



GlobalSign Enterprise Solutions
Managing PersonalSign and DocumentSign Certificates
Across Your Organization Effectively

GlobalSign Enterprise Solution ePKI Administrator guide v1.9

TABLE OF CONTENTS

Getting Started:.....	4
Logging into your GlobalSign Certificate Center (GCC) Account:	4
Establishing ePKI service	5
Establishing your initial ePKI Service.....	6
Establishing a Pre-Vetted Certificate Profile.....	6
Types of Pre-Vetted Identity Profiles.....	7
Option 1: Fixed Organization Name with an Optional Variable Organization Unit	7
Option 2: Fixed Organization Name with a Fixed Organization Unit.....	8
Option 3: Fixed Organization Name with a Fixed “RESERVED*” Organization Unit in the Base Distinguished Name (DN).....	9
Additional Profile specific configuration options.....	10
Purchasing Certificate License Packs	13
Certificate type:	13
Certificate Packs:.....	13
Certificate Validity:.....	13
CUSTOMIZING EMAIL TEMPLATES.....	15
Renewal:	16
Requesting Certificates:	17
Using the Portal Link	17
Approving Requests (Orders).....	20
Register Users via ePKI Administrator	21
Bulk Enrollment.....	25
End user Installation	28
Bulk Provisioning.....	31
Reporting	40
LDIF	42
Configuring LDIF.....	42
Generating a LDIF Report.....	44
Certificate Life-cycle Management – Revocation, Reissuance, and Cancelation	46
Establishing other ePKI Administrators	47

GCC Account Administrators	47
Manager	47
Staff in Charge	47
Registering additional Administrators	48
Administration Delegation	49
Getting Help	50
GlobalSign Contact Information:	51

Getting Started:

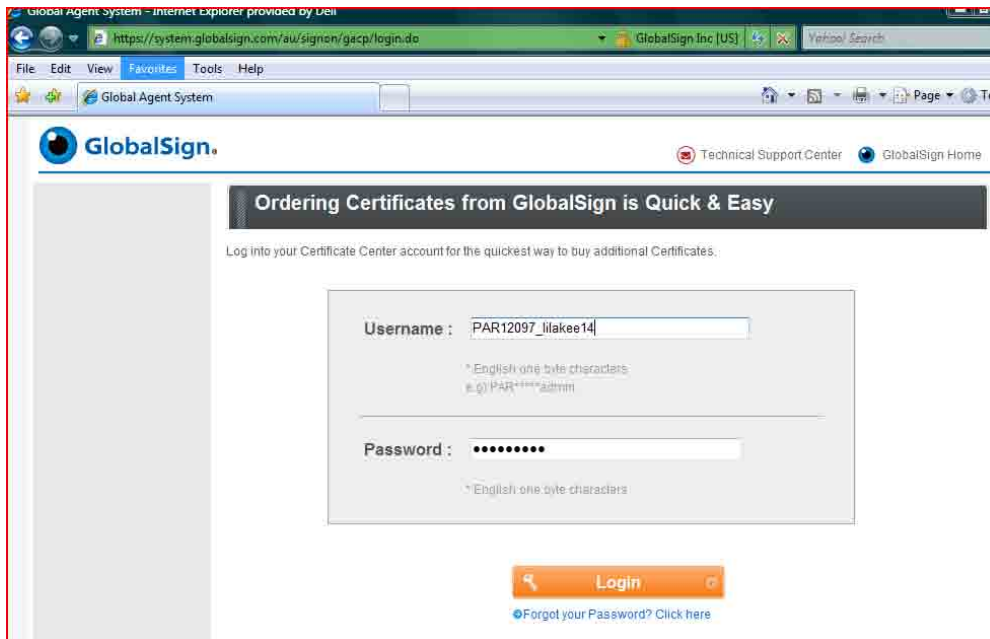
Logging into your GlobalSign Certificate Center (GCC) Account:

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 DocumentSign Pro Certificates.

Go to www.globalsign.com and click "Certificate Center LOGIN".



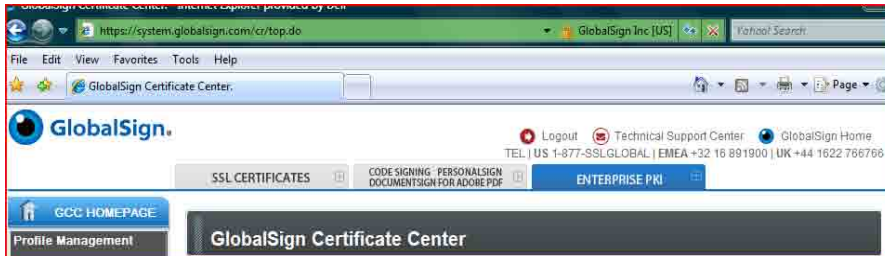
Enter your **User ID** and **Password**. Your User ID is the *PARXXXX_xxxxx* number given to you at the end of the GCC signup process, you can also find it in your Welcome Email. Your Password is the password you entered during the signup process.

A screenshot of the GlobalSign Certificate Center login page. The page title is "Ordering Certificates from GlobalSign is Quick & Easy". Below the title, there is a message: "Log into your Certificate Center account for the quickest way to buy additional Certificates." The login form contains two input fields: "Username" with the value "PAR12097_lilakee14" and "Password" with masked characters. Below the password field, there is a "Forgot your Password? Click here" link. At the bottom of the form is an orange "Login" button.

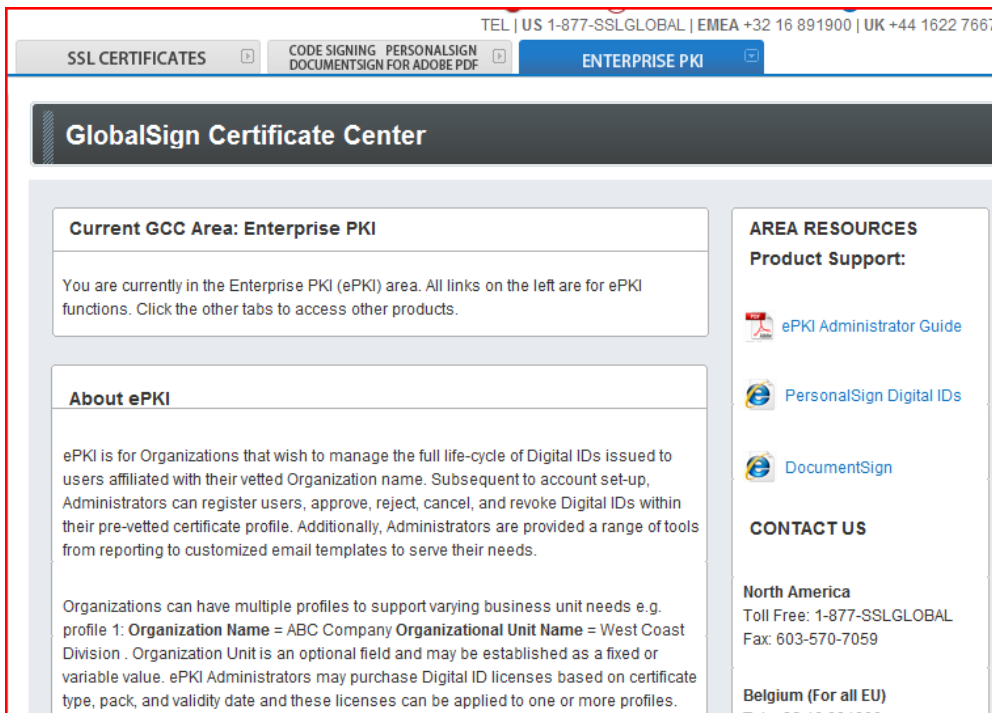
If you have difficulties logging in or forget your password please contact Support at www.globalsign.com/support



Establishing ePKI service

After successfully logging in, you will enter the GCC home page that will provide three certificate ordering options. Select the upper tab labeled “ENTERPRISE PKI”.



You will arrive on the ePKI home page. All functions are accessed through the left hand menu system:



type, pack, and validity date and these licenses can be applied to one or more profiles.	Belgium (For all EU) Tel: +32 16 891900 Fax: +32 16 891909
Certificate Types available through ePKI	United Kingdom Tel: +44 1622 766766 Fax: +44 1622 235590 Create Support Ticket
 PersonalSign - Digital IDs for secure email, authentication and digital signatures for Microsoft Office Documents. More product info...	
 DocumentSign for Adobe PDF (Adobe Certified Document Services) - Enable more secure, reliable electronic document exchange by digitally signing / certifying Adobe PDF documents. More product info...	

Establishing your initial ePKI Service

Note for first time users. You will have limited functionality displayed in the left pane. A full menu of certificate management options will be displayed after an initial license has been ordered and Certificate Profile(s) have been established. To establish your first license and Profile, click on the “Profile/License Order” link found on the left menu pane under “Profile Management”

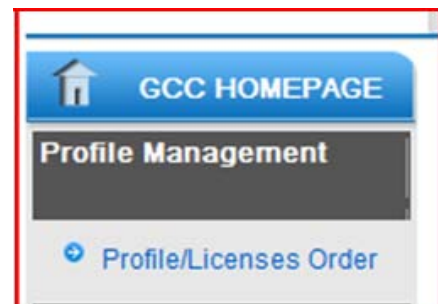
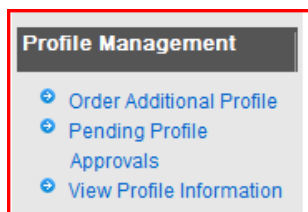
Certificate Profiles will be the content of the Digital ID as seen by anyone viewing and relying on the certificate, so it’s important to ensure the Profile is accurate and representative of the holder of the certificate. Accuracy is also essential because GlobalSign will validate and verify the Organizational details as prescribed by the governing Certificate Practice Statement (CPS). Once vetted the ePKI Administrator can select a vetted profile when creating and approving certificate requests. You can create multiple profiles should you have multiple offices or multiple parent subsidiary companies that you require certificates for through a single account.



Establishing a Pre-Vetted Certificate Profile

The ePKI Managed Service offers you the ability to use pre-vetted identity profiles to greatly accelerate the issuance of client certificates to users affiliated with your organization or subsidiary organizations. 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. Certificates can be issued from available certificate license balances that will be adjusted as certificates are drawn from the service.

Your initial Certificate Profile is established using the “Profile/Licenses Order” link displayed at initial login.



Subsequent Profiles can be added after the initial Profile has been approved by clicking the “Order Additional Profile” link under “Profile Management” found in the left pane menu.

Certificate Profile Details

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

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

Organization <small>Required</small>	GlobalSign Inc.
Organizational Unit <small>Optional unless locked as unique</small>	
Lock a unique OU	<input type="checkbox"/> Check this box if the Certificate DistinguishedName (DN) needs to have a fixed and unique Organizational Unit (OU)
Locality	Portsmouth
State or Province	NH
Country <small>Required</small>	United States

[Next](#)

Types of Pre-Vetted Identity Profiles

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

Certificate Profiles determine which fields in the end user digital ID 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 ID issued from the Profile. However, these same fields if left blank will be optional variable fields available to the ePKI Administrator at Digital ID registration. Common Name and email are variable fields and unique to each Digital ID 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..

- **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 option1:

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 <i>Required</i>	<input type="text"/>
Organization	GlobalSign
Organizational Unit	West Coast Sales - authenticated by LRA
Locality	Portsmouth
State or Province	NH
Country	United States
Email Address <i>Required</i>	<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 option3:

Certificate Identity Details

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

The screenshot shows the 'Manage Portal' interface. On the left is a sidebar menu under 'Account Management' with options: Amend Company Details, Manage Users, Change Administrator, Change Billing Manager, Manage E-mail Templates, Manage Portal, Profile Configuration (highlighted with a mouse cursor), Manage LDIF, and Administrator Delegation. The main area shows a list of profiles under the 'Portal' heading. Each profile entry includes fields for Profile ID, Organization, Organization Unit, URL, and URL(PKCS12 Option).

