

GlobalSign Enterprise Solutions

# Enterprise PKI Administrator Guide

Version 3.0



## TABLE OF CONTENTS

INTRODUCTION:.....	4
RELEASE NOTES:.....	4
Intermediate CA Certificates (ICAs): .....	4
GETTING STARTED: .....	5
Logging into your GCC account: .....	5
Establishing PKI Service:.....	5
Client Authentication Certificate: .....	6
Installing your client authentication certificate:.....	6
Establishing pre-vetted certificate profile: .....	8
Types of pre-vetted identity profiles: .....	9
BR Complaint S/MIME Profile: .....	9
NON-S/MIME Profile:.....	10
MY PROFILE:.....	12
Profile Configuration:.....	12
Order Addition Profiles: .....	14
Search Profiles: .....	15
Email domain list :.....	16
MY LICENSES: .....	16
Order License: .....	17
Certificate Packs:.....	19
Search License Orders :.....	19
PURCHASING PERMISSIONS:.....	19
CUSTOMIZING EMAIL TEMPLATES:.....	19
CERTIFICATE ISSUANCE: .....	20
Using Portal link: .....	21
Approving request orders: .....	22
REGISTER USERS FOR CERTIFICATES VIA EPKI ADMINISTRATOR: .....	23
My Certificates: .....	23
Order Certificates.....	23
How to Obtain your Certificates: .....	26
Download using Internet Explorer (IE) Compatibility Mode:.....	27

Download as .pfx (PKCS12): .....	27
Download using a CSR:.....	28
Order Certificate – BULK:.....	31
Search Certificate:.....	34
PKCS#12 Bulk Registration and Pickup: .....	34
Before you Begin with PKCS#12:.....	36
Where to find these certificates: .....	37
Approving Pending Request :.....	37
Bulk Cancel or Revocation Order:.....	38
Email domain registration:.....	39
HOW TO REGISTER EMAIL DOMAINS.....	39
HOW TO SUSPEND/UNSUSPEND EMAIL DOMAINS.....	41
CERTIFICATE LIFECYCLE MANAGEMENT – REVOCATION, REISSUANCE, AND CANCELLATION: .....	42
REPORTING: .....	44
Other functions : .....	45
Acton Log : .....	45
Configure LDIF:.....	45
Generating a LDIF Report:.....	47
GCC ACCOUNT USERS: .....	48
TYPES OF GCC ACCOUNT USERS: .....	49
REGISTERING ADDITIONAL GCC ACCOUNT USERS: .....	49
ADMINISTRATION DELEGATION: .....	50
GETTING HELP:.....	52
GLOBALSIGN CONTACT INFORMATIONL .....	52

## INTRODUCTION:

This manual is for administrators who use Enterprise PKI. After obtaining a GlobalSign Certificate Centre (GCC) account, it is necessary to perform initial configuration (register profile, purchase license, etc.) before certificates are issued. The general flow is as follows.

1. Login to GCC and go to the "Enterprise PKI" tab.
2. Purchase a license and register a profile. (GlobalSign will validate the profile, then approve the license.)
3. Issue certificates to sponsored users.

## RELEASE NOTES:

This manual is based on the specifications as of August 2023 with the following changes:

### Intermediate CA Certificates (ICAs):

Depending on the certificate use case you are looking for, select the associated intermediate CA certificate under "Profile applied for" Option while creating profile.

- For Secure Email & Client Authentication use BR Compliant S/MIME Profile – based on GlobalSign GCC R6 SMIME CA 2023
- For Client Authentication use case only use Non – S/MIME option – based on GlobalSign GCC R3 PersonalSign 2 CA 2020

NOTE: In order to access S/MIME certificates, we request you to create profile basis the steps given in this support article i.e. [How to create a new Profile in EPKI:: How to create a new Profile in EPKI :: GlobalSign Support](#)

To use profile that is capable for Secure Email, the following conditions are required:

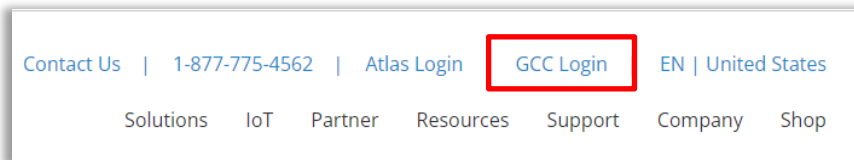
- Organization Identifier (see page#)
- Validated Email Domain as per S/MIME
- No Organization Unit (OU) field

## GETTING STARTED:

### Logging into your GCC account:

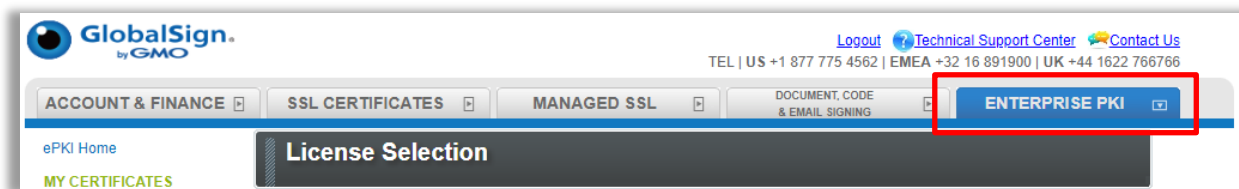
Once your EPKI Account has been approved, you can log into the GlobalSign Certificate Center (GCC) straight away to start configuring and managing the lifecycle of your PersonalSign and AATL Certificates for PDF Signing.

Go to [www.globalsign.com](http://www.globalsign.com) and click “Login” in the upper right-hand corner or go to [www.globalsign.com/login](http://www.globalsign.com/login)



Enter your **User ID** and **Password**. Your User ID is a combination of the Corporate ID that GlobalSign assigns you and the username you specified during account signup (e.g. **PAR12345\_username**). Your assigned User ID is provided at the end of the signup process and in the GCC Welcome Email.

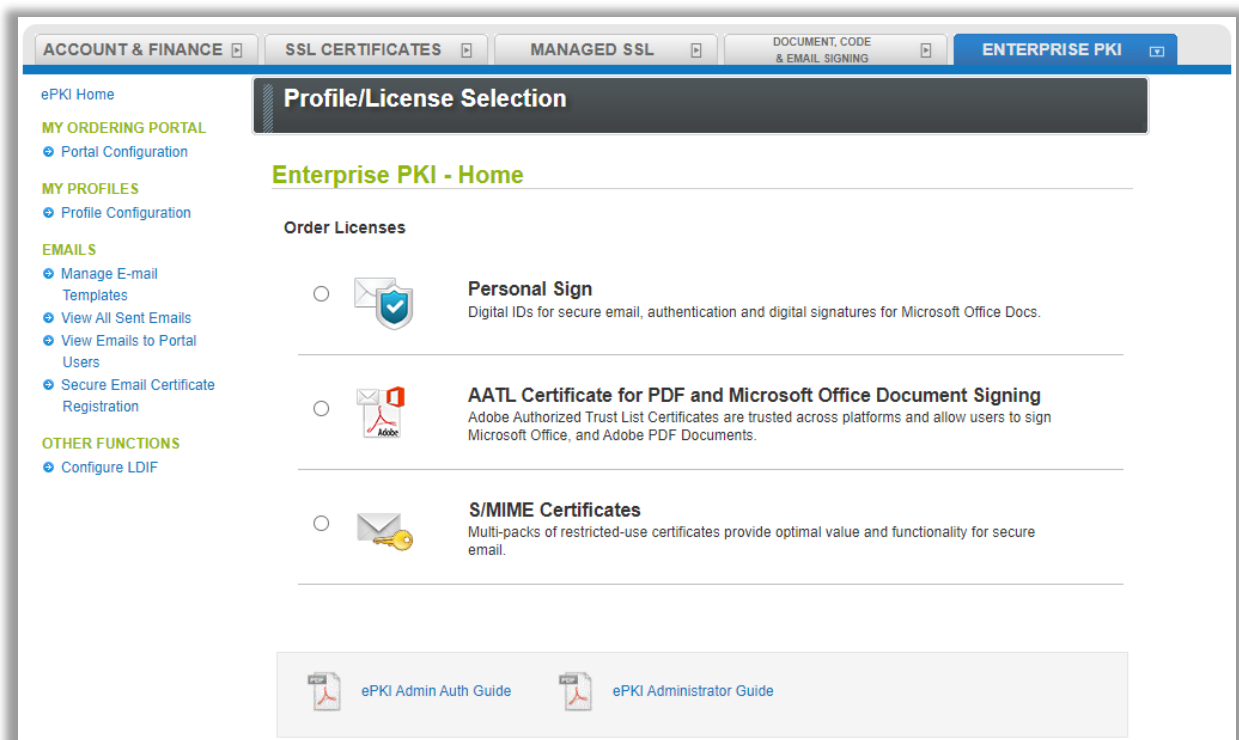
If you forget your password, you can click “[Forgot your Password? Click here](#)” on the login screen. If you have further difficulties logging in, please contact Support at: [support.globalsign.com](mailto:support.globalsign.com)



### Establishing PKI 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 five top tabs or sections for managing your Account and/or different types of Certificates. Select the 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 named as Enterprise PKI Lite for personal Digital ID, Enterprise PKI Lite for Department Digital ID, and Enterprise PKI Lite for S/MIME and AATL Certificate for Document Signing. All functions are accessed from the left-hand menu system. You can also access the main features using the icons on the Enterprise PKI home page.

