

GlobalSign Enterprise PKI Support

GlobalSign Enterprise Solution EPKI Administrator Guide v2.4



TABLE OF CONTENTS

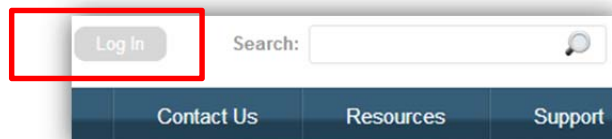
GETTING STARTED.....	3
ESTABLISHING EPKI SERVICE	3
EPKI ADMINISTRATOR/USER CERTIFICATE	4
ESTABLISHING A PRE-VETTED CERTIFICATE PROFILE.....	8
TYPES OF PRE-VETTED IDENTITY PROFILES.....	9
ADDITIONAL PROFILE SPECIFIC CONFIGURATION OPTIONS.....	12
RENEWAL	14
PURCHASING CERTIFICATE LICENSE PACKS	15
CERTIFICATE TYPE	15
CERTIFICATE PACKS.....	15
CERTIFICATE VALIDITY.....	15
CUSTOMIZING EMAIL TEMPLATES.....	17
REQUESTING CERTIFICATES	18
USING THE PORTAL LINK.....	18
APPROVING REQUESTS (ORDERS).....	20
REGISTER USERS VIA EPKI ADMINISTRATOR.....	20
SINGLE USER REGISTRATION.....	21
BULK ENROLLMENT.....	24
BULK PROVISIONING (PKCS#12)	26
CERTIFICATE LIFECYCLE MANAGEMENT – REVOCATION, REISSUANCE, AND CANCELLATION.....	29
REPORTING	30
LDIF	31
CONFIGURING LDIF	31
GENERATING A LDIF REPORT	32
ESTABLISHING OTHER EPKI USERS	34
TYPES OF EPKI USERS	34
REGISTERING ADDITIONAL USERS	34
ADMINISTRATION DELEGATION	35
GETTING HELP.....	37
GLOBALSIGN CONTACT INFORMATION	37

GETTING STARTED

LOGGING INTO YOUR GLOBALSIGN CERTIFICATE CENTER (GCC) ACCOUNT

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

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

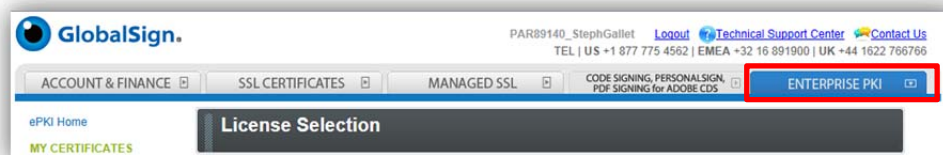


Enter your **User ID** and **Password**. Your User ID is the *PARXXXXX_XXXXX* number given to you at the end of the GCC signup process that you can also find in your Welcome Email. Your Password is the password you entered during the signup process.

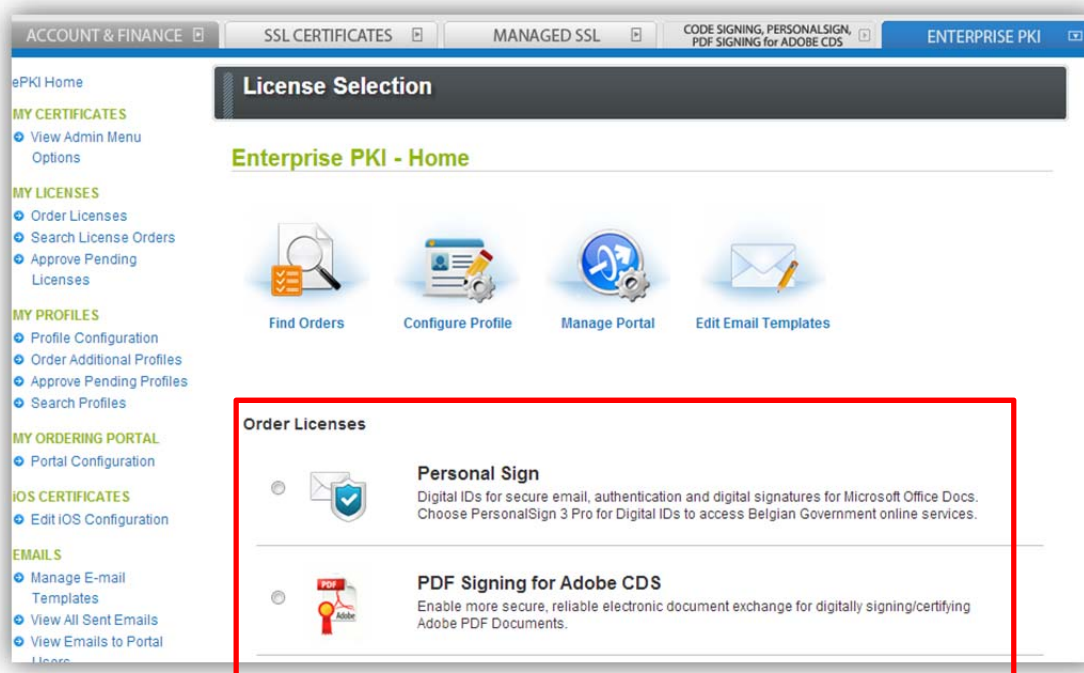
If you have difficulties logging in or forget your password please contact Support at:
www.globalsign.com/support

ESTABLISHING EPKI SERVICE

The first time you log in, you will be prompted to choose which default tab you wish to land on every time you access your account. Select **Enterprise PKI**. You will then enter the GCC home page that will provide four certificate tabs. Select the upper tab labeled “**ENTERPRISE PKI**”.



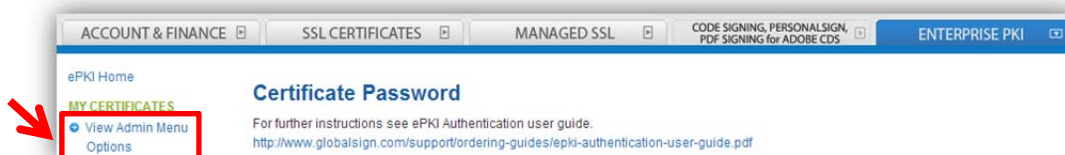
You will land on the EPKI home page where you can find two types of certificates available for you to order: PersonalSign and PDF Signing Digital Certificates. All functions are accessed through the left hand menu system. You can also access the main features using the icons on the Enterprise PKI home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



EPKI ADMINISTRATOR/USER CERTIFICATE

Once you have set up your Profile and ordered your License pack(s) you will need to obtain an EPKI Administrator certificate to gain access to the portal to start issuing and managing your account.