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=852e1c9668a0b7b42f2630103dc9b5f903321e0
Profile ID	MP200907210051
Organization	GlobalSign Inc.
Organization Unit	
URL	https://system.globalsign.com/cr/public/certificate/order.do?p=c41a3c480299ac3b833ec93438af9e84b7b2d180

Select the Profile and Click “Next” to configure the following additional options:

The screenshot shows the 'Profile Configuration' screen. It contains a table with the same profile information as the previous screenshot. Below the table are three configuration options, each with a radio button and a label:

- PKCS12 Key Length *Required*: 1024 Bit 2048 Bit
- Encrypting File System *Required*: No Yes
- MS SmartCard Logon *Required*: No Yes

At the bottom of the screen are two buttons: 'Back' and 'Next'.

1. PKCS12 Key size restriction- In the event you wish GlobalSign to create the public and private keys on behalf of the subscriber, a 1024 or 2048 (recommended) key size restriction can be established

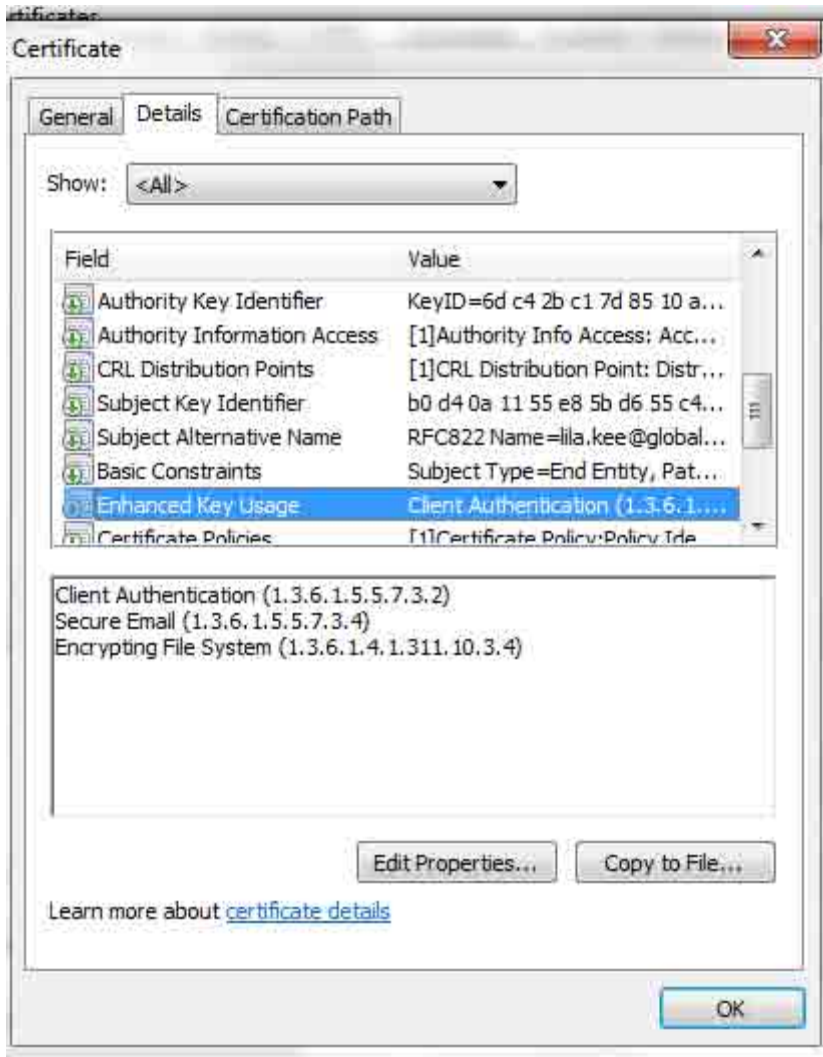
2. Encrypted File Systems (EFS): Selecting the EFS option will display EFS as an option at certificate registration

3. MS SmartCard: Selecting the MS SmartCard logon option will display a field at certificate registration that should be populated with the User Principal Name (UPN).

Certificate Identity Details

Common Name <small>Required</small>	EFS Test
Organization	GlobalSign Inc.
Organizational Unit	Test Account - Do not rely upon - authenticated by LRA
Locality	Portsmouth
State or Province	NH
Country	United States - US
Email Address <small>Required</small>	lila.kee@globalsign.com
Encrypting File System	<input checked="" type="checkbox"/>

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

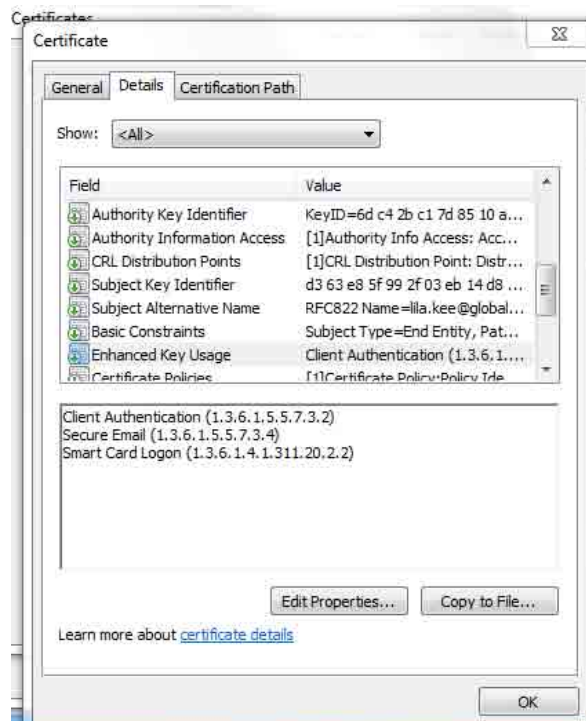
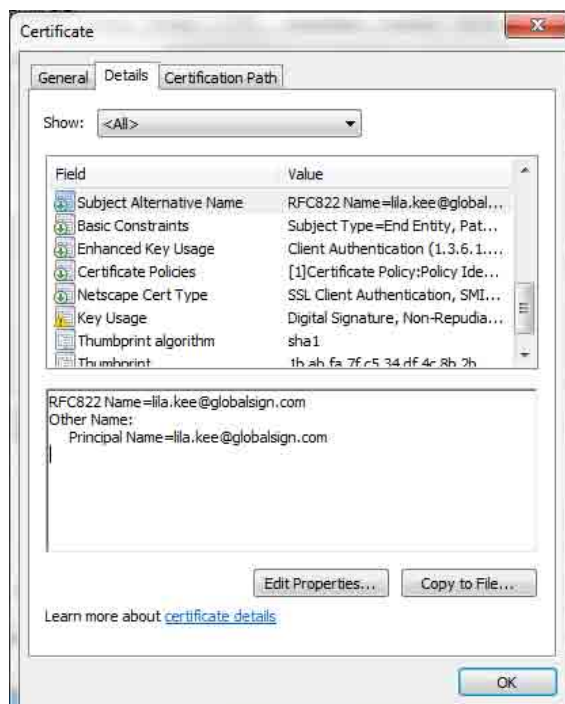


3. **Microsoft (MS) SmartCard logon:** Selecting the MS SmartCard logon option will display a field at certificate registration that should be populated with the User Principal Name (UPN). Often this is the email address of the Subscriber, but in some cases it may not. Note you may optionally select both EFS and MS SmartCard Options for a given profile:

Certificate Identity Details

Common Name <i>Required</i>	MS Log in and EFS
Organization	GlobalSign Inc.
Organizational Unit	Test Account - Do not rely upon - authenticated by LRA
Locality	Portsmouth
State or Province	NH
Country	United States - US
Email Address <i>Required</i>	lila.kee@globalsign.com
Encrypting File System	<input type="checkbox"/>
MS SmartCard Logon	lila.kee@globalsign.com

The resulting certificate would include the Smart Card Logon (1.3.6.1.4.1.311.20.2.2) extended key usage and the User Principal Name in the Subject Alternative name extension as required by Microsoft: KB814394 (<http://support.microsoft.com/kb/814394>)



Purchasing Certificate License Packs

Certificate licenses may be purchased based on several certificate configurations including

Certificate type:

- PersonalSign for Windows trusted applications. • For a detailed product description go to http://www.globalsign.com/digital_certificate/personalsign/personalsign2-pro.htm
- DepartmentSign for Windows trusted applications. For a detailed product description go to http://www.globalsign.com/digital_certificate/personalsign/personalsign2-department.htm
- DocumentSign PersonalSign for Adobe Trusted documents. For a detailed product description go to <http://www.globalsign.com/document-security/adobe-cds/index.htm>
- DocumentSign DepartmentSign for Adobe Trusted documents. For a detailed product description go to <http://www.globalsign.com/document-security/adobe-cds/index.htm>

Certificate Packs:

- Depending on the Certificate Type selected above, you may order certificate packs starting from as low as “5 ” 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 Life-cycle 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 Additional licenses” found under the “License Management” tab.

The screenshot displays the GlobalSign web application interface. The browser window shows the URL 'GlobalSign Certificate ...'. The page header includes the GlobalSign logo, a navigation menu with 'SSL CERTIFICATES', 'CODE SIGNING PERSONAL SIGN DOCUMENT SIGN FOR ADOBE PDF', and 'ENTERPRISE PKI'. The main content area is titled 'License Selection' and features a '1. Product Details' step indicator and a 'Select Product' button. Below this, the 'Product Details' section lists various 'Personal Sign' license packs, including 'Enterprise PKI Lite For Personal Digital ID 10 pack' through 'Enterprise PKI Lite For Department Digital ID 25 pack'.

Product Details
Personal Sign
Enterprise PKI Lite For Personal Digital ID 10 pack
Enterprise PKI Lite For Personal Digital ID 25 pack
Enterprise PKI Lite For Personal Digital ID 50 pack
Enterprise PKI Lite For Personal Digital ID 100 pack
Enterprise PKI Lite For Personal Digital ID 250 pack
Enterprise PKI Lite For Personal Digital ID 500 pack
Enterprise PKI Lite For Personal Digital ID 1,000 pack
Enterprise PKI Lite For Department Digital ID 5 pack
Enterprise PKI Lite For Department Digital ID 10 pack
Enterprise PKI Lite For Department Digital ID 25 pack

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

The screenshot shows the GlobalSign Certificate Center interface in Internet Explorer. The browser address bar displays <https://system.globalsign.com/cr/profile/license/neworder.do>. The page title is "GlobalSign Certificate Center." The main navigation menu includes "GCC HOMEPAGE", "Profile Management" (with sub-items: Profile/Licenses Order), "Account Management" (with sub-items: Amend Company Details, Manage Users, Change Administrator, Change Billing Manager, Manage E-mail Templates, Manage Portal), "Financial Management" (with sub-items: View/Request Invoices, View Statements), and "Useful Function" (with sub-items: View All Sent Emails, View All Emails Sent to Portal Users, Get Technical Support).

The main content area is titled "Profile/License Selection" and shows a progress bar with two steps: "1. Product Details" (active) and "2. Completed". Below the progress bar is a breadcrumb trail: "Select Product >> Product Details >> Certificate Identity Details >> Payment >> Confirm Details".

The "Payment Details" section contains a form with the following fields:

Purchase Order Number	12345 <small>Enter if you have a PO Number. This will be displayed in your invoice.</small>
Payment Method	<input checked="" type="radio"/> Payment in arrears <input type="radio"/> Credit Card

Below this is the "Credit Card Details & Billing Address" section, which includes logos for VISA, MasterCard, and AMERICAN EXPRESS. It contains the following instructions and form fields:

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 <small>Required</small>	<input type="text"/>
Last Name <small>Required</small>	<input type="text"/>
Card Type <small>Required</small>	<input checked="" type="radio"/> VISA <input type="radio"/> MasterCard

Review and confirm your order and then Accept ePKI Service Agreement. Note the ePKI Service Agreement binds you to Local Registration Authority and other obligations as outlined in the GlobalSign Certificate Practice Statements found at <http://www.globalsign.com/repository/index.htm> .