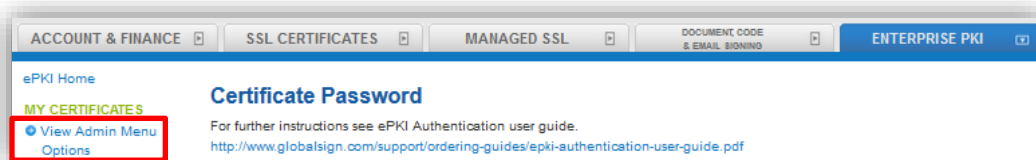


## Client Authentication Certificate:

You have the option to enable two-factor authentication (2FA) 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 submit a client authentication certificate to gain access to MY CERTIFICATES section for certificate lifecycle management.

## Installing your client authentication certificate:

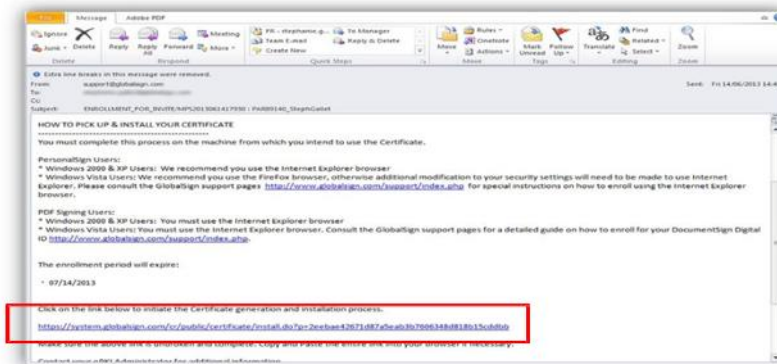
Login to your account, click on the **Enterprise PKI** tab and click on **View Admin Menu Options** under the **My Certificates** menu on the left side.



Follow the prompts to set up 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.

The screenshot shows the 'ePKI Home' interface with a sidebar menu on the left containing sections like MY CERTIFICATES, MY LICENSES, MY PROFILES, MY ORDERING, and PORTAL. The main content area is titled 'Certificate Password' and includes instructions: 'For further instructions see ePKI Authentication user guide. http://www.globalsign.com/support/ordering-guides/epki-authentication-user-guide.pdf'. It states: 'Please create a certificate password. You will be required to enter this password to install your certificate file into your browser. Next you will receive an email with a link to pick up your certificate which will require you to use this certificate password.' Below this text are two input fields: 'Certificate Password:' and 'Certificate Password(Re-enter):'. A blue 'Next' button is at the bottom right.

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 **User ID** (ex. PAR12345\_username).

The screenshot shows a dialog box titled 'Select a certificate for authentication'. It contains the text 'Site ctl2.system.globalsign.com:443 needs your credentials:'. Below this is a list of certificates with a certificate icon on the left. The selected certificate is 'PAR12345\_username', with details 'GlobalSign GCC R3 PersonalSign 2 CA 2020' and '6/19/2023'. At the bottom, there is a link 'Certificate information' and two buttons: 'OK' and 'Cancel'.

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

## Establishing 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 set up 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.

**Profile Selection**

**Certificate Profile Details**

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

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

S/MIME	<input checked="" type="radio"/> BR Compliant S/MIME (Legacy Profile) <input type="radio"/> Non - S/MIME Use Cases, like for authentication access
Organization Required	GMO GlobalSign, Inc.
Organizational Unit	<input type="text"/> <input type="text"/> <input type="text"/> <input type="checkbox"/> Lock a unique OU
Locality Optional	Portsmouth
State or Province Optional	New Hampshire
Country Required	United States - US
Signature Algorithm	<input checked="" type="radio"/> sha256RSA <input type="radio"/> RSASSA-PSS (sha256) <small>For the moment, RSASSA - PSS accepts 1 year validity only.</small>
organizationIdentifier(2.5.4.97) <small>This field is required when using S/MIME.</small>	<input checked="" type="radio"/> VAT <input type="radio"/> NTR <input type="radio"/> LEI <input type="radio"/> GOV <input type="radio"/> INTXG Country that issued your VAT number: United States - US Please enter your VAT number: <input type="text"/>



## 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 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 a unique OU", to "Reserve" the settings, as shown on the next few pages.

The screenshot shows a web form titled "Certificate Profile Details". It contains several sections for configuring a certificate profile. The "S/MIME" section has two radio buttons: "BR Compliant S/MIME Profile" (selected) and "Non - S/MIME Use Cases, like for authentication access". The "Organization" field is required and contains "GlobalSign". The "Organizational Unit" field is optional and empty, with a checkbox "Lock a unique OU" below it. The "Locality" field is optional and contains "Portsmouth". The "State or Province" field is optional and contains "NH". The "Country" field is required and is a dropdown menu showing "United States - US". The "Signature Algorithm" section has two radio buttons: "sha256RSA" (selected) and "RSASSA-PSS (sha256)". Below the second radio button is a red note: "For the moment, RSASSA - PSS accepts 1 year validity only." The "organizationIdentifier(2.5.4.97)" section has a red note: "This field is required when using S/MIME." It contains four radio buttons: "VAT" (selected), "NTR", "LEI", "GOV", and "INTXG". Below these are two dropdown menus: "Country that issued your VAT number:" showing "United States - US" and "Please enter your VAT number:" with an empty text box.

S/MIME	<input checked="" type="radio"/> BR Compliant S/MIME Profile <input type="radio"/> Non - S/MIME Use Cases, like for authentication access
Organization <small>Required</small>	GlobalSign
Organizational Unit	<input type="text"/> <input type="text"/> <input type="text"/> <input type="checkbox"/> Lock a unique OU
Locality <small>Optional</small>	Portsmouth
State or Province <small>Optional</small>	NH
Country <small>Required</small>	United States - US
Signature Algorithm	<input checked="" type="radio"/> sha256RSA <input type="radio"/> RSASSA-PSS (sha256) <small>For the moment, RSASSA - PSS accepts 1 year validity only.</small>
organizationIdentifier(2.5.4.97) <small>This field is required when using S/MIME.</small>	<input checked="" type="radio"/> VAT <input type="radio"/> NTR <input type="radio"/> LEI <input type="radio"/> GOV <input type="radio"/> INTXG Country that issued your VAT number: United States - US Please enter your VAT number: <input type="text"/>

A pre-vetted identity has two (2) main profile options:

- **BR Compliant S/MIME Profile** – for email signing and encryption, and authentication access
- **Non-S/MIME Use Cases** – for authentication access only

### BR Compliant S/MIME Profile:

This will have the following attributes defined.

- Organization Name: Required and fixed after validation.
- Organization Unit: Not available for S/MIME
- Locality: Optional and fixed after validation
- State: Optional and fixed after validation
- Country: Required and fixed after validation
- Signature Algorithm: sha256RSA by default, RSASSA-PSS if you require.
- Organization Identifier: Required and fixed during validation.

Certificate Identity Details	
Common Name <small>Required</small>	<input type="text"/>
Organization	GMO GlobalSign Inc.
Locality	Makati
State or Province	Metro Manila
Country	Philippines - PH
Email Address <small>Required</small>	<p>Enter an email prefix and select a domain</p> <p><small>※ Select an Email domain from the list, and complete your Email address. The @ symbol is required.</small></p> <p><input type="text"/> . <span>Select Email domain ▼</span></p> <p><small>Email address preview Enter your Email Address above.</small></p>

After validation, the identity profile is ready to use for issuing certificates. The following fields are available:

- Common Name: Required (i.e., John Doe or Jane Smith)
- Email Address: Required, input user email account, then select the email domain. (see domain configuration on page X)

#### NON-S/MIME Profile:

This will have the following attributes as described below.

- **Option 1: Fixed** Organization Name with an Optional Variable Organization Unit
- **Option 2: Fixed** Organization Name with a **Fixed** Organization Unit

#### Option 1: Fixed Organization Name with An Optional Variable Organization Unit

- Common Name: Required (i.e., John Doe or Jane Smith)
- Organization Name: Required and fixed after validation.
- Organization Unit: Optional and variable
- Locality: Optional and fixed after validation
- State: Optional and fixed after validation
- Country: Required and fixed after validation
- Email Address: Required (This is included in the certificate.  
This is also where the certificate will be sent.)

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	GMO GlobalSign Inc
Organizational Unit	<input type="text"/> <input type="text"/>
Locality	Portsmouth
State or Province	NH
Country	United States - US
Email Address <small>Required</small>	<input type="text"/>

## Option 2: Fixed Organization Name with A Fixed Organization Unit

- Common Name: Required (i.e., John Doe or Jane Smith)
- Organization Name: Required and fixed after validation.
- Organization Unit: Populated and fixed after validation, additional OU available.
- Locality: Optional and fixed after validation
- State: Optional and fixed after validation
- Country: Required and fixed after validation
- Email Address: Required (This is included in the certificate.  
This is also where the certificate will be sent.)

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	GMO GlobalSign Inc.
Organizational Unit [Profile]	Support
Organizational Unit	<input type="text"/>
Locality	Portsmouth
State or Province	NH
Country	United States - US
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/>.

