GlobalSign Enterprise Solutions
ePKI Quick Start Guide
Managing PersonalSign and DocumentSign Certificates
Across Your Organization Effectively

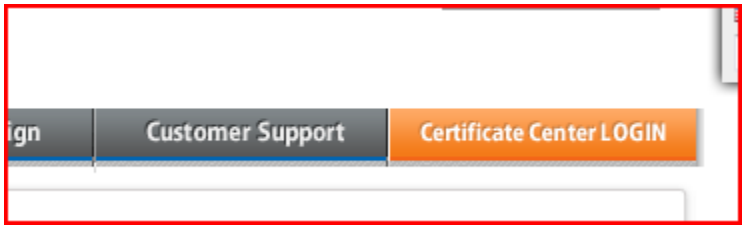
GlobalSign Enterprise Solution ePKI Administrator guide v1.9

TABLE OF CONTENTS

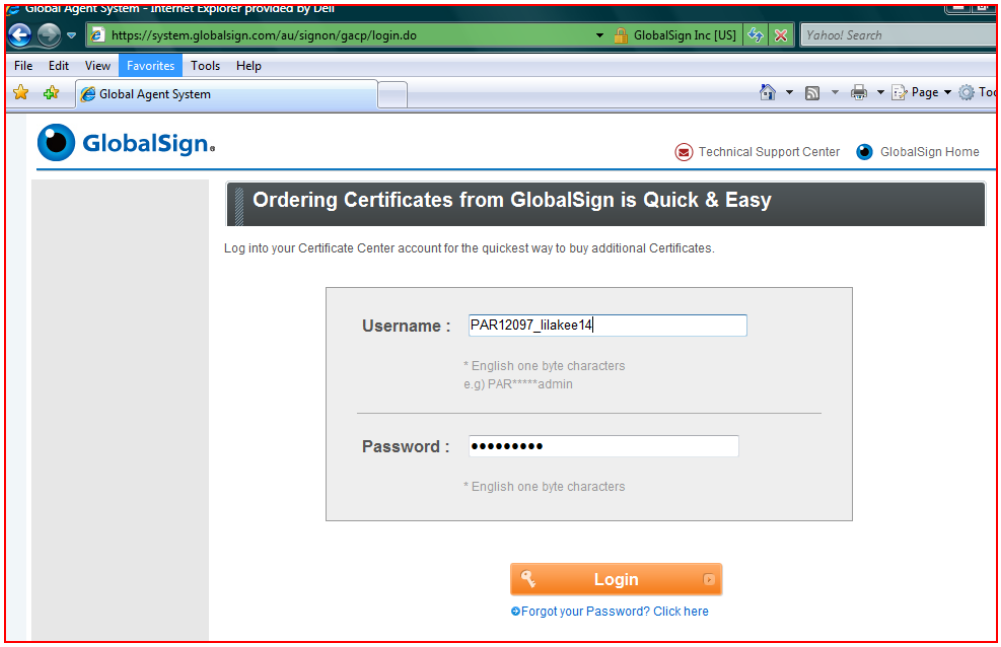
Getting Started:

Logging into your GlobalSign Certificate Center (GCC) Account:

Once your ePKI Account has been approved, you can log into the GlobalSign Certificate Center (GCC) straight away to start configuring and managing the lifecycle of your PersonalSign and DocumentSign Pro Certificates.
Go to www.globalsign.com and click ”Certificate Center LOGIN”.



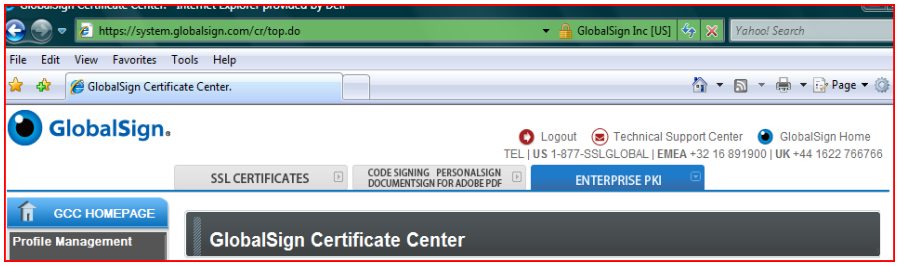
Enter your **User ID** and **Password**. Your User ID is the *PARXXXX_xxxxx* number given to you at the end of the GCC signup process, you can also find it in your Welcome Email. Your Password is the password you entered during the signup process.



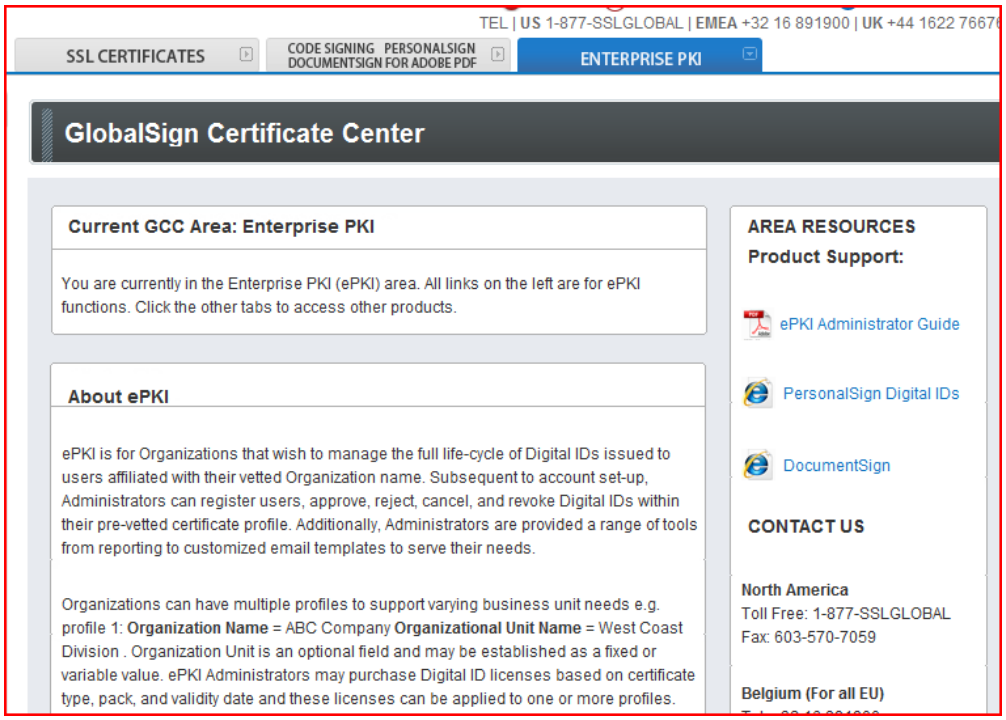
If you have difficulties logging in or forget your password please contact Support at www.globalsign.com/support

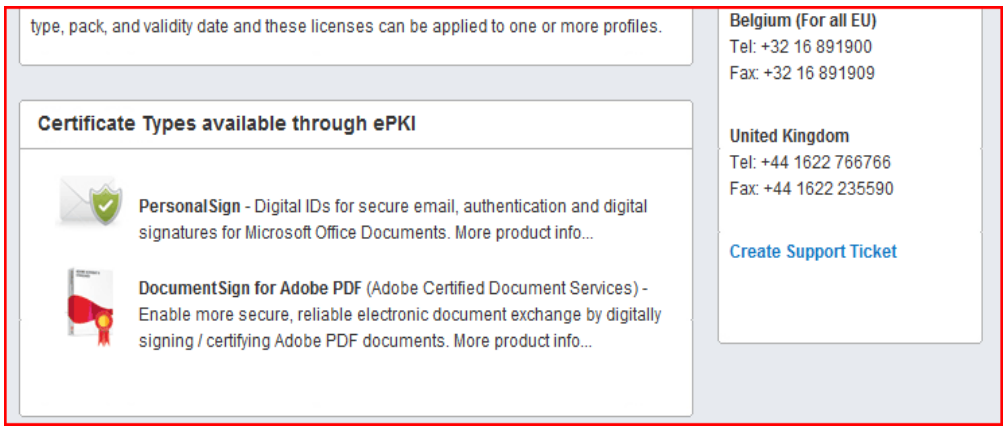
Establishing ePKI service

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**".



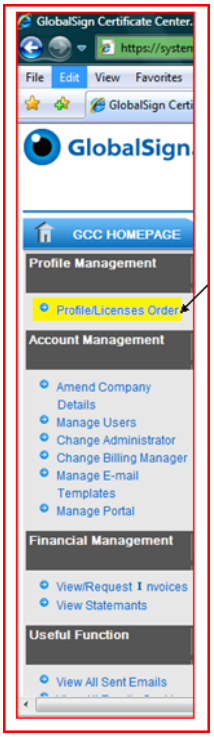
You will arrive on the ePKI home page. All functions are accessed through the left hand menu system:





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"

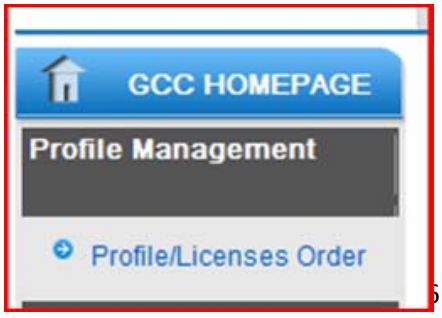


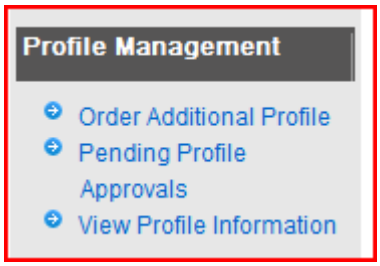
Certificate Profiles will be the content of the Digital ID as seen by anyone viewing and relying on the certificate, so it's important to ensure the Profile is accurate and representative of the holder of the certificate. Accuracy is also essential because GlobalSign will validate and verify the Organizational 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

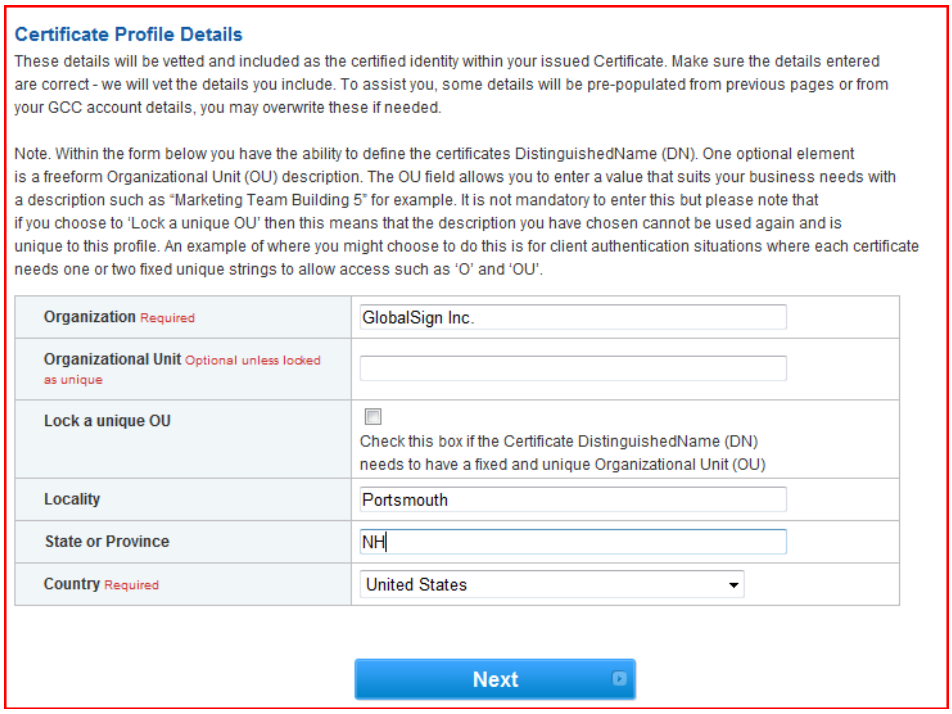
The ePKI Managed Service offers you the ability to use pre-vetted identity profiles to greatly accelerate the issuance of client certificates to users affiliated with your organization or subsidiary organizations. Your company identity and your authorization to issue digital certificates, using the requested 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.



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..

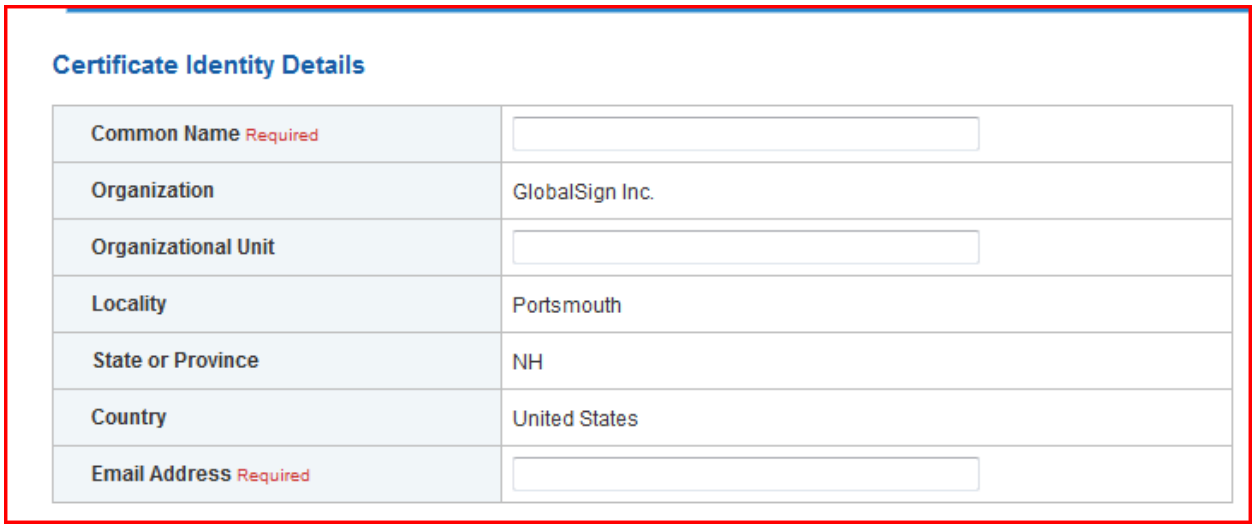
- **Option 1:** Fixed Organization Name with an Optional Variable Organization Unit
- **Option 2:** Fixed Organization Name with a Fixed Organization Unit
- **Option 3:** Fixed Organization Name with a Fixed and “Reserved” Organization Unit in the Base Distinguished Name.