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 Email” found under the “Account Management” menu.

The edit and the delivery setting are good at the content of mail.

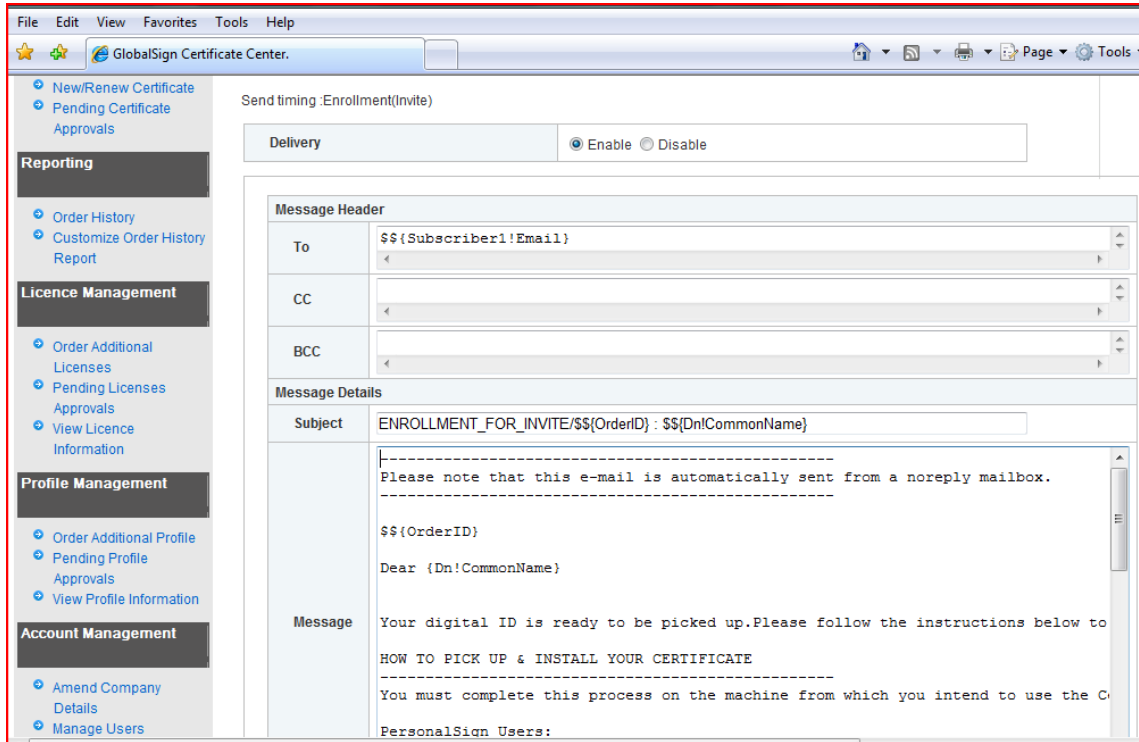
To customize email content:Please click contents "Edit" button.
Subject/address/main body of the message of the mail to be changed can be edited.

Enable and Disable: When "Enable" is selected, the automatic mail sending is done.
Please select "Disable" to stop the auto dialing of an unnecessary mail type to send.

mail type	Delivery	Contents
Cancellation Completed	true	Edit
Enrollment(Invite)	true	Edit
Enrollment(Portal)	true	Edit
Enrollment Information 15 days	true	Edit
Enrollment Information 30 days	true	Edit
Enrollment Information 31 days	true	Edit
Issuance Completed	true	Edit
Cancellation Completed(Not consent)	true	Edit

Click “Edit” next to the mail type you wish to customize. Then add additional email address 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 e-mail is sent out. They should not be modified, as they contain necessary information to complete the intended action.



Renewal:

There are two 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.

Periodic reminder settings can be enabled or disabled in the “Manage Email Template” link found under “Account Management”. In either case, renewed certificates will include the identical identity information included in the original certificate. Please note, sufficient certificate inventory must be available for the order to successful be completed.

To enable Automatic Renewal, go to “Profile Configuration” and select “yes” next to the “Auto Renewal Option”.

Profile Configuration

Profile ID	MP201006170458
Organization	Lila June 16 2010 test
Organization Unit	
URL	https://gas-eval1.globalsign.com:10001/cr/public/certificate/order.do?p=73a623803075f4d76026d8ceecfa0f3988ed2310
URL(PKCS12 Option)	https://gas-eval1.globalsign.com:10001/cr/public/certificate/order.do?p=f4de97780bb491f3d157cf9f8cc57fa3d896dc8f
PKCS12 Key Length <small>Required</small>	<input checked="" type="radio"/> 1024 Bit <input type="radio"/> 2048 Bit
Encrypting File System <small>Required</small>	<input checked="" type="radio"/> No <input type="radio"/> Yes
MS SmartCard Logon <small>Required</small>	<input checked="" type="radio"/> No <input type="radio"/> Yes
Auto Renewal Option <small>Required</small>	<input checked="" type="radio"/> No <input type="radio"/> Yes
Non Exportable Option <small>Required</small> <small>Limited to only Internet Explorer.</small>	<input checked="" type="radio"/> No <input type="radio"/> Yes

 Back
 Next

Requesting Certificates:

There are three main methods to 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 registers a user via the GCC ePKI Portal.

The main difference is that in the Portal enrolment process the end user sets their own pickup password for the enrollment process, where as with the Administrator registration process, the Administrator must ensure that the pickup password is provided securely to the end user.

Using the Portal Link

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. 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=852e1c9668a0b7b42f72630103dc9b5f903321e0

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

Portal	
Profile ID	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
Logo GIF	mark_basic_l.jpg <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/> Recommended size 176x37 pixel The maximum capacity 2MB Valid image types jpg,gif,png
Footer GIF	mark_horizon_l.jpg <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/> Recommended size 950x7 pixel The maximum capacity 2MB Valid image types jpg,gif,png
Title Required	GlobalSign Digital Certificates

Other Portal Configurable Options:

1. **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 Subscriber Agreement and prompted to accept the terms prior to certificate installation.
2. **Enforcing Key Size:** If you decide to have users enroll via the Portal with the PKCS12 approach where GlobalSign Servers create the public/private key and send the PKCS12 container password protected with a strong passphrase, you can enforce the key size by selecting either 1024 or 2048:

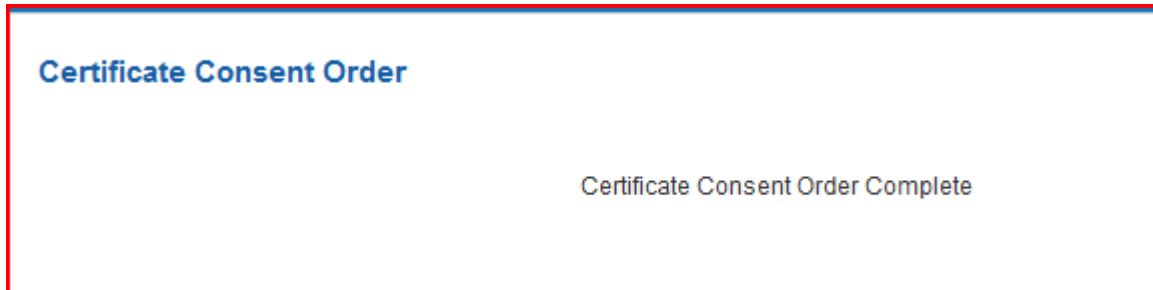
PKCS12 Key Length Required	<input checked="" type="radio"/> 1024 Bit <input type="radio"/> 2048 Bit
---	--

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 Pending Certificate Approval link. “Check” the request and click “Next”. Review the order and after appropriate identity verification is completed click “Next”.



The following screen will display at confirmation and an email will be sent to the end user with a link to install the digital certificate. Note the end user will need their Pick up password they established at registration in order to install the certificate.



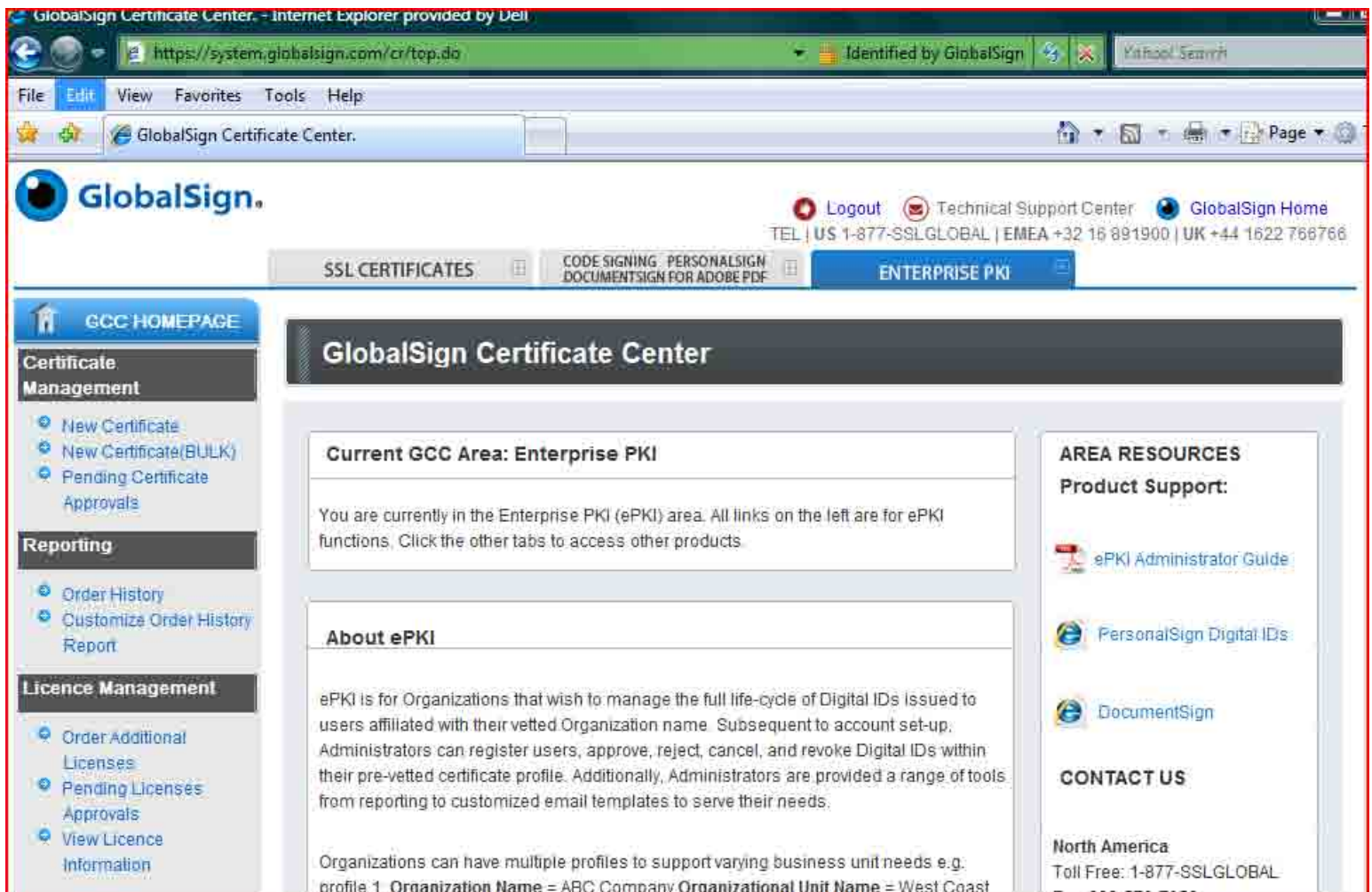
Register Users via ePKI Administrator

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

1. Single – New Certificate
2. Multiple – New Certificate (BULK)



These links are found under the Certificate Management menu.



GlobalSign Certificate Center. - Internet Explorer provided by Dell

https://system.globalsign.com/cr/top.do

Identified by GlobalSign

File Edit View Favorites Tools Help

GlobalSign Certificate Center.

GlobalSign.

