICATE TYPE

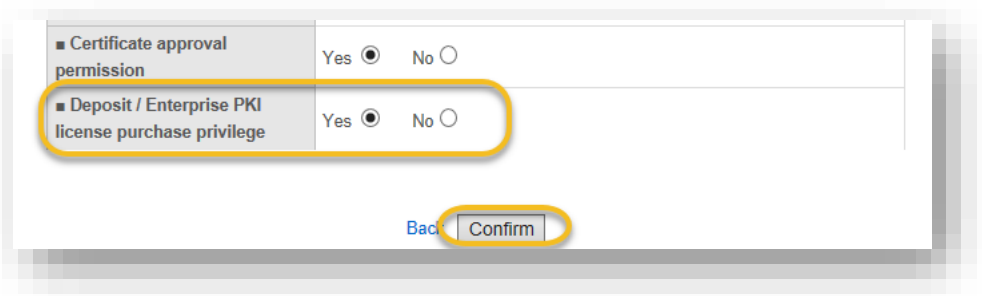
- PersonalSign & DepartmentSign for Windows trusted applications. For a detailed product description go to https://www.globalsign.com/personalsign/
- PDF, Microsoft Office, and Email Signing For AATL for a detailed product description go to: https://www.globalsign.com/en/digital-signatures/

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.

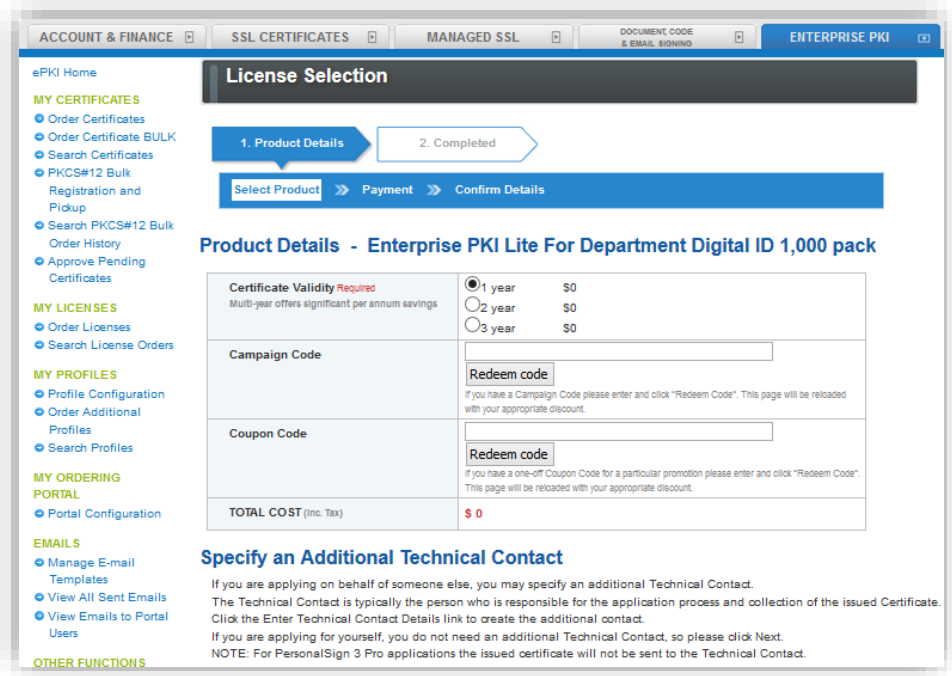
PURCHASING PERMISSIONS

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.



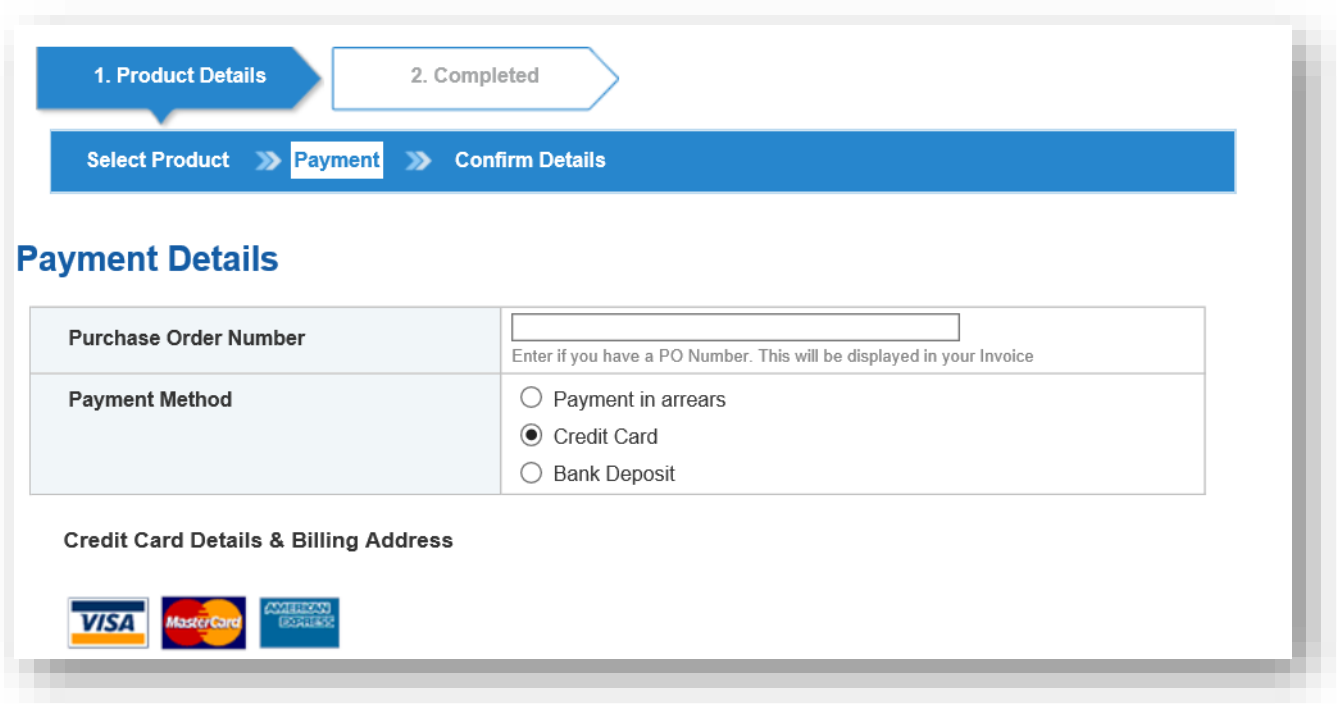
CERTIFICATE VALIDITY

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**.



Select one of the following Payment methods:

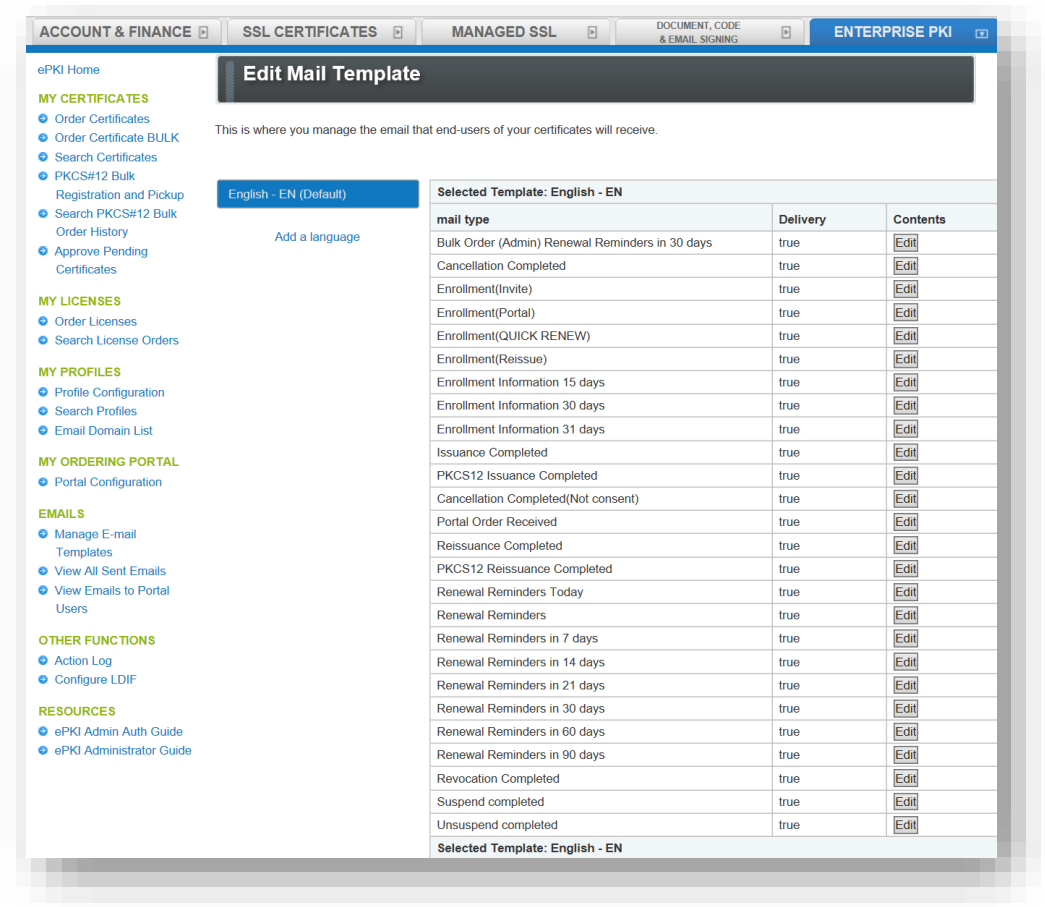
- **Payment in arrears** – Select this option if you are paying by **Purchase Order** (which must be pre-arranged with your GlobalSign Account Manager) and supply the Purchase Order Number.
- **Bank Deposit** – Select this option to use existing **Account funds** that have been deposited into your account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



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.