## MY PROFILE:

### Profile Configuration:

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 sidebar menu titled 'MY PROFILES' with four options: 'Profile Configuration' (highlighted with a red arrow), 'Order Additional Profiles', 'Approve Pending Profiles', and 'Search Profiles'. To the right is the 'Step 1: Configure Profile' form. The form has a 'Portal' section with a table containing the following data:

Field	Value
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]

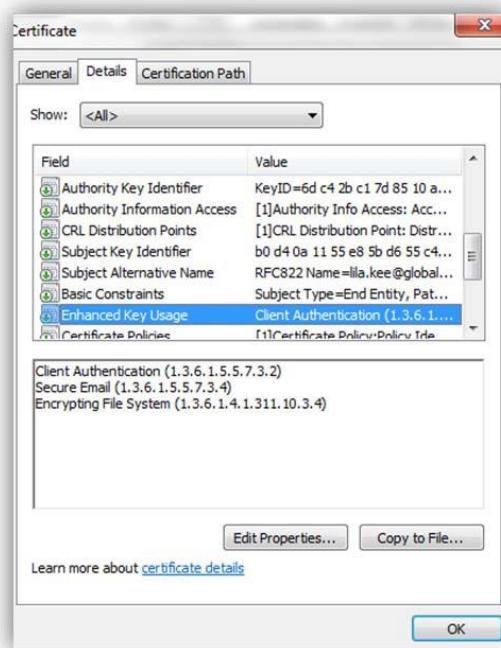
At the bottom of the form is a blue 'Next' button.

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

The image shows the 'Profile Configuration' form. It contains the following sections:

- Profile Information:** Profile ID (MP202309191852), Organization (GMO GlobalSign Inc.), Organization Unit, URL (https://test-gcc.globalsign.com/cr/public/certificate/order.do?p=91bdb556ae841b62de371e85accc6b951edc5043), and URL(PKCS12 Option) (https://test-gcc.globalsign.com/cr/public/certificate/order.do?p=52820f4b182dfce5d75a57c42c3438c146cbd2d).
- User Permission:** A 'Configure' button.
- Email Domains:** A 'Configure' button.
- IntermediateCA:** Radio buttons for 'BR Compliant S/MIME Profile' (selected) and 'Non - S/MIME Use Cases, like for authentication access'.
- Signature Algorithm:** Radio buttons for 'sha256RSA' (selected) and 'RSASSA-PSS (sha256)'. A red note below states: 'For the moment, RSASSA - PSS accepts 1 year validity only.'
- Encrypting File System:** Radio buttons for 'Disabled' (selected) and 'Enabled'.
- MS SmartCard Logon:** Radio buttons for 'Disabled' (selected) and 'Enabled'.
- Renewal Type:** Radio buttons for 'Manual' (selected), 'Auto', and 'Quick'.
- Non Exportable Option:** Radio buttons for 'Disabled' (selected) and 'Enabled'. A note below states: 'Limited to only Internet Explorer.'
- API IP Address range:** A text input field. A note below states: 'IP Address is limited to only at the time of API e.g) \*.\*.\*.\* e.g) 211.11.149.249,211.11.149.250'.

1. **Intermediate CA:** If your profile is set to BR Compliant Option that means, you can use this profile for issuing S/MIME Certificate: Note that certificate issued from this profile can also be used for client authentication. On the other hand, if profile is set to Non – S/MIME then this profile can only be used for client authentication uses case.
2. **Signature Algorithm:** The default signature algorithm is **sha256RSA**. GlobalSign also offers **RSASSA-PSS (sha256)** ([see more information here](#)).
3. **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).



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

#### 5. Renewal Type:

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 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:

The screenshot shows the 'Profile Configuration' form. A modal titled 'Renewal Type' is open, showing three radio button options: 'Manual' (selected), 'Auto', and 'Quick'. The background form includes fields for Profile ID, Organization, Organization Unit, URL, URL (PKCS12 Option), User Permission, Email Domains, IntermediateCA, and a 'Renewal Type' dropdown. Below the dropdown are checkboxes for 'MS SmartCard Logon', 'Non Exportable Option', and 'API IP Address range'.

Profile Configuration	
Profile ID	MP202309191852
Organization	GMO GlobalSign Inc.
Organization Unit	
URL	https://test-gcc.globalsign.com/cr/public/certificate/order.do?p=91bdb556ae841b62de371e85acc6b951edc5043
URL (PKCS12 Option)	https://test-gcc.globalsign.com/cr/public/certificate/order.do?p=52820f4b182dfe5d75a57c42c3438c146c0bd2d
User Permission	<a href="#">Configure</a>
Email Domains	<a href="#">Configure</a>
IntermediateCA	<input checked="" type="radio"/> BR Compliant S/MIME Profile
<b>Renewal Type</b>	
<input checked="" type="radio"/> Manual <input type="radio"/> Auto <input type="radio"/> Quick	
MS SmartCard Logon	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Renewal Type	<input checked="" type="radio"/> Manual <input 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) ***.***.***.*** 211.11.140.240, 211.11.140.250</small>	<input type="text"/>

## Order Addition Profiles:

This section allows you to create a new profile, you can select S/MIME option under your profile, if you wish to use your profile for S/MIME Certificate. Please choose Non – S/MIME option if you wish to use your profile for client authentication certificates.

Furthermore, Email domain is mandatory for S/MIME Profile, which you will need to provide in email domain option. GlobalSign currently has three option that you can choose, so that we can validate your domain. Choose the appropriate option and hit Next. This will provide you with acknowledgement number for your profile. You can use this profile, once it is approved via our vetting team.

Certificate Profile Details
Email Domains
Domain Validation
Confirm Details

### Email Verification

We send an email to one of the addresses displayed below and you follow the instructions inside.

#### Constructed Domain Email Addresses

#### WHOIS Email Address

We couldn't find any email addresses in the WHOIS record for this domain.  
If this is an error and you'd like to verify using an email address in the WHOIS record, please choose the WHOIS option below and contact our support team.

☐ admin@ashish.com  
☐ administrator@ashish.com  
☐ hostmaster@ashish.com  
☐ postmaster@ashish.com  
☐ webmaster@ashish.com  
☐ Please enter your WHOIS address

#### HTTP Verification

We provide a Domain Verification Code (DVC) and you place that DVC in a text file in a specific location on your website.

☐ Use HTTP verification

#### DNS Verification

We provide a Domain Verification Code (DVC) and you create a DNS record containing the DVC.

☐ Use DNS verification

Back
Next

## Search Profiles:

This section will help you search various profiles you might have into your account, if you know the Profile number enter in search box, or just simply click on search.

Edit	Profile ID	Country	State or Province	Locality	Organization	Organization Unit	OrganizationalIdentifier	BaseDN	Person in charge of registration	Profile Order Status	Date of application	Issue Date	Starting Profile validity date	Closing Profile validity date	Intermediate CA
<a href="#">Edit</a>	MP202310036270	United Kingdom - GB	London	London	GMO GlobalSign		VATAX-erenerenerenerene232	Disabled	PAR69585_AshishD	VALIDATING	10/03/2023 10:00(GMT+00:00)				Non - S/MIME Use Cases, like for authentication access
<a href="#">Edit</a>	MP202308245187	United Kingdom - GB	London	London	GMO GlobalSign		VATAX-erenerener	Disabled	PAR69585_AshishD	VALIDATING	09/24/2023 11:18(GMT+00:00)				Non - S/MIME Use Cases, like for authentication access
<a href="#">Edit</a>	MP202308025940	United Kingdom - GB	London	London	GMO GlobalSign		VATAX-43434434	Disabled	PAR69585_AshishD	VALIDATING	08/02/2023 05:38(GMT+00:00)				Non - S/MIME Use Cases, like for authentication access
<a href="#">Edit</a>	MP202308025939	United Kingdom - GB	London	London	GMO GlobalSign		GOVIN	Disabled	PAR69585_AshishD	VALIDATED	08/02/2023 02:33(GMT+00:00)	08/02/2023 02:49(GMT+00:00)	08/02/2023 02:41(GMT+00:00)	11/03/2025 02:41(GMT+00:00)	BR Compliant S/MIME Profile

Here you can see Intermediate CA, this section actually tells you that for which use case this profile can be used.

- If BR Compliant S/MIME is shown, then this can be used for ordering S/MIME Certificates
- If Non -S/MIME then this profile can only issue certificates for client authentication.

There are two action items here that can be used.

- Edit: Use this for cancellation request, you can cancel the profile; if that has not been approved by Vetting yet that is, if its greyed out.
- Profile ID: This will show the details and action status on the particular profile.

## Email domain list:

You can search your profile basis various search options like profile no, email domain and current status under Any column.

Profile ID	Email Domain	ePki Domain ID	Status	Use this for S/MIME Specific Email Domain	Starting domain validity date	Closing domain validity date
MP202310036270	ashish12.com	20231003001778	Pending			
MP202308246187	example.com	20230824001699	Pending			
MP202308025940	ashish.com	20230802001470	Pending			
MP202308025939	example.com	20230824001686	Pending			
MP202308025939	aegdomain2.com	20230809001500	Approved		2023-08-10 13:16:10.924	2024-09-10 13:16:10.924
MP202308025939	aegdomain1.com	20230809001499	Approved		2023-08-10 13:16:00.852	2024-09-10 13:16:00.852
MP202308025939	ashish.com	20230802001469	Pending			
MP202307315937	ashish.com	20230731001467	Pending			
MP202307265910	indanow.com	20230726001450	Pending			
MP202307265909	confirm.com	20230726001449	Pending			

If you see the starting domain validity date and closing domain validity, then that domain can be used for S/MIME cases. Note: After every 397 days, domain needs to be revalidated to be used for S/MIME Certificates.

In case you wish your current added domain to be also applicable for S/MIME Case then you can do so in following conditions.

There should be no Organization Unit and their should be Organization Identifier under the Profile for which you want your domain to be made applicable for S/MIME.