Logout Technical Support Center GlobalSign Home

TEL | US 1-877-SSLGLOBAL | EMEA +32 16 891900 | UK +44 1622 766766

SSL CERTIFICATES CODE SIGNING PERSONALSIGN DOCUMENTSIGN FOR ADOBE PDF ENTERPRISE PKI

GCC HOMEPAGE

Certificate Management

- New Certificate
- New Certificate(BULK)
- Pending Certificate Approvals

Reporting

- Order History
- Customize Order History Report

Licence Management

- Order Additional Licenses
- Pending Licenses Approvals
- View Licence Information

GlobalSign Certificate Center

Current GCC Area: Enterprise PKI

You are currently in the Enterprise PKI (ePKI) area. All links on the left are for ePKI functions. Click the other tabs to access other products.

About ePKI

ePKI is for Organizations that wish to manage the full life-cycle of Digital IDs issued to users affiliated with their vetted Organization name. Subsequent to account set-up, Administrators can register users, approve, reject, cancel, and revoke Digital IDs within their pre-vetted certificate profile. Additionally, Administrators are provided a range of tools from reporting to customized email templates to serve their needs.

Organizations can have multiple profiles to support varying business unit needs e.g. profile 1. **Organization Name** = ABC Company **Organizational Unit Name** = West Coast

AREA RESOURCES

Product Support:

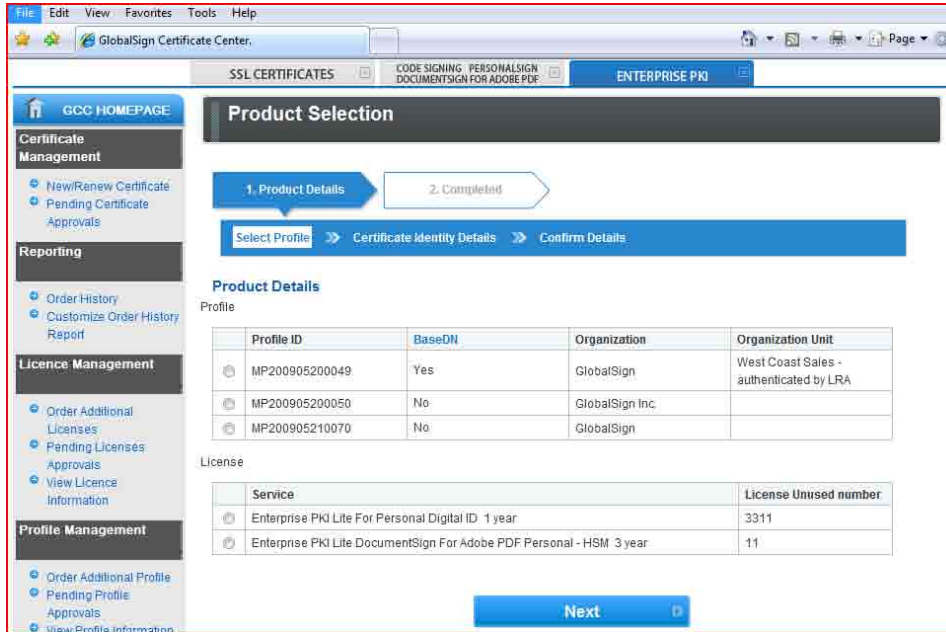
- ePKI Administrator Guide
- PersonalSign Digital IDs
- DocumentSign

CONTACT US

North America
Toll Free: 1-877-SSLGLOBAL

Single User Registration

For individual registrations, Click “New Certificate” and then select the Certificate Profile and License you wish to apply the certificate request to:



Click “Next” and complete the certificate identity details for the end user Subscribers. Note certain pre-vetted fields will be hardcoded. 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 e-mail address.

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 pick up (this is different than the “Pick up password” that is used to authenticate all requests regardless of enrollment method selected). See screen shot below:

GlobalSign Digital Certificates

Certificate Password Required	<input type="password"/>
Password must be a minimum of 12 characters. Alpha-numeric values only (A-Z, 0-9)	
Certificate Password (re-enter) Required	<input type="password"/>

- 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).

The screenshot shows the GlobalSign Certificate Center interface in Internet Explorer. The browser address bar shows the URL: https://system.globalsign.com/cn/certificate/neworder.do. The page title is "GlobalSign Certificate Center." The GlobalSign logo is visible in the top left. The top navigation bar includes links for "Logout", "Technical Support Center", and "GlobalSign Home". Below this, there are tabs for "SSL CERTIFICATES", "CODE SIGNING PERSONALSIGN DOCUMENTSIGN FOR ADOBE PDF", and "ENTERPRISE PKI".

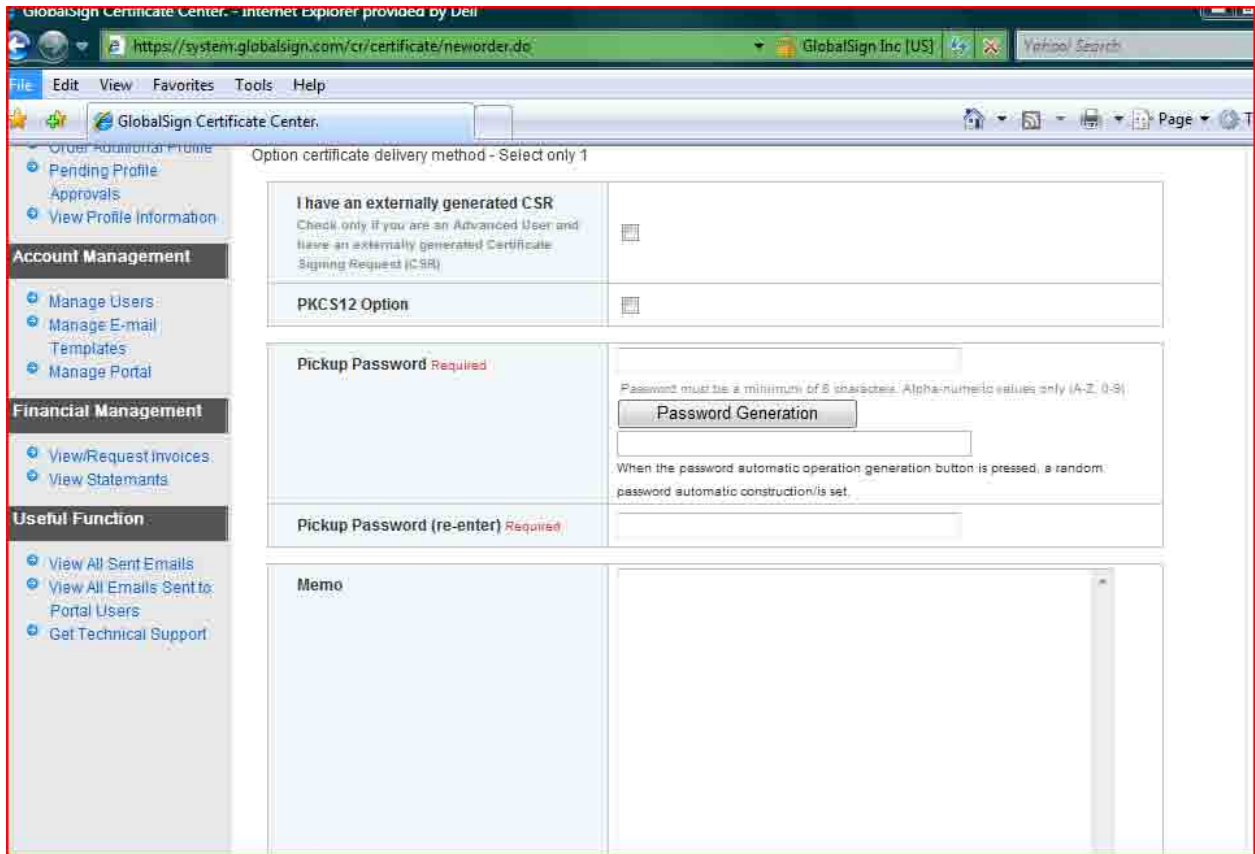
The main content area is titled "Product Selection" and shows a progress bar with two steps: "1. Product Details" (active) and "2. Completed". Below the progress bar, there are three buttons: "Select Profile", "Certificate Identity Details" (selected), and "Confirm Details".

The "Certificate Identity Details" form is displayed below. It contains the following fields:

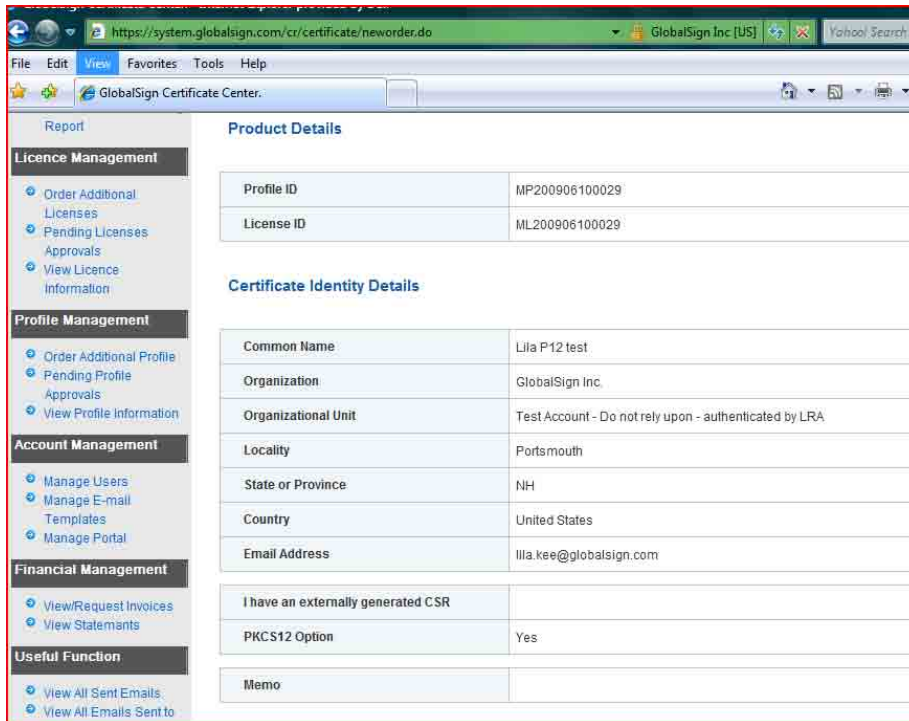
Common Name Required	<input type="text"/>
Organization	GlobalSign Inc.
Organizational Unit	Test Account - Do not rely upon - authenticated by LRA
Locality	Portsmouth
State or Province	NH
Country	United States
Email Address Required	<input type="text"/>

On the left side of the page, there is a sidebar menu with the following sections:

- GCC HOMEPAGE**
- Certificate Management**
 - New Certificate
 - New Certificate(BULK)
 - Pending Certificate Approvals
- Reporting**
 - Order History
 - Customize Order History Report
- Licence Management**
 - Order Additional Licenses
 - Pending Licenses Approvals
 - View Licence Information
- Profile Management**



Confirm details, and if correct, click NEXT



1. Product Details 2. Completed

Application Completed

Application Completed

Order Number	MPS200906152321
--------------	-----------------

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 "New Certificate (BULK)" and then select the Certificate Profile and License you wish to apply the certificate requests to. Click NEXT to continue.

You will then be instructed to browse for a Comma Separated Value (CSV) file typically created in Notepad that 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."

GlobalSign Certificate Center. - Internet Explorer provided by Dell

https://system.globalsign.com/cr/certificate/neworderbycsv.do

Identified by GlobalSign

GlobalSign Certificate Center.