Once logged into your account, click on the **Enterprise PKI** tab. Then, click on **View Admin Menu Options** under the **My Certificates** menu on the left side of the page.



You will have to create a password for your EPKI Administrator certificate called the **Pick-up password**. This password must be a minimum of 12 alphanumeric characters. **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.

ACCOUNT & FINANCE | SSL CERTIFICATES | MANAGED SSL | CODE SIGNING, PERSONAL SIGN, PDF SIGNING for ADOBE CDS | ENTERPRISE PKI

ePKI Home

MY CERTIFICATES

- View Admin Menu
- Options

MY LICENSES

- Order Licenses
- Search License Orders
- Approve Pending Licenses

MY PROFILES

- Profile Configuration
- Order Additional Profiles
- Approve Pending Profiles
- Search Profiles

Certificate Password

For further instructions see ePKI Authentication user guide.
<http://www.globalsign.com/support/ordering-guides/epki-authentication-user-guide.pdf>

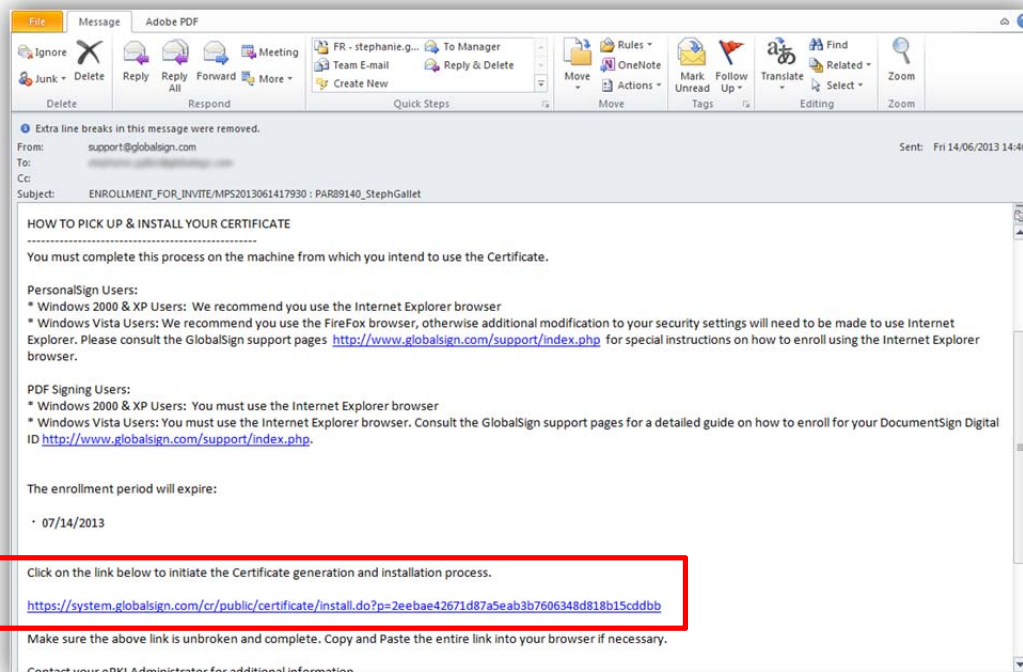
Please create a certificate password. You will be required to enter this password to install your certificate file into your browser. Next you will receive an email with a link to pick up your certificate which will require you to use this certificate password.

Certificate Password:


Certificate Password(Re-enter):

Next

A message will appear on your screen saying that your EPKI Administrator certificate registration is complete. You will then receive an email confirming that your Digital Certificate is ready to be picked up. Click on the Certificate pick-up URL in order to start installing your certificate.



A pop-up window will appear, asking you to enter your **Pick-up Password**. Then click **Next**.



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


Enter your Temporary Certificate Pick-up Password

Enter the Pickup Password to continue.

Forgotten the Pickup Password? [Contact Support](#) immediately for assistance.

Next

You will be requested to create a new password, that we will refer to as the **Private Key password**. Next you will need to agree to the EPKI Subscriber Agreement and then click **Next**.



Certificate Password *Required*

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

Certificate Password (re-enter) *Required*

ePKI Subscriber Agreement

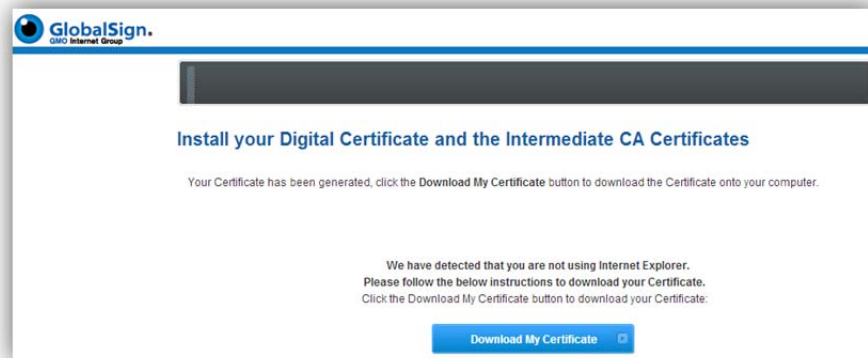
GlobalSign Subscriber Agreement - Digital Certificates and Services - Version 2.5

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A DIGITAL CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY CANCEL THE ORDER WITHIN 7 DAYS OF THE APPLICATION FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS

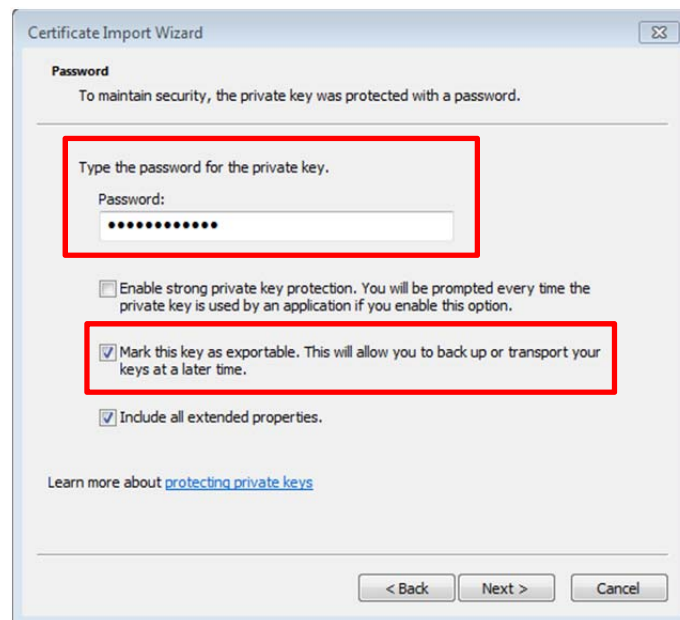
☐ I AGREE TO THE SUBSCRIBER AGREEMENT

Next

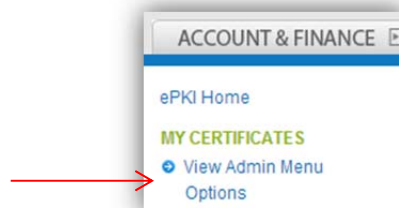
You can now download your Certificate.