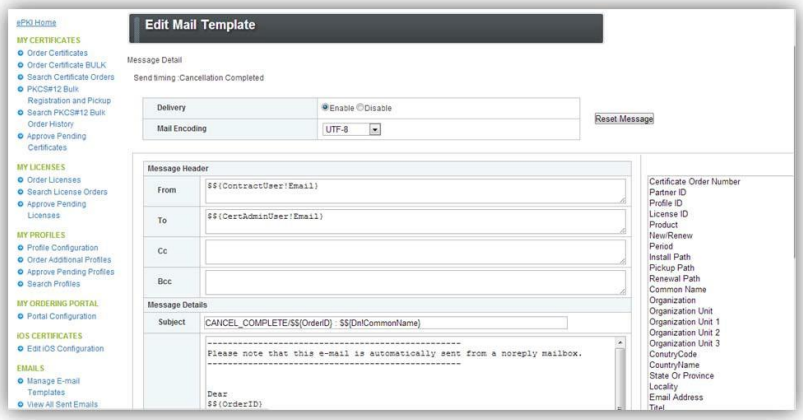
CUSTOMIZING EMAIL TEMPLATES

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.



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.



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.

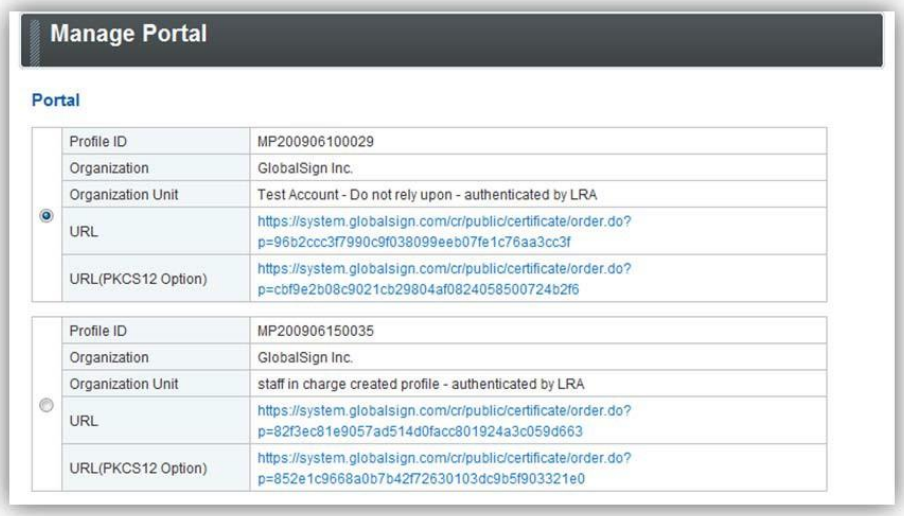
With the End User Initiated/Portal Enrollment process, end users set their own pickup password for the enrollment process; whereas with the EPKI Administrator registration process, the Administrator generates or creates the certificate pickup password which must be securely provided to the end user.

USING THE PORTAL LINK

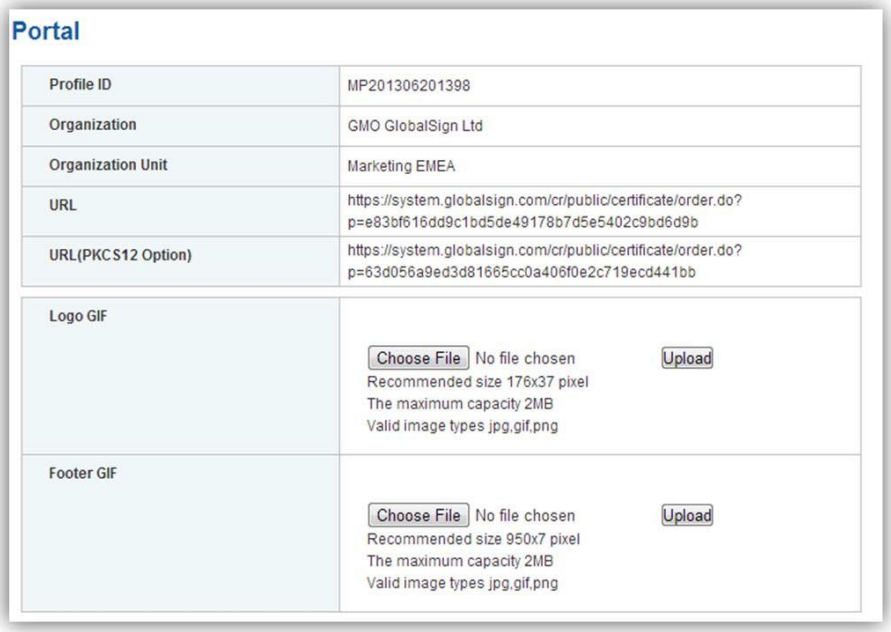
The EPKI Managed Service offers the ability for organizations with dispersed offices or departments to centralize the Certificate ordering process. Administrators have the option of publishing a certificate enrollment page (Portal Link). Anybody within your organization will then be able to complete 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.



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.

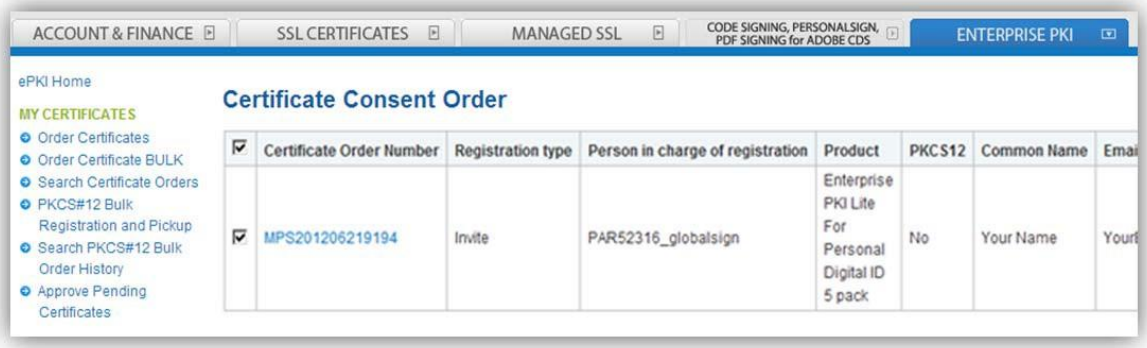


Other Portal Configurable Options:

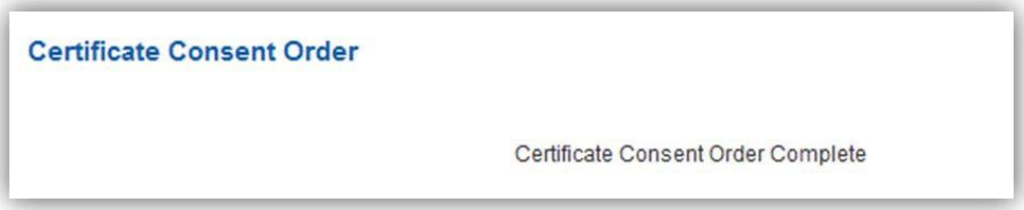
Modify Subscriber Agreement: You may add additional subscriber terms to the Mandatory GlobalSign Subscriber Agreement to capture unique or additional terms above and beyond the required GlobalSign terms. End users will be presented with the Subscriber Agreement and prompted to accept the terms prior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

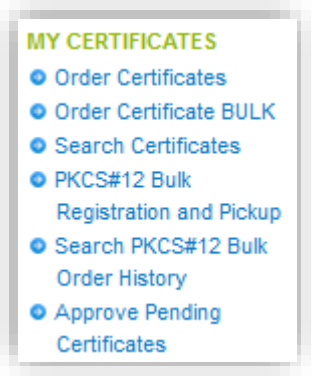


REGISTER USERS FOR CERTIFICATES VIA EPKI ADMINISTRATOR

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

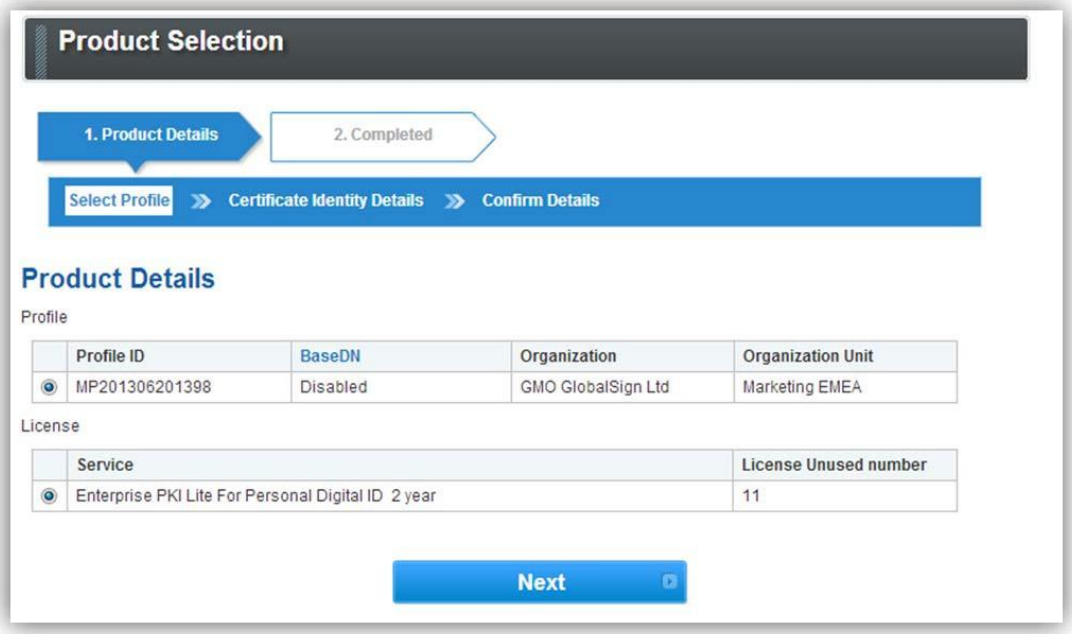
1. Individual – New Certificate (**Order Certificates**)
2. Multiple – New Certificate BULK Issuance (**Order Certificate BULK**)
3. Multiple – New Certificate BULK Registration and Pickup (**PKCS#12 Bulk Registration and Pickup**)