GCC HOMEPAGE

Certificate Management

- New Certificate
- New Certificate(BULK)
- Pending Certificate Approvals

Reporting

- Order History
- Customize Order History Report

Licence Management

- Order Additional Licenses
- Pending Licenses Approvals
- View Licence Information

Profile Management

- Order Additional Profile
- Pending Profile Approvals
- View Profile Information

Account Management

- Manage Users

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,OrganizationUnit,Email, PickupPassword

Kate Jones,,kate.jones@globalsign.com,853gLJAHS
 Jennifer Jones,abc,Jennifer.jones@globalsign.com,9o719ghsa3
 George Jones,xzy,George.jones@globalsign.com,93JGL29ag

Item name	Explanation	Limitation
CommonName	Common name	Up to 64 alphanumeric characters
OrganizationUnit	Organization Unit	Up to 41 alphanumeric characters
Email	Email Address	Email Address
		Enter 8 to 64 alphanumeric

- Manage E-mail Templates
- Manage Portal

Financial Management

- View/Request Invoices
- View Statements

Useful Function

- View All Sent Emails
- View All Emails Sent to Portal Users
- Get Technical Support

PickupPassword	Pickup Password	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

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

```

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

```

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

After uploading the CSV, you may specify optional 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.

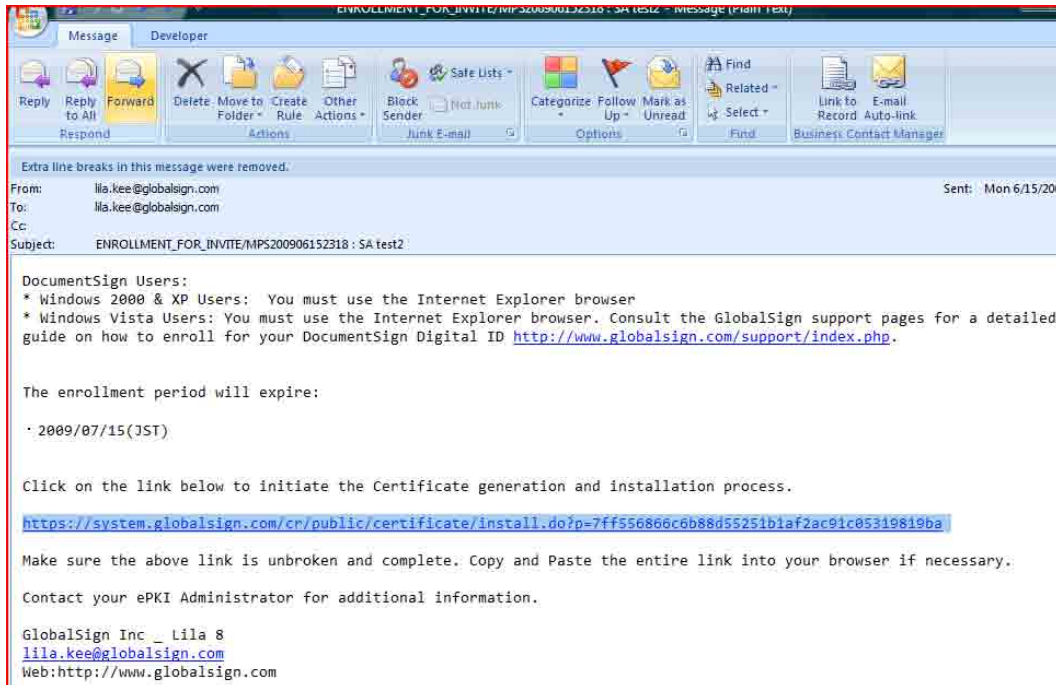
No	CommonName <small>Required</small>	OrganizationUnit	Email Address <small>Required</small>	Pickup Password <small>Required</small>	haveCSR	PKCS12
1	Mary Smith	staff in charge created profile - authenticated by LRA	mary.smith@globalsign.com	\$&^(S2334	<input type="checkbox"/>	<input type="checkbox"/>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

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

End user Installation

Subsequent to a certificate registration initiated by an ePKI Administrator, an email will be sent to the address identified in the certificate details.

Email contents may be modified (see Customize Email Templates), however a standard message will include a “pick-up” url used to enroll for the digital certificate.



Clicking on the Certificate Pick up URL will direct the subscriber to several additional steps depending on specific product configuration selected by the ePKI Administrator. Following is an example of a PersonalSign Pro certificate enrollment using a standard browser key generation method.

logo test

You will now go through the Certificate generation and installation process.
Note that if you continue on this computer, your Certificate will be installed on this computer.

Step One: Enter your Pickup Password

Your Pickup Password will have been set by your ePKI Administrator during the application.

Enter the Pickup Password to continue.

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

Next 

Step Two: Select the Cryptographic Service Provider (CSP)

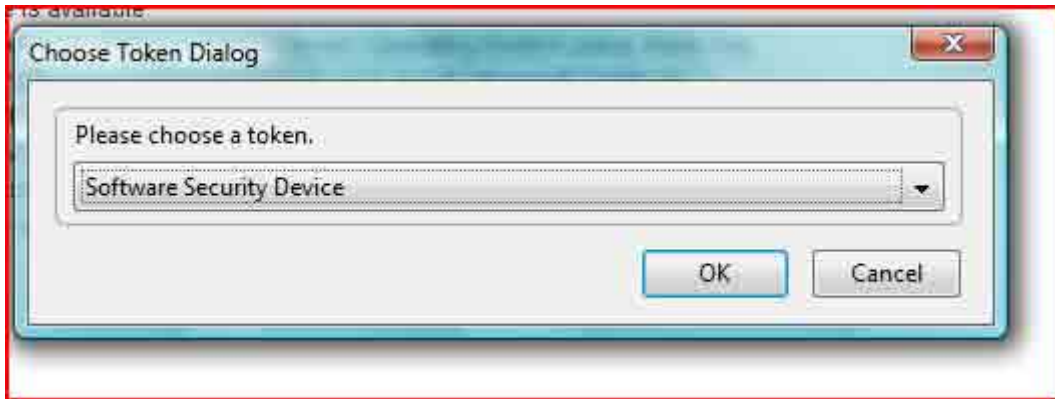
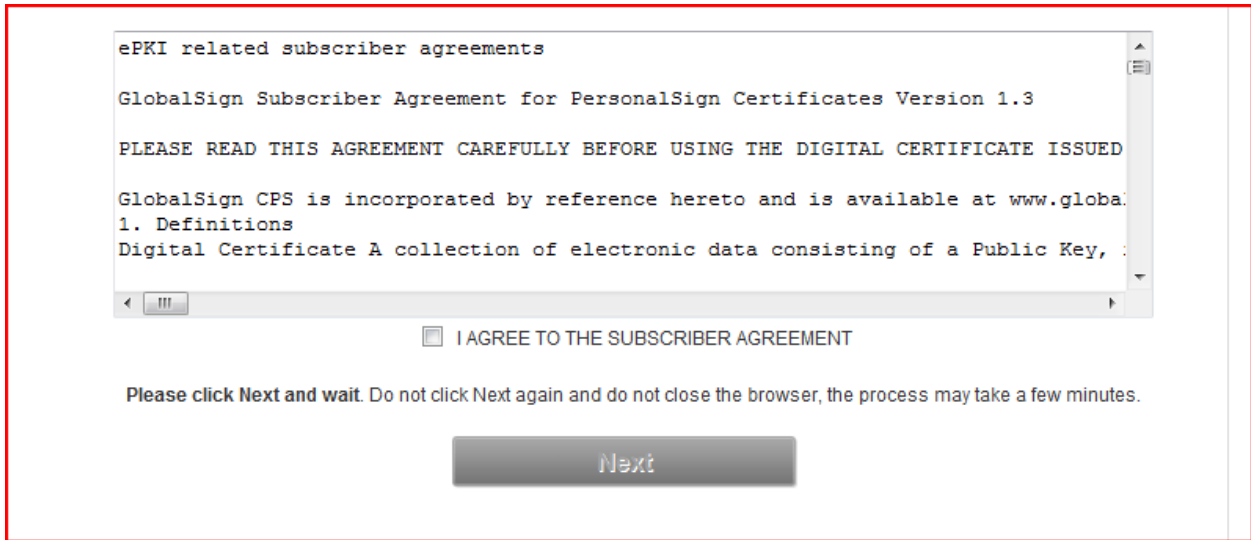
The CSP is used to generate the cryptographic keys within your Certificate.

We have listed the CSPs found on your computer. For further assistance on using CSPs and which may be appropriate if you are installing your Certificate onto a hardware device such as crypto USB, view the [CSP Support Guide](#).

Please note! Depending on your browser / Operating System setup, there may be a information bar or Pop Up asking you to install "Microsoft Certificate Enrolment Control" displayed at the top of this page.

If so, you MUST allow this to run. It is a safe program that your browser uses to install your certificate. To run it, click on the information bar or Pop Up and follow the instructions.

Make Certificate Exportable?	<input checked="" type="checkbox"/> Yes, make this Certificate exportable Check if you wish to allow the Certificate and associated cryptographic keys to be exportable. This means you can back up the Certificate or move it to another computer at a later time.
Cryptographic Service Provider	Microsoft Enhanced Cryptographic Provider v1.0 ▾



Secure email digital IDs

Install your Digital Certificate and the Intermediate CA Certificates

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

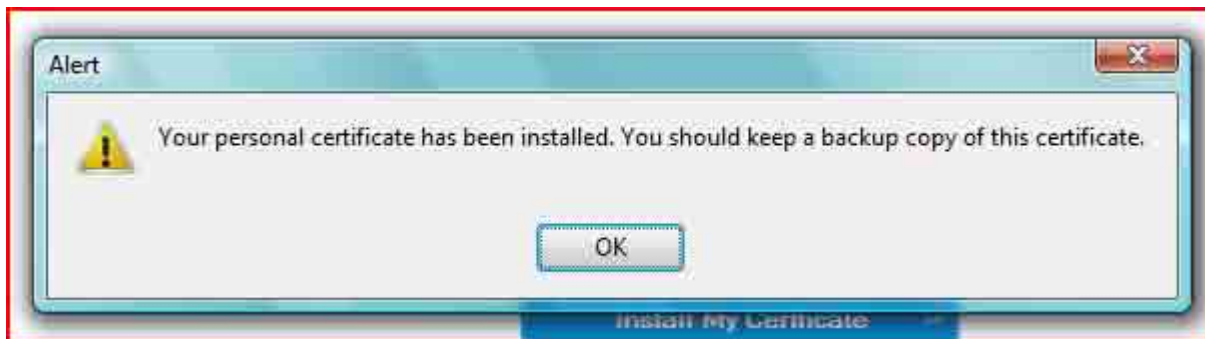
We have detected that you are not using Internet Explorer.
Please follow the below instructions to install your Certificate.
Click the Install My Certificate button to install your Certificate:

Install My Certificate

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

Install CA Certificate 1

Install CA Certificate2



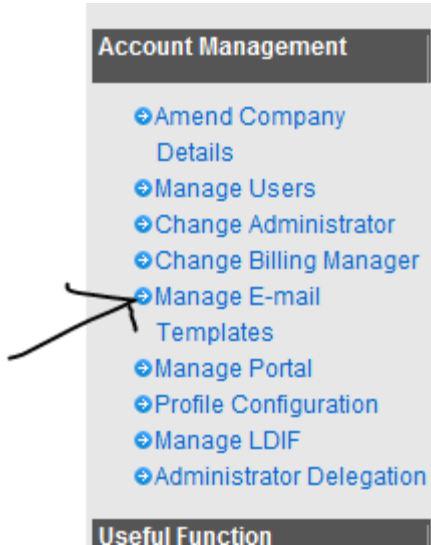
Please consult PersonalSign and DocumentSign Product specific guides for additional details
<http://www.globalsign.com/support/index.php>.

Bulk Provisioning

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 Template”:




- b) And “edit” 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	false	Edit
Renewal Reminders in 90 days	false	Edit

- c. If True, change Delivery from “Enable” to “Disable”

Send timing :Renewal Reminders in 60 days

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

Click “Next” and then “Complete”

3. Verify the PKCS12 key length is configured to the desired key length by setting either 1024 or 2048 key lengths via the “Manage Portal” link. Note GlobalSign recommends 2048 key lengths until end of 2010 and will require 2048 key sizes after that date.
 - a. Go to “Profile Configuration”
 - b) If you have more than a single Profile, click on the radio button next to the Profile you wish to configure and then Click Next.