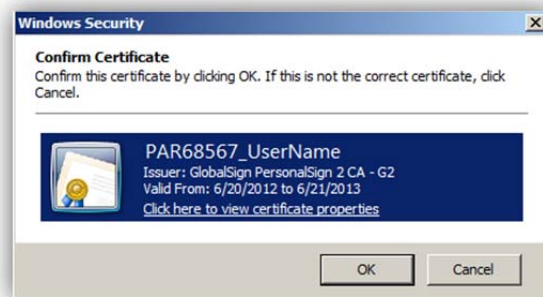
The Certificate Import Wizard will start when you open the .pfx document. Simply follow the steps by clicking **Next**. On the second step, you will have to enter the **Private Key password** you created earlier and you will also be given the choice to select whether or not you wish the key to be exportable.



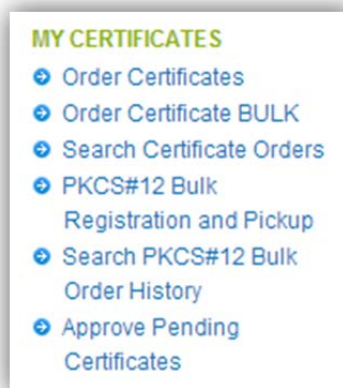
At the end of the process, a message will confirm that it was successful. You can then go back to your account, click **View Admin Menu Options** in the **My Certificates** menu.



You will be prompted to choose the Administrator Certificate that you just installed. You can verify the correct certificate as its common name will be your account login.



You will then have full access to all of the EPKI portal's functionality.



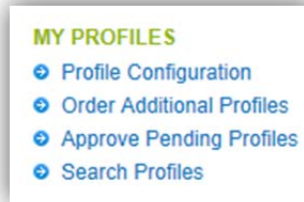
For more detailed step by step instructions on installing the EPKI Administrator certificate, please see our Administrator Certificate Guide <https://www.globalsign.com/support/ordering-guides/epki-authentication-user-guide.pdf>.

ESTABLISHING A PRE-VETTED CERTIFICATE PROFILE

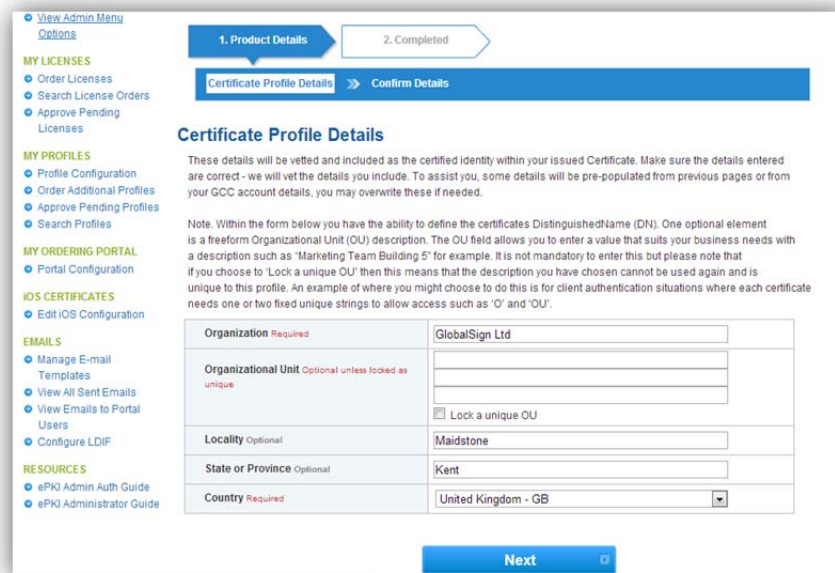
Certificate Profiles will be the content of the Digital Certificate as seen by anyone viewing and relying on the certificate, so it is important to ensure the Profile is accurate and representative of the holder of the certificate. You can create multiple profiles should you have multiple offices or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

The EPKI Managed Service offers you the ability to use pre-vetted identity profiles. Your company identity and your authorization to issue digital certificates, using the requested organization details, will be vetted and verified by third party independent checks performed by GlobalSign. Once the verification is completed, Administrators may then purchase certificate license "packs" against approved certificate profiles, without having to go through the usual individual validation process when you buy a certificate outside the EPKI platform.

Your initial Certificate Profile is established using the **Profile Configuration** link displayed at initial login.



Subsequent Profiles can be added after the initial Profile has been approved by clicking the **Order Additional Profiles** link under the **My Profiles** section in the left panel menu.

A screenshot of a web application showing the "Certificate Profile Details" form. The left sidebar contains a "MY PROFILES" section with a link to "Order Additional Profiles". The main content area has a progress bar at the top with "1. Product Details" (active) and "2. Completed". Below the progress bar are two tabs: "Certificate Profile Details" and "Confirm Details". The form title is "Certificate Profile Details". Below the title is a note: "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." Below this is another note: "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'." The form contains several fields: "Organization Required" (text input with "GlobalSign Ltd"), "Organizational Unit Optional unless locked as unique" (text input), "Locality Optional" (text input with "Maidstone"), "State or Province Optional" (text input with "Kent"), and "Country Required" (dropdown menu with "United Kingdom - GB"). A checkbox labeled "Lock a unique OU" is also present. At the bottom right is a blue "Next" button.

TYPES OF PRE-VETTED IDENTITY PROFILES

Certificate Profiles determine which fields in the end user Digital Certificate will be reflected as fixed values (verified by GlobalSign) or variable for each end user registration. Organization and Country Code are required to be fixed since GlobalSign will verify these values. Providing values for **Organization Unit**, **Locality** and **State** produces constant values for each Digital Certificate issued from the Profile. However, these same fields if left blank will be optional variable fields available to the EPKI Administrator at registration. Common Name and email are variable fields and unique to each application. The end result of a submitted certificate profile is referred to as the Base Distinguished Name (DN). If you wish to secure that a particular Organization and Organization Unit value is never used in another Certificate Profile, select "Lock Unique OU", to "Reserve" the settings as illustrated in Option 3.