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:

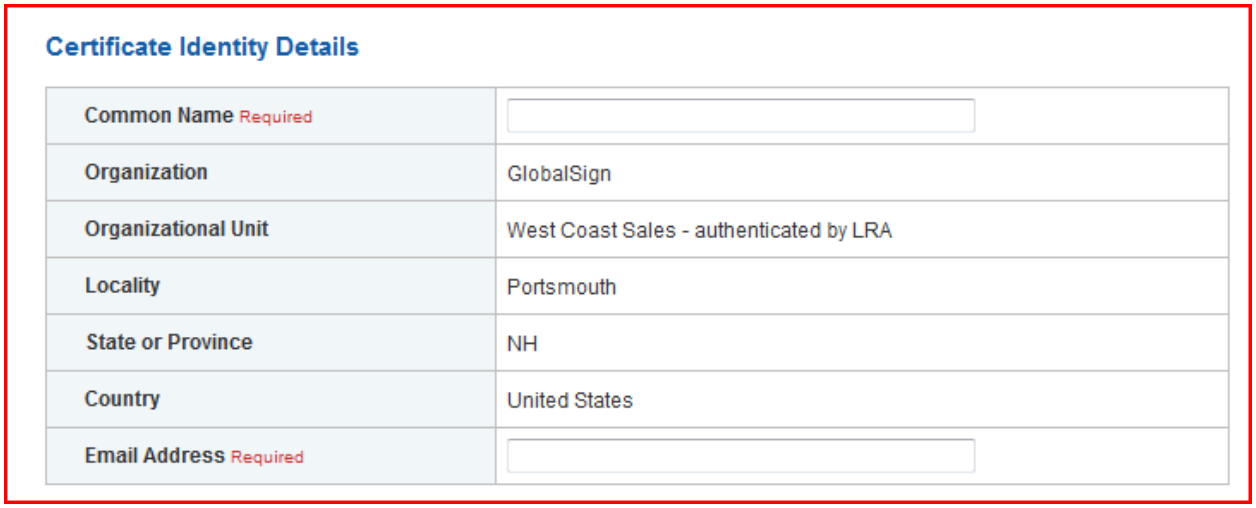


Option 2: Fixed Organization Name with a Fixed Organization Unit

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:

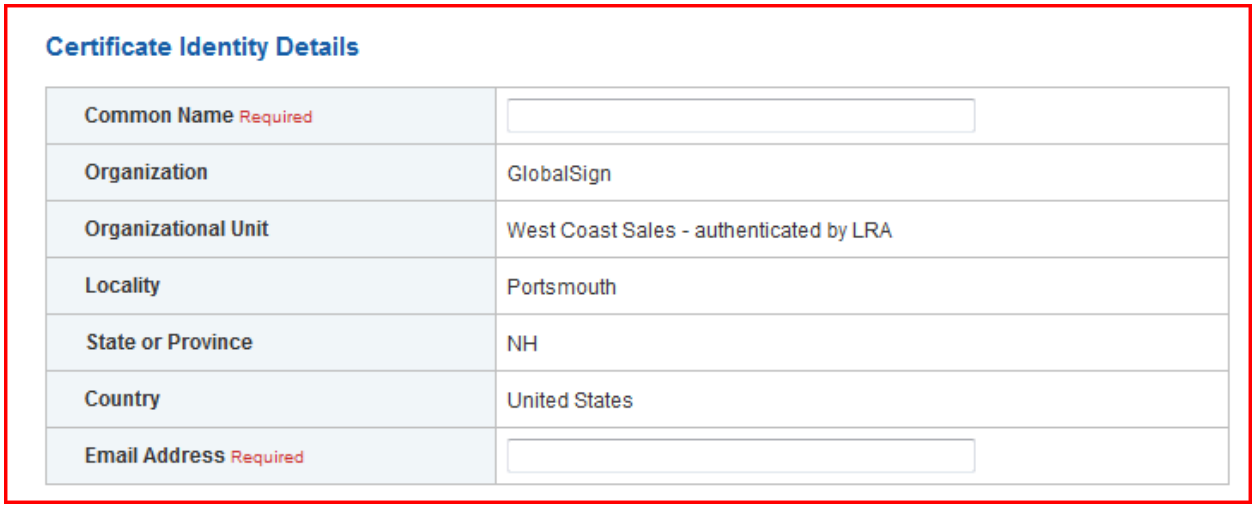


Option 3: Fixed Organization Name with a Fixed "RESERVED*" Organization Unit in the Base Distinguished Name (DN)

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 Required	
Organization	GlobalSign
Organizational Unit	West Coast Sales - authenticated by LRA
Locality	Portsmouth
State or Province	NH
Country	United States
Email Address Required	

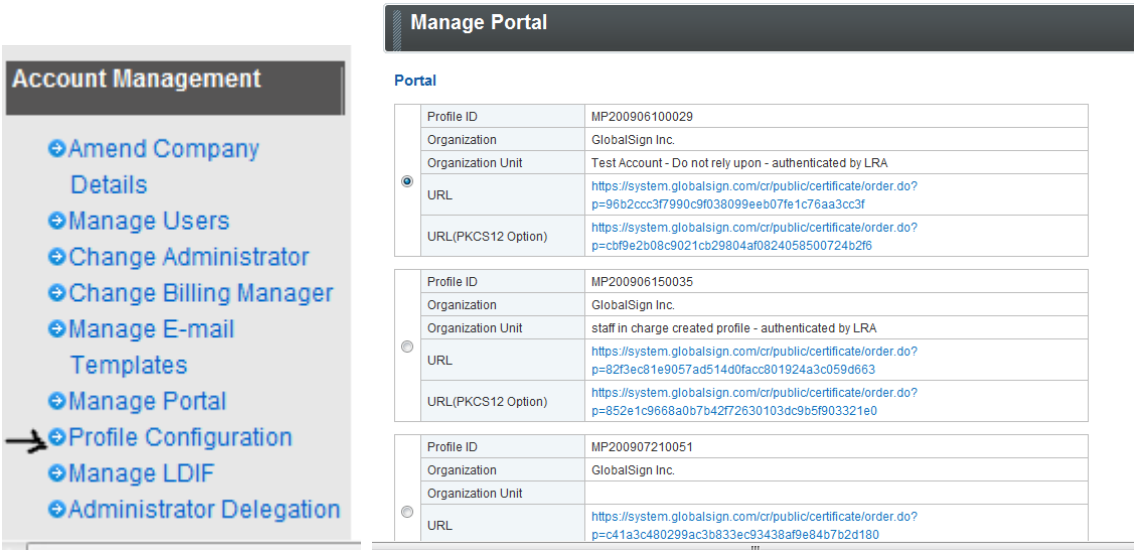
*To address concerns surrounding secure web access, new / additional profiles cannot be established using a "Locked" Organization and Organization Unit combined value. By checking the 'Lock OU' selection box, you'll prohibit this combination from being used in future Profiles.

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.

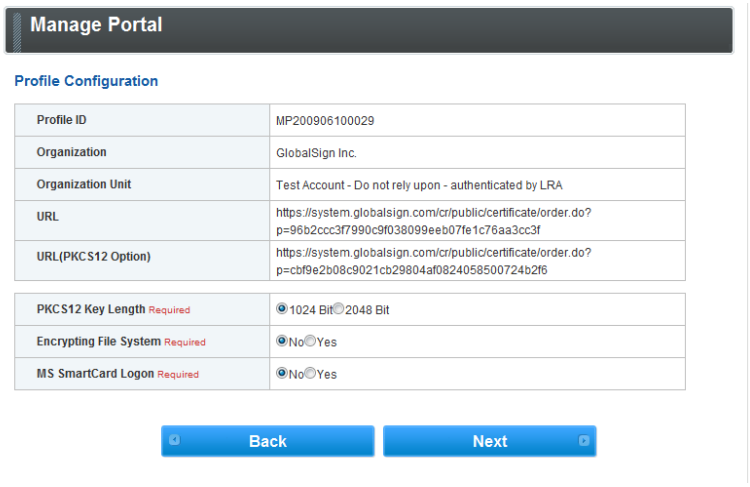
Once you have entered your profile(s) click the **Confirm** button and the vetting department will be notified of your request and begin the vetting process.
Should you have any questions regarding the status of your Profile request, please open a Support case at http://www.globalsign.com/help/

Additional Profile specific configuration options

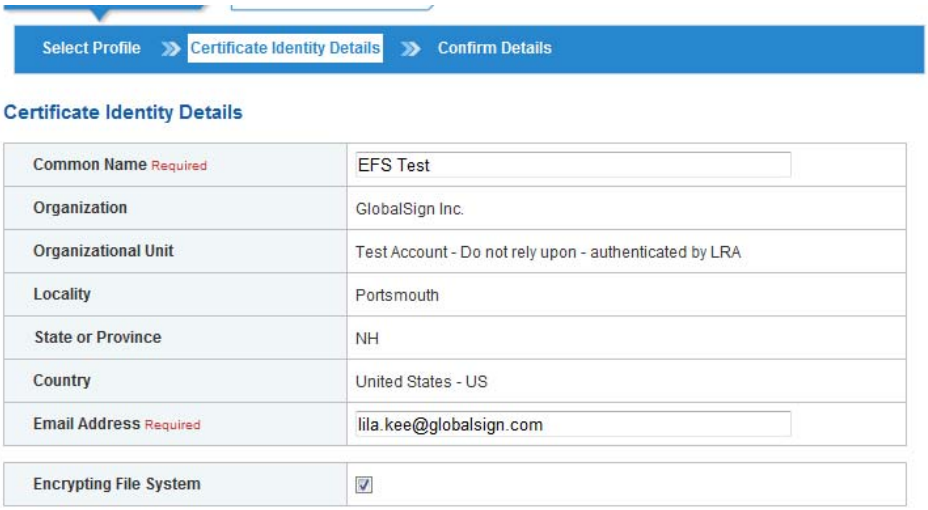
By selecting, “Profile Configuration” the ePKI Administrator can make available support for additional PKI-enabled applications that require specific key usages. Additionally, key size restrictions can be enforced for PKCS12 delivery options.



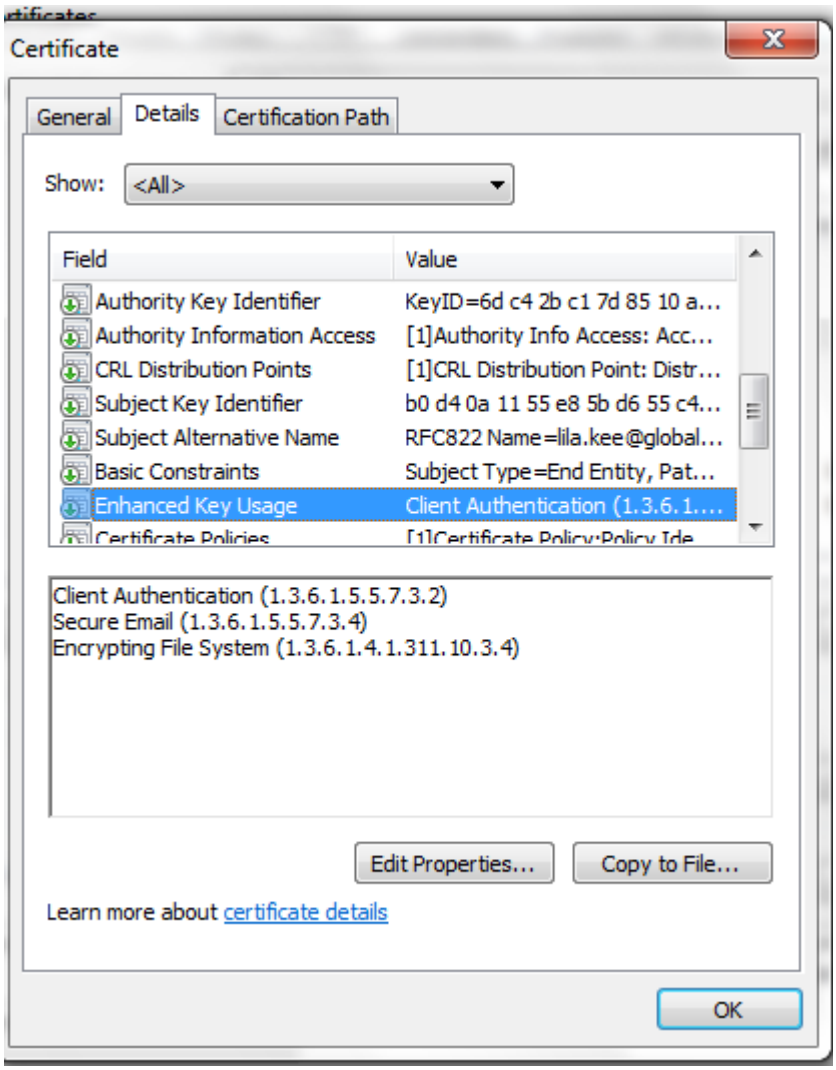
Select the Profile and Click “Next” to configure the following additional options:



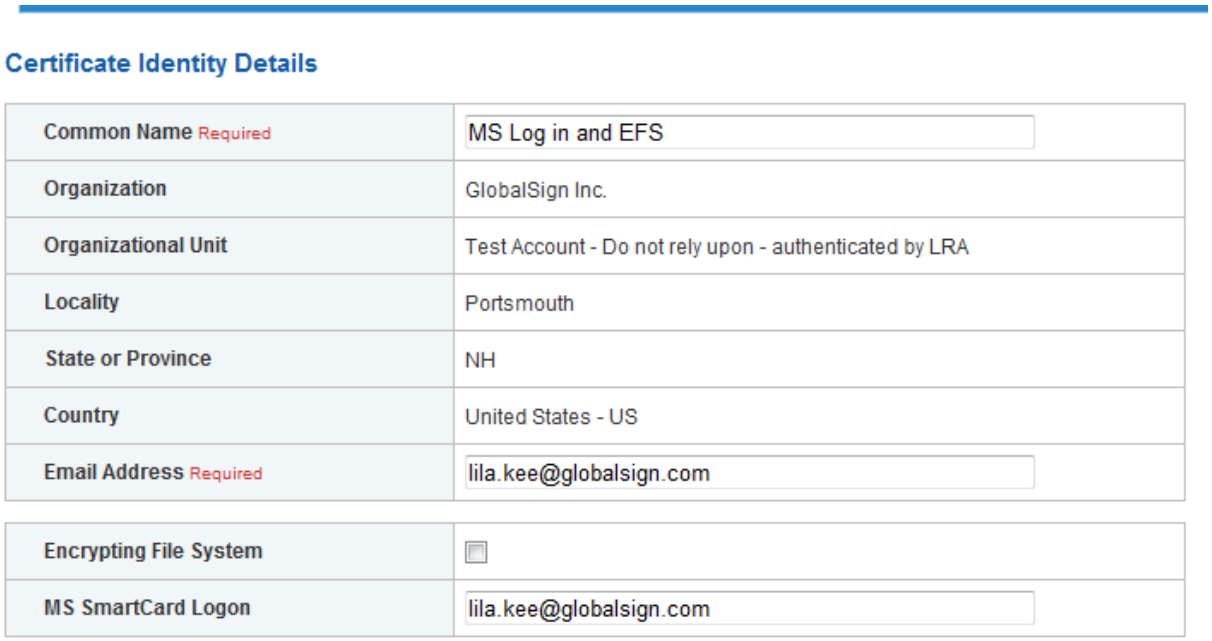
1. **PKCS12 Key Size restriction:** In the event you wish GlobalSign to create the public and private keys on behalf of the subscriber, a 1024 or 2048 (Recommended) key size restriction can be established.
2. **Encrypted File Systems (EFS):** Selecting the EFS option will display EFS as an option at certificate registration:



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



3. **<u>Microsoft (MS) SmartCard logon</u>**: 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:

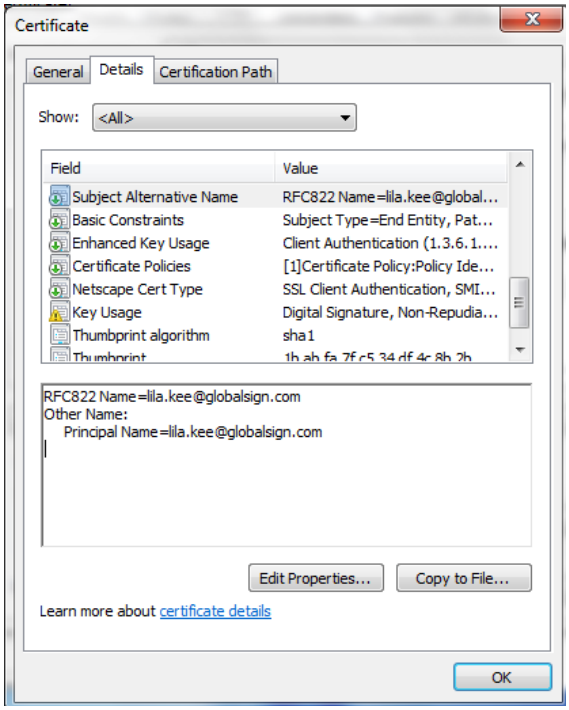


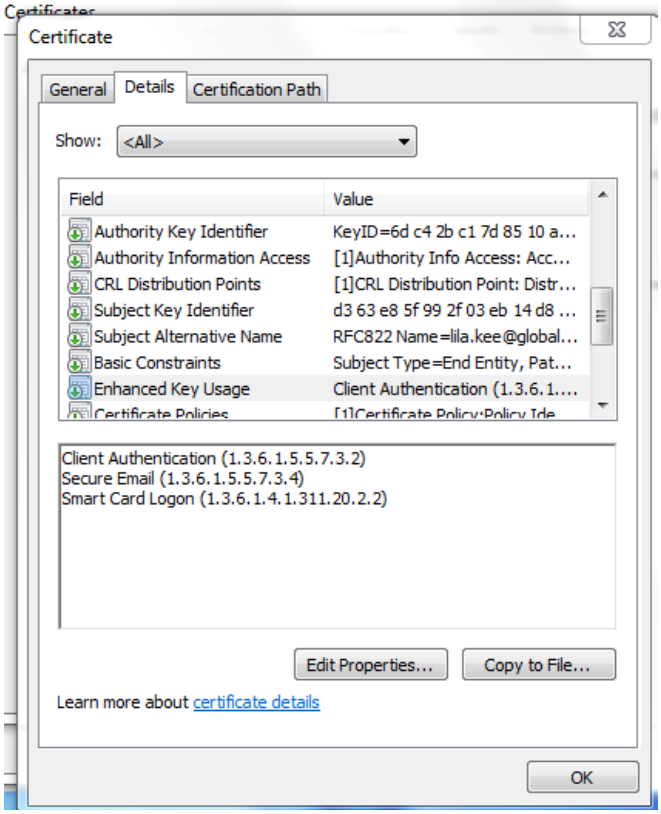
Certificate Identity Details

Common Name Required	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 Required	lila.kee@globalsign.com

Encrypting File System	☐
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:

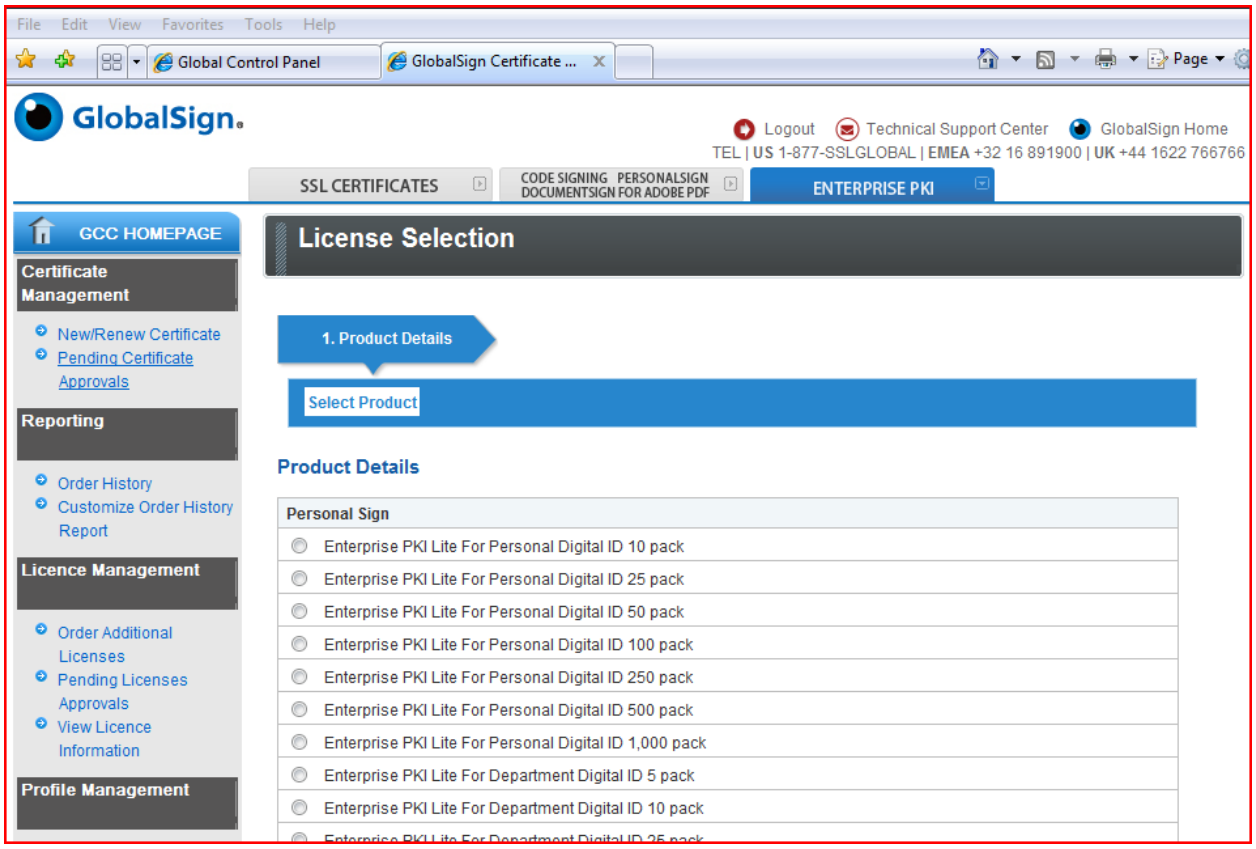
- PersonalSign for Windows trusted applications. • For a detailed product description go to http://www.globalsign.com/digital_certificate/personalsign/personalsign2-pro.htm
- DepartmentSign for Windows trusted applications. For a detailed product description go to http://www.globalsign.com/digital_certificate/personalsign/personalsign2-department.htm
- 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

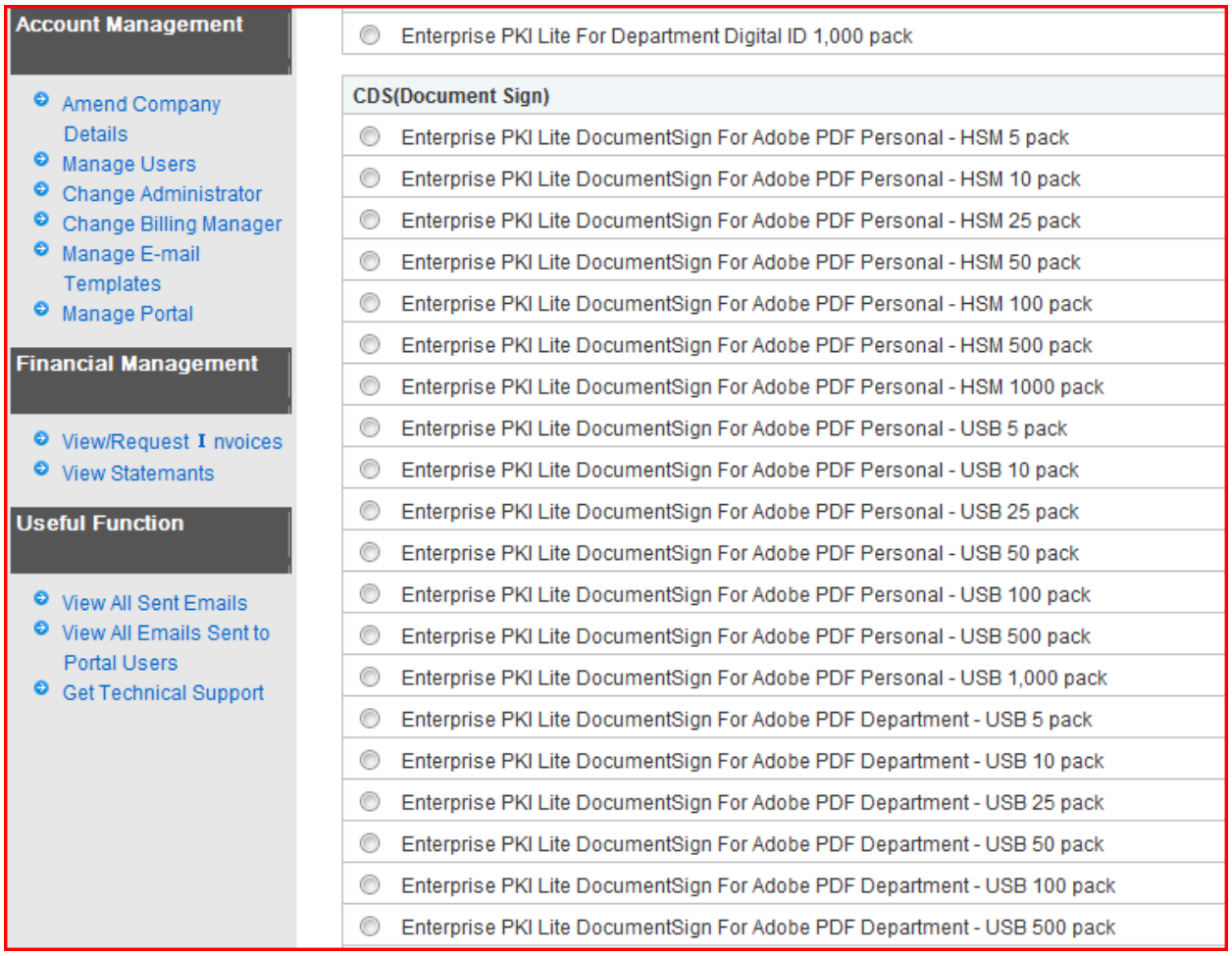
Certificate Packs:

- 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 Cancelation’

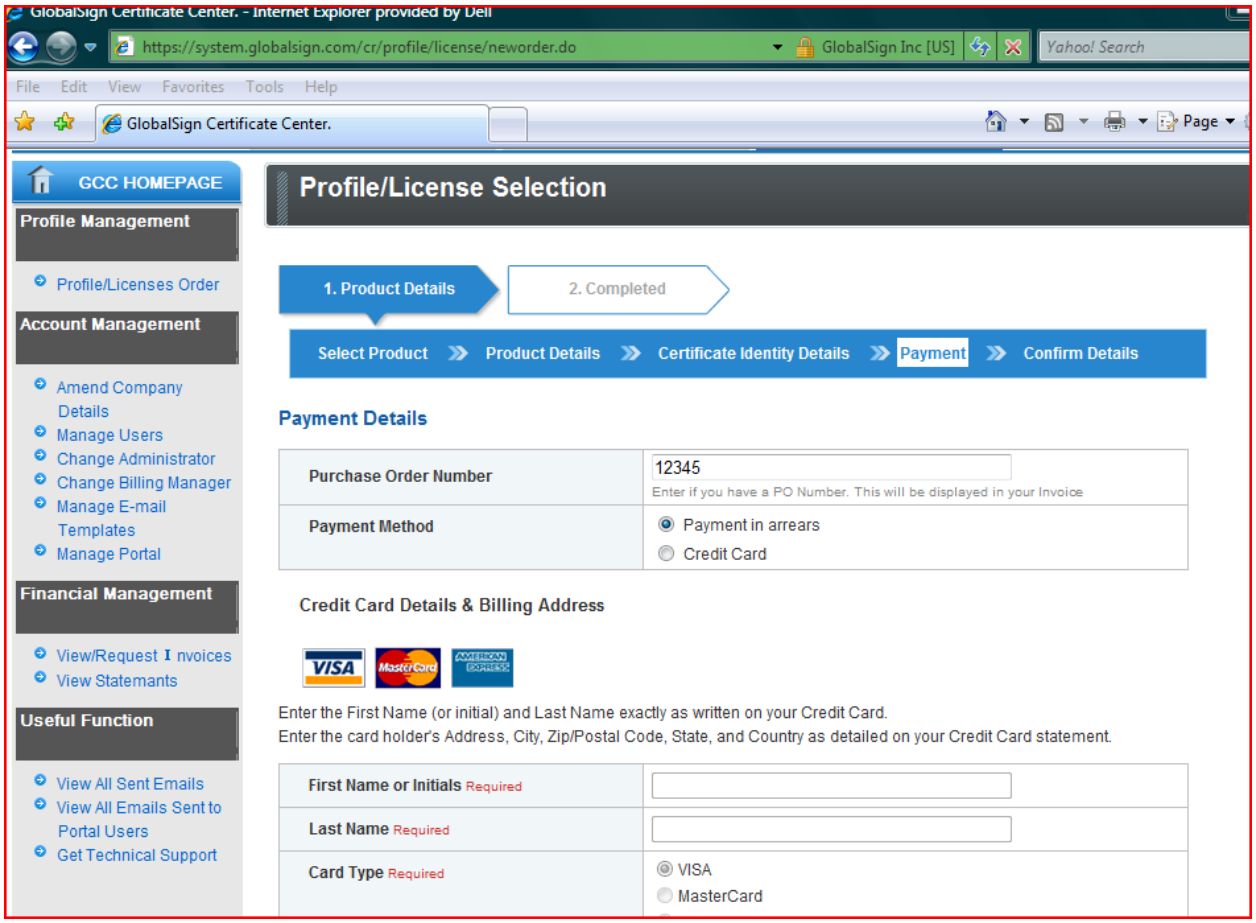
Certificate Validity:

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.