<input type="radio"/>	<table border="1"><tr><td>Profile ID</td><td>MP201007080301</td></tr><tr><td>Organization</td><td>GlobalSign Test</td></tr><tr><td>Organization Unit</td><td>Audioptic Trade Services - authenticated by LRA</td></tr><tr><td>URL</td><td>https://system.globalsign.com/cr/public/certificate/order.do?p=7a525cb15ee1c32592d4510f31485d8e2b4be2b5</td></tr><tr><td>URL(PKCS12 Option)</td><td>https://system.globalsign.com/cr/public/certificate/order.do?p=c48a4c6ea3b06fc22091857f237d234ab9de8941</td></tr></table>	Profile ID	MP201007080301	Organization	GlobalSign Test	Organization Unit	Audioptic Trade Services - authenticated by LRA	URL	https://system.globalsign.com/cr/public/certificate/order.do?p=7a525cb15ee1c32592d4510f31485d8e2b4be2b5	URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=c48a4c6ea3b06fc22091857f237d234ab9de8941
Profile ID	MP201007080301										
Organization	GlobalSign Test										
Organization Unit	Audioptic Trade Services - authenticated by LRA										
URL	https://system.globalsign.com/cr/public/certificate/order.do?p=7a525cb15ee1c32592d4510f31485d8e2b4be2b5										
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=c48a4c6ea3b06fc22091857f237d234ab9de8941										
<input checked="" type="radio"/>	<table border="1"><tr><td>Profile ID</td><td>MP200907210051</td></tr><tr><td>Organization</td><td>GlobalSign Inc.</td></tr><tr><td>Organization Unit</td><td></td></tr><tr><td>URL</td><td>https://system.globalsign.com/cr/public/certificate/order.do?p=c41a3c480299ac3b833ec93438af9e84b7b2d180</td></tr><tr><td>URL(PKCS12 Option)</td><td>https://system.globalsign.com/cr/public/certificate/order.do?p=e5103fd1288f509ced6455266d36e8fdaddc9292</td></tr></table>	Profile ID	MP200907210051	Organization	GlobalSign Inc.	Organization Unit		URL	https://system.globalsign.com/cr/public/certificate/order.do?p=c41a3c480299ac3b833ec93438af9e84b7b2d180	URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=e5103fd1288f509ced6455266d36e8fdaddc9292
Profile ID	MP200907210051										
Organization	GlobalSign Inc.										
Organization Unit											
URL	https://system.globalsign.com/cr/public/certificate/order.do?p=c41a3c480299ac3b833ec93438af9e84b7b2d180										
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=e5103fd1288f509ced6455266d36e8fdaddc9292										

Account Management

- [Amend Company Details](#)
- [Manage Users](#)
- [Change Administrator](#)
- [Change Billing Manager](#)
- [Manage E-mail Templates](#)
- [Manage Portal](#)
- [Profile Configuration](#)
- [Manage LDIF](#)
- [Administrator Delegation](#)



- c) Select desired key size.

Manage Portal

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=96b2ccc3f7990c9f038099eeb07fe1c76aa3cc3f
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=cbf9e2b08c9021cb29804af0824058500724b2f6
PKCS12 Key Length Required	<input type="radio"/> 1024 Bit <input checked="" type="radio"/> 2048 Bit
Encrypting File System Required	<input type="radio"/> No <input checked="" type="radio"/> Yes
MS SmartCard Logon Required	<input type="radio"/> No <input checked="" type="radio"/> Yes
Auto Renewal Option Required	<input checked="" type="radio"/> No <input type="radio"/> Yes
Non Exportable Option Required Limited to only Internet Explorer.	<input checked="" type="radio"/> No <input type="radio"/> Yes

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 keygen
- Single file PKCS12 delivery allows for easy back up especially important if the certificate/keys are to be used for encryption
- Administrator enroll "on behalf" of end user allowing more control on certificate provisioning and back-up.

1. Start by going to "New Certificate (PKCS#12 BULK)
2. Select the Profile and License pack

The screenshot displays a web application interface for certificate management. On the left is a vertical navigation menu with categories: 'New Certificate', 'Reporting', 'License Management', and 'Profile Management'. The main content area shows a progress bar with steps '1. Product Details' and '2. Completed'. Below the progress bar is a breadcrumb trail: 'Product Details >> File specification >> Edit Details >> Confirm Details'. The 'Product Details' section contains two tables:

Profile

	Profile ID	BaseDN	Organization	Organization Unit
<input type="radio"/>	MP200909170373	No	GlobalSign Inc.	dedicated profile for new epki admin - authenticated by LRA
<input type="radio"/>	MP200909180374	No	GlobalSign Inc.	2nd admin new profile - authenticated by LRA
<input type="radio"/>	MP200909180375	No	GlobalSign Inc.	super admin established profile - authenticated by LRA

License

	Service	License Unused number
<input type="radio"/>	Enterprise PKI Lite For Department Digital ID 1 year	9
<input type="radio"/>	Enterprise PKI Lite For Personal Digital ID 1 year	119

At the bottom of the main content area is a blue 'Next' button with a right-pointing arrow.

3. Browse and Upload csv formatted based on Profile selection. Note the CSV must be formatted based on the characteristics of the Profile. In the below case, only Common Name and email were established as variable fields. Other values such as Organization Name, Organization Unit, and Country code will be automatically included into the certificate identity details a.k.a. Subject Distinguished name. After CSV has been uploaded, Click "Next"

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,OrganizationUnit,Email,PickupPassword

Kate Jones,,kate.jones@globalsign.com,853gLJAHs
 Jennifer Jones,abc,Jennifer.jones@globalsign.com,9o7t9ghsa3
 George Jones,xzy,George.jones@globalsign.com,93JGL29ag

Item name	Explanation	Limitation
CommonName	Common name	Up to 64 alphanumeric characters
Email	Email Address	Email Address
PKCS#12 Password	PKCS#12 Password	Enter 8 to 64 alphanumeric characters.

CSV file	bulk upload provisioning no OU.txt	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upload"/>
----------	------------------------------------	----------------------	--	---------------------------------------

◀ Back
Next ▶

Product Selection

1. Product Details

2. Completed

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

Edit Details

No	CommonName <small>Required</small>	Email Address <small>Required</small>	PKCS#12 Password <small>Required</small>
1	Mary Smith	lila.kee@globalsign.com	123456789abc1
2	John Johns	lila.kee@globalsign.com	123456789abc2
3	Kate Bates	lila.kee@globalsign.com	123456789abc3
4	Jennifer Williams	lila.kee@globalsign.com	123456789abc4
5	George Yak	lila.kee@globalsign.com	123456789abc4

◀ Back
Next ▶

4. Certificate generation complete

Product Selection

1. Product Details 2. Completed

Completed

Certificate issue batch application

Certificate issue batch application Complete

5.

6. Review records and make changes as required. Click “Next” to continue.

Product Selection

1. Product Details 2. Completed

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

Edit Details

No	CommonName <small>Required</small>	Email Address <small>Required</small>	PKCS#12 Password <small>Required</small>
1	Mary Smith	lila.kee@globalsign.com	123456789abc
2	John Johns	lila.kee@globalsign.com	123456789abc
3	Kate Bates	lila.kee@globalsign.com	123456789abc
4	Jennifer Williams	lila.kee@globalsign.com	123456789abc
5	George Yak	lila.kee@globalsign.com	123456789abc

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

Special Note for EFS or MS Smartcard users: if the Profile specified special key usages such as EFS or MS Smartcard logon, then the CSV would need to specify if these features with the following characteristics:

Encrypting File System	Encrypting File System	if "Encrypting File System", sets "true"
MS SmartCard Logon	MS SmartCard Logon Email Address	MS SmartCard Logon Email Address

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,OrganizationUnit,Email,PickupPassword

Kate Jones,,kate.jones@globalsign.com,853gLJAHs

Jennifer Jones,abc,Jennifer.jones@globalsign.com,9o7t9ghsa3

George Jones,xzy,George.jones@globalsign.com,93JGL29ag

Item name	Explanation	Limitation
CommonName	Common name	Up to 64 alphanumeric characters
Email	Email Address	Email Address
PKCS#12 Password	PKCS#12 Password	Enter 8 to 64 alphanumeric characters.

CSV file	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upload"/>
----------	----------------------	--	---------------------------------------



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 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 (sometime referred to as private key passwords).

Search | Reset

0% of download ZippedP12.do from dev4gacp.globalsign...

File Download

Do you want to open or save this file?

Name: dev4_UP201007130008.zip
 Type: WinZip File
 From: dev4gacp.globalsign.co.jp

Open Save Cancel

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

PKCS#12 Bulk Order ID	Edit	Date	Profile Order ID	License Order ID	Upload Number	Download
dev4_UP201007130010	Edit	07/11/2010 05:37 (GMT-05:00)	MP200909180375	ML200911211919	5	
dev4_UP201007130008	Edit	07/13/2010 05:37 (GMT-05:00)	MP200909180375	ML200911211919	5	Download
dev4_UP201007120005	Edit	07/12/2010 06:34 (GMT-05:00)	MP200909180375	ML200909171875	5	Download

Download complete

Download Complete

dev4_UP201007130008.zip from dev4gacp.globalsign.co.jp

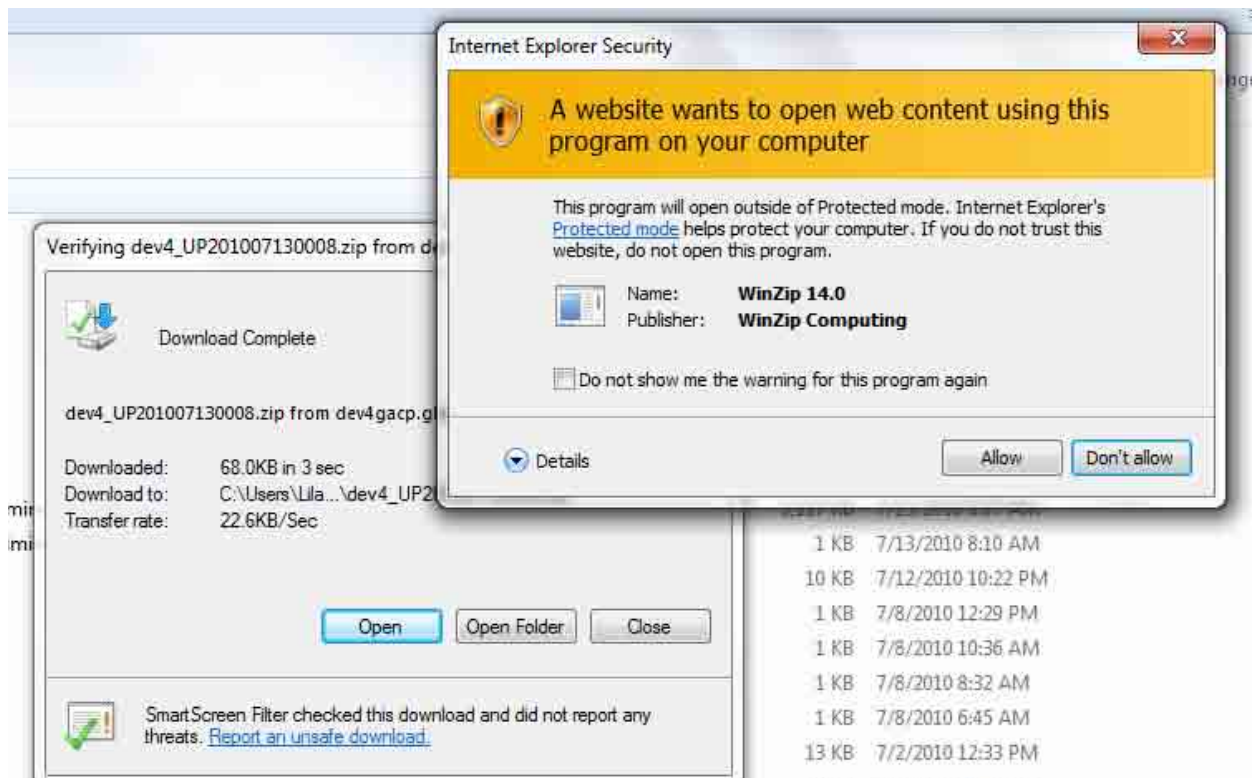
Downloaded: 68.0KB in 3 sec
 Download to: C:\Users\Lila...\dev4_UP201007130008.zip
 Transfer rate: 22.6KB/Sec