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

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

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

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

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

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

OPTION 2: FIXED ORGANIZATION NAME WITH A FIXED ORGANIZATION UNIT

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

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

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

Certificate Identity Details

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

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

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

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

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

Certificate Identity Details

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

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

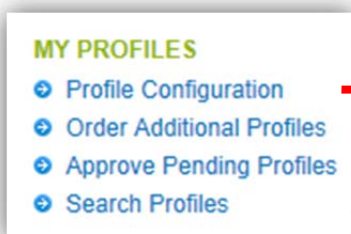
After your Profile has been vetted, you will be able to order certificate licenses that certificate requests can be applied against. Certificate license packs can draw off as many pre-vetted certificate Profiles as you establish.

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

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

ADDITIONAL PROFILE SPECIFIC CONFIGURATION OPTIONS

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



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

Manage Portal

Portal

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=96b2ccc3f7990c9f038099eeb07fe1c76aa3cc3f
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=cbf9e2b08c9021cb29804af0824058500724b2f6

Profile ID	MP200906150035
Organization	GlobalSign Inc.
Organization Unit	staff in charge created profile - authenticated by LRA
URL	https://system.globalsign.com/cr/public/certificate/order.do?p=82f3ec81e9057ad514d0facc801924a3c059d663
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=852e1c9668a0b7b42f72630103dc9b5f903321e0

Profile ID	MP200907210051
Organization	GlobalSign Inc.
Organization Unit	
URL	https://system.globalsign.com/cr/public/certificate/order.do?p=c41a3c480299ac3b833ec93438af9e84b7b2d180

Step 1: Configure Profile

Profile Configuration

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=83d056a9ed3d81665cc0a40f0e2c719ecd441bb
User Permission	Configure
Hash Algorithm	<input checked="" type="radio"/> SHA-1 <input type="radio"/> SHA-256
Encrypting File System	<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
OCSP Option	<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) *.*.*.* e.g) 211.11.149.249,211.11.149.250</small>	<input type="text"/>

Back

Next

1. Encrypted File Systems (EFS): Enabling the EFS option will display EFS as an option at certificate registration.

The resulting certificate will include the enhanced key usage extension Encrypted File System (1.3.6.1.4.1.311.10.3.4).

Certificate

General

Details

Certification Path

Show: <All>

Field	Value
Authority Key Identifier	KeyID=6d c4 2b c1 7d 85 10 a...
Authority Information Access	[1]Authority Info Access: Acc...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Subject Key Identifier	b0 d4 0a 11 55 e8 5b d6 55 c4...
Subject Alternative Name	RFC822 Name=lla.kee@global...
Basic Constraints	Subject Type=End Entity, Pat...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Certificate Policies	[1]Certificate Policy: Policy Ide...

Client Authentication (1.3.6.1.5.5.7.3.2)

Secure Email (1.3.6.1.5.5.7.3.4)

Encrypting File System (1.3.6.1.4.1.311.10.3.4)

Edit Properties...

Copy to File...

Learn more about [certificate details](#)

OK

2. Microsoft (MS) SmartCard Logon: This option is only available to EPKI Pro customers. Please contact your Account Manager for more information.

RENEWAL

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

1. **Manual** (Default setting) – Reminder notice 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** – Reminder notice sent to subscriber at periodic intervals; successful client authentication will automatically generate a renewed certificate.
3. **Quick** – 30 days before certificate expiration active certificate holders are automatically sent an email to immediately install a renewed certificate.

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

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

Profile Configuration

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
User Permission	Configure
Hash Algorithm	<input checked="" type="radio"/> SHA-1 <input type="radio"/> SHA-256
Encrypting File System	<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
OCSP Option	<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) *.*.*.* e.g) 211.11.149.249,211.11.149.250</small>	<input type="text"/>

PURCHASING CERTIFICATE LICENSE PACKS

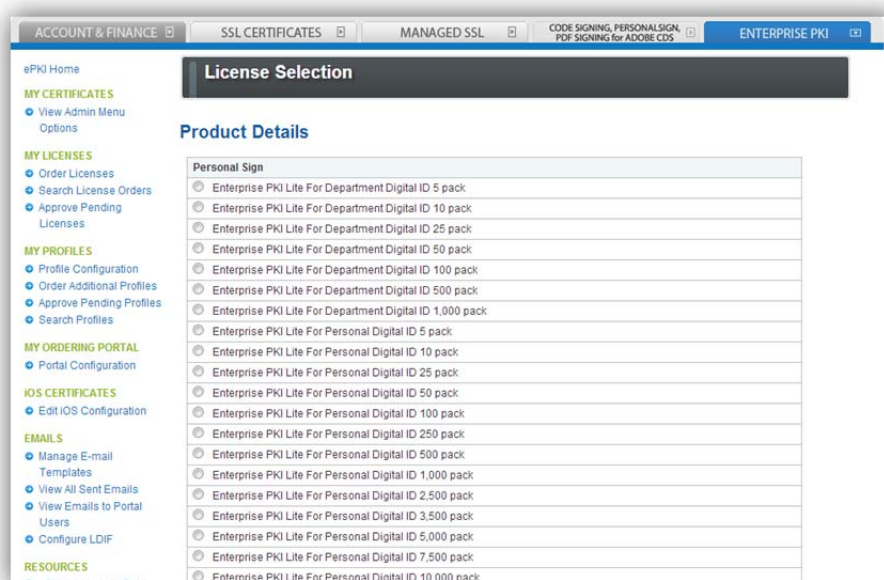
Certificate licenses may be purchased based on several certificate configurations, including:

CERTIFICATE TYPE

- PersonalSign & DepartmentSign for Windows trusted applications. For a detailed product description go to <https://www.globalsign.com/personalsign/>
- PDF Signing for Adobe CDS Personal, Pro & Department. For a detailed product description go to <https://www.globalsign.com/pdf-signing/>

CERTIFICATE PACKS

Depending on the Certificate Type selected above, you may order certificate packs starting from as low as 1 up to and including 1,000. Note that an additional 10% quantity of certificates will be added to address attrition due to employee turn-over. Employees who lose private keys can be provided a re-issuance link to establish a new certificate, the expiry of which is the same as the previous one. Please see the section labeled **Certificate Lifecycle Management – Revocation, Reissuance, and Cancellation**.



CERTIFICATE VALIDITY

Depending on the Certificate types, validities range from 1 to 5 years resulting in significant discounts the longer the validity. Licenses can be purchased by clicking **Order Licenses** found under the **My Licenses** tab.

Select the Certificate validity you wish to apply and click **Next**.