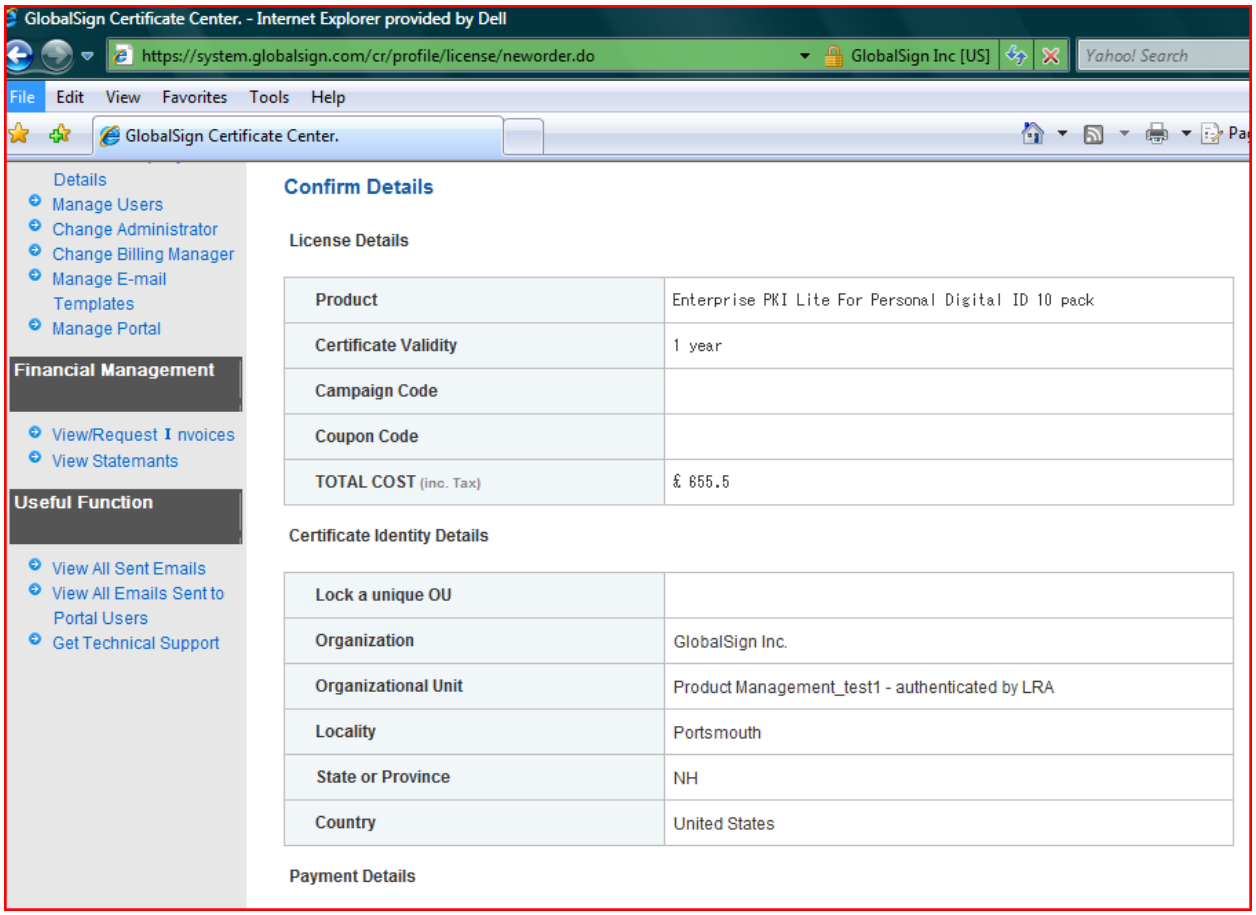



Account Management
Amend Company Details
Manage Users
Change Administrator
Change Billing Manager
Manage E-mail Templates
Manage Portal
Financial Management
View/Request Invoices
View Statemants
Useful Function
View All Sent Emails
View All Emails Sent to Portal Users
Get Technical Support
Enterprise PKI Lite For Department Digital ID 1,000 pack
CDS(Document Sign)
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - HSM 5 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - HSM 10 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - HSM 25 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - HSM 50 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - HSM 100 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - HSM 500 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - HSM 1000 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 5 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 10 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 25 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 50 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 100 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 500 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Personal - USB 1,000 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 5 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 10 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 25 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 50 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 100 pack
Enterprise PKI Lite DocumentSign For Adobe PDF Department - USB 500 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.

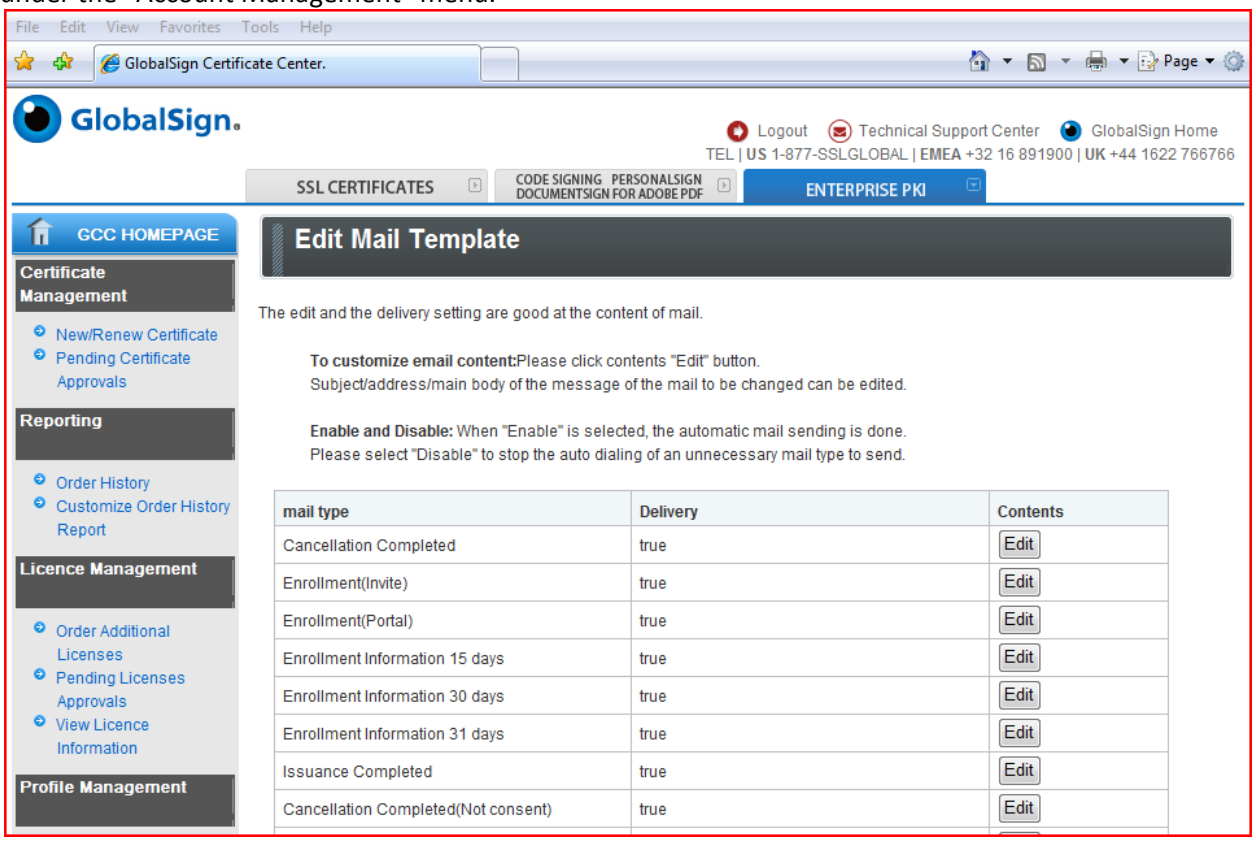


Review and confirm your order and then Accept ePKI Service Agreement. Note the ePKI Service Agreement binds you to Local Registration Authority and other obligations as outlined in the GlobalSign Certificate Practice Statements found at http://www.globalsign.com/repository/index.htm .



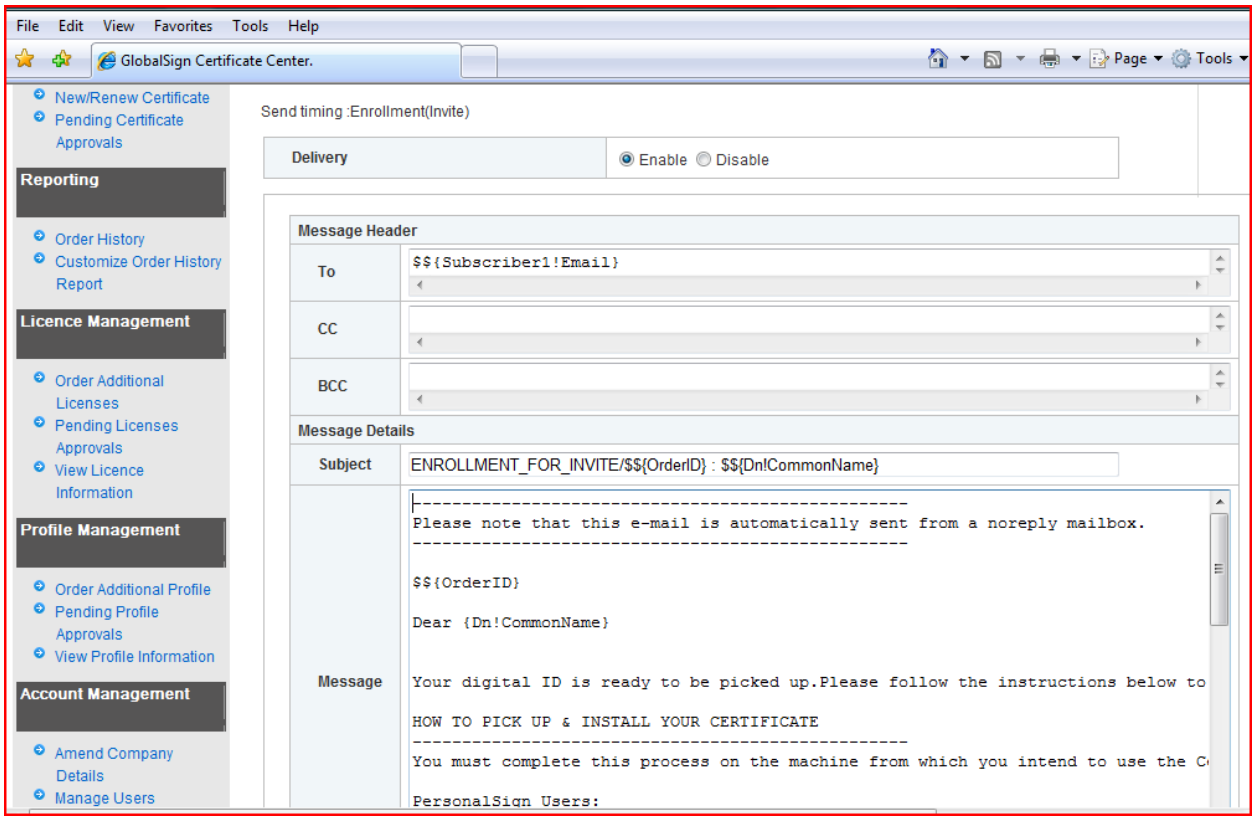
CUSTOMIZING EMAIL TEMPLATES

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.



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.



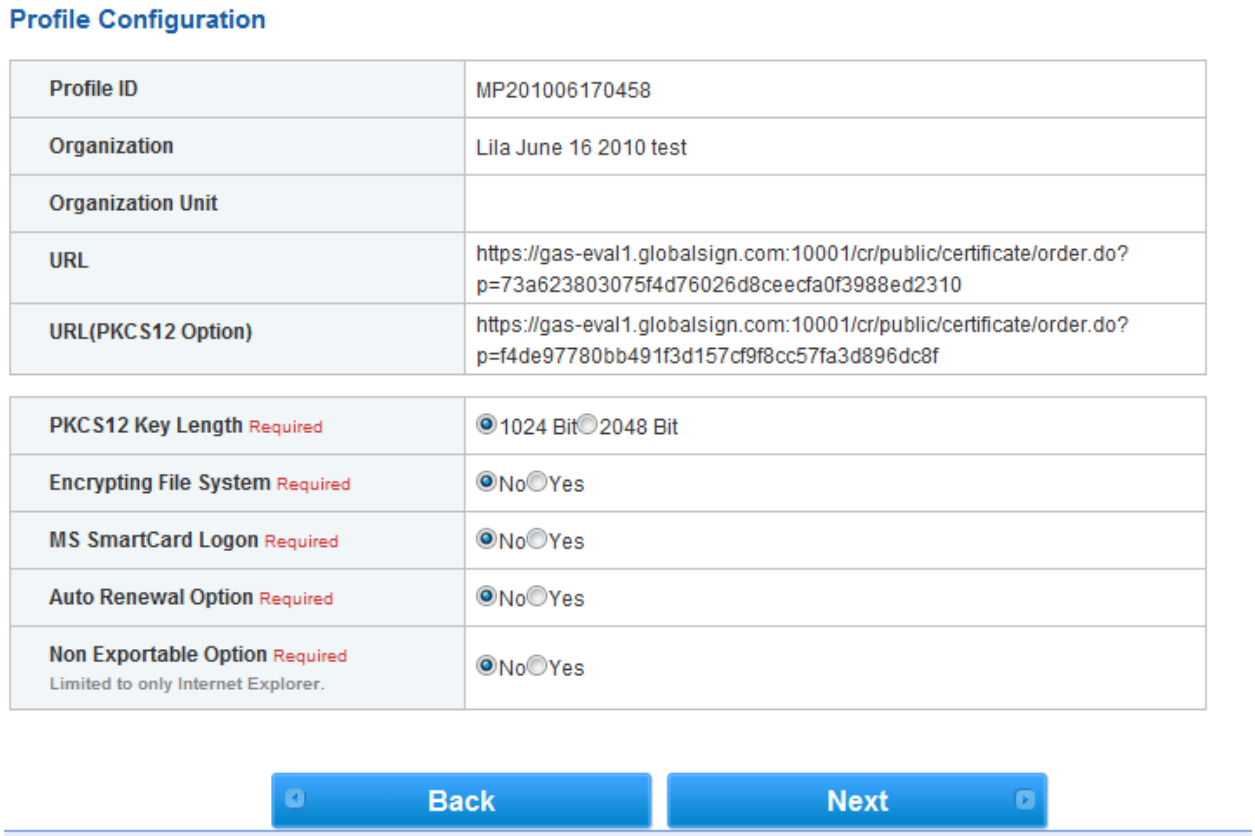
Renewal:

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”.