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

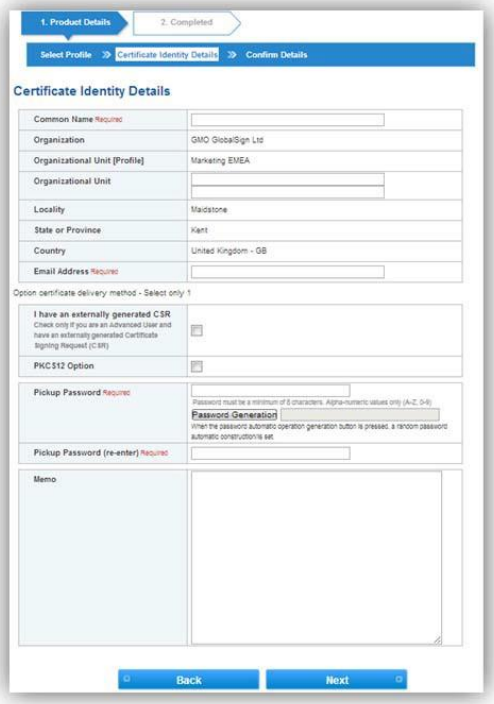


INDIVIDUAL CERTIFICATE REGISTRATION

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.



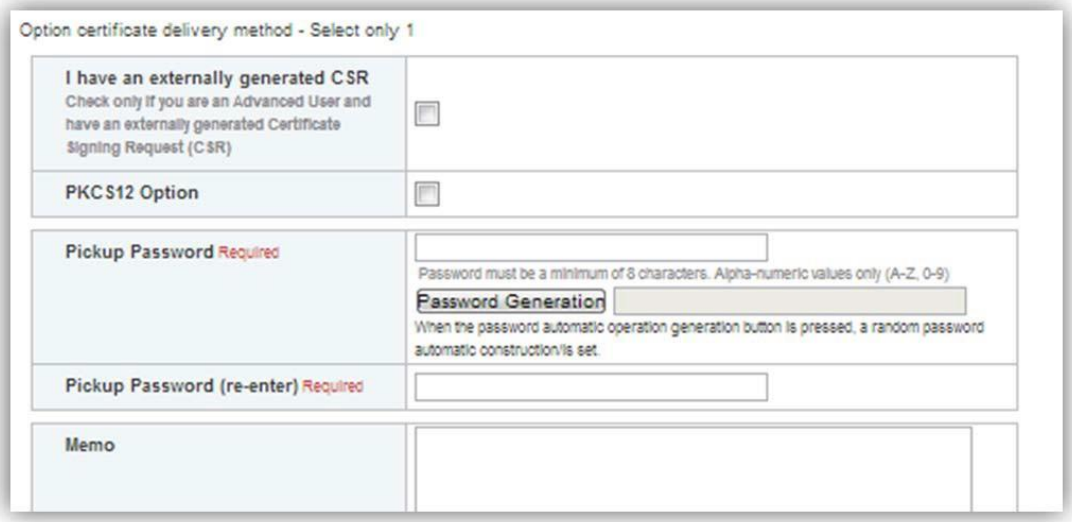
Click **Next** and complete the certificate identity details for the end user/ subscriber. Note: Certain pre-vetted fields will be hardcoded.



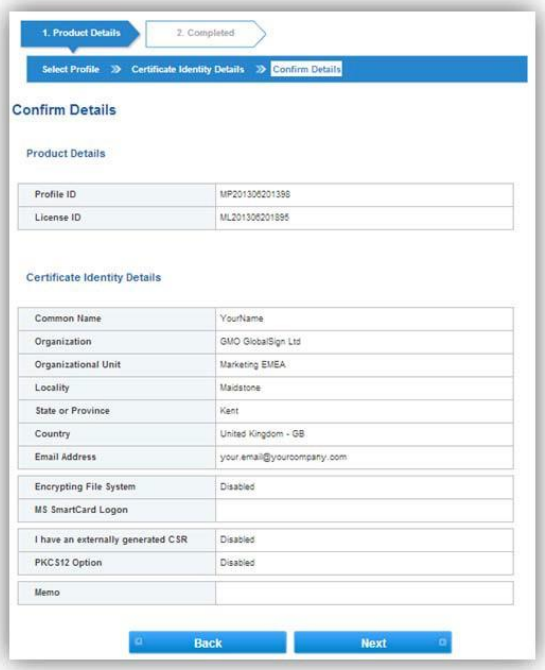
Optionally, the EPKI Administrator may select an alternative certificate delivery method, other than the default PKCS7 method, where key generation is performed locally via the Subscriber's browser:

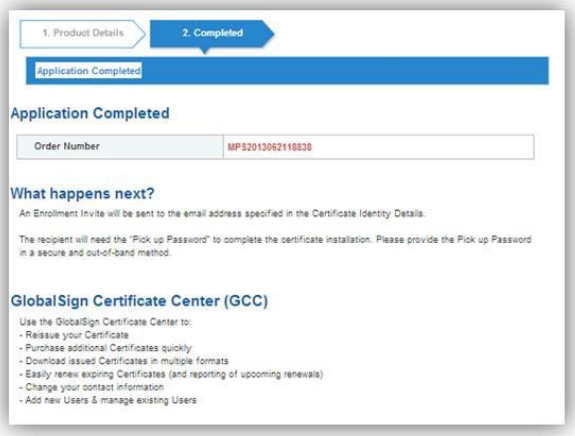
1. Certificate Signing Request (CSR) – in this case, the Subscriber is expected to provide a CSR created either from a different system (e.g. Hardware security Module) or outside the browser session used to enroll for the digital certificate. This is typically for advanced users.
2. P12 – PKCS12 – in 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).



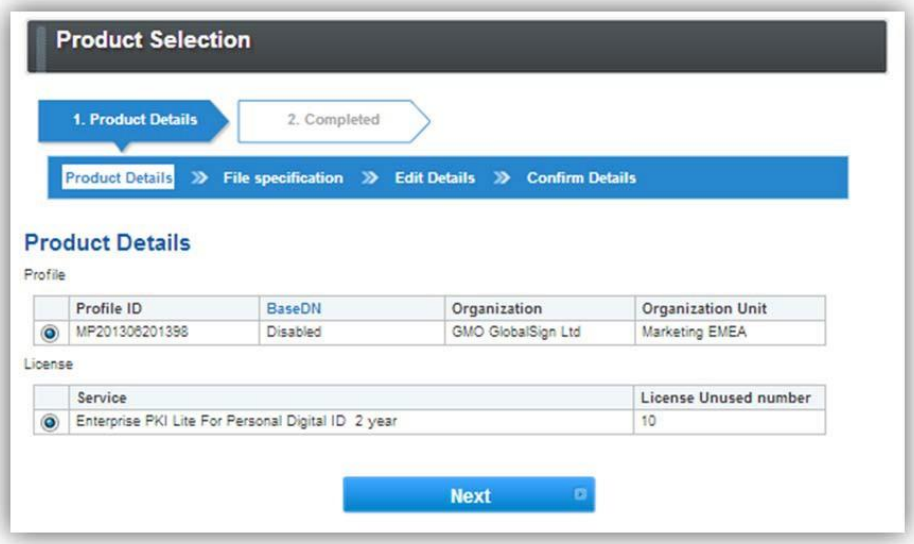
Additionally, the EPKI Administrator will need to establish a "Pickup Password", or use the "Password Generation" tool, that you are required to deliver to the Subscriber in an "Out of Band" secure method. As a security precaution, the certificate cannot be installed unless the user has received the 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.**



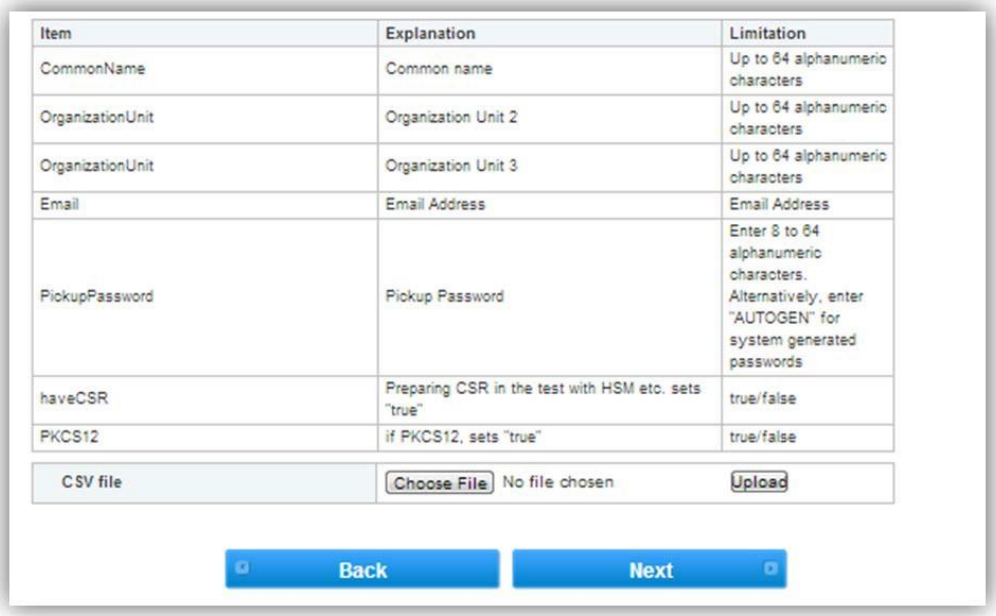


BULK ENROLLMENT

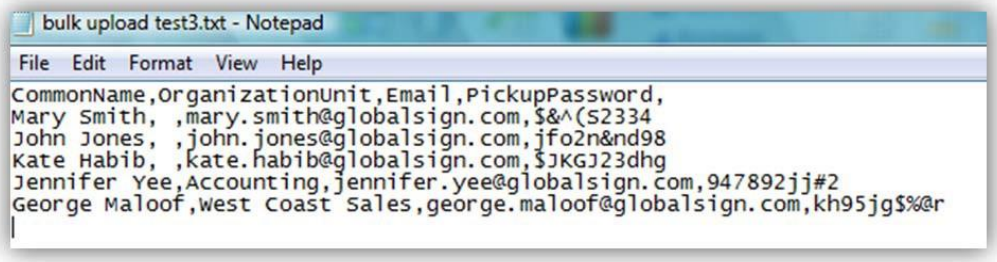
For multiple user registrations, click **Order Certificate BULK** under the **My Certificates** menu then select the appropriate Certificate Profile and License pack you wish to apply the certificate requests to. Click **Next** to continue.