[ePKI Home](#)

License Selection

1. Product Details 2. Completed

Select Product >> Payment >> Confirm Details

Product Details - Enterprise PKI Lite PDF Signing for Adobe CDS Personal - USB 5 pack

Certificate Validity <i>Required</i> Multi-year offers significant per annum savings	<input type="radio"/> 1 year <input checked="" type="radio"/> 2 year <input type="radio"/> 3 year
Campaign Code	<input type="text"/> 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>
Coupon Code	<input type="text"/> 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>
TOTAL COST (inc. Tax)	€ 3,774

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.

[Enter Technical Contact Information](#)

MY CERTIFICATES

- View Admin Menu Options

MY LICENSES

- Order Licenses
- Search License Orders
- Approve Pending Licenses

MY PROFILES

- Profile Configuration
- Order Additional Profiles
- Approve Pending Profiles
- Search Profiles

MY ORDERING PORTAL

- Portal Configuration

IOS CERTIFICATES

- Edit IOS Configuration

EMAILS

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

RESOURCES

- ePKI Admin Auth Guide
- ePKI Administrator Guide

Provide payment by either credit card or Purchase Order pre-arranged with your GlobalSign Account Representative. Select "Payment in arrears" and supply a Purchase Order number if paying by Purchase Order. Otherwise, supply your credit card details as prompted. Please note, you may not order certificates until confirmation of the PO has taken place.

[ePKI Home](#)

License Selection


1. Product Details 2. Completed

Select Product >> Payment >> Confirm Details

Payment Details

Purchase Order Number	<input type="text"/>
Payment Method	<input type="radio"/> Payment in arrears <input checked="" type="radio"/> Credit Card

Credit Card Details & Billing Address



Enter the First Name (or initial) and Last Name exactly as written on your Credit Card.
Enter the card holder's Address, City, Zip/Postal Code, State, and Country as detailed on your Credit Card statement.

First Name or Initials <i>Required</i>	<input type="text"/>
Last Name <i>Required</i>	<input type="text"/>
Card Number <i>Required</i>	<input type="text"/>
Card Expiration Date <i>Required</i>	<input type="text"/> / <input type="text"/> <small>Month / Year (i.e. 01/2014)</small>

MY CERTIFICATES

- View Admin Menu Options

MY LICENSES

- Order Licenses
- Search License Orders
- Approve Pending Licenses

MY PROFILES

- Profile Configuration
- Order Additional Profiles
- Approve Pending Profiles
- Search Profiles

MY ORDERING PORTAL

- Portal Configuration

IOS CERTIFICATES

- Edit IOS Configuration

EMAILS

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

RESOURCES

- ePKI Admin Auth Guide
- ePKI Administrator Guide

Review and confirm the details of your order and then for your first ever order, you will need to accept the EPKI Service Agreement. 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 application is now completed.

CUSTOMIZING EMAIL TEMPLATES

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

The screenshot shows the ePKI Admin console interface. The top navigation bar includes tabs for ACCOUNT & FINANCE, SSL CERTIFICATES, MANAGED SSL, and ENTERPRISE PKI. The left sidebar menu is expanded, showing categories like MY CERTIFICATES, MY LICENSES, MY PROFILES, MY ORDERING PORTAL, IOS CERTIFICATES, and EMAILS. The EMAILS category is highlighted with a red box, and an arrow points to the 'Manage E-mail Templates' option. The main content area is titled 'Edit Mail Template' and contains instructions for customizing email content. Below the instructions is a table with columns for mail type, Delivery, and Contents. Each row in the table has an 'Edit' button next to the Contents column.

mail type	Delivery	Contents
Cancellation Completed	true	Edit
Enrollment(Invite)	true	Edit
Enrollment(Portal)	true	Edit
Enrollment(QUICK RENEW)	true	Edit
Enrollment(Reissue)	true	Edit
Enrollment Information 15 days	true	Edit
Enrollment Information 30 days	true	Edit
Enrollment Information 31 days	true	Edit
Mobile Enrollment(Invite)	true	Edit
Mobile Enrollment(Reissue)	true	Edit
Issuance Completed	true	Edit
PKCS12 Issuance Completed	true	Edit
Mobile Issuance Completed	true	Edit
Cancellation Completed(Not consent)	true	Edit
Portal Order Received	true	Edit

Click **Edit** next to the mail type 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.

REQUESTING CERTIFICATES

There are two main methods of requesting certificates:

1. **End User Initiated** – 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.

The main difference is that in the End User Initiated/Portal Enrollment process end users sets their own pickup password for the enrollment process; whereas with the EPKI Administrator registration process, the Administrator must ensure that the pickup password is provided securely to the end user.

USING THE PORTAL LINK

The EPKI Managed Service offers the ability for organizations with distributed 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 make 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 URL link is provided to support both local and GlobalSign Server key generation that you can find by clicking **Portal Configuration** under the **My Ordering Portal** 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	https://system.globalsign.com/cr/public/certificate/order.do?p=96b2ccc3f7990c9f038099eeb07fe1c76aa3cc3f
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=cbf9e2b08c9021cb29804af0824058500724b2f6

Profile ID	MP200906150035
Organization	GlobalSign Inc.
Organization Unit	staff in charge created profile - authenticated by LRA
URL	https://system.globalsign.com/cr/public/certificate/order.do?p=82f3ec81e9057ad514d0facc801924a3c059d663
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=852e1c9668a0b7b4272630103dc9b5f903321e0

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

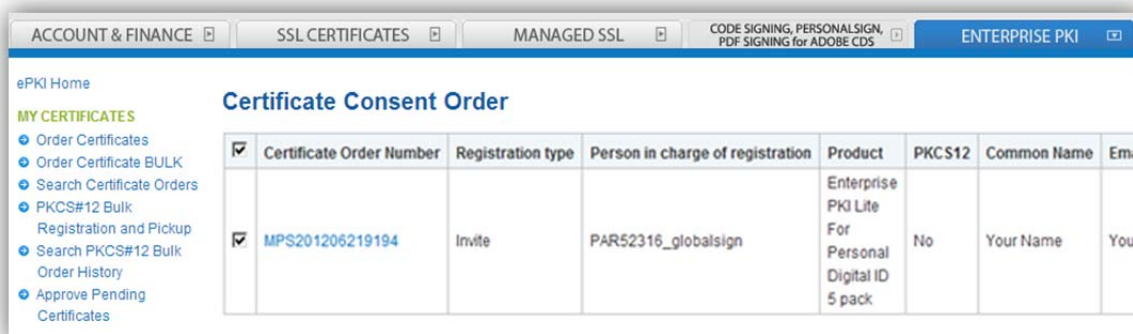
Logo GIF	<div> <div>Choose File</div> <div>No file chosen</div> <div>Upload</div> </div> <div> Recommended size 176x37 pixel The maximum capacity 2MB Valid image types jpg,gif,png </div>
Footer GIF	<div> <div>Choose File</div> <div>No file chosen</div> <div>Upload</div> </div> <div> Recommended size 950x7 pixel The maximum capacity 2MB Valid image types jpg,gif,png </div>