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.

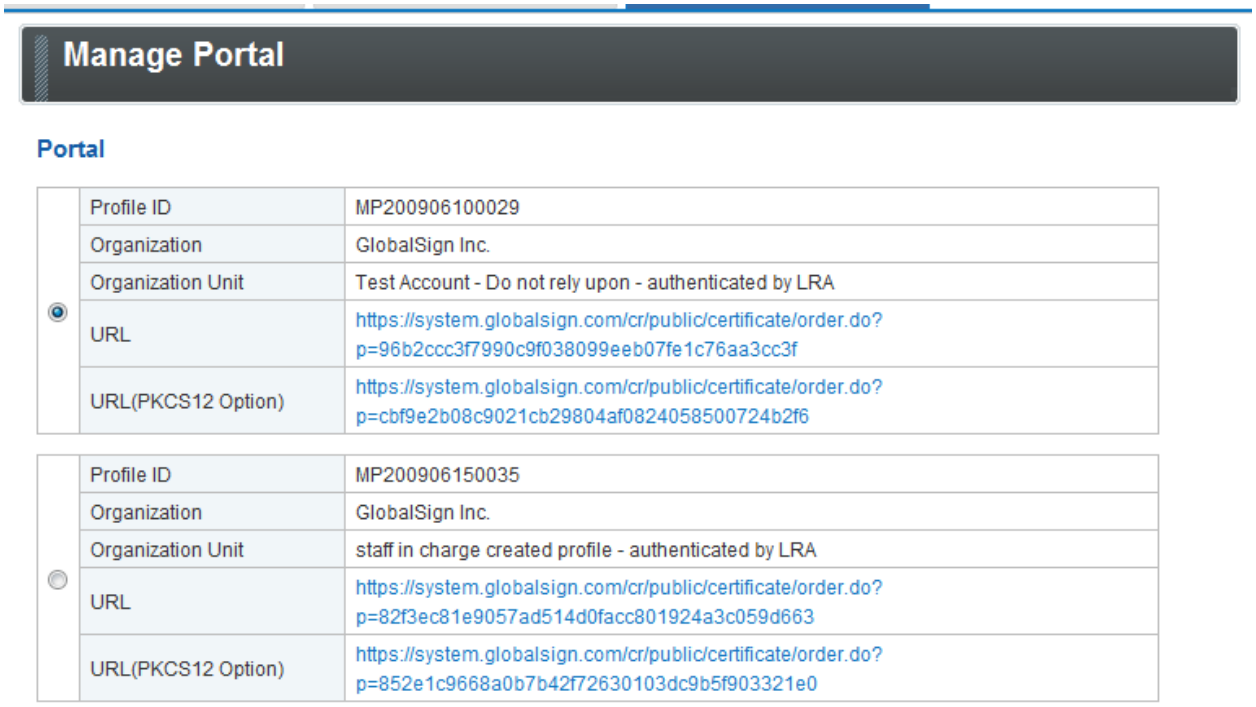
Using the Portal Link

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

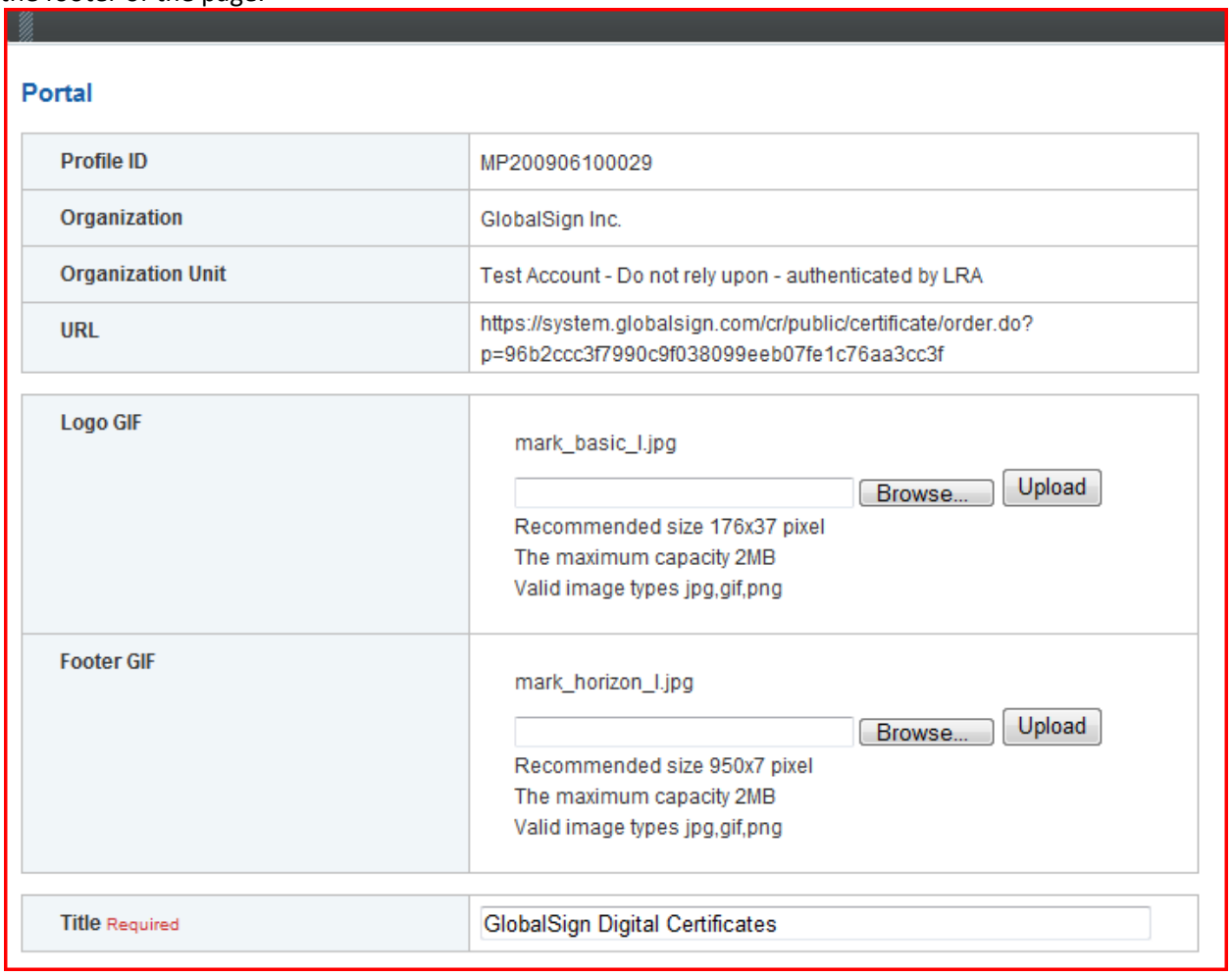
enrollmentpage (Portal Link). Anybody within your organization will then be able to make an application for a Certificate through the account by leveraging the Pre-vetted company information.

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.

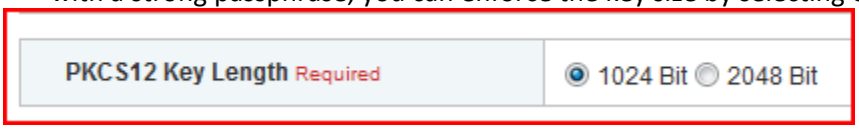


Optionally, by clicking Next after selecting a particular profile, the ePKI Administrator may upload a logo to be displayed on the top banner of the end user enrollment page as well as a GIF to be displayed at the footer of the page.



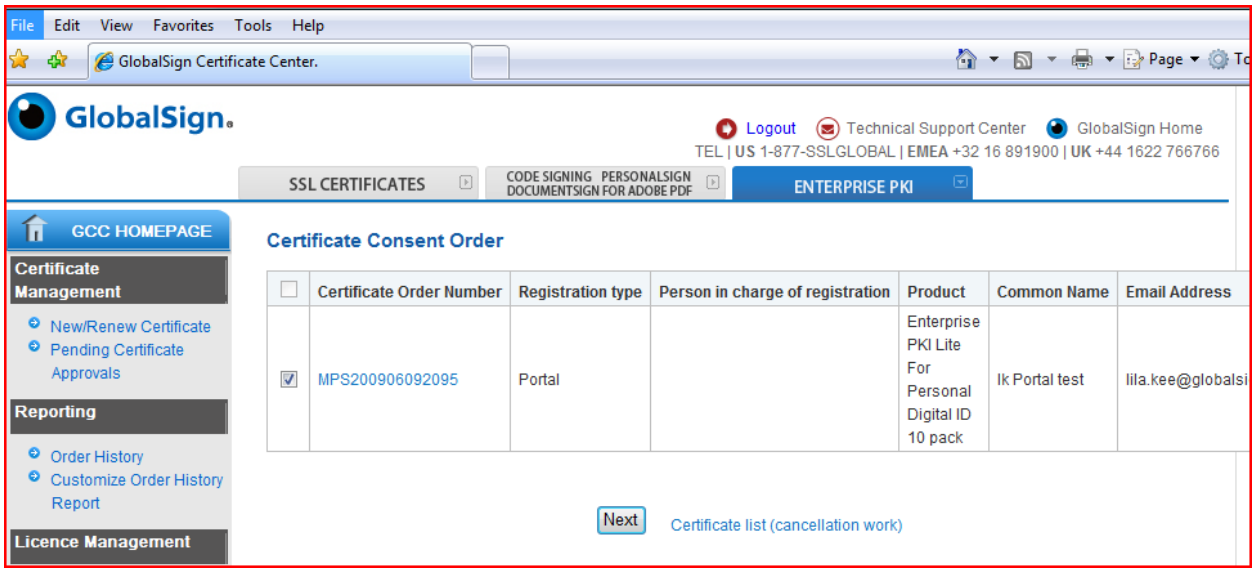
Other Portal Configurable Options:

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:

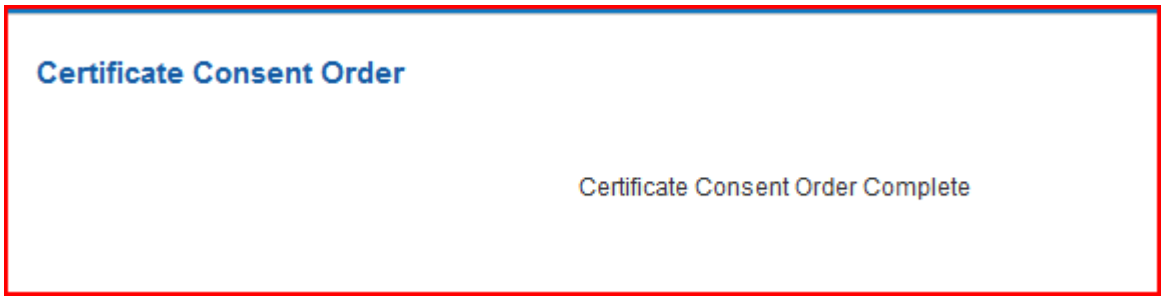


Approving Requests (Orders)

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 will 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.