If the condition in step 1, matches then you will see Settings button under “Use this for S/MIME Specific Email domain”. You can click on the settings button and add the email domain again. After that please select the domain validation method as desired and click on next.

Once our vetting team approves your domain then you can also see the Starting domain validation date and closing domain validation date.

## MY LICENSES:

There are two action items that you can take from this section i.e., Order License and search those licenses. Let’s first understand various certificate types under license. Their behavior as per profile chosen will be different.

Product Details	Profile type	Use Case Supported	Common Name
Enterprise PKI Lite for Department Digital ID	BR Compliant S/MIME Profile	Certificate issued from this combination will have S/MIME and client authentication as standard.	Email or organization name
Enterprise PKI Lite for Personal Digital ID	BR Compliant S/MIME Profile	Certificate issued from this combination will have S/MIME and client authentication as standard.	Email or Personal name
Enterprise PKI Lite for S/MIME	BR Compliant S/MIME Profile	Certificate issued from this combination will have S/MIME only.	Email or Personal name



Enterprise PKI Lite for Department Digital ID	Non – S/MIME Use case for authentication access	Certificate issued form this combination can only use client authentication.	Email or organization name
Enterprise PKI Lite for Personal Digital ID	Non – S/MIME Use case for authentication access	Certificate issued form this combination can only use client authentication.	Email or Personal name
Enterprise PKI AATL Signing for Adobe PDF	Both types can be used I.E. BR Compliant S/MIME Profile and Non – S/MIME	<u>PDF, Microsoft Office, and Email Signing For AATL</u> for a detailed product description go to: <a href="https://www.globalsign.com/en/digital-signatures/">https://www.globalsign.com/en/digital-signatures/</a>	-

## Order License:

This section will allow you to purchase a license pack, select your product details and pack you want to issue and then hit next for payment.

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 for 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**

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

**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.

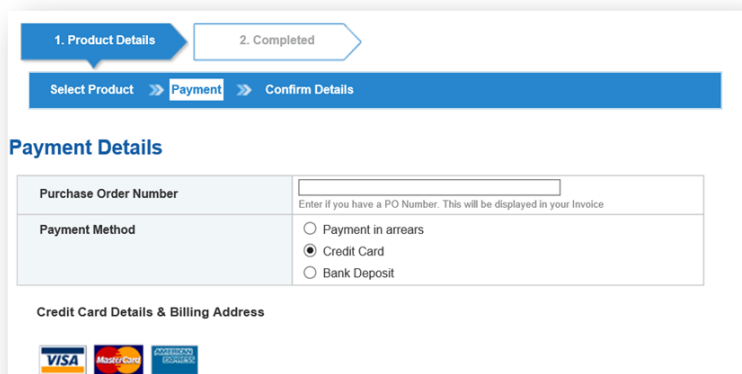
If you are applying for yourself, you do not need an additional Technical Contact, so please click Next.

NOTE: For PersonalSign 3 Pro applications the issued certificate will not be sent to the Technical Contact.

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 web form for payment details. At the top, there are two progress steps: '1. Product Details' (active) and '2. Completed'. Below this is a blue navigation bar with three links: 'Select Product', 'Payment' (highlighted), and 'Confirm Details'. The main section is titled 'Payment Details'. It contains a table with two rows: 'Purchase Order Number' with a text input field and a placeholder 'Enter if you have a PO Number. This will be displayed in your Invoice', and 'Payment Method' with three radio button options: 'Payment in arrears', 'Credit Card' (selected), and 'Bank Deposit'. Below the table, there is a section for 'Credit Card Details & Billing Address' which includes 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.

## 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.

## Search License Orders:

This section will allow you to view your license order history and its validity date and current status. It has two action items i.e., Edit and License ID

### License List

[Show Advanced Search](#)

Display Number:

1 - 10 / 16

< 1 2 Next >

	License ID	Corporate ID(Contractor User)	Date of application	Product	Certificate Period	License Order Status	Starting License validity date	Closing License validity date	License Total	License Unused number
<a href="#">Edit</a>	ML202309211899	PAR09585_AshishD	09/21/2023 03:55(GMT+00:00)	Enterprise PKI Lite For Personal Digital ID 1 pack	2 year	ISSUED	09/21/2023 03:59(GMT+00:00)	09/21/2024 03:59(GMT+00:00)	1	1

Edit:

Application: This shows the license details and its license action information depicting action details and action time.

## PURCHASING PERMISSIONS:

By default, the Account Administrator has permission to purchase license packs. The admin can choose to enable purchasing permissions for Managers and/or Staff. Managers can also provide 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.

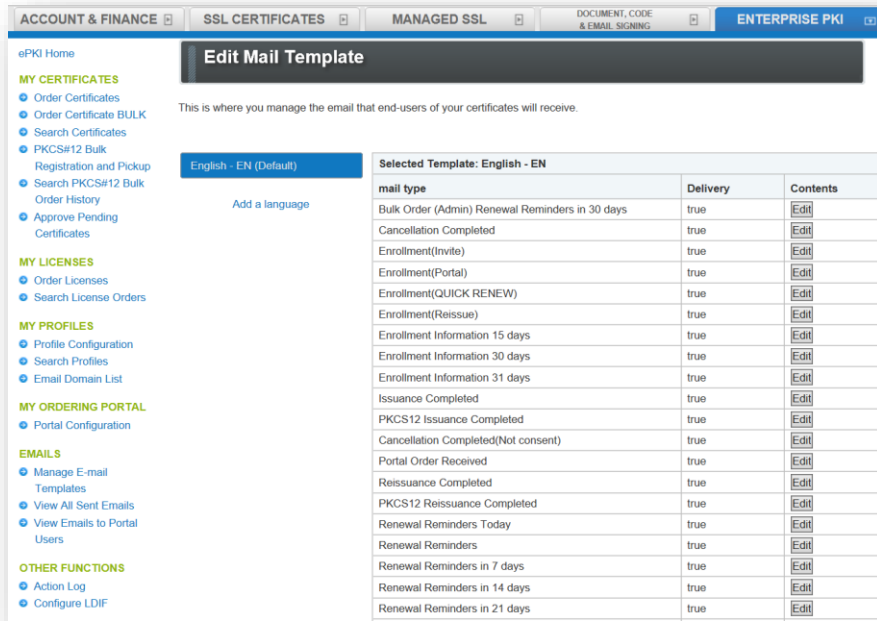
■ Certificate approval permission Yes ☒ No ☐

■ Deposit / Enterprise PKI license purchase privilege Yes ☒ No ☐

[Back](#)

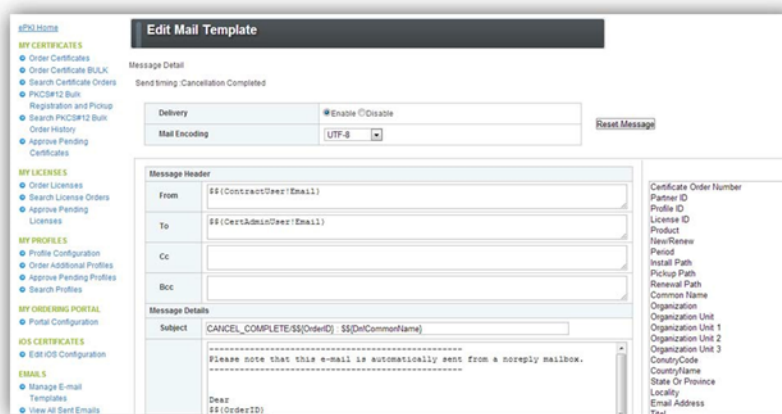
## CUSTOMIZING EMAIL TEMPLATES:

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 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.

Manage Portal	
Portal	
Profile ID	MP200906100029
Organization	GlobalSign Inc.
Organization Unit	Test Account - Do not rely upon - authenticated by LRA
URL	<a href="https://system.globalsign.com/cr/public/certificate/order.do?p=96b2ccc3f7990c9f038099eeb07fe1c76aa3cc3f">https://system.globalsign.com/cr/public/certificate/order.do?p=96b2ccc3f7990c9f038099eeb07fe1c76aa3cc3f</a>
URL(PKCS12 Option)	<a href="https://system.globalsign.com/cr/public/certificate/order.do?p=cbf9e2b08c9021cb29804af0824058500724b2f6">https://system.globalsign.com/cr/public/certificate/order.do?p=cbf9e2b08c9021cb29804af0824058500724b2f6</a>
Profile ID	MP200906150035
Organization	GlobalSign Inc.
Organization Unit	staff in charge created profile - authenticated by LRA
URL	<a href="https://system.globalsign.com/cr/public/certificate/order.do?p=82f3ec81e9057ad514d0facc801924a3c059d963">https://system.globalsign.com/cr/public/certificate/order.do?p=82f3ec81e9057ad514d0facc801924a3c059d963</a>
URL(PKCS12 Option)	<a href="https://system.globalsign.com/cr/public/certificate/order.do?p=852e1c9668a0b7b42f72630103dc9b5f903321e0">https://system.globalsign.com/cr/public/certificate/order.do?p=852e1c9668a0b7b42f72630103dc9b5f903321e0</a>

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:

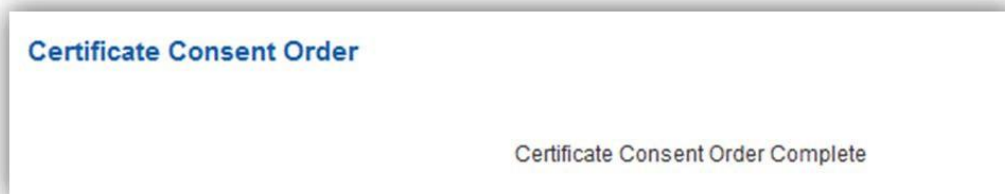
**Modify Subscriber Agreement:** You may add additional subscriber terms to the Mandatory GlobalSign Subscriber Agreement to capture unique or additional terms above and beyond the required GlobalSign terms. End users will be presented with the Subscriber Agreement and prompted to accept the terms prior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

Approving request 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**.