Close this dialog box when download completes

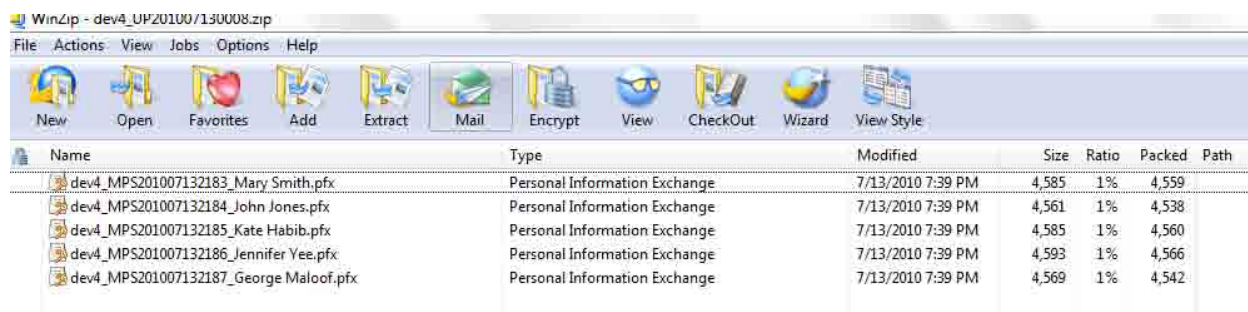
Open Open Folder Close

SmartScreen Filter checked this download and did not report any threats. [Report an unsafe download.](#)

When download is complete, Click open and if prompted "Allow" IE security warning.:



Note, individual file names will be identified using the common name of the certificate specified at registration. Also note, you will need the P12 passphrase also established at Registration to install the certificate.



Reporting

ePKI Administrators can manage the full life-cycle of digital IDs issued from their service. Locating a particular order/certificate is easy. Start by clicking on the "Order History" link found under the "Reporting" header. Search by order, date, Product etc.

The screenshot shows the GlobalSign Certificate Center web interface. The browser address bar displays <https://system.globalsign.com/ct/certificate/orderlist.do>. The page header includes the GlobalSign logo, a "Logout" link, a "Technical Support Center" link, and contact information: "GlobalSign Home TEL | US 1-877-SSLGLOBAL | EMEA +32 16 891900 | UK +44 1622 766". Navigation tabs for "SSL CERTIFICATES", "CODE SIGNING PERSONALSIGN DOCUMENTSIGN FOR ADOBE PDF", and "ENTERPRISE PKI" are visible.

The main content area is titled "Certificate List" and includes the instruction "Please Click Search Button:". Below this is a search form with the following fields:

Product	<input type="text"/>
Date of application	<input type="text"/> - <input type="text"/> e.g)2005/05/01
Issue Date	<input type="text"/> - <input type="text"/> e.g)2005/05/01
Closing certificate validity date	<input type="text"/> - <input type="text"/> e.g)2005/05/01
Common Name	<input type="text"/>
Email Address	<input type="text"/>
Certificate Order Number	<input type="text"/> Alphanumeric Character
Certificate Order Status	ALL <input type="text"/>
Certificate Status	ALL <input type="text"/>
Person in charge of registration	<input type="text"/>
Profile ID	<input type="text"/> Alphanumeric Character
License ID	<input type="text"/> Alphanumeric Character

The left sidebar contains navigation menus for "GCC HOMEPAGE", "Certificate Management" (New/Renew Certificate, Pending Certificate Approvals), "Reporting" (Order History, Customize Order History Report), "Licence Management" (Order Additional Licenses, Pending Licenses Approvals, View Licence Information), and "Profile Management" (Order Additional Profile, Pending Profile Approvals).

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

< 1 >

Various application	Update	Certificate Order Number	Organization Name	Common Name	Product	Period	Email Address
Application		MPS200906027638	GlobalSign	Lila Kee	Enterprise PKI Lite For Personal Digital ID 10 pack	1 year	lila.kee@globalsign.com
Application		MPS200905266703	GlobalSign Inc.	Portal	Enterprise PKI Lite For Personal Digital ID 10 pack	1 year	lakee1@rcn.com
Application		MPS200905205200	GlobalSign	lila kee	Enterprise PKI Lite For Personal Digital ID 10 pack	1 year	lakee1@rcn.com

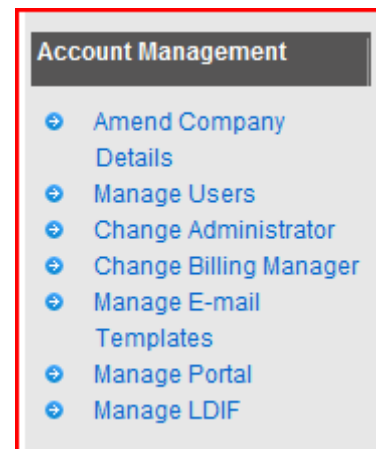
LDIF

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 “Manage LDIF” link found under “Account Management”.

The LDIF message format can be modified by clicking on a variety of substitution variables available in the far right pane. 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:



Edit LDIF Template

Message Detail

LDIF Template

Reset Message

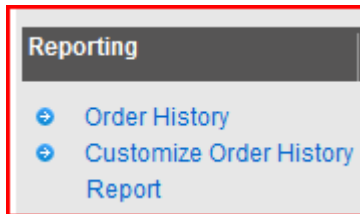
Certificate Order Number
Common Name
Organization
Organization Unit
CountryCode
State Or Province
Locality
Email Address
Starting certificate validity date
Closing certificate validity date
Certificate-SerialNo
Certificate-PEM
Certificate-PKCS7
Memo

Message

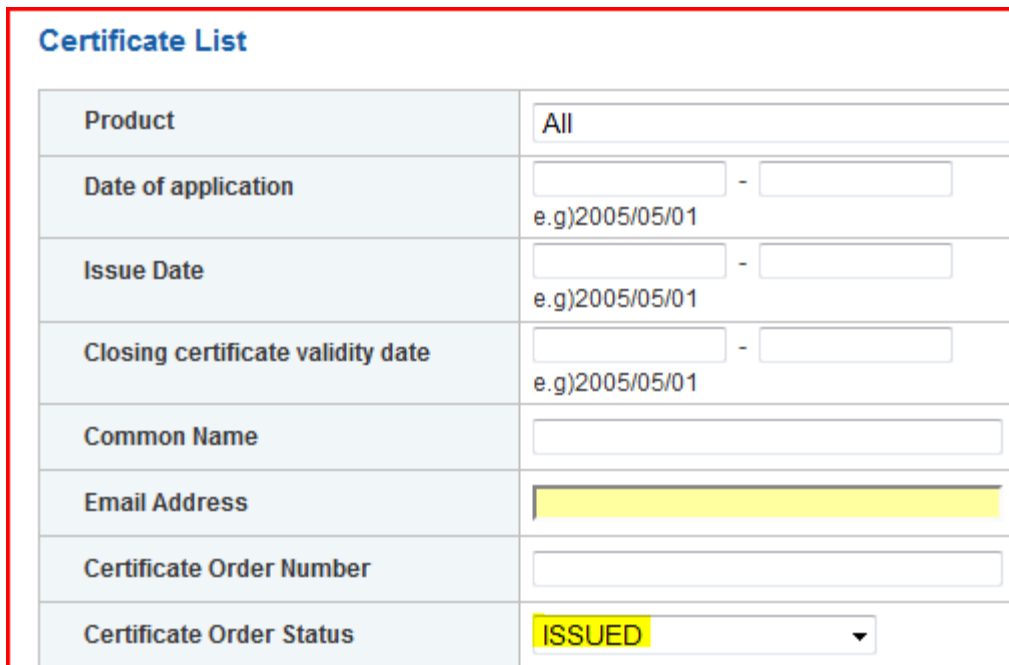
```
$$ {Certificate!Pkcs7} #dn: dc=input here , dc=input here
#objectclass: top
#objectclass: pkiUser
#objectclass: person
usercertificate;binary:: $$ {Certificate!PEM}
mail: $$ {Dn!Email}
CN: $$ {Dn!CommonName}
O: $$ {Dn!Organization}
OU: $$ {Dn!OrganizationUnit}
ST: $$ {Dn!StateOrProvince}
L: $$ {Dn!Locality}
C: $$ {Dn!CountryCode}
```

Generating a LDIF Report

LDIF reports are generated from the "Order History" link.



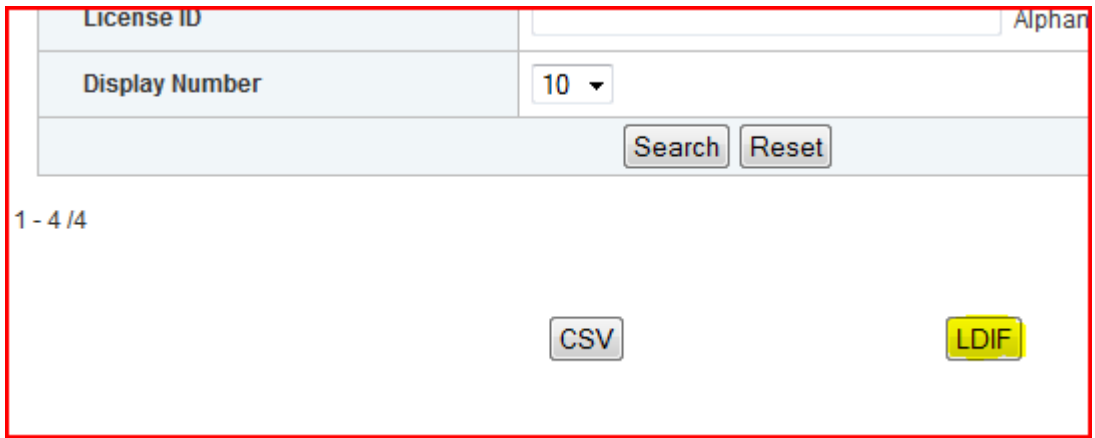
Select the appropriate date range, Profile (if you have more than 1) and set "Certificate Order Status = Issued" via the drop down menu. Note: If a certificate has been "Re-issued", the replacement certificate will have a status = Issued and be included in the LDIF report. The original, "replaced" certificate will not be included in the query since it's status will change to "reissued". Only non-revoked and unexpired certificates will be included.