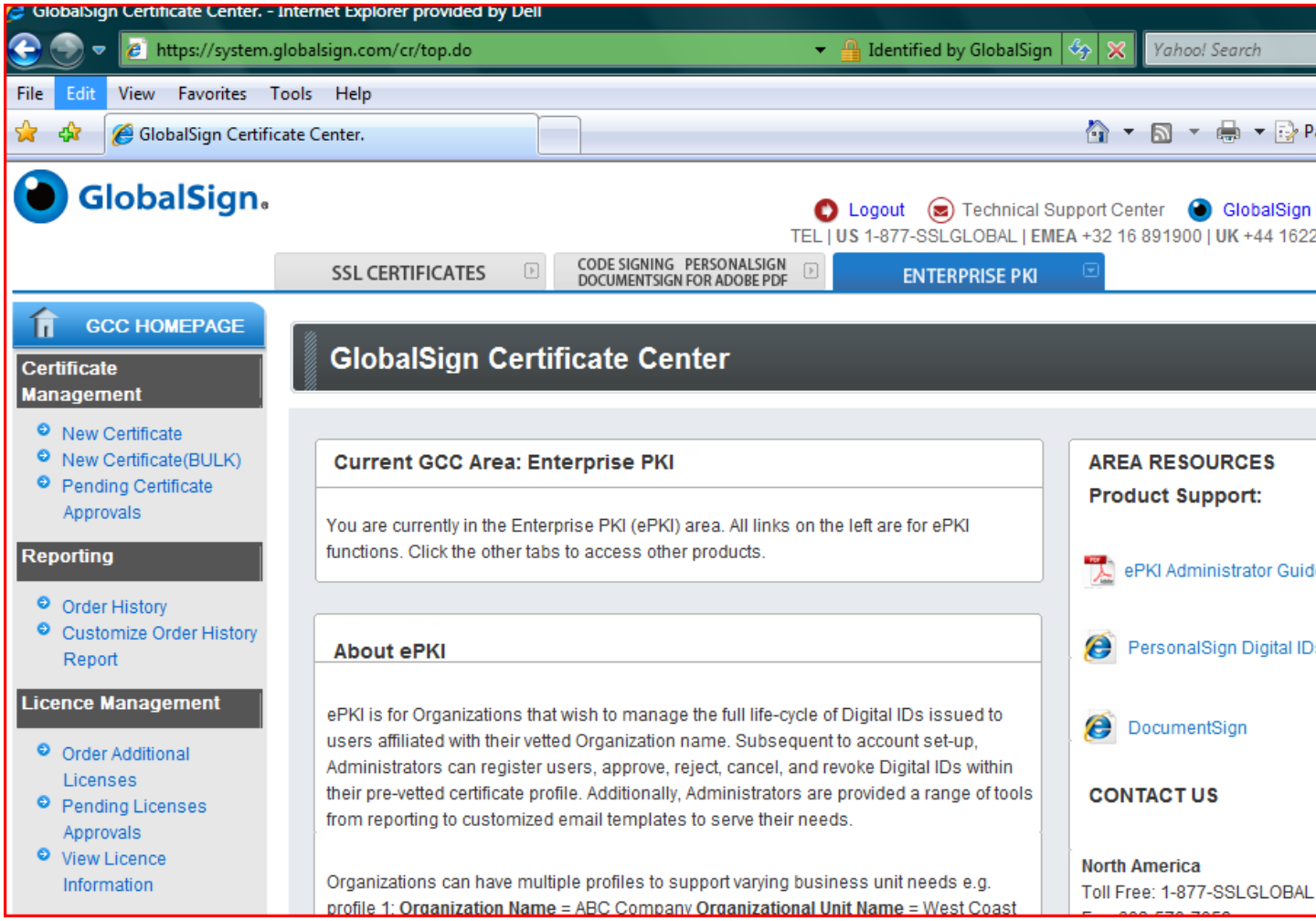


Register Users via ePKI Administrator

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

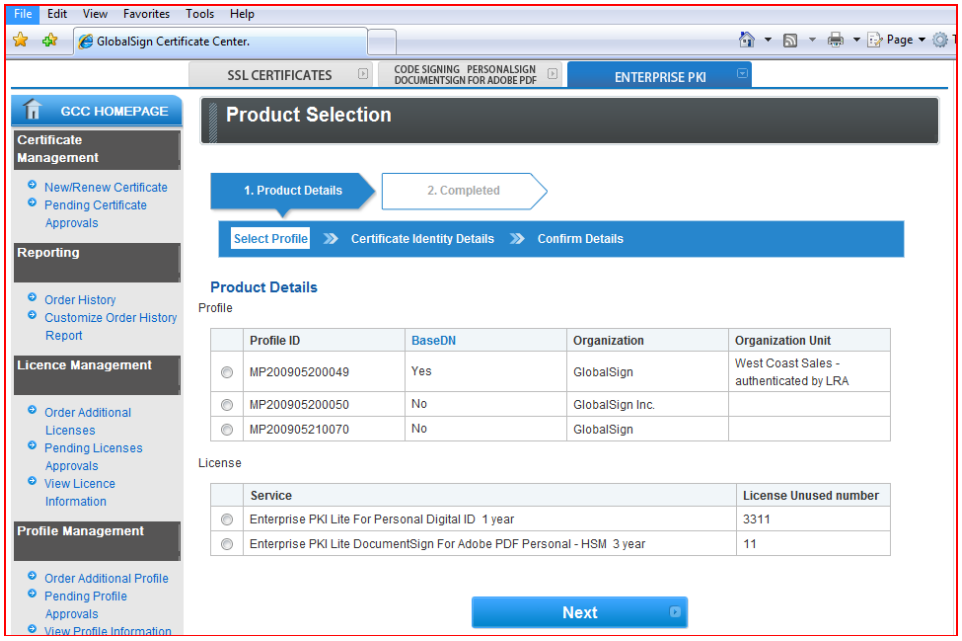
1. Single – New Certificate
2. Multiple – New Certificate (BULK)

These links are found under the Certificate Management menu.



Single User Registration

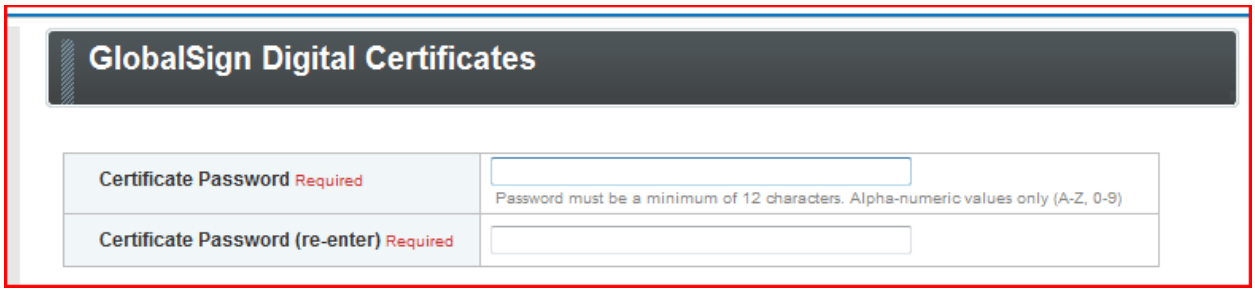
For individual registrations, Click “New Certificate” and then select the Certificate Profile and License you wish to apply the certificate request to:



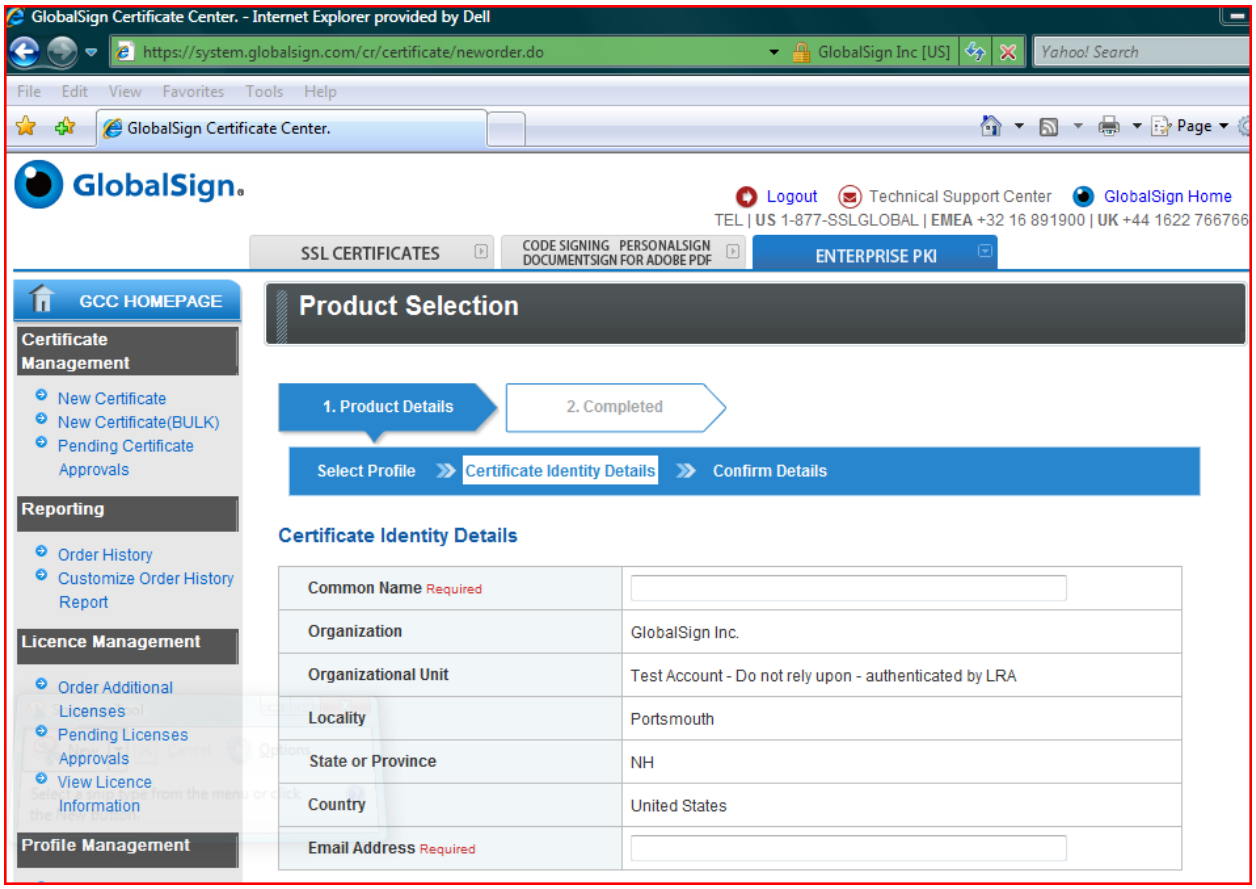
Click “Next” and complete the certificate identity details for the end user Subscribers. Note certain pre-vetted fields will be hardcoded. Additionally, establish a “Pickup Password” or use the “Password Generation” tool that you are required to deliver to the Subscriber in an “Out of Band” method. As 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.

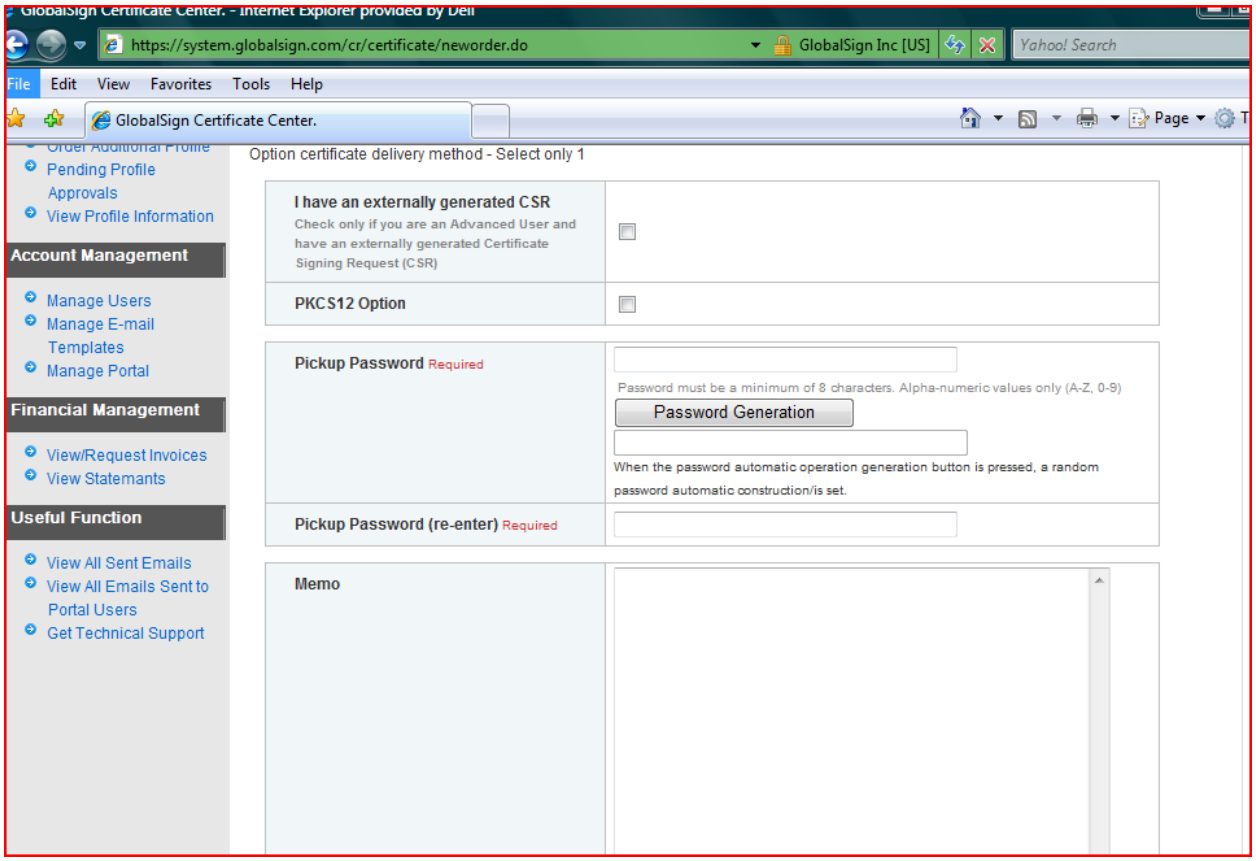
Optionally, the ePKI Administrator may select alternative certificate enrollment methods to the default PKCS7 method where key generation is performed locally via the Subscriber’s browser.

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:

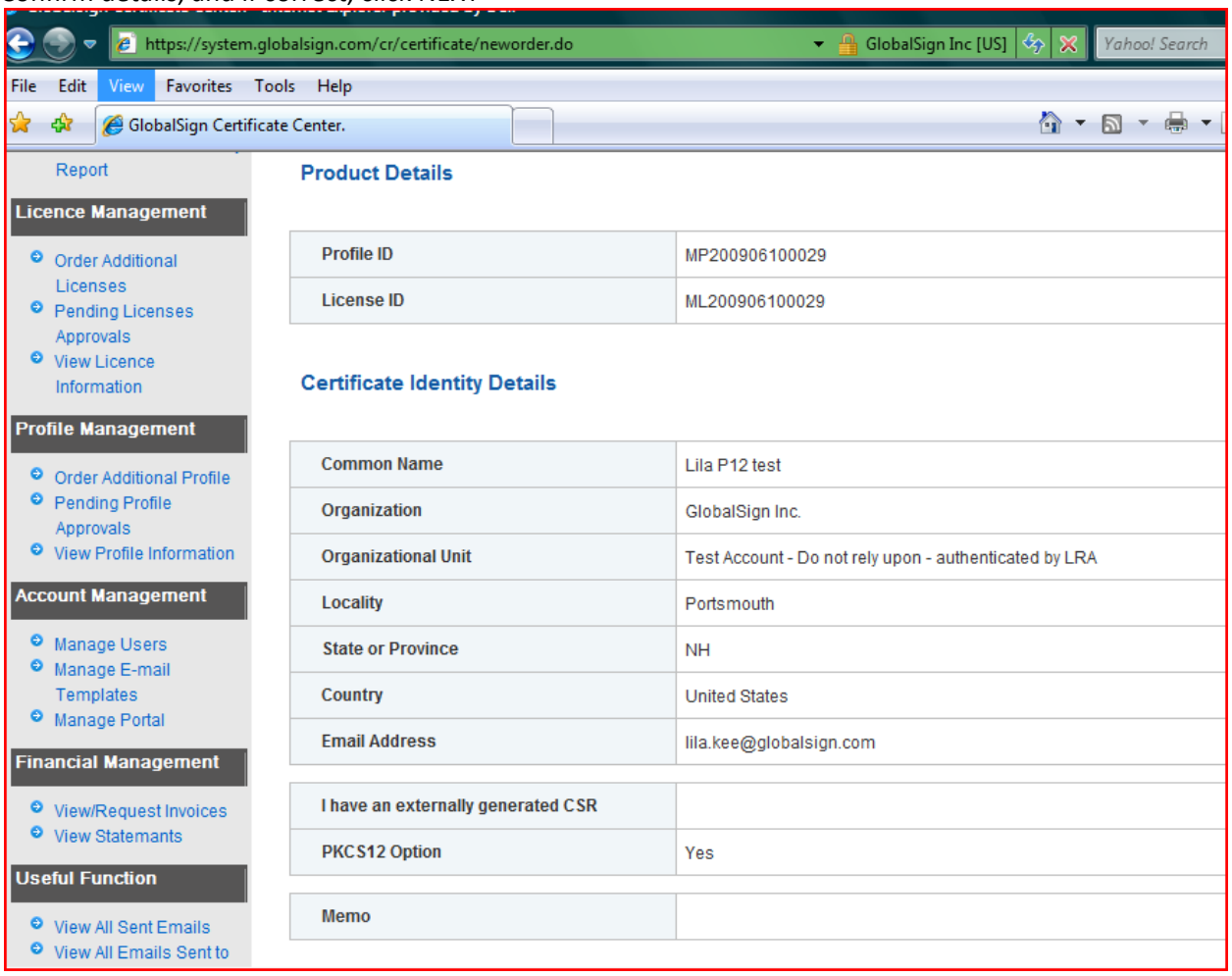


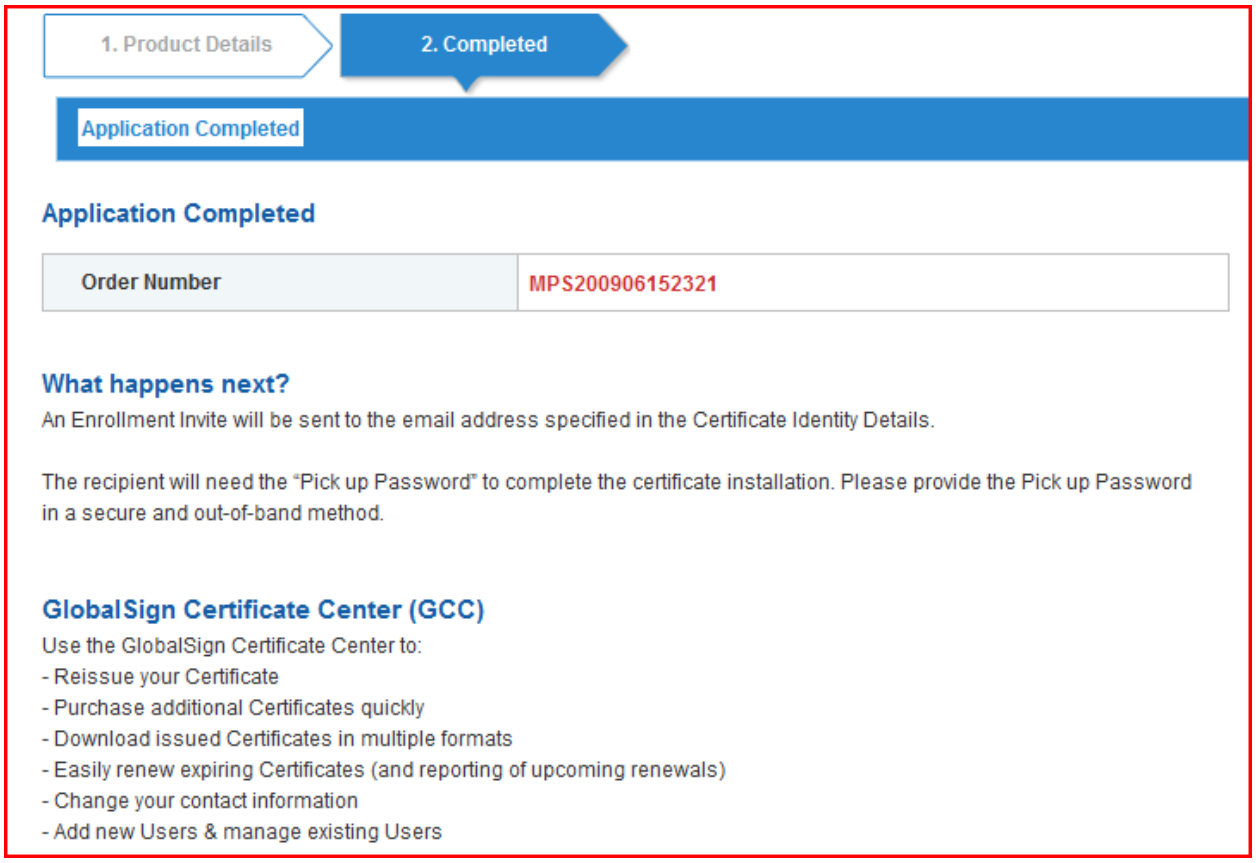
b. P12 file purge. Note GlobalSign will purge all P12 files . therefore it is recommended that Subscribers import the P12 file by marking the private key as exportable and then make a back-up. (See GlobalSign Support for additional details).




GlobalSign Certificate Center. - Internet Explorer provided by Dell
https://system.globalsign.com/cr/certificate/neworder.do
GlobalSign Inc [US]
Yahoo! Search
File Edit View Favorites Tools Help
GlobalSign Certificate Center.
Page
Pending Profile Approvals
View Profile Information
Account Management
Manage Users
Manage E-mail Templates
Manage Portal
Financial Management
View/Request Invoices
View Statemants
Useful Function
View All Sent Emails
View All Emails Sent to Portal Users
Get Technical Support
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)
PKCS12 Option
Pickup Password Required
Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9)
Password Generation
When the password automatic operation generation button is pressed, a random password automatic construction/is set.
Pickup Password (re-enter) Required
Memo

Confirm details, and if correct, click NEXT

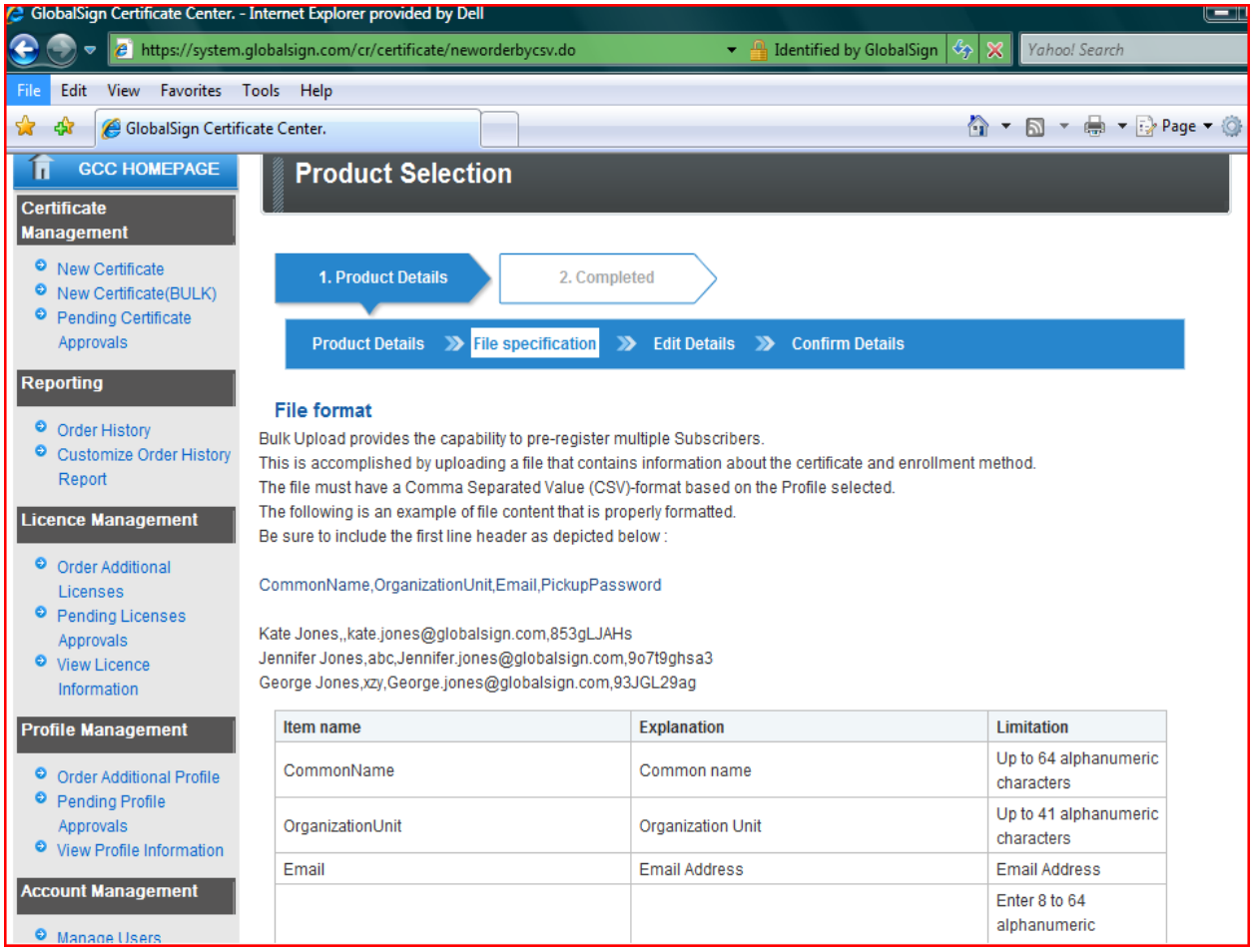


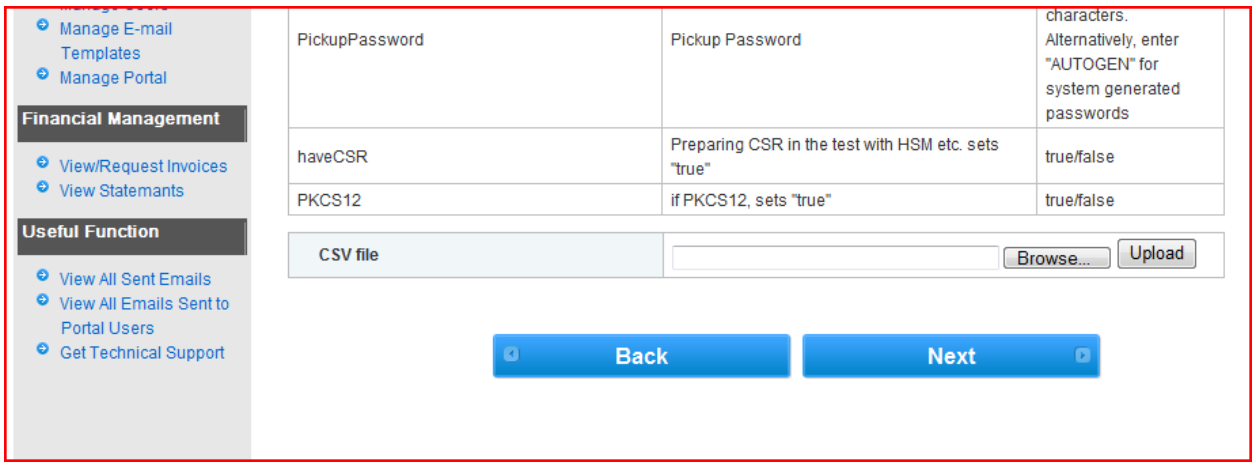

1. Product Details
2. Completed
Application Completed
Application Completed
Order Number
MPS200906152321
What happens next?
An Enrollment Invite will be sent to the email address specified in the Certificate Identity Details.
The recipient will need the "Pick up Password" to complete the certificate 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

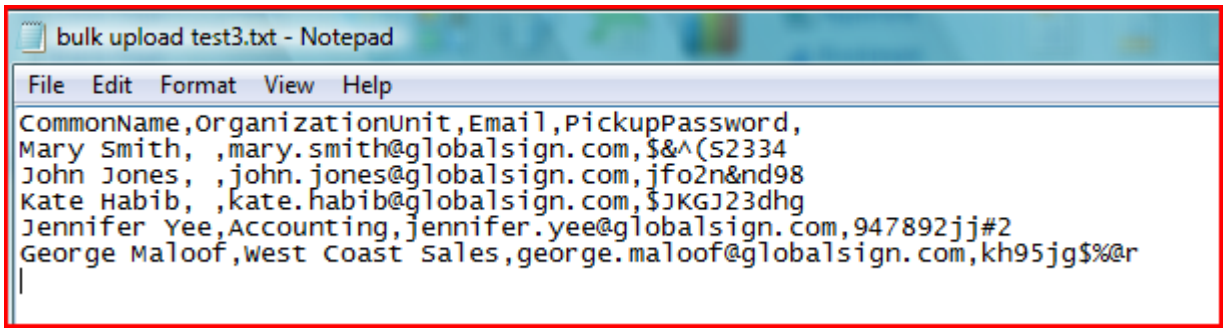
For multiple user registration, Click “New Certificate (BULK)” and then select the Certificate Profile and License you wish to apply the certificate requests to. Click NEXT to continue.

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 be pre-established as part of a “Locked O and OU Profile.