ACCOUNT & FINANCE							
SSL CERTIFICATES							
MANAGED SSL							
CODE SIGNING, PERSONAL SIGN, PDF SIGNING for ADOBE CDS							
ENTERPRISE PKI							
ePKI Home							
<b>MY CERTIFICATES</b>							
<ul style="list-style-type: none"> <li>Order Certificates</li> <li>Order Certificate BULK</li> <li>Search Certificate Orders</li> <li>PKCS#12 Bulk               <ul style="list-style-type: none"> <li>Registration and Pickup</li> </ul> </li> <li>Search PKCS#12 Bulk               <ul style="list-style-type: none"> <li>Order History</li> </ul> </li> <li>Approve Pending Certificates</li> </ul>							
<b>Certificate Consent Order</b>							
<input checked="" type="checkbox"/>	Certificate Order Number	Registration type	Person in charge of registration	Product	PKCS12	Common Name	Email
<input checked="" type="checkbox"/>	MPS201206219194	Invite	PAR52316_globalsign	Enterprise PKI Lite For Personal Digital ID 5 pack	No	Your Name	Your Email

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.

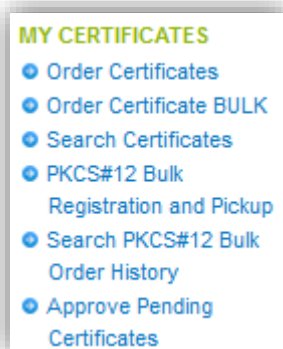


## REGISTER USERS FOR CERTIFICATES VIA EPKI ADMINISTRATOR:

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.



### My Certificates:

This tab will enable you to order the certificates, you can use this to search, order certificates in bulk, cancel and approve the requests.

#### [Order Certificates.](#)

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.

Select Profile

>> Certificate Identity Details

>> Confirm Details

Certificate Identity Details

Common Name <small>Required</small>	<input type="text"/>
Organization	GMO GlobalSign
Locality	London
State or Province	London
Country	United Kingdom - GB
Email Address <small>Required</small>	<div>Enter an email prefix and select a domain</div> <div>※ Select an Email domain from the list, and complete your Email address. The @ symbol is required.</div> <div> <input type="text"/> <div>Select Email domain</div> </div> <div>Email address preview</div> <div>Enter your Email Address above.</div>
Use e-mail address for authentication <small>Required</small>	<input checked="" type="radio"/> No <input type="radio"/> Yes
User Principal Name	<input type="text"/>
Key Generation Options	<input checked="" type="radio"/> <b>Download as .pfx (PKCS12)</b> Certificate and private key will be available for <b>download using any browser</b> .  <input type="radio"/> <b>Download using a CSR</b> <b>Advanced Users</b> - Externally generate and provide a Certificate Signing Request (CSR).  <input type="radio"/> <b>Download using Internet Explorer (IE) Compatibility Mode</b> Certificate Signing Request (CSR) is automatically generated using IE Compatibility mode. Use this option to install a certificate on an eToken (i.e. Code Signing, AATL & Qualified Certificates).

Description of fields users need to input.



1. Common Name: Use your personal name here like Ashish Dhiman, if in case you are ordering department digital ID product then you will have the option to choose either email or organization.
2. Organization, Locality, state or province and country are hardcoded as per profile chosen.
3. Email address: Input email ID here, choose domain from drop down and write your initial email address like ashish.dhiman@, rest will be auto created by domain you chosen, and you can see that under email address preview.
4. Use email address for authentication: Select Yes if you need email address to be included in certificate and need email in it for any authentication needs.
5. User Principal Name: Your registered name in Microsoft Active directory. This is optional to fill in.
6. Key Generation Option
  - a. Download as .pfx(PKCS12) : Select this method, where you will get the PKCS12 file that you can install into your client machine.
  - b. 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.
  - c. Download using Internet Explorer (IE) Compatibility Mode: Certificate Signing Request (CSR) is automatically generated using IE Compatibility mode. Use this option to install a certificate on an eToken (i.e., Code Signing, AATL & Qualified Certificates). This can be done using Microsoft edge support for internet explorer.

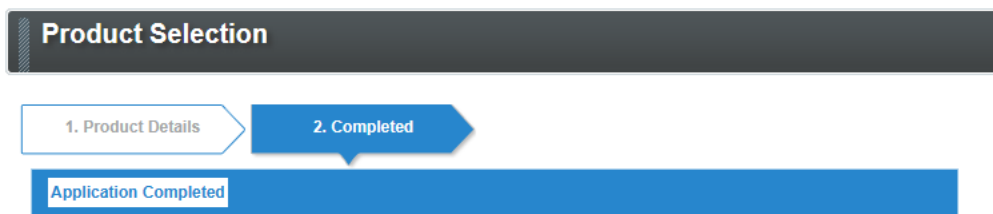
Email Template <small>Required</small>	English - EN ▼
Pickup Password <small>Required</small>	<div>Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9)</div> <div>Password Generation</div> <div>When the password automatic operation generation button is pressed, a random password automatic construction/is set.</div>
Pickup Password (re-enter) <small>Required</small>	
Memo	

Back

Next

Once all the basic fields are filled in then the user will need to enter the Pickup password, alternatively they can use random generation i.e., using Password Generation button / or enter their own password. This password is needed at the time of certificate pick up.

Hit complete, once you navigate from Next button after checking the details provided and then you will get the Order Number acknowledgment like this.



## Application Completed

Order Number	MPS20231009541712
--------------	-------------------

## What happens next?

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

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

## GlobalSign Certificate Center (GCC)

Use the GlobalSign Certificate Center to:

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

## How to Obtain your Certificates:

Once you have ordered the certificate, then there is primary three ways you can get the certificate as explained here.

Client certificates can be obtained using the following browsers or mobile terminals. Please note that the storage location of the certificate differs depending on each environment.

Windows	▪ Microsoft Edge	Windows certificate store
	▪ Chrome	
	▪ Firefox	Fire Fox certificate store
Mac	▪ Chrome ▪ Safari	Mac key chain
	▪ Firefox	Fire Fox certificate store

iOS	▪ Safari	iOS trust store
Android	▪ Chrome	certificate store

The next page will show you how to obtain (install) a certificate in the following environment.

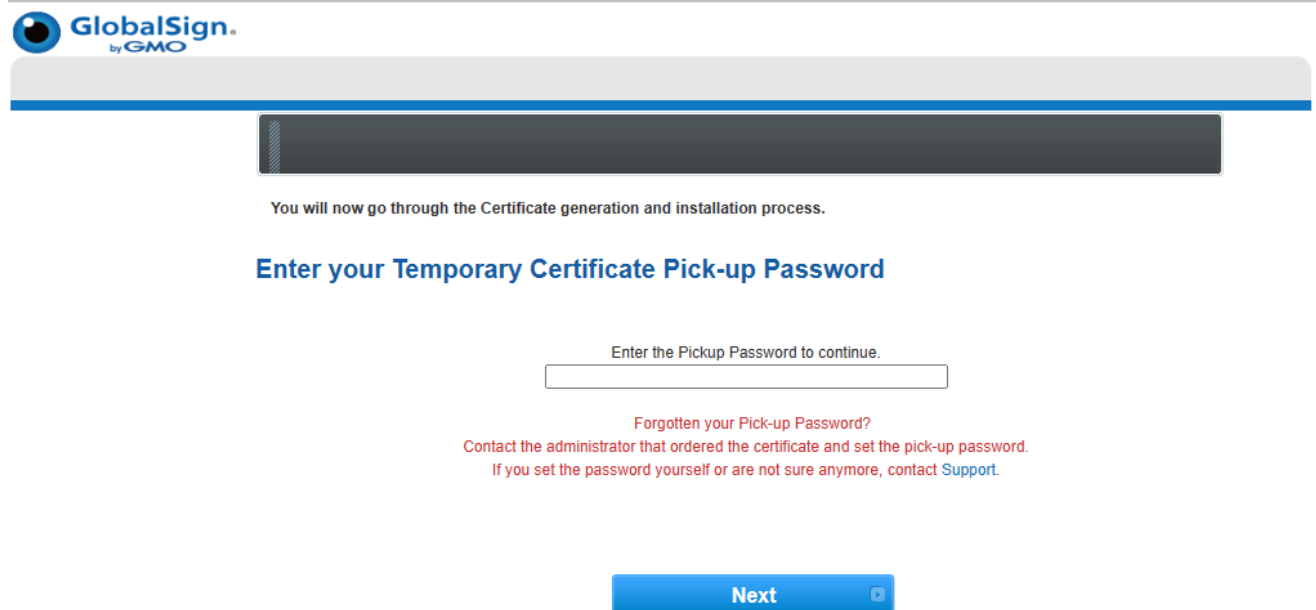
Download using Internet Explorer (IE) Compatibility Mode:

Certificate Ordered through “Download using Internet Explorer (IE) Compatibility Mode” under Key generation option.