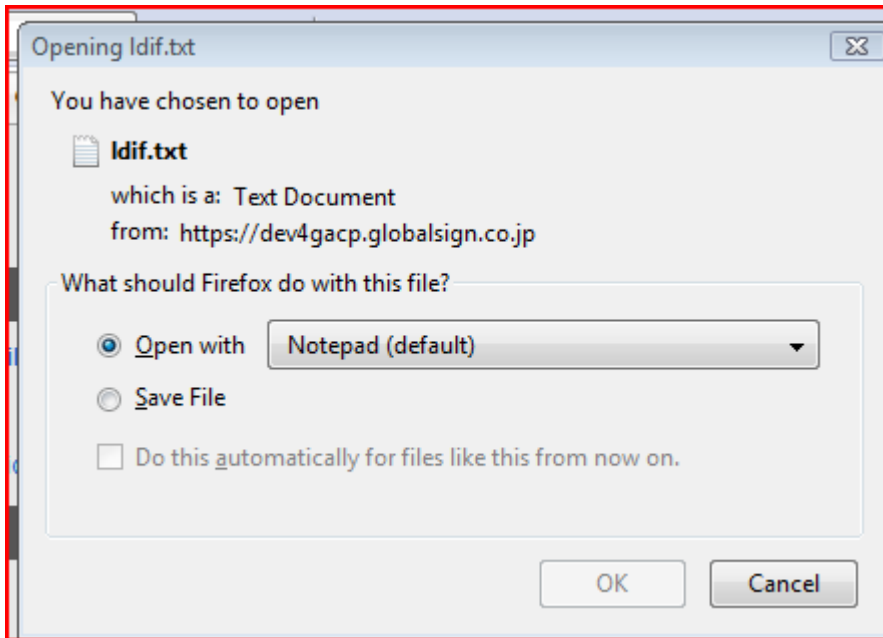
A screenshot of a web application's "Certificate List" form. The form is titled "Certificate List" and is highlighted with a red border. It contains several search criteria:

Product	All
Date of application	<input type="text"/> - <input type="text"/> e.g)2005/05/01
Issue Date	<input type="text"/> - <input type="text"/> e.g)2005/05/01
Closing certificate validity date	<input type="text"/> - <input type="text"/> e.g)2005/05/01
Common Name	<input type="text"/>
Email Address	<input type="text"/>
Certificate Order Number	<input type="text"/>
Certificate Order Status	ISSUED ▼

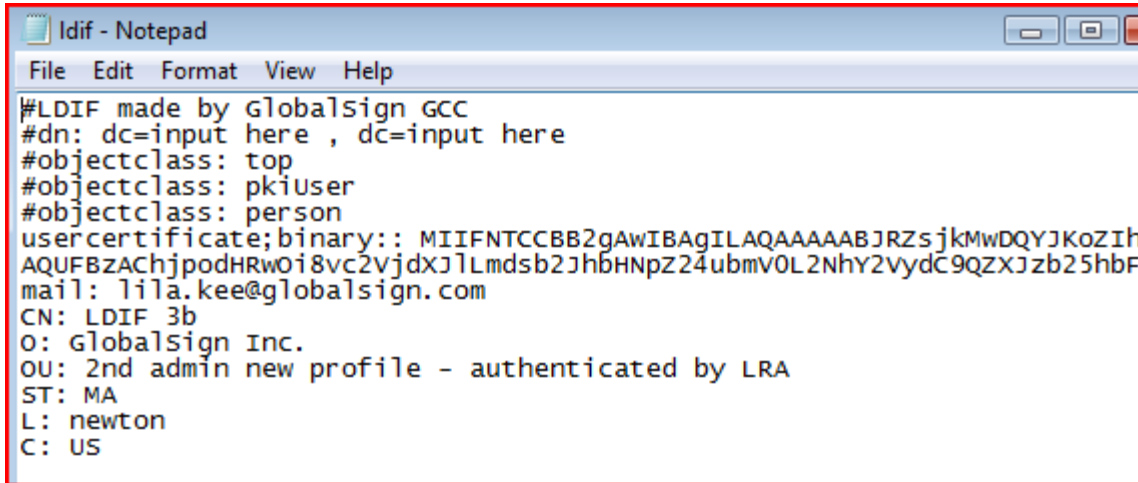
Click on the "LDIF" Button:



Open the file with your prefer application.



Below is an example entry:



```
ldif - 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:: MIIFNTCCBB2gAwIBAgILAQAAAAABJRZsjkMwDQYJKoZIh
AQUFBZACHjpodHRwOi8vc2VjdXJlLmVudC9QZXBzZ25hbF
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
```

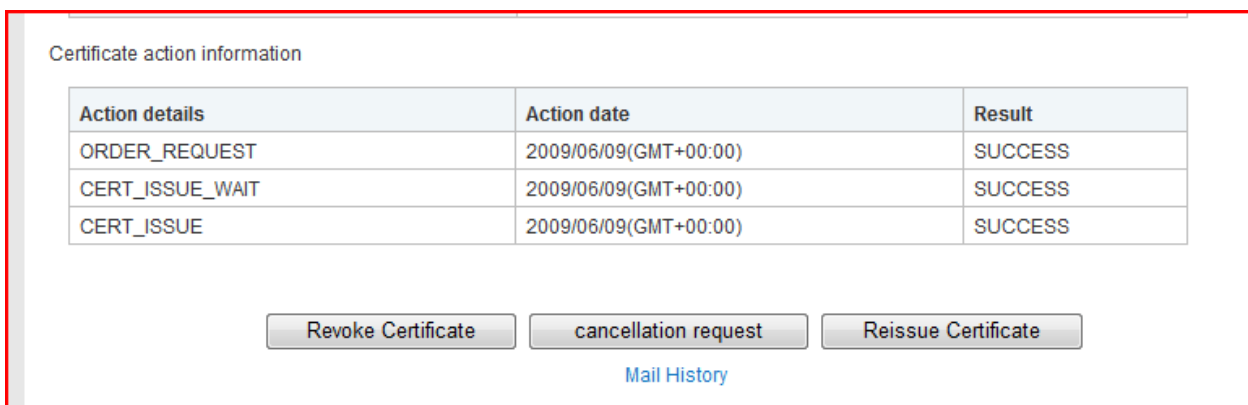
Upload to LDAP directory according to your product specific instructions.

Certificate Life-cycle Management – Revocation, Reissuance, and Cancelation

Scroll to the bottom of the report illustrated above to revoke, cancel or reissue the certificate.

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 email that was encrypted using the original 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

[Mail History](#)

Click "Mail History" to review or resend system generated emails:

History	Certificate Order Number	Case name:SUBJECT	Destination:TO	Date Sent	Status
92	MPS200906092097	ISSUE_COMPLETE/MPS200906092097 : Lila Test 4	lila.kee@globalsign.com \${ConsentUser!Email}	2009/06/09 (GMT+00:00)	Sent

Establishing other ePKI Administrators

ePKI Administrators can add other Administrators to the service by clicking “Manage Users” found under “Account Management”. Note, all ePKI Administrators have equal access to established profiles and certificate licenses, however, Administrator rights depends on the Administrator role established. There are three main Administrator Roles:

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

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

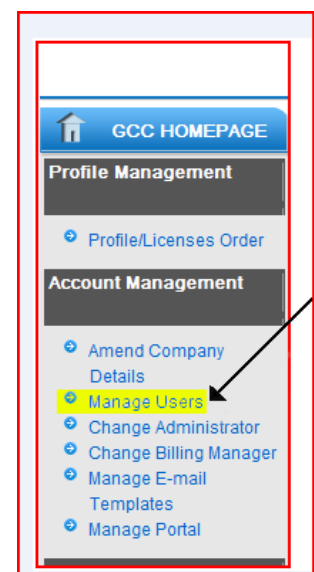
Managers may add other Staff administrators and establish certificate Profiles and approve orders if the GCC Administrator has enabled Certificate Approval Permissions by setting = True.

Staff in Charge

Staff in Charge may initiate orders, resulting in “Pending Certificate Request” that the GCC Administrator or Managers with Certificate Approval Rights must review and approve.

The “Order History” will note the Administrator associated with the user registration under the ‘Person in charge of registration’ heading.

A list of active ePKI Administrators can be found under “Manage Users”. New ePKI registrations can also be created at this link.



Manage Users								
Edit	User ID	Full name	Department name	Official position	Zip code	Address	TEL	FAX No.
<input type="button" value="Edit"/>	PAR12097_lilakee14	Administrator Test			02459	MANewton2 International Drive	5555555555	
<input type="button" value="Edit"/>	PAR12097_lakee	Lkee Kee			02345	MANewton56 Hanson Road	5555555555	

Registering additional Administrators

To create either “Managers” or “Staff in Charge” Administrators, Select “Manage Users” under “Account Management” begin by assigning a User ID and Password that will need to be distributed out-of-band to the appointed Administrator. Complete the registration including User information and Administrator 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.

New user registration page

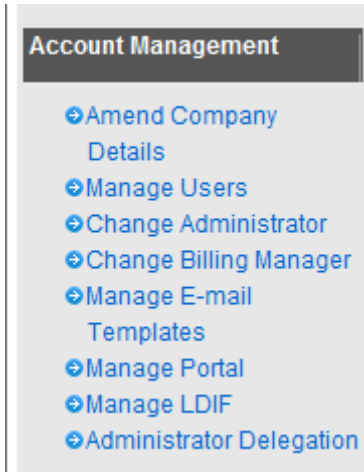
- User ID:** PAR04369 (Note: *Enter under 10 characters.)
- Password:** [Input field]
- Password(confirmation):** [Input field]
- Organization Name:** e.g. Globalsign Inc
- Department:** e.g. Marketing
- First Name:** [Input field]
- Middle Name:** [Input field]
- Last Name:** [Input field]
- Job Title:** e.g. Web Administrato
- Street Address 1:** e.g. Suite 330

New user registration page

- City:** e.g. Portsmouth
- State or County:** e.g. New Hampshire
- Zip Code / Postal Code:** e.g. 03801
- Country:** United Kingdom
- Other address info:** [Input field]
- Telephone (inc. region code):** e.g. +44 (0) 1622 766766
- Fax (inc. region code):** e.g. +44 (0) 1622 662255
- Email Address:** [Input field] (Note: *Please be careful when providing email address)
- User permissions:** Manager
- Language:** [Dropdown menu]
- Hoping for guide from this company:** [Input field]
- Certificate approval permission:** true
- Deposit purchase authority:** true

Administration Delegation

Shared administration can be established by enabling the Administration Delegation feature found on the left pane menu under Account Management:



Tick off the box next to the User ID that you wish to extend full administrative rights across all profiles established. Extended rights allows the User to view, approve, cancel, reissue, and revoke certificates initiated by any other User with either Staff or Manager rights for a given PAR.

SSL CERTIFICATES CODE SIGNING PERSONALSIGN DOCUMENTSIGN FOR ADOBE PDF ENTERPRISE PKI

Administrator Delegation

Administrator Delegation

Admin Delegation	User ID	First Name	Last Name
<input type="checkbox"/>	PAR12694_eric	Eric	Sprague
<input type="checkbox"/>	PAR12694_janine	Janine	Marchi
<input type="checkbox"/>	PAR12694_johnm	John	Murray
<input type="checkbox"/>	PAR12694_katsuo	Katsuo	Chujo
<input type="checkbox"/>	PAR12694_lila2	Lila2	Kee
<input type="checkbox"/>	PAR12694_lila20	Manager	Certificate approval permission false
<input checked="" type="checkbox"/>	PAR12694_lilakee8	Lila	Kee April 29
<input type="checkbox"/>	PAR12694_matt	Matthew	Greene
<input type="checkbox"/>	PAR12694_sic	staff	in charge

Next, confirm selection by clicking "Next":

Administrator Delegation

License Consent Order

Admin Delegation	User ID	First Name	Last Name
false	PAR12694_eric	Eric	Sprague
false	PAR12694_janine	Janine	Marchi
false	PAR12694_johnm	John	Murray
false	PAR12694_katsuo	Katsuo	Chujo
false	PAR12694_lila2	Lila2	Kee
false	PAR12694_lila20	Manager	Certificate approval permission false
true	PAR12694_lilakee8	Lila	Kee April 29
false	PAR12694_matt	Matthew	Greene
false	PAR12694_sic	staff	in charge

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

Note changes have been confirmed when the following screen appears:

Administrator Delegation

Administrator Delegation

delegation complete

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 <http://www.globalsign.com/help/>.

GlobalSign Contact Information:

GMO GlobalSign, Inc

2 International Drive
Suite 105, Portsmouth
New Hampshire 03801
Toll Free: 1-877-SSLGLOBAL
Fax: 603-570-7059
www.globalsign.com
sales@globalsign.com

GlobalSign NV

UbiCenter, Philipssite 5
3001 Leuven
Belgium
Tel: +32 16 891900
Fax: +32 16 891909
<http://eu.globalsign.com>
sales@globalsign.com

GlobalSign Ltd

Springfield House
Sandling Road, Maidstone,
ME14 2LP, United Kingdom
Tel: +44 1622 766766
Fax: +44 1622 662255
<http://www.globalsign.co.uk>
sales@globalsign.com