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”.

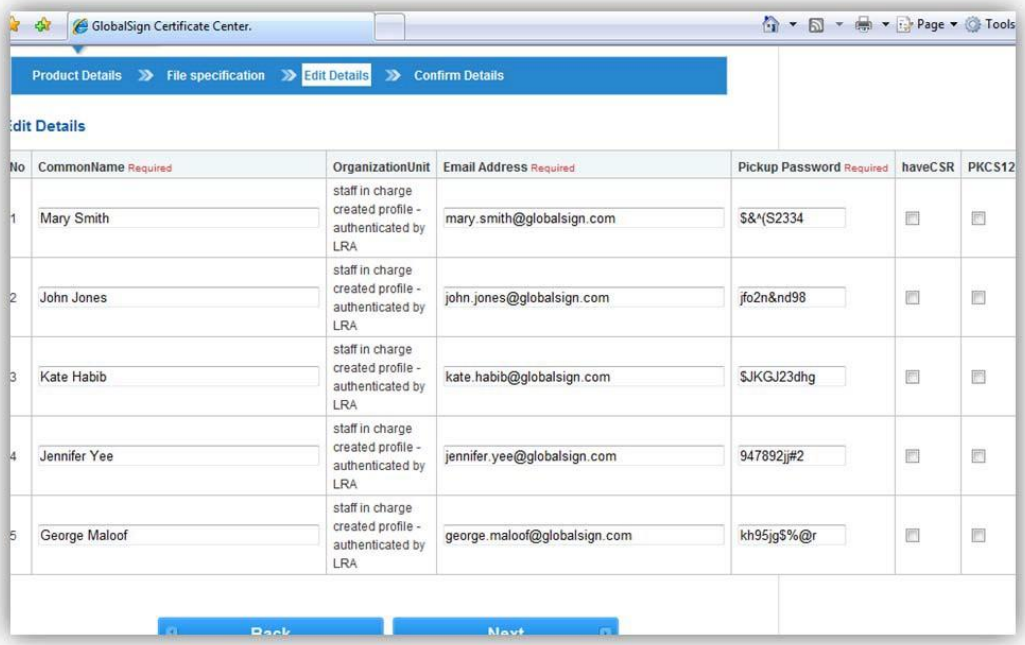


Below is an example of a CSV created for a Profile that allows for an Optional Variable Organization Unit. Note, for the records, where OU is desired "blank", a space was created in the second value of the record.



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.



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

BULK PROVISIONING (PKCS#12)

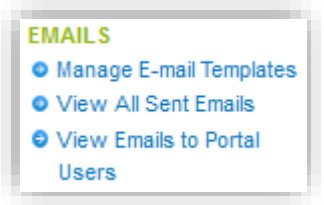
Bulk provisioning provides an alternative to bulk enrollment in that the enrollment steps performed by the end user are minimized or in some cases totally eliminated. The bulk provisioning feature provides the following benefits:

- 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".

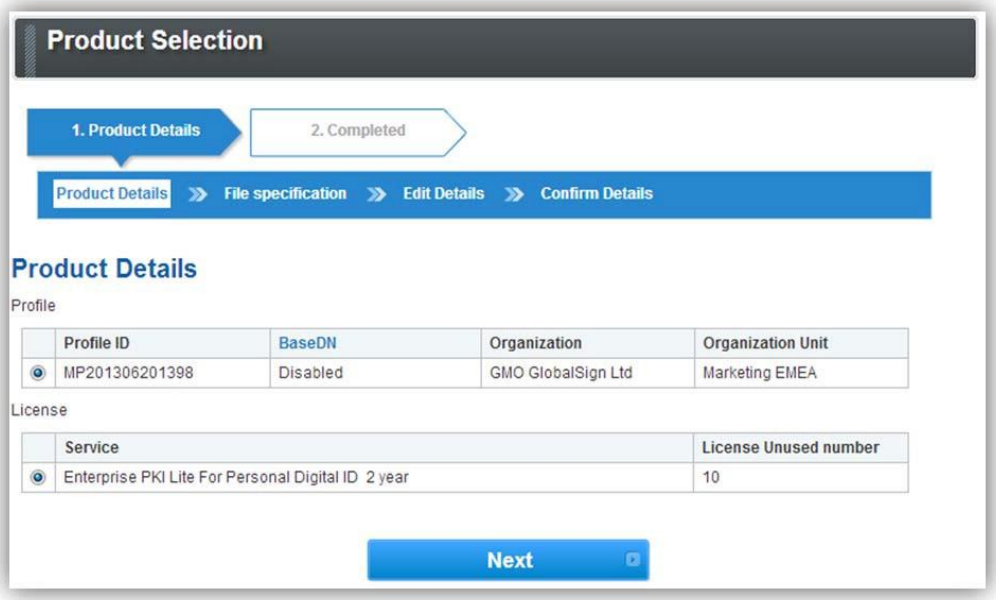
Renewal Reminders Today	true	Edit
Renewal Reminders	true	Edit
Renewal Reminders in 7 days	true	Edit
Renewal Reminders in 14 days	true	Edit
Renewal Reminders in 21 days	true	Edit
Renewal Reminders in 30 days	true	Edit
Renewal Reminders in 60 days	true	Edit
Renewal Reminders in 90 days	true	Edit

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

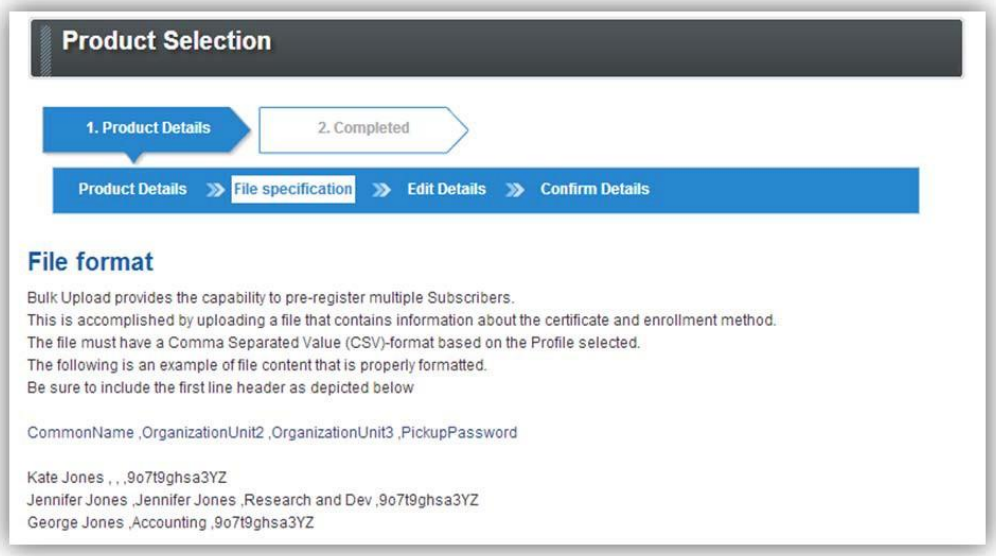
d. Click “Next” and then “Complete”.

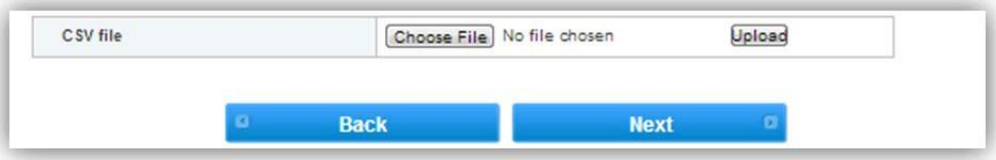
USING THE BULK PROVISIONING (PKCS#12) METHOD