Once your certificate is ready, you will get a certificate pick up link on your email. You have to open that link in Microsoft edge. Also, please make sure that you have your edge configured to use internet explorer. Please look into this support article for configuration instruction and install process. [IE Compatibility in Microsoft Edge: GlobalSign Support](#)

Download as .pfx (PKCS12):

If you have applied for a certificate in PKCS12 format, it will be downloaded as a file with a .pfx extension. Access the Pickup - URL to obtain the certificate described in the email. Enter the pickup password for obtaining the certificate that was set at the time of application and click "Next".



**GlobalSign**  
by GMO

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

**Enter your Temporary Certificate Pick-up Password**

Enter the Pickup Password to continue.

[Forgotten your Pick-up Password?](#)  
Contact the administrator that ordered the certificate and set the pick-up password.  
If you set the password yourself or are not sure anymore, contact [Support](#).

**Next**

2. Enter your certificate password and click Next

Certificate Password Required

j2(Zj-4b-6i\_OQ-aW

Make sure to remember this password.

Subscriber Agreement

GlobalSign Subscriber Agreement - Version 3.3

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY CANCEL THE ORDER WITHIN SEVEN (7) DAYS OF THE AVAILABILITY OF THE CERTIFICATE FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT [legal@globalsign.com](mailto:legal@globalsign.com)

This GlobalSign Subscriber Agreement (the "Agreement") between GlobalSign and

☒ I agree to the terms above

Next

3. Download screen will be displayed, so please download and install it in your environment.

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

Download My Certificate

### What to do next.

Now you have your Certificate please review the Product Guide support pages for instructions on how to use your Certificate.  
> [Go to Product Guide pages](#)

© GlobalSign All rights reserved.

### Download using a CSR:

Access the Pickup - URL to obtain the certificate that you will receive once your certificate is ready for installation. Enter the Pickup password for obtaining the certificate that was set at the time of application and click "Next".

GS

## Enter your Temporary Certificate Pick-up Password

Enter the Pickup Password to continue.

Forgotten your Pick-up Password?

Contact the administrator that ordered the certificate and set the pick-up password.  
If you set the password yourself or are not sure anymore, contact [Support](#).

Next

© GlobalSign All rights reserved.

Copy and paste the CSR in the CSR input field and click "Next".

## Enter your CSR (Certificate Signing Request)

The CSR will contain your cryptographic keys used within your Certificate.

For assistance on generating your CSR, please refer to the online [Technical Support](#)

Make sure that your CSR contains the complete header and footer "-----BEGIN..." and "...END-----" lines.

<b>Enter Certificate Signing Request</b> <span style="color: red;">Required</span>	
--	--

### Subscriber Agreement

GlobalSign Subscriber Agreement - Version 5.3

Notwithstanding the translation of this Agreement into a language other than English, the English language version of this Agreement shall at all times be controlling and the sole basis for interpretation of the terms herein.

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A CERTIFICATE, YOU ARE AGREEING TO BE

☐ I agree to the terms above

Next

Now, please click on download my certificate button once you have entered your CSR in Enter Certificate Signing request.

## Download your Digital Certificate and the Intermediate CA Certificates

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

Please click the Download My Certificate button to install your Certificate and all appropriate Intermediate CA Certificates that enable the Certificate to be trusted.

**Download My Certificate**

Also click the below buttons to download the Intermediate CA Certificates. Installing the CA Certificates together with your certificate will ensure that your Certificate will be trusted by your computer, and by others.

**Download CA Certificate1**

The certificates are available as .cer files after download.  
For converting into other formats please see our support guide for instructions.

[Go to Support Guide](#)

There are three actions items that customer will have to take here:

1. Download My Certificate: This contains your certificate PEM File
2. Download CA Certificate1: This contains your Intermediate CA Certificate.
3. Please place these certificates on the system where you created CSR.

### Order Certificate – BULK:

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 Details

### Profile

	Profile ID	BaseDN	Organization	Organization Unit	OrganizationalIdentifier	Country	State or Province	Locality	Intermediate CA
<input checked="" type="radio"/>	MP202308025939	Disabled	GMO GlobalSign		GOVIN	United Kingdom - GB	London	London	BR Compliant S/MIME Profile
<input type="radio"/>	MP202307315937	Disabled	GMO GlobalSign		INTXG	United Kingdom - GB	London	London	Non – S/MIME Use Cases, like for authentication access
<input type="radio"/>	MP202307245888	Disabled	GMO GlobalSign		VATAX-32332323	United Kingdom - GB	London	London	Non – S/MIME Use Cases, like for authentication access
<input type="radio"/>	MP202202184751	Disabled	GMO GlobalSign	Product Managemetrn		United Kingdom - GB	London	London	Non – S/MIME Use Cases, like for authentication access
<input type="radio"/>	MP202202184750	Disabled	GMO GlobalSign	Product Managemetrn		United Kingdom - GB	London	London	Non – S/MIME Use Cases, like for authentication access

### License

Service	License Unused number
<input checked="" type="radio"/> Enterprise PKI Lite For Department Digital ID 1 year	14
<input type="radio"/> Enterprise PKI Lite For Personal Digital ID 1 year	62
<input type="radio"/> Enterprise PKI Lite For Personal Digital ID 1 year	unlimited
<input type="radio"/> Enterprise PKI Lite For Personal Digital ID 2 year	1
<input type="radio"/> Enterprise PKI Personal Signing Custom 1 year	10
<input type="radio"/> Enterprise PKI Lite for S/MIME 1 year	21

Next

You will then be instructed to browse for a Comma Separated Value (CSV) file, typically created in Notepad or excel, 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”.



## 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 ,Email ,SANRFC822 Email Address ,PickupPassword ,haveCSR ,PKCS12 ,UPN

```
true ,kate.jones@globalsign.com ,kate.jones@globalsign.com ,1h2hd8kw ,true ,false ,admin@globalsign.com
false ,Jennifer.jones@globalsign.com ,Jennifer.jones@globalsign.com ,9o7t9ghsa3 ,false ,false ,admin@globalsign.com
true ,George.jones@globalsign.com ,George.jones@globalsign.com ,9o7t9ghsa3 ,false ,true ,admin@globalsign.com
```

Item	Explanation	Limitation
CommonName	If you want to include your Emailaddress True/ON , Organization False/OFF	E =True/ON O=False/OFF
Email	Email Address	Email Address
SANRFC822 Email Address	SANRFC822 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
UPN	User Principal Name	Email Address

CSV file	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>
Email Template	
Please select a mail template to apply to all orders	English - EN ▼

Please note: The item name which was displayed as "MS SmartCard Logon" has been changed to "UPN".

Below is an example of a CSV file that contains the order details.

	A	B	C	D	E	F	G
1	CommonName	Email	SANRFC822 Email Address	PickupPassword	haveCSR	PKCS12	UPN
2	Deepak Sharma	deepak.sharma@aegdomain1.com	deepak.sharma@aegdomain1.com	autogen	FALSE	TRUE	
3	Ashish Dhiman	ashish.dhiman@aegdomain1.com	ashish.dhiman@aegdomain1.com	autogen	FALSE	TRUE	

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.

1. Product Details

2. Completed

Product Details
File specification
Edit Details
Confirm Details

### Edit Details

No	CommonName <small>Required</small>	Email Address	SANRFC822 Email Address <small>Required</small>	Pickup Password <small>Required</small>	haveCSR	PKCS12	UPN
1	<input type="radio"/> Email Address <input checked="" type="radio"/> Organization	ashish.dhiman@aegdomain1.com	ashish.dhiman@aegdomain1.com	123@r45D7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Email Template		EN					

Back
Next

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

Search Certificate:

This section will allow you to look into the history of all certificates issued, and you can also click on Application to request any cancellation if you want. There are two action items beside the detail that you can view for you certificate.

Application: This can help you cancel the certificate, if needed; and also check the application details.

Certificate Order Number: This can help you check the certificate details and also check the certificate action information.

Search Certificates

Show Advanced Search

Search

Display Number: 10

1 - 10 / 175

CSV

CSV(Lite)

LDIF

<

1

2

3

4

5

6

7

8

9

10

11

Next

>


Various application	Certificate Order Number	Organization Name	Common Name	Product	Period	Email Address	Person in charge of registration
<div>Application</div>	MPS20231009541712	GMO GlobalSign	ashish.dhiman@aegdomain2.com	Enterprise PKI Lite For Department Digital ID 10 pack	1 year		PAR69585_AshishD

PKCS#12 Bulk Registration and Pickup:

Bulk provisioning provides an alternative to order certificate - 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.
- GlobalSign will generate a PKCS12 password for you, and there is no need for Pick Up password as we do it Order Certificate – Bulk.

34



NOTE: By default, the Bulk PKCS12 registration option will only support user registration that does 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 the Email Domain Registration section below.

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).

The process for ordering will remain the same i.e., you need to upload CSV as you did for Order Certificate Bulk, difference is there is no need to provide pick up password. Once CSV is uploaded, we will generate the PKCS#12 password like this, just hit complete. Please remember to click on PKCS12 Password Download, this file will contain all your PKCS12 passwords generated by us (Containing common name and PKCS12 Password)

[Product Details](#) >> [File specification](#) >> [Edit Details](#) >> [Confirm Details](#)

### Confirm Details

No	CommonName	Email Address	SANRFC822 Email Address	PKCS#12 Password	UPN
1	Ashish	ashish.dhiman@aegdomain1.com	ashish.dhiman@aegdomain1.com	<USA.(k)n_.T?0IGc5	
2	Adil Dhiman	adil.dhiman@aegdomain1.com	adil.dhiman@aegdomain1.com	_59mm[lhz5UaW9l=mW	

[Back](#) [Complete](#)

PKCS12 Password Download

Finally, you will get the acknowledgement like this.