Other Portal Configurable Options:

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

APPROVING REQUESTS (ORDERS)

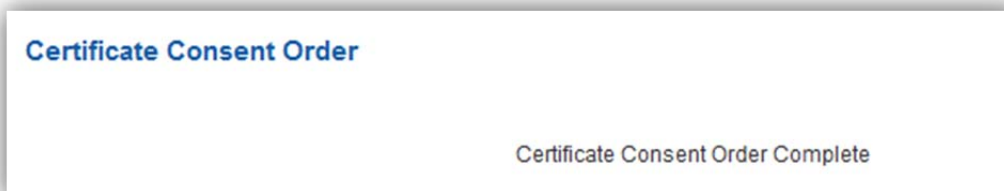
Applications made by Users / Departments using the Portal must be approved by an EPKI Administrator. When such applications are made, an email alert will be sent to the EPKI Administrator(s) and the appropriate Administrator must log into the account and click the **Approve Pending Certificates** link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



The screenshot shows the ePKI Home portal with a navigation menu on the left and a main content area titled 'Certificate Consent Order'. The navigation menu includes 'MY CERTIFICATES' with sub-links: '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 main content area displays a table with the following data:

<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.

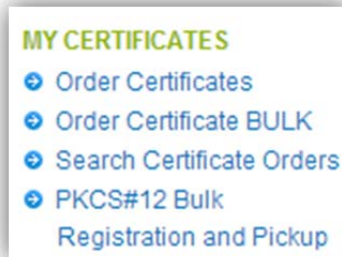


REGISTER USERS VIA EPKI ADMINISTRATOR

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

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

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



SINGLE USER REGISTRATION

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

Product Selection

1. Product Details 2. Completed

Select Profile >> Certificate Identity Details >> Confirm Details

Product Details

Profile

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

License

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

Next

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

Optionally, the EPKI Administrator may select alternative certificate enrollment methods to the default PKCS7 method where key generation is performed locally via the Subscriber's browser.

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

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

Option certificate delivery method - Select only 1

I have an externally generated CSR Check only if you are an Advanced User and have an externally generated Certificate Signing Request (CSR)	<input type="checkbox"/>
PKCS12 Option	<input type="checkbox"/>
Pickup Password Required	<input type="password"/> <small>Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9)</small> Password Generation <input type="button" value="Generate"/> <small>When the password automatic operation generation button is pressed, a random password automatic construction is set.</small>
Pickup Password (re-enter) Required	<input type="password"/>
Memo	<input type="text"/>

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

1. Product Details 2. Completed

Select Profile → Certificate Identity Details → **Confirm Details**

Confirm Details

Product Details

Profile ID	MP201306201386
License ID	ML201306201386

Certificate Identity Details

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

1. Product Details 2. Completed

Application Completed

Application Completed

Order Number	MP32013062110030
--------------	------------------

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

BULK ENROLLMENT

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

The screenshot shows a 'Product Selection' window. At the top, a progress bar indicates '1. Product Details' is active and '2. Completed' is finished. Below this is a breadcrumb trail: 'Product Details >> File specification >> Edit Details >> Confirm Details'. The main section is titled 'Product Details' and contains two tables. The first table, labeled 'Profile', has columns for Profile ID, BaseDN, Organization, and Organization Unit. The second table, labeled 'License', has columns for Service and License Unused number. A 'Next' button is at the bottom right.

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

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

Next

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

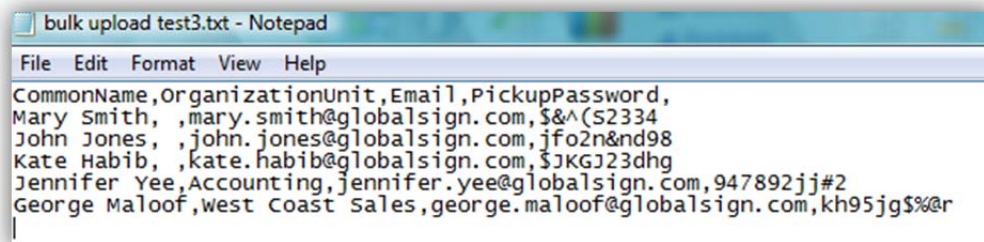
The screenshot shows a screen for uploading a CSV file. It features a table with columns 'Item', 'Explanation', and 'Limitation'. Below the table is a 'CSV file' section with a 'Choose File' button, the text 'No file chosen', and an 'Upload' button. At the bottom are 'Back' and 'Next' buttons.

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

CSV file No file chosen

Back Next

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



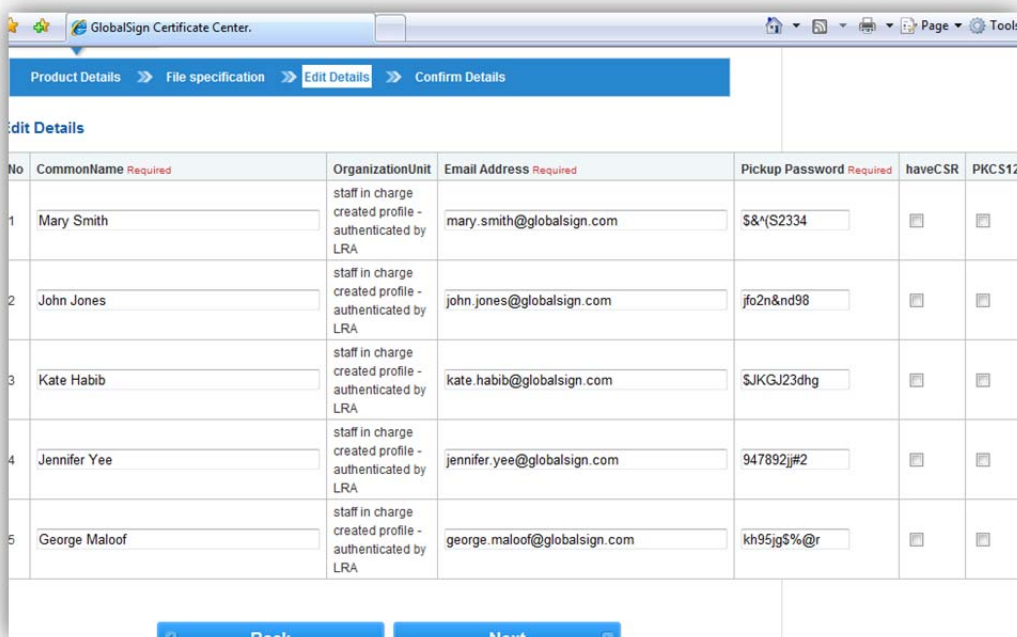
```

CommonName,OrganizationUnit,Email,PickupPassword,
Mary Smith, ,mary.smith@globalsign.com,$&^(S2334
John Jones, ,john.jones@globalsign.com,jfo2n&nd98
Kate Habib, ,kate.habib@globalsign.com,$JKGJ23dhg
Jennifer Yee,Accounting,jennifer.yee@globalsign.com,947892jj#2
George Maloof,west coast sales,george.maloof@globalsign.com,kh95jg$%@r