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

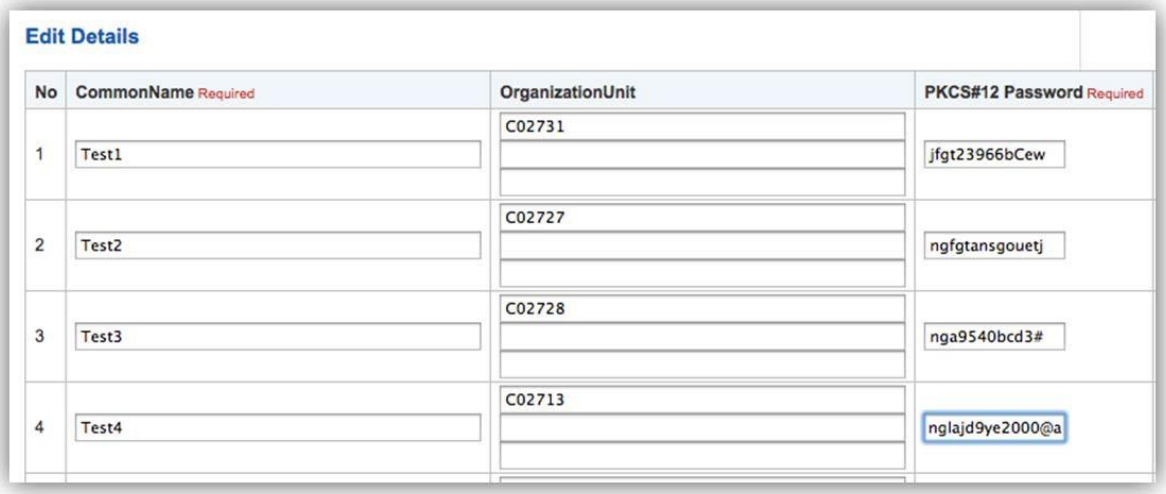


3. Browse and Upload a CSV file, formatted based on your certificate profile selection. Note, the CSV file format guidance will be based on the Profile settings associated with the selected profile. To include the email field, you must pre-register email domain(s) prior to ordering (refer to the Email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

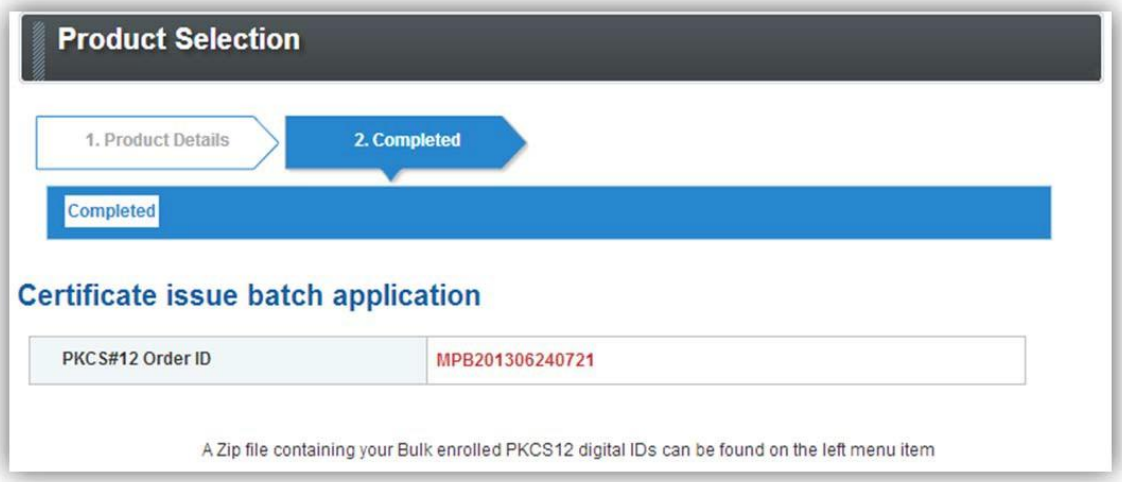




4. Review the certificate details pulled from the CSV file and make changes as necessary. Click "Next" to continue.



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).

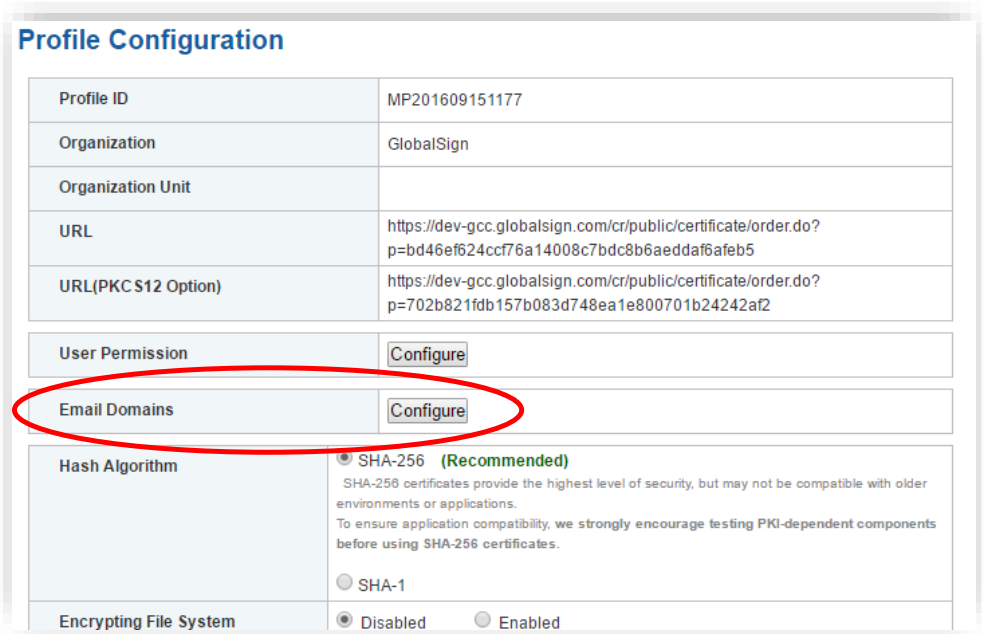
EMAIL DOMAIN REGISTRATION

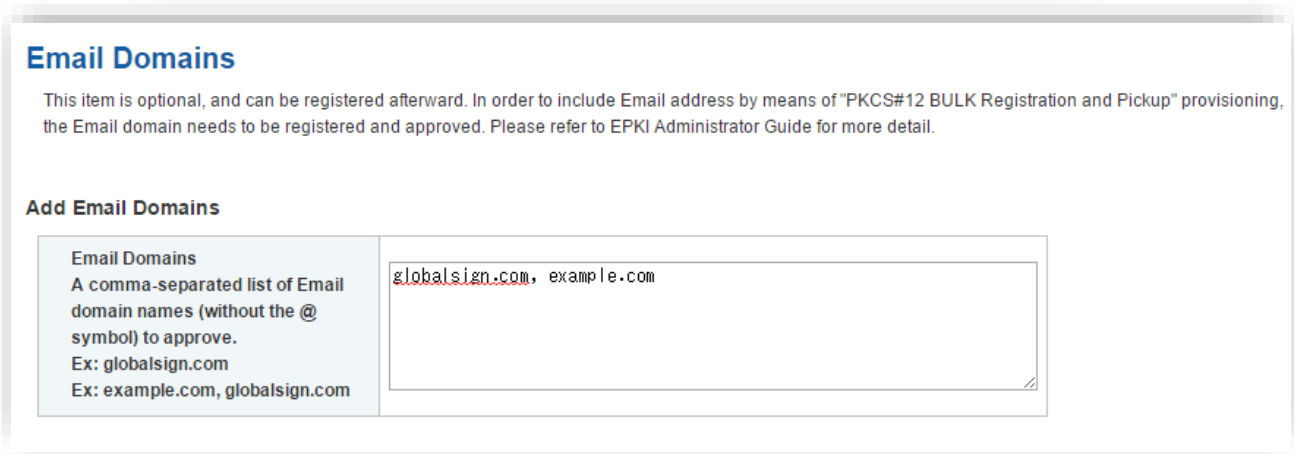
The Email Domain Registration feature allows organizations to register the domain(s), which they own or are approved to use, and link the registered domains to an EPKI Profile. By registering email domain names to a Profile, you can then order certificates containing corresponding email addresses when 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)

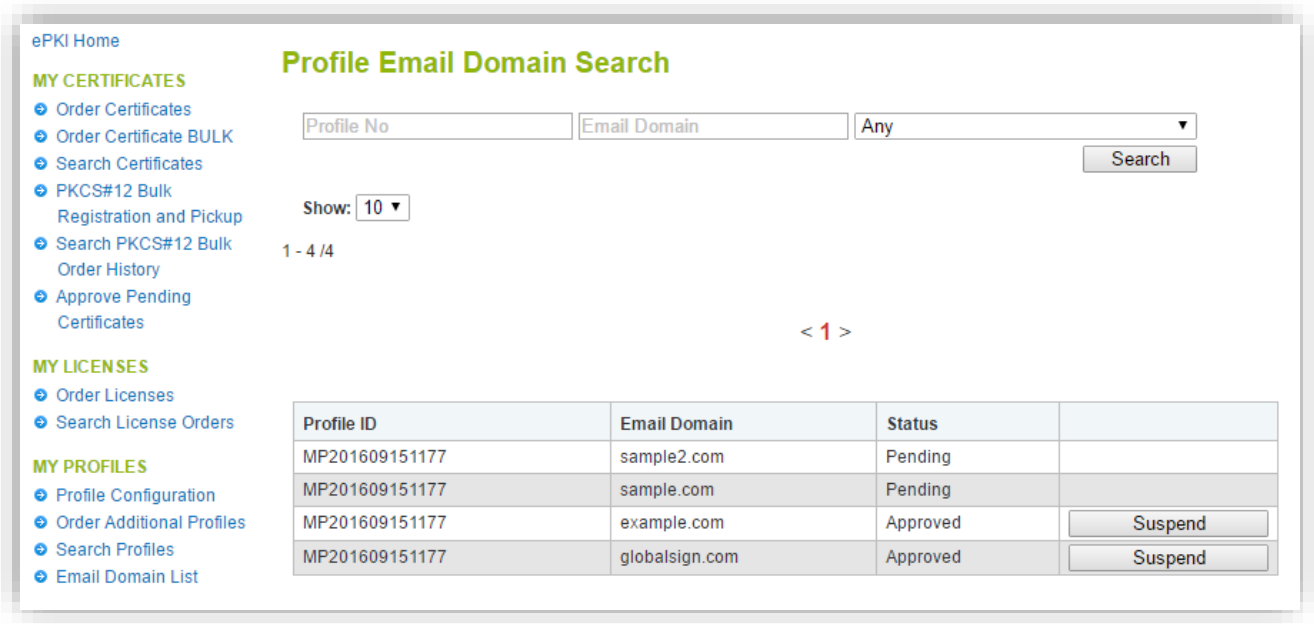
HOW TO REGISTER EMAIL DOMAINS

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





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.