## Product Selection

1. Product Details

2. Completed

Completed

### Certificate issue batch application

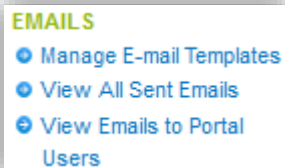
PKCS#12 Order ID

MPB202310090779

A Zip file containing your Bulk enrolled PKCS12 digital IDs can be found on the left menu item

Before you Begin with PKCS#12:

1. There is a 200-record limit (3.2M) and depending on key size selected, the Zip File 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

d. Click “Next” and then “Complete”.

Where to find these certificates:

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).

Click on “Search PKCS#12 Bulk Order History” and click on search or enter your specific search criteria.

P#12 Bulk Order ID	Edit	Date of application	Issue Date	Order Status	Product	Certificate Validity	Profile Order ID	License Order ID	Upload Number	Download
MPB202310096532	<a href="#">Edit</a>	10/09/2023 10:45(GMT+00:00)	10/09/2023 10:55(GMT+00:00)	ISSUED	Enterprise PKI Lite For Department Digital ID 10 pack	1 year	MP202308025939	ML202306271008	2	<a href="#">Download</a>

Once your order is issued, you will see the Download button, click on it to download the ZIP file containing your certificates.

### Approving Pending Request:

This section is needed when you need to approve certificate request from user who does not have permission to Approve Order and has placed Order. There are various user settings that Admin can apply to apply to user which we will discuss in detail below.

#### Certificate Consent Order

<input type="checkbox"/> Edit	Certificate Order Number	Registration type	Person in charge of registration	Product	PKCS12	Common Name	Email Address	Period	New/Renew
<input type="checkbox"/> <a href="#">Edit</a>	MAS20211028750195	Invite	PAR43801_Benjamin	Enterprise PKI AATL Signing For Adobe PDF 1 pack	Disabled	Benjamin Hook		1 year	Renew
<input type="checkbox"/> <a href="#">Edit</a>	MPS20211028750194	Invite	PAR43801_Benjamin	Enterprise PKI Lite For Personal Digital ID 5 pack	Disabled	Benjamin Hook	benjamin.hook@globalsign.com	1 year	Renew

[Cancel Consent](#) [Give Consent](#)

There are two actions users can take here for orders i.e., Cancel Consent and Give Consent. If you cancel your consent then user order request will not be processed, and on the other hand, clicking Give Consent will approve the order request.

## Bulk Cancel or Revocation Order:

This section will allow you to cancel any issued certificate or revoke the same, if needed. Cancellation for certificate can only be performed within 7 days from the date of issue. By canceling, the consumed license will be restored.

Revocation is generally done when you report any theft, or loss etc. The revoking certificate request will be displayed in the next Certificate Revocation list. You can perform cancellation and revocation for one certificate or select multiple via using check box.

The screenshot shows the GlobalSign ePKI Home interface. The top navigation bar includes the GlobalSign logo, user information (PAR69585\_AshishD), and links for Logout, Technical Support Center, and Contact Us. Below the navigation bar, there are tabs for ACCOUNT & FINANCE, SSL CERTIFICATES, MANAGED SSL, DOCUMENT, CODE & EMAIL SIGNING, and ENTERPRISE PKI. The main content area is titled "Bulk Cancel or Revocation Order". It features a search bar with the text "e.g. MPS201207030574 OR John Smith" and a "Show Advanced Search" link. Below the search bar, there are two buttons: "Cancelable certificate list" and "Available revocation list". A "Display Number" dropdown is set to "10", and the page shows "1 - 10 / 78" results. A pagination link "< 1 2 3 4 5 6 7 8 Next >" is visible. On the left sidebar, there are sections for "MY CERTIFICATES", "MY LICENSES", and "MY PROFILES". The "MY CERTIFICATES" section is expanded, showing a list of actions: Order Certificates, Order Certificate BULK, Reissue Certificate BULK, Search Certificates, PKCS#12 Bulk, Registration and Pickup, Search PKCS#12 Bulk, Order History, Approve Pending Certificates, Bulk Cancel or Revocation Order, and Search License Orders. The "Bulk Cancel or Revocation Order" option is selected. Below the sidebar, there is a table with the following columns: Various application, Certificate Order Number, Organization Name, Common Name, Product, Period, Email Address, and Person in charge of registration. The table contains one row with the following data: [checkbox], MPS20230824534642, GMO GlobalSign, aegadmin dc, Enterprise PKI Lite For Personal Digital ID unlimited, 1 year, aegadmindc@aegdomain1.com, and PAR69585\_AsthaB.

Various application	Certificate Order Number	Organization Name	Common Name	Product	Period	Email Address	Person in charge of registration
<input type="checkbox"/>	MPS20230824534642	GMO GlobalSign	aegadmin dc	Enterprise PKI Lite For Personal Digital ID unlimited	1 year	aegadmindc@aegdomain1.com	PAR69585_AsthaB

There is main two cancellation action items that can help you perform these actions.

- Cancelable certificate list: This shows the list of certificates that are eligible for cancellation.
- Available revocation list: This shows the list of certificates that can be revoked.

Revoked certificates will be put on the Certificate Revocation List within 24 hours, making the certificate unusable for most applications.

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).

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.

## 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	MP202308025939
Organization	GMO GlobalSign
Organization Unit	
URL	<a href="https://stg-gcc.globalsign.com/cr/public/certificate/order.do?p=a9160c521723309e14ccba24436a52e5cfc2e476">https://stg-gcc.globalsign.com/cr/public/certificate/order.do?p=a9160c521723309e14ccba24436a52e5cfc2e476</a>
URL(PKCS12 Option)	<a href="https://stg-gcc.globalsign.com/cr/public/certificate/order.do?p=cd8f3124c2f93b03174fb46fd316793d6ad96d81">https://stg-gcc.globalsign.com/cr/public/certificate/order.do?p=cd8f3124c2f93b03174fb46fd316793d6ad96d81</a>
User Permission	<button>Configure</button>
Email Domains	<button>Configure</button>
IntermediateCA	<input checked="" type="radio"/> BR Compliant S/MIME Profile <input type="radio"/> Non - S/MIME Use Cases, like for authentication access
Signature Algorithm	<input checked="" type="radio"/> sha256RSA <input type="radio"/> RSASSA-PSS (sha256) <b>For the moment, RSASSA - PSS accepts 1 year validity only.</b>
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 checked="" type="radio"/> Manual <input 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

4. Enter domain name(s) into the Email Domains field.

Email Domains

This is required when using S/MIME. You can also register additional e-mail addresses later.  
If you do not use S/MIME, this item is optional.  
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.

Add Email Domains

Email Domains  
This field is required when using S/MIME.

- ☒ We use S/MIME. The mail domain will have an expiration date of 397 days.
- ☐ We do not use S/MIME. No expiration date will be applied to the mail domain.

Registered Email Domains

Email Domain (Case-Insensitive)	Status
aegdomain1.com	Approved
aegdomain2.com	Approved
ashish.com	Pending
example.com	Pending

Back

Next

5. Submit the email domain(s), select your domain verification method like HTTP / DNS / Constructed mail 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.

Profile Email Domain Search

Profile No

Email Domain

Any

Search

Show: 10

1 - 10 /24

< 1 2 3 Next >

Profile ID	Email Domain	ePki Domain ID	Status	Use this for S/MIME Specific Email Domain	Starting domain validity date	Closing domain validity date
MP202310036270	ashish12.com	20231003001778	Pending			
MP202308246187	example.com	20230824001699	Pending			
MP202308025940	ashish.com	20230802001470	Pending			
MP202308025939	example.com	20230824001686	Pending			
MP202308025939	aegdomain2.com	20230809001500	Approved		2023-08-10 13:16:10.924	2024-09-10 13:16:10.924
MP202308025939	aegdomain1.com	20230809001499	Approved		2023-08-10 13:16:00.852	2024-09-10 13:16:00.852
MP202308025939	ashish.com	20230802001469	Pending			
MP202307315937	ashish.com	20230731001467	Pending			
MP202307265910	indanow.com	20230726001450	Pending			
MP202307265909	confirm.com	20230726001449	Pending			



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.

ePKI Home

### Profile Email Domain Search

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

Profile No:  Email Domain:  Any

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"/>

## EMAIL DOMAIN OPTIONS FOR EPKI PORTAL USERS

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

1. Portal users can manually input their full email address.
  1. Note for profiles which are used for S/MIME Certificate in those cases, user can only choose from email domain drop box.
2. Our 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**.

<b>MY PROFILES</b> <a href="#">Profile Configuration</a> <a href="#">Order Additional Profiles</a> <a href="#">Search Profiles</a> <a href="#">Email Domain List</a> <b>MY ORDERING PORTAL</b> <a href="#">Portal Configuration</a> <b>EMAILS</b> <a href="#">Manage E-mail Templates</a>	<b>Portal</b>	
	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.