```

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

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



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

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

BULK PROVISIONING (PKCS#12)

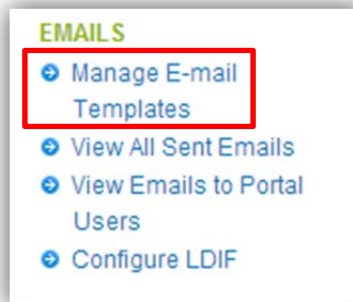
Bulk provisioning provides an alternative to bulk enrollment in that the enrollment steps performed by the end user are minimized or in some cases totally eliminated. The bulk provisioning feature provides the following benefits:

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

NOTE: Per recent policy change, Bulk PKCS12 registration option will only support user registrations that do not include email address in the certificate subject name. Therefore this feature should not be associated with “local key recovery” or S/MIME since email will not be supported. This option should be positioned for Organizations that wish to bypass end user direct registration using emails / web pages from GCC-EPKI. (e.g. Network access, Microsoft Office Document signing).

BEFORE YOU BEGIN

1. There is a 200 record limit (3.2M) and depending on key size selected, the ZipFile containing PKCS12s may take up to 40 minutes to process.
2. Disable all renewal messages to prevent system generated email reminders from going directly to your end user. You can do this by:
 - a. Disable Renewal reminder emails by logging into EPKI and clicking on **Manage E-mail Templates**



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

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

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

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

- d. Click “Next” and then “Complete”.

HOW TO

1. Start by going to PKCS#12 BULK Registration and Pickup
2. Select the Profile and License pack and click **Next**

Product Selection

1. Product Details

2. Completed

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

Product Details

Profile

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

License

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

Next

3. Browse and Upload CSV formatted based on Profile selection. Note the csv file format guidance will be based on the Profile settings associated with the selected profile. Please note, even if the Profile includes email, email will not be included as a field.

Product Selection

1. Product Details

2. Completed

Product Details

File specification

Edit Details

Confirm Details

File format

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

```
CommonName ,OrganizationUnit2 ,OrganizationUnit3 ,PickupPassword
Kate Jones , ,9o7t9ghsa3YZ
Jennifer Jones ,Jennifer Jones ,Research and Dev ,9o7t9ghsa3YZ
George Jones ,Accounting ,9o7t9ghsa3YZ
```

CSV file

Choose File

No file chosen

Upload

Back

Next

4. Review the certificate details pulled from the csv file and make any changes as necessary. Again, note email is no longer an option. Click “Next” to continue.

Edit Details

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

5. Certificate generation is complete.

Product Selection

1. Product Details

2. Completed

Completed

Certificate issue batch application

PKCS#12 Order ID	MPB201306240721
------------------	-----------------

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

6. After confirmation, a Zipfile containing the PKCS12 files can be found in the “PKCS#12 Bulk order history Report” found on the left pane. Click on the link and search for Order ID then click, “Download”. The Zip file will be purged from your EPKI portal 1 month after creation, therefore it is important to download the file prior to 30 days after creation. 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).

CERTIFICATE LIFECYCLE MANAGEMENT – REVOCATION, REISSUANCE, AND CANCELLATION

To revoke, cancel or reissue the certificate, please go in the left menu to the **Search Certificate Orders** link under **My Certificates**. Search for the order you wish to access, like you would do for the reports. Click on the **Application** button next to the order you wish to select.

Various application	Certificate Order Number	Organization Name	Common Name	Product	Period	Email Address	Person in charge of registration	Order Status	Certificate Status	Date of application
Application	MPS2013062118838	GMO GlobalSign Ltd	YourName	Enterprise PKI Lite For Personal Digital ID 10 pack	2 year	your.email@yourcompany.com	PAR89496_SGMidg2013	ISSUE_WAIT	NONE	06/21/2013 16:41(GMT+00:00)

At the bottom of the report, you can choose to revoke, cancel or reissue the certificate.

Certificate action information

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

Revoke Certificate

cancellation request

Reissue Certificate

Mail History

Notes:

1. Revoked certificates will be put on the Certificate Revocation List within 24 hours, making the certificate unusable by most applications.
2. Cancellations are allowed up to 7 days of certificate delivery.
3. Reissued certificates will be issued with an expiration date equal to the original certificate. Note a new private key will be generated, therefore, a replacement certificate will not allow decryption of the emails that were encrypted using the original certificate.

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

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

REPORTING

EPKI Administrators can manage the full lifecycle of Digital Certificates issued from their service. Locating a particular order/certificate is easy. Start by clicking on the **Search Certificate Orders** link found under the **My Certificates** header. Click on **Show Advanced Search** and search by order, date, product etc.

ePKI Home

MY CERTIFICATES

Order Certificates

Order Certificate BULK

Search Certificate Orders

PKCS#12 Bulk

Registration and Pickup

Search PKCS#12 Bulk

Order History

Approve Pending Certificates

MY LICENSES

Order Licenses

Search License Orders

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

Any Order State

Any Certificate Status

Profile ID...

License ID...

User in Charge...

Organization Unit...

Email address...

Search

Display Number: 10

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

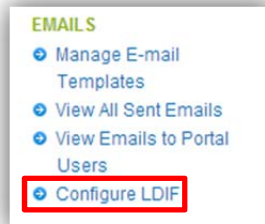
Various application	Certificate Order Number	Organization Name	Common Name	Product	Period	Email Address	Person in charge of registration	Order Status	Certificate Status	Date of application
Application	MPS2013062118838	GMO GlobalSign Ltd	YourName	Enterprise PKI Lite For Personal Digital ID 10 pack	2 year	your.email@yourcompany.com	PAR89496_SGMldg2013	ISSUE_WAIT	NONE	06/21/2013 16:41(GMT+00:00)

LDIF

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

CONFIGURING LDIF

LDIF reports can be formatted by the EPKI Administrator via the **Configure LDIF** link found under **Emails**.