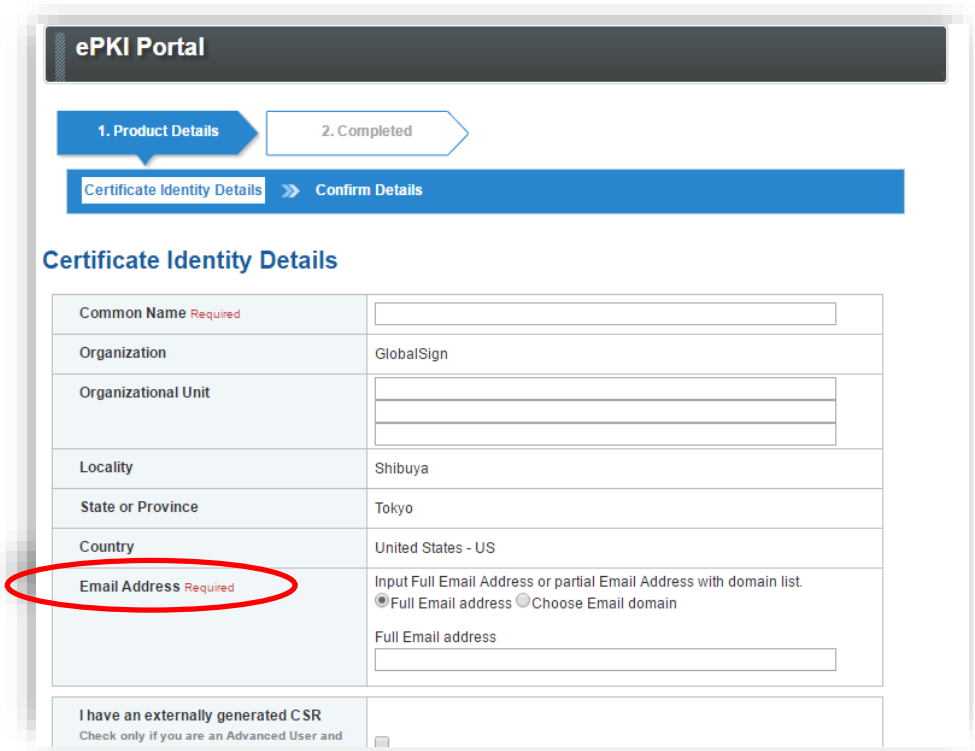
HOW TO SUSPEND/UNSUSPEND EMAIL DOMAINS

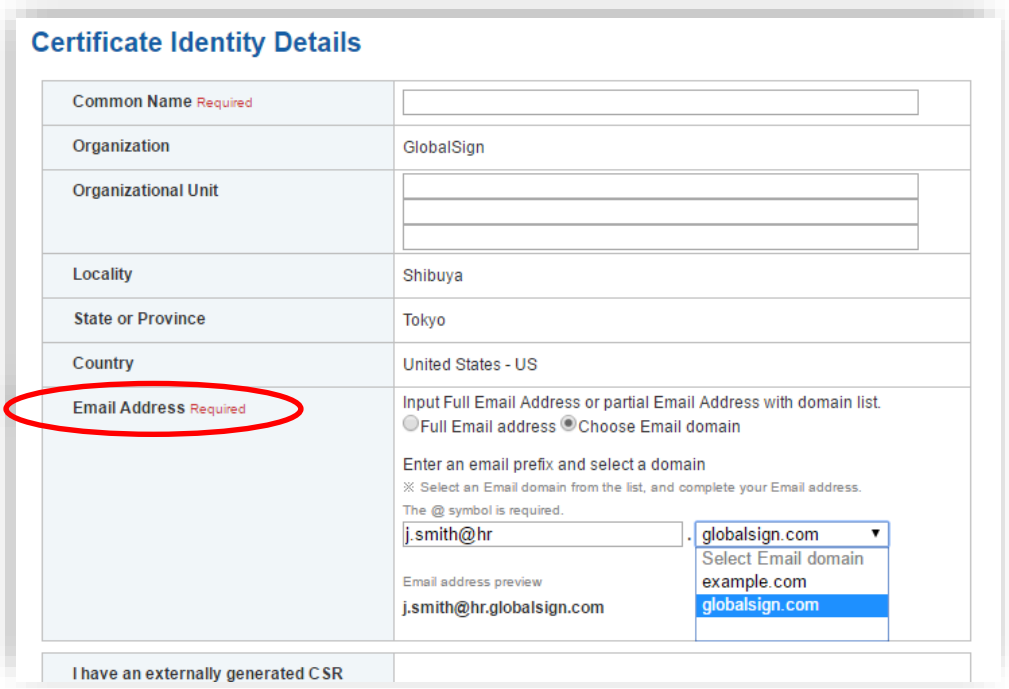
1. Registered Email Domains can be suspended temporarily, by clicking **Suspend** in the Email Domain List menu.
2. Suspended domains cannot be included in the certificate orders. Also, Portal users cannot select suspended domains.
3. Suspended Email Domains can be unsuspended, by clicking **Unsuspend**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

EMAIL DOMAIN OPTIONS FOR EPKI PORTAL USERS

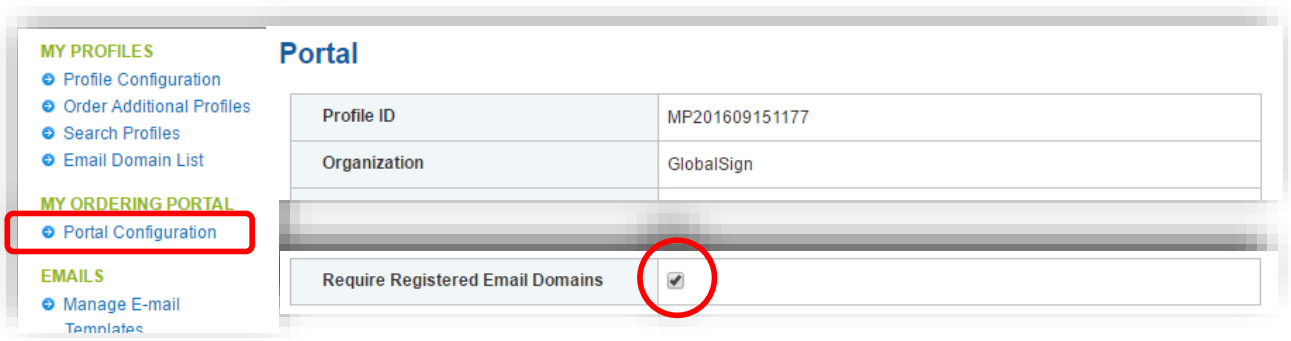
The EPKI Portal has two option for portal users to input their email address/domain:

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.

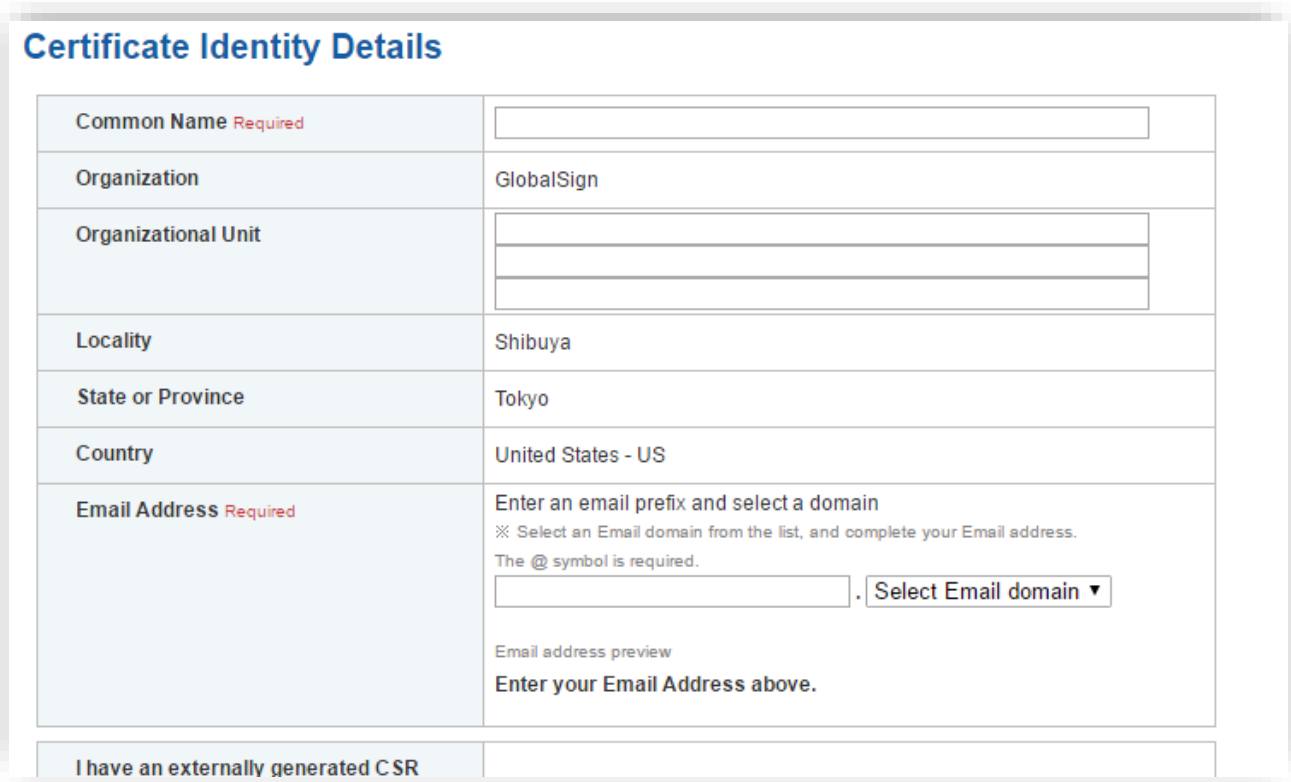




3. The EPKI Admin can restrict portal users and only allow the “choose email domain” option by checking the box: “**Require Registered Email Domains**” under **Portal Configurations**.