<b>Certificate Identity Details</b>	
Common Name <small>Required</small>	<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 <small>Required</small>	<p>Enter an email prefix and select a domain</p> <p>※ 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
<a href="#">Application</a>	MPS2013062118838	GMO GlobalSign Ltd	YourName	Enterprise PKI Life For Personal Digital ID 10 pack	2 year	your.email@yourcompany.com	PAR89496_SGIMtg2013	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 for 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 with 'MY CERTIFICATES' and 'MY LICENSES' sections. The 'MY CERTIFICATES' section includes links for 'Order Certificates', 'Order Certificate BULK', 'Search Certificate Orders', 'PKCS#12 Bulk: Registration and Pickup', 'Search PKCS#12 Bulk: Order History', and 'Approve Pending Certificates'. The 'MY LICENSES' section includes 'Order Licenses' and 'Search License Orders'. The main 'Certificate List' section has a search bar with the placeholder text 'e.g. ML201207030574 OR John Smith' and a 'Hide Advanced Search' link. Below the search bar are several filters: 'Application Date is' with a dropdown, 'between' with a date range selector (i.e. mm/dd/yyyy), and 'and' with another date range selector. There are also dropdowns for 'Any Product', 'Any Order State', and 'Any Certificate Status'. Below these are input fields for 'Profile ID...', 'License ID...', 'User in Charge...', 'Organization Unit...', and 'Email address...'. A 'Search' button is located at the bottom right of the filter section. At the bottom left of the search section, there is a 'Display Number:' label followed by a dropdown 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
<a href="#">Application</a>	MP2013062118838	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)

## Other functions:

### Acton Log:

This section will allow you to check all the actions that are performed on the EPKI account and user who performed it.

Action	Order No	User ID	IP	Date
CERTIFICATE_P12_BULK_DOWNLOAD	<a href="#">MPB202310096532</a>	PAR69585_AshishD	172.17.210.245	2023-10-09 20:30:40.031
CERTIFICATE_P12_BULK_DOWNLOAD	<a href="#">MPB202310096532</a>	PAR69585_AshishD	172.17.210.245	2023-10-09 20:30:08.875
CERTIFICATE_ORDER	<a href="#">MP202308025939</a>	PAR69585_AshishD	172.17.210.245	2023-10-09 16:15:14.733
PROFILE_ORDER	<a href="#">MP202310036270</a>	PAR69585_AshishD	172.17.210.245	2023-10-03 19:00:15.513
PROFILE_EDIT	<a href="#">MP202308025939</a>	PAR69585_DevanR	172.17.210.245	2023-09-26 04:14:53.491
LICENSE_ORDER	<a href="#">ML202309211899</a>	PAR69585_AshishD	172.17.210.245	2023-09-21 12:55:27.258
LICENSE_ORDER	<a href="#">ML202309211898</a>	PAR69585_AshishD	172.17.210.245	2023-09-21 12:54:34.493
PROFILE_EDIT	<a href="#">MP202308025939</a>	PAR69585_AshishD	172.17.210.245	2023-09-20 18:22:44.798
PROFILE_EDIT	<a href="#">MP202308025939</a>	PAR69585_AshishD	172.17.210.245	2023-09-19 20:33:40.993
LICENSE_ORDER	<a href="#">ML202309181889</a>	PAR69585_DevanR	172.17.210.245	2023-09-19 02:00:42.88

### Configure 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 an LDAP directory.

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

#### OTHER FUNCTIONS

- Action Log
- Configure LDIF

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
Message	dn: CN=\${Dn!CommonName}, CN=Users, DC=edit here changetype: modify replace: userCertificate userCertificate:: \${Certificate!Pem} -
Footer	

- 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

## 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

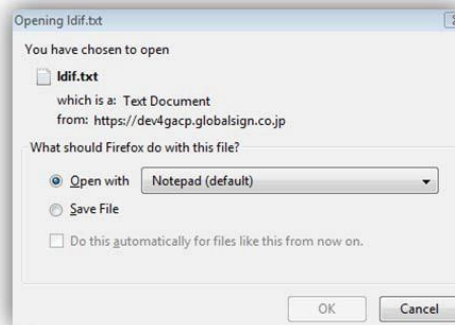
Profile ID...  License ID...  User in Charge...

Organization Unit...  Email address...

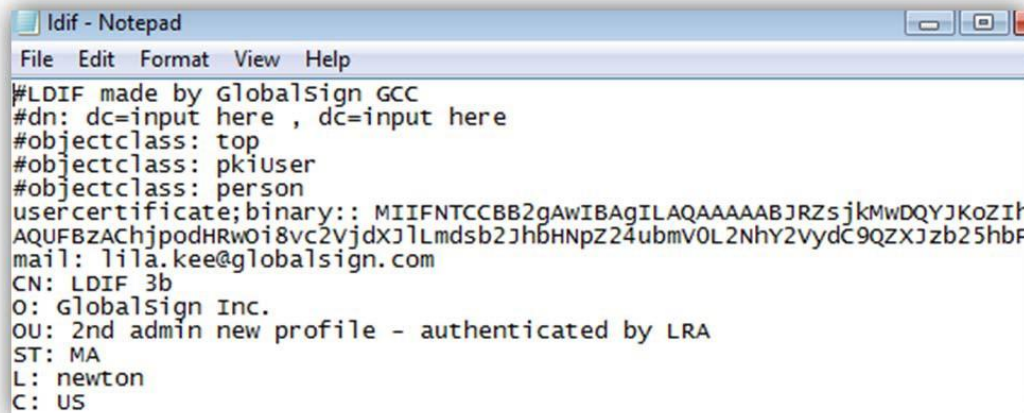
Display Number:

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.

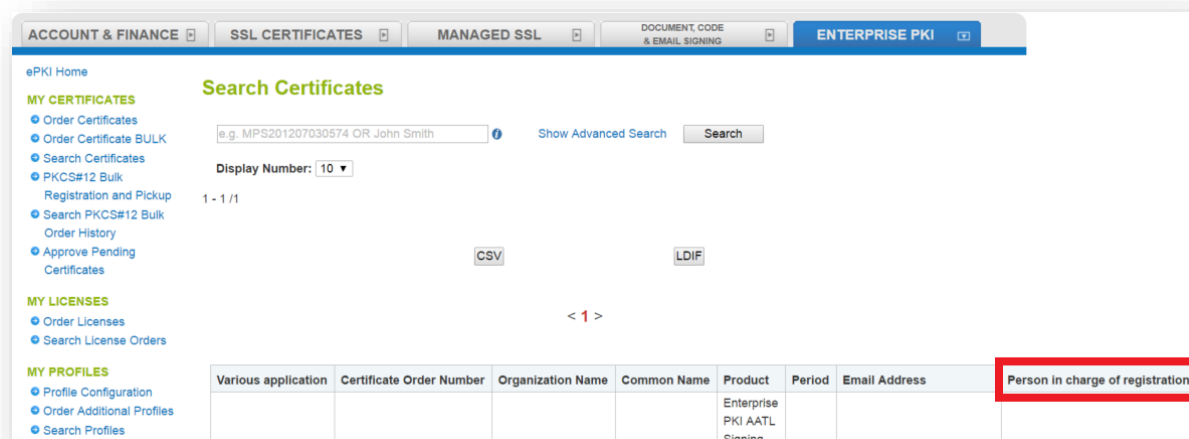
### MANAGER

**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.



## 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.

SSL CERTIFICATES MANAGED SSL PERSONAL SIGN ENTERPRISE PKI

### New user registration page

User ID	PAR89140_
Password	
Password(confirmation)	
Organization Name	e.g. GlobalSign Inc
Department	e.g. Marketing
First Name	
Middle Name	
Last Name	
Job Title	e.g. Web Administrator
Street Address 1	

Street Address 2	
City	e.g. Portsmouth
State or County	e.g. New Hampshire
Zip Code / Postal Code	e.g. 03801
Country	Germany
Other address info	
Telephone (inc. region code)	e.g. +44 ( 0 ) 1622 766766
Fax (inc. region code)	e.g. +44 ( 0 ) 1622 662255
Email Address	
User permissions	Manager
Language	
Hoping for guide from this company	<input type="checkbox"/>
Certificate approval permission	<input checked="" type="radio"/> true <input type="radio"/> false
Deposit purchase authority	<input checked="" type="radio"/> true <input type="radio"/> false

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=96b2ccc3f7990c9f038099eeb071e1c76aa3cc3f
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=cbf9e2b08c9021cb29804af0824058500724629f
User Permission	<a href="#">Configure</a>
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>	<input type="text"/>

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

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	Backup Kee	<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"/>

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

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/](http://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/](http://www.globalsign.com/help/).

## GLOBALSIGN CONTACT INFORMATIONL

<b>GlobalSign Americas</b> Tel: 1-877-775-4562 <a href="http://www.globalsign.com">www.globalsign.com</a> <a href="mailto:sales-us@globalsign.com">sales-us@globalsign.com</a>	<b>GlobalSign EU</b> Tel: +32 16 891900 <a href="http://www.globalsign.eu">www.globalsign.eu</a> <a href="mailto:sales@globalsign.com">sales@globalsign.com</a>	<b>GlobalSign UK</b> Tel: +44 1622 766766 <a href="http://www.globalsign.co.uk">www.globalsign.co.uk</a> <a href="mailto:sales@globalsign.com">sales@globalsign.com</a>
<b>GlobalSign FR</b> Tel: +33 9 75 1832 00 <a href="http://www.globalsign.fr">www.globalsign.fr</a> <a href="mailto:ventes@globalsign.com">ventes@globalsign.com</a>	<b>GlobalSign DE</b> Tel: +49 30 8878 9310 <a href="http://www.globalsign.de">www.globalsign.de</a> <a href="mailto:verkauf@globalsign.com">verkauf@globalsign.com</a>	<b>GlobalSign NL</b> Tel: +31 85 888 2424 <a href="http://www.globalsign.nl">www.globalsign.nl</a> <a href="mailto:verkoop@globalsign.com">verkoop@globalsign.com</a>