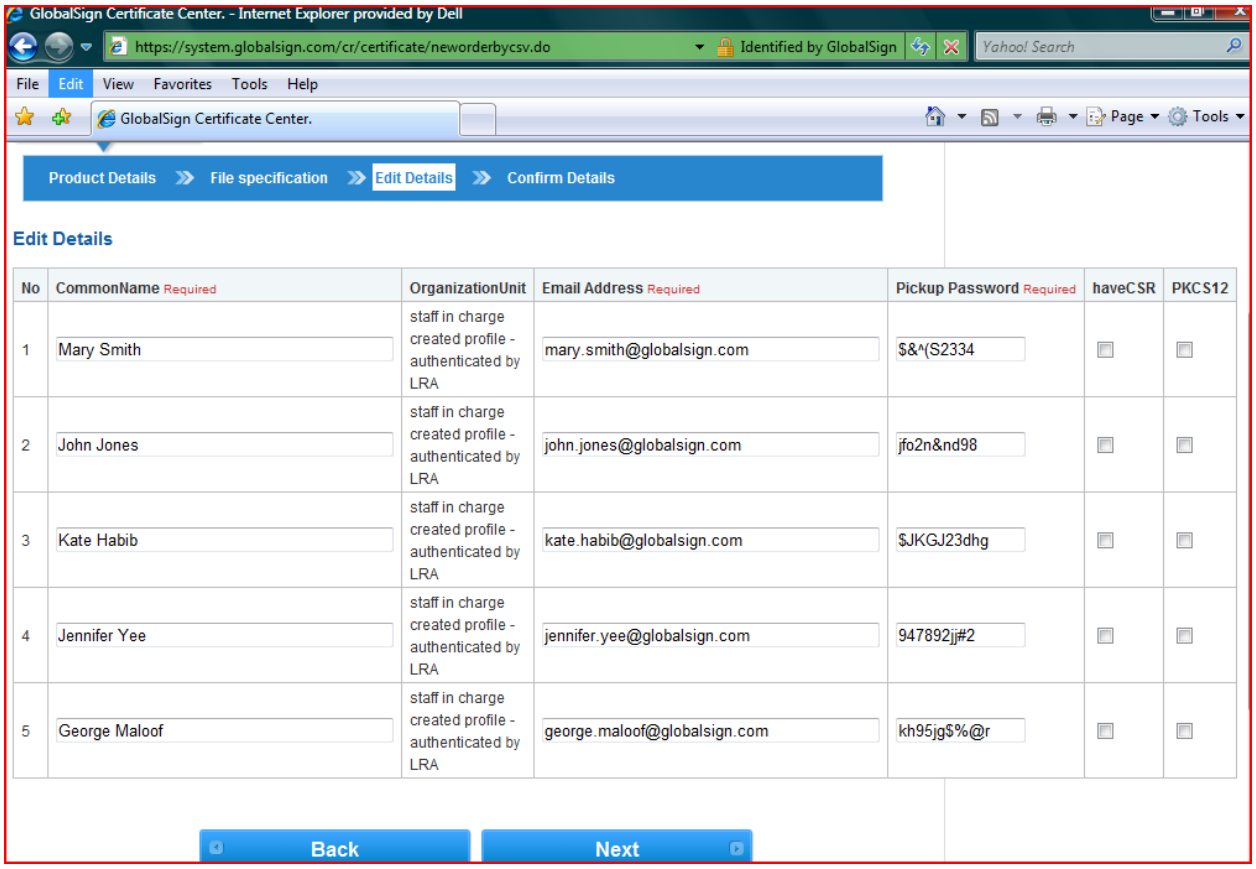

Manage E-mail Templates
Manage Portal
Financial Management
View/Request Invoices
View Statemants
Useful Function
View All Sent Emails
View All Emails Sent to Portal Users
Get Technical Support
PickupPassword
Pickup Password
characters. Alternatively, enter "AUTOGEN" for system generated passwords
haveCSR
Preparing CSR in the test with HSM etc. sets "true"
true/false
PKCS12
if PKCS12, sets "true"
true/false
CSV file
Browse...
Upload
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.



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.

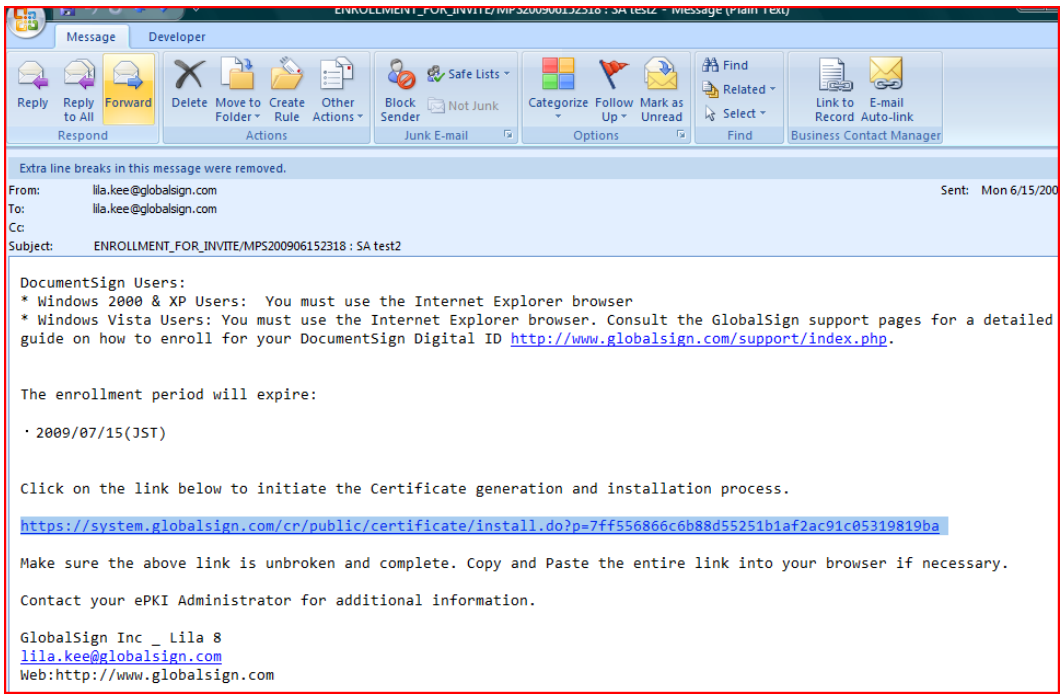


To complete the process, click NEXT and securely distribute the Certificate pick-up passwords to the Users.

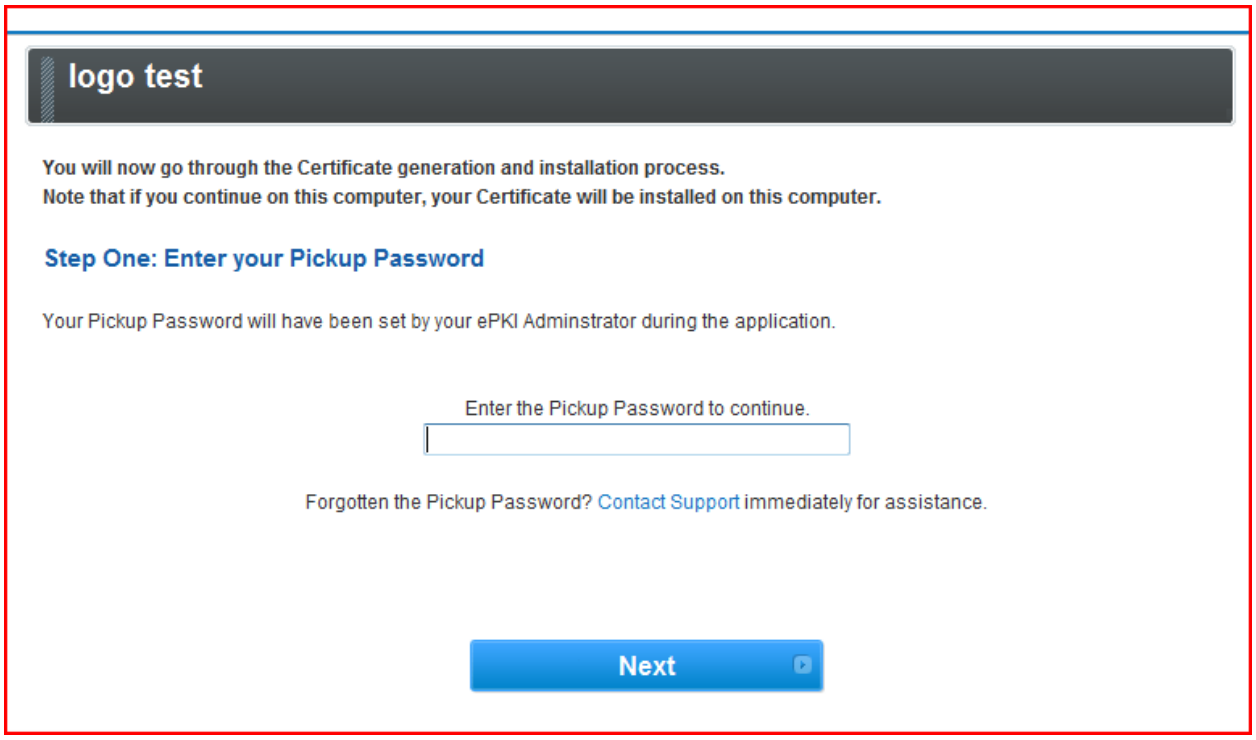
End user Installation

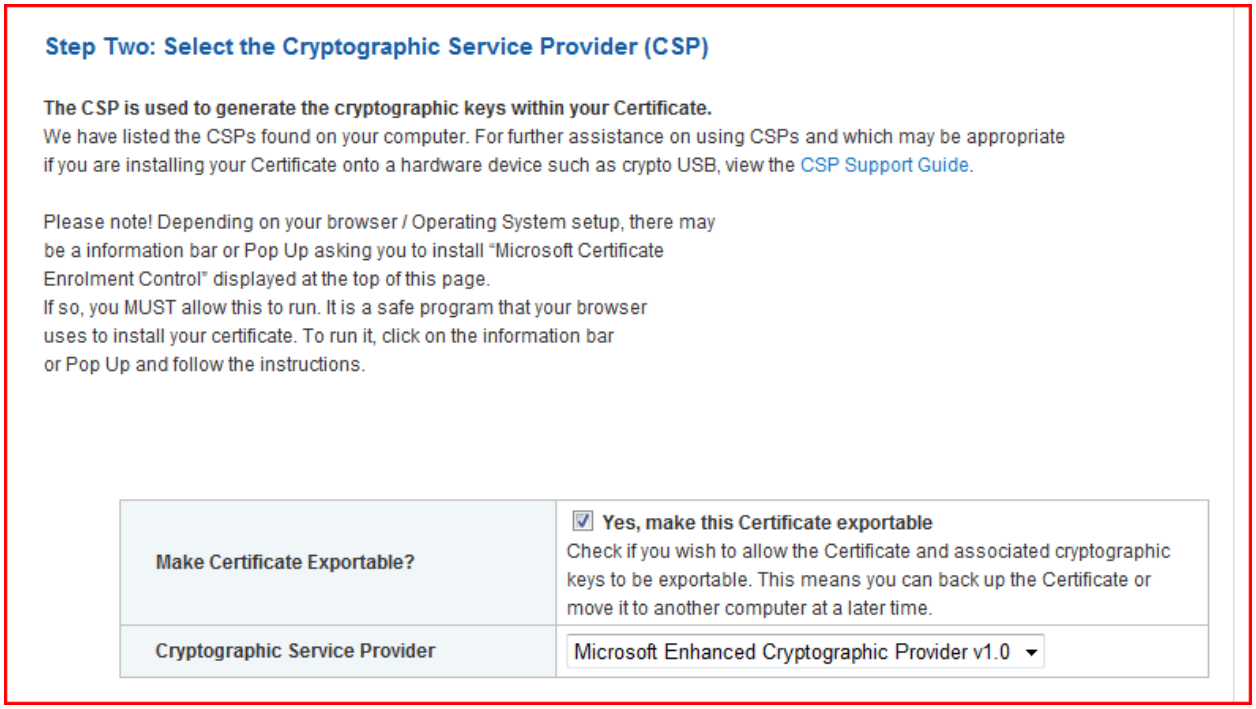
Subsequent to a certificate registration initiated by an ePKI Administrator, an email will be sent to the address identified in the certificate details.

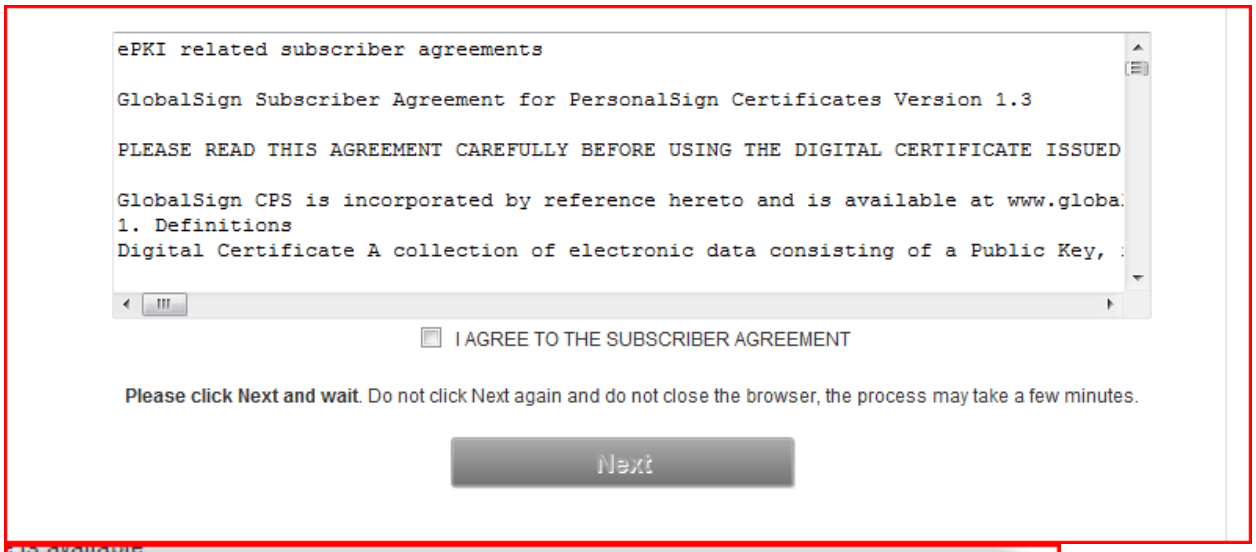
Email contents may be modified (see Customize Email Templates), however a standard message will include a “pick-up” url used to enroll for the digital certificate.

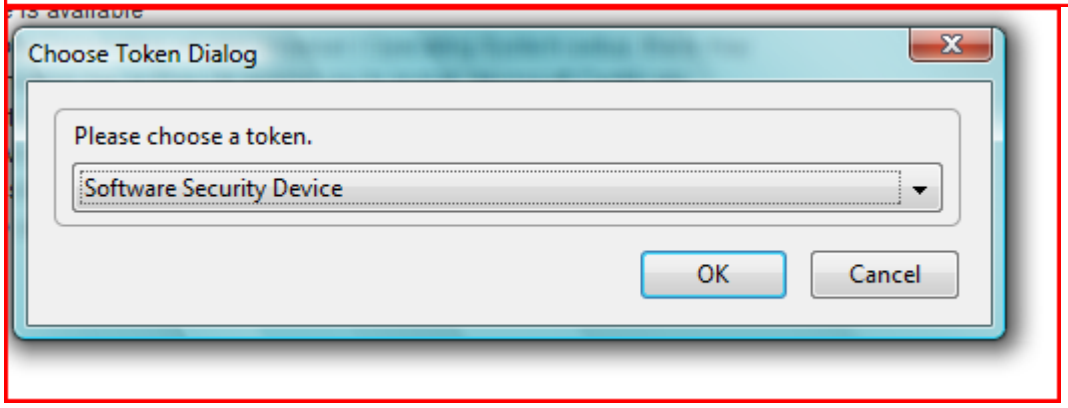