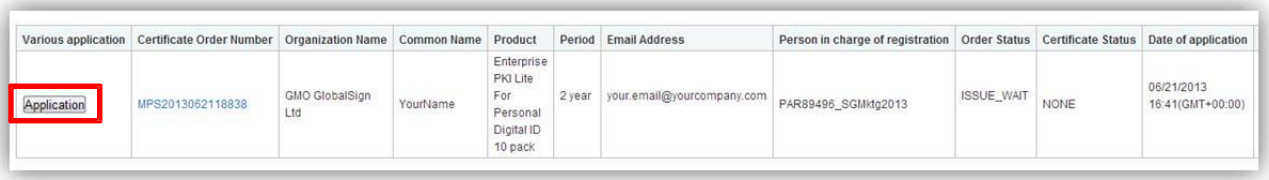


4. This option will hide the full email address entry field for portal users.

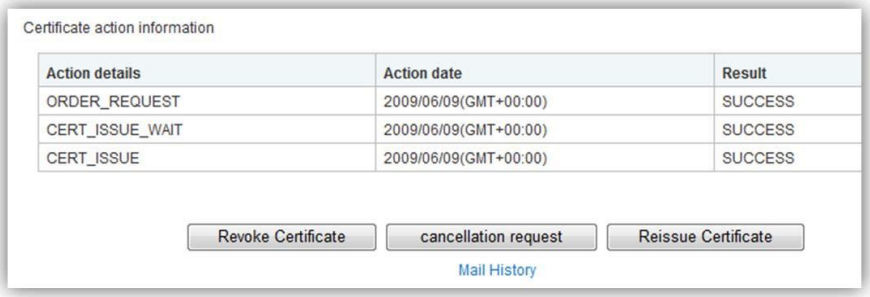


CERTIFICATE LIFECYCLE MANAGEMENT – REVOCATION, REISSUANCE, AND CANCELLATION

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_SGMktg2013	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

Revoke Certificate | cancellation request | Reissue Certificate

Mail History

Notes:

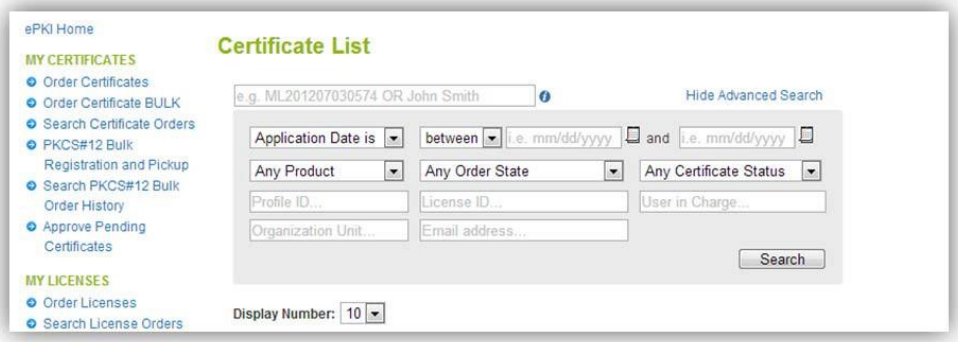
1. Revoked certificates will be put on the Certificate Revocation List within 24 hours, making the certificate unusable by most applications.
2. The cancellation request option will be available for 7 days after initial issuance of the certificate. Choose this to completely cancel your order and have 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

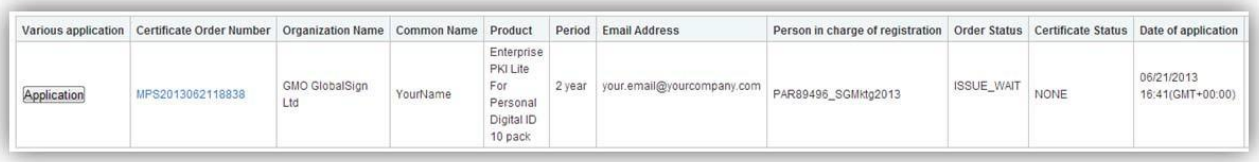
Click **Mail History** to review or resend system generated emails.

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.



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_SGMktg2013	ISSUE_WAIT	NONE	06/21/2013 16:41(GMT+00:00)

LDIF

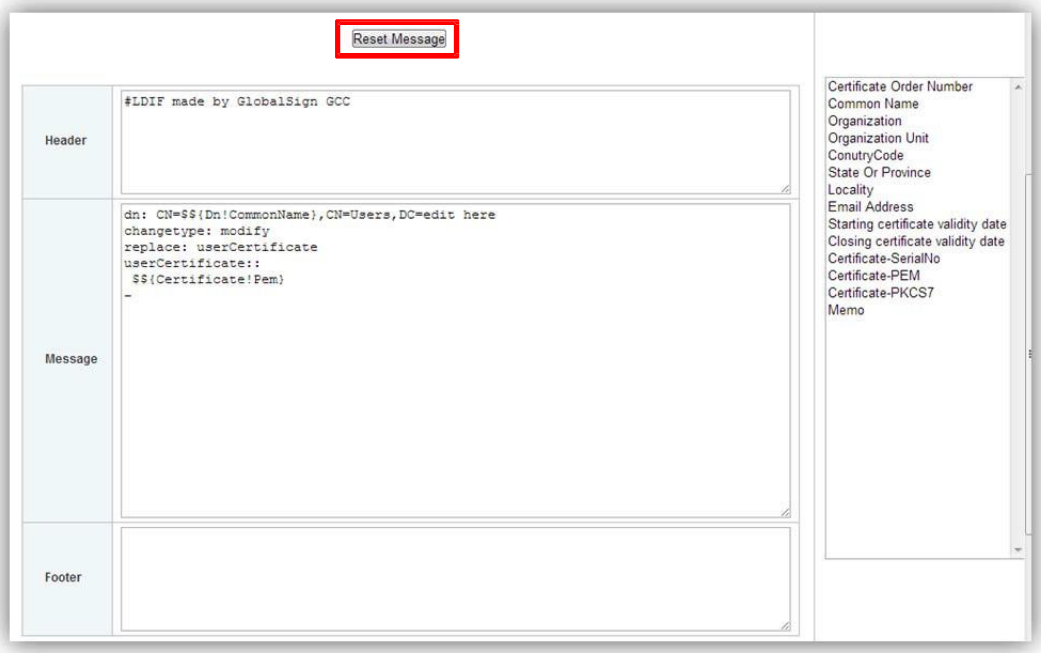
EPKI Administrators may wish to upload the public certificates associated with their EPKI account to a directory. EPKI provides a method to generate a LDIF (Lightweight Directory Access Protocol) report for upload to a LDAP directory.

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**.

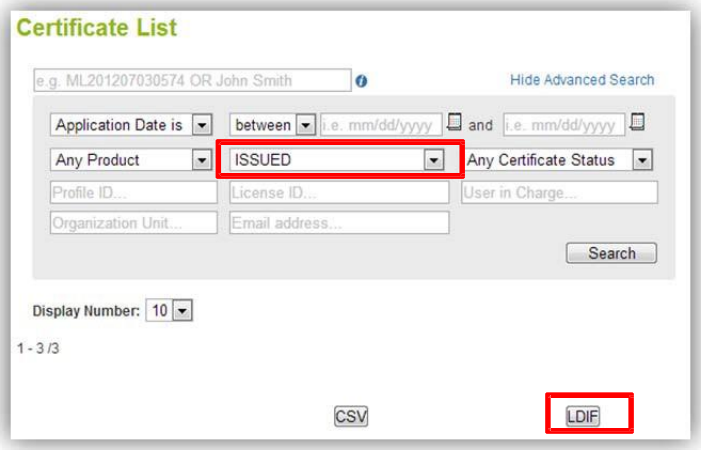
Please note the initial LDIF default format has been established by GlobalSign. The EPKI Administrator must modify the LDIF Template based on the “Profile” the LDIF query will run against. You can reset the format back to the default values anytime by clicking **Reset Message** as illustrated below.



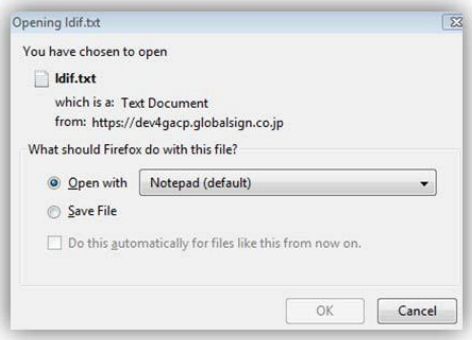
GENERATING A LDIF REPORT

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

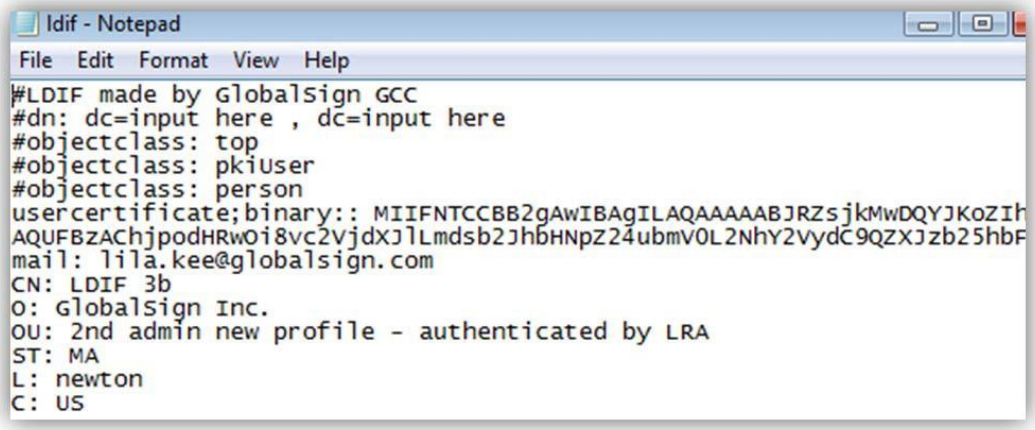
Click **Show Advanced Search** and select the appropriate date range, the Profile and set the Order State to **ISSUED** via the drop down menu. Note: If a certificate has been "re-issued", the replacement certificate will have a status = Issued and be included in the LDIF report. The original, "replaced" 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.