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

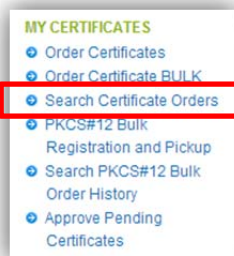
Please note the initial LDIF default format has been established by GlobalSign. The EPKI Administrator must modify the LDIF Template based on the "Profile" the LDIF query will run against. You can reset the format back to the default values anytime by clicking **Reset Message** as illustrated below.

Reset Message

Header	#LDIF made by GlobalSign GCC	<div style="border: 1px solid #ccc; padding: 2px;"> 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 </div>
Message	<pre>dn: CN=\${Dn!CommonName},CN=Users,DC=edit here changetype: modify replace: userCertificate userCertificate:: \${Certificate!Pem} -</pre>	
Footer		

GENERATING A LDIF REPORT

LDIF reports are generated from the **Search Certificate Orders** link.



Select the appropriate date range, Profile (if you have more than 1) and set “Order State = 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

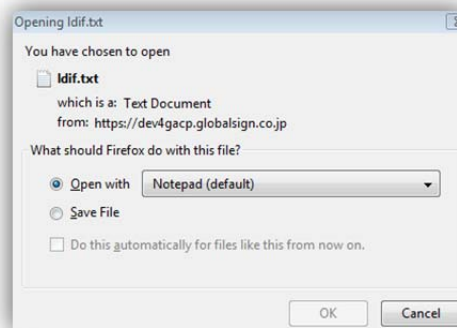
Profile ID... License ID... User in Charge...

Organization Unit... Email address...

Display Number:

1 - 3 / 3

Open the file with your prefer application.



Below is an example entry.

```

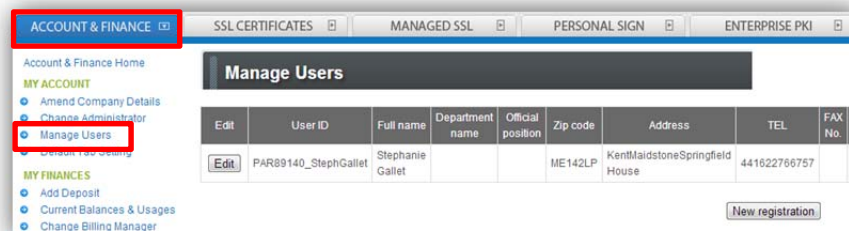
Idif - Notepad
File Edit Format View Help
#LDIF made by GlobalSign GCC
#dn: dc=input here , dc=input here
#objectclass: top
#objectclass: pkiuser
#objectclass: person
usercertificate;binary:: MIIFNTCCBB2gAwIBAgILAQAAAAABJRZs jkMwDQYJKoZIh
AQUFBZACHjpodHRwoi8vc2VjdXJlLmdsb2JhbHNpZ24ubmV0L2Nhy2vydC9QZXJzb25hbF
mail: lila.kee@globalsign.com
CN: LDIF 3b
O: GlobalSign Inc.
OU: 2nd admin new profile - authenticated by LRA
ST: MA
L: newton
C: US

```

Upload to LDAP directory according to your product specific instructions.

ESTABLISHING OTHER EPKI USERS

A list of active EPKI Users can be found by selecting the **Account & Finance** tab, then clicking **Manage Users** under **My Account**. This is also where new users can be added.



Note, all EPKI Users have equal access to established profiles and certificate licenses, however, user rights depend on the role established. There are three main User Roles:

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

TYPES OF EPKI 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 administrators and establish certificate profiles and approve orders if the GCC Administrator has set the **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.

In the “**Search Certificates Orders**” section, you can see who the Administrator associated with the user registration is under the “Person in charge of registration” heading.

REGISTERING ADDITIONAL USERS

To create either “Managers” or “Staff in charge”, select the **Account & Finance** tab, then select **Manage Users** under **My Account**. 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 filling-up the required fields, including user information and user type – either “Manager” or “Staff in charge”. Set **Certificate Approval Permission** to **True** if you wish the “Manager” to have certificate approval and profile creation rights. “Staff in charge” is unable to approve certificates or establish new profiles. Ignore settings related to **Deposit purchase authority**.

SSL CERTIFICATES MANAGED SSL PERSONAL SIGN ENTERPRISE PKI

New user registration page

■ User ID	PAR89140_
■ Password	<small>Enter under 10 characters.</small>
■ Password(confirmation)	
■ Organization Name	<small>e.g. GlobalSign Inc.</small>
■ Department	<small>e.g. Marketing</small>
■ First Name	
■ Middle Name	
■ Last Name	
■ Job Title	<small>e.g. Web Administrator</small>
■ Street Address 1	<small>e.g. Trust International Drive</small>

■ Street Address 2	<small>e.g. Suite 330</small>
■ City	<small>e.g. Portsmouth</small>
■ State or County	<small>e.g. New Hampshire</small>
■ Zip Code / Postal Code	<small>e.g. 03801</small>
■ Country	Germany
■ Other address info	
■ Telephone (inc. region code)	<small>e.g. +44 (0) 1622 766766</small>
■ Fax (inc. region code)	<small>e.g. +44 (0) 1622 662255</small>
■ Email Address	<small>Please be careful when providing email address</small>
■ 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 type="radio"/> true <input checked="" type="radio"/> false

Back Confirm

ADMINISTRATION DELEGATION

Shared administration can be established. 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/certificateorder.do?pn=96b2ccc3f7990c9f038099eeb07fe1c76aa3cc3f
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificateorder.do?pn=cbf9e2b08c9021cb29804af0824058500724b29b
User Permission	Configure
Hash Algorithm	<input checked="" type="radio"/> SHA-1 <input type="radio"/> SHA-256
Encrypting File System	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
MS SmartCard Logon	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Renewal Type	<input type="radio"/> Manual <input checked="" type="radio"/> Auto <input type="radio"/> Quick
Non Exportable Option <small>Limited to only Internet Explorer.</small>	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
API IP Address range <small>(IP Address is limited to only at the time of API e.g. "1.1.1.1" - e.g.) 211.11.148.248, 211.11.148.250</small>	<input type="text"/>

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

You can now select the permissions you wish to give to each user, providing 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	Rebackup 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](#)

Tick off the box next to the User ID that you wish to extend full administrative rights across all profiles established. Extended rights allow the User to view, approve and revoke certificates initiated by any other User with either Staff or Manager rights for a given PAR (account). You can now 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 and technical queries you may have about the EPKI service. GlobalSign also provides technical support through our Client Service departments around the world.

www.globalsign.com/support/

GlobalSign urges 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 www.globalsign.com/help/.

GLOBALSIGN CONTACT INFORMATION

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