Open the file with your preferred application.



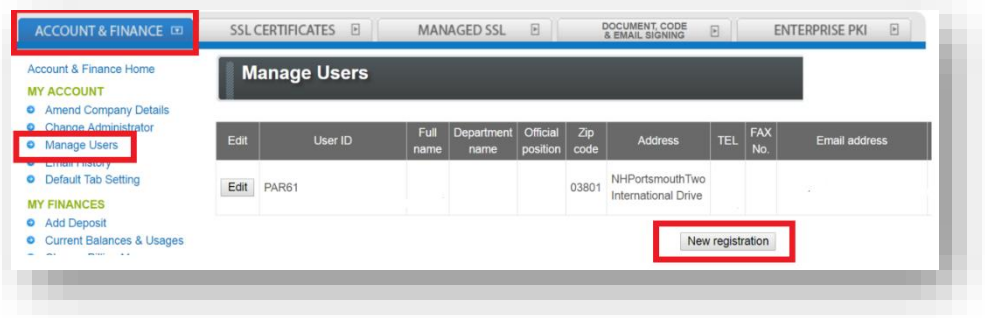
Below, is an example of an LDIF Report opened in Notepad.



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.

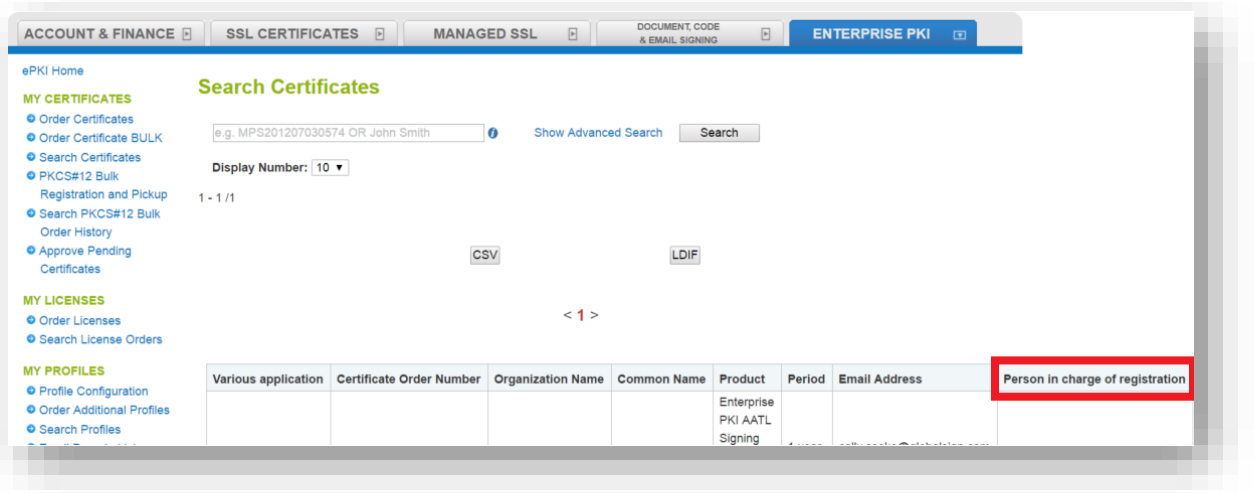
MANAGER

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.

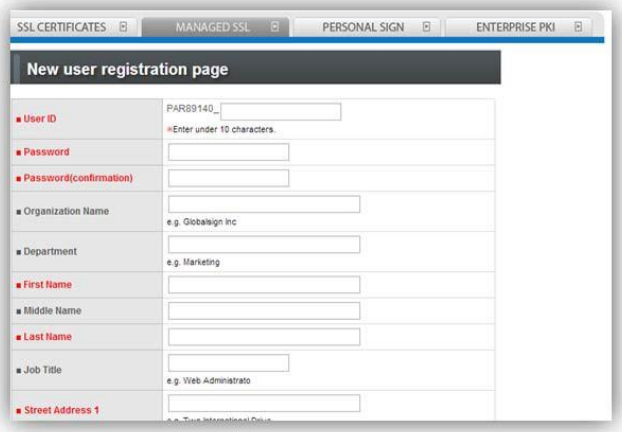
Note, under the "**Search Certificates**" section, you can view the Administrator associated the issued Certificate, under the "Person in charge of registration" heading.

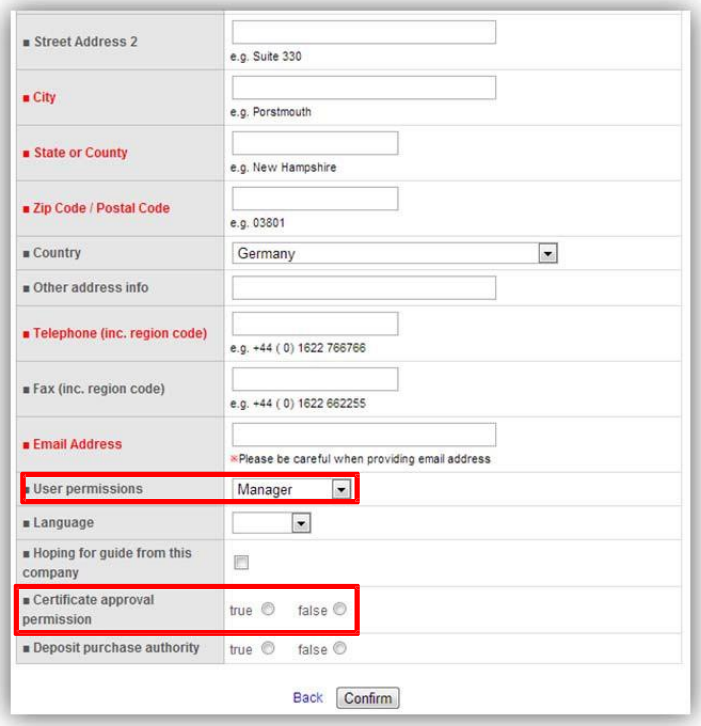


REGISTERING ADDITIONAL GCC ACCOUNT USERS

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

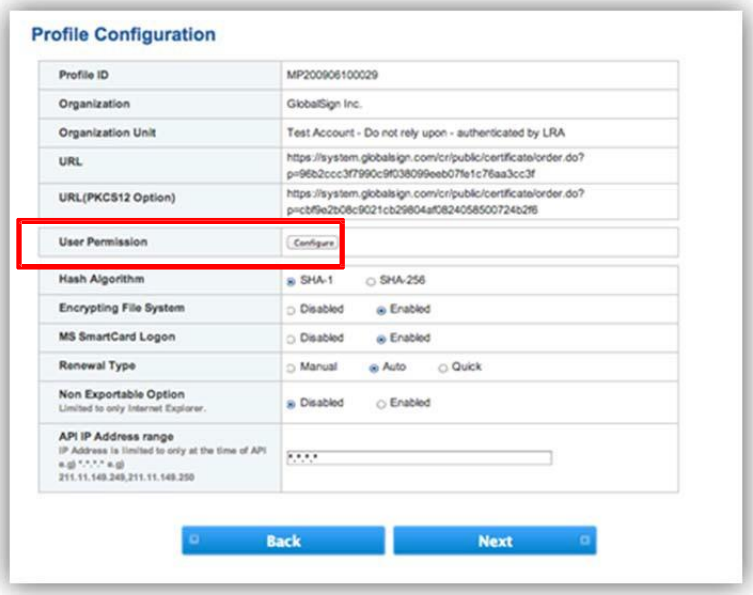
charge". Set **Certificate Approval Permission** to **True,** to grant certificate approval and profile creation rights to a "Manager". Note, "Staff in charge" will be unable to approve certificates or establish new profiles.



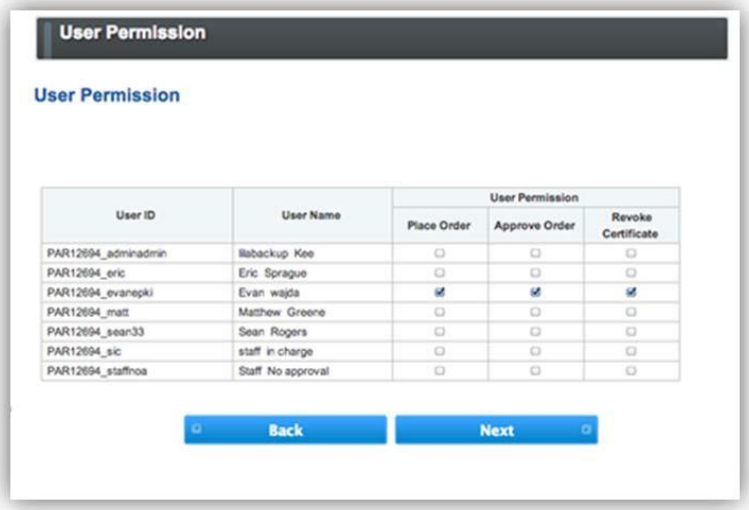


ADMINISTRATION DELEGATION

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**.



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.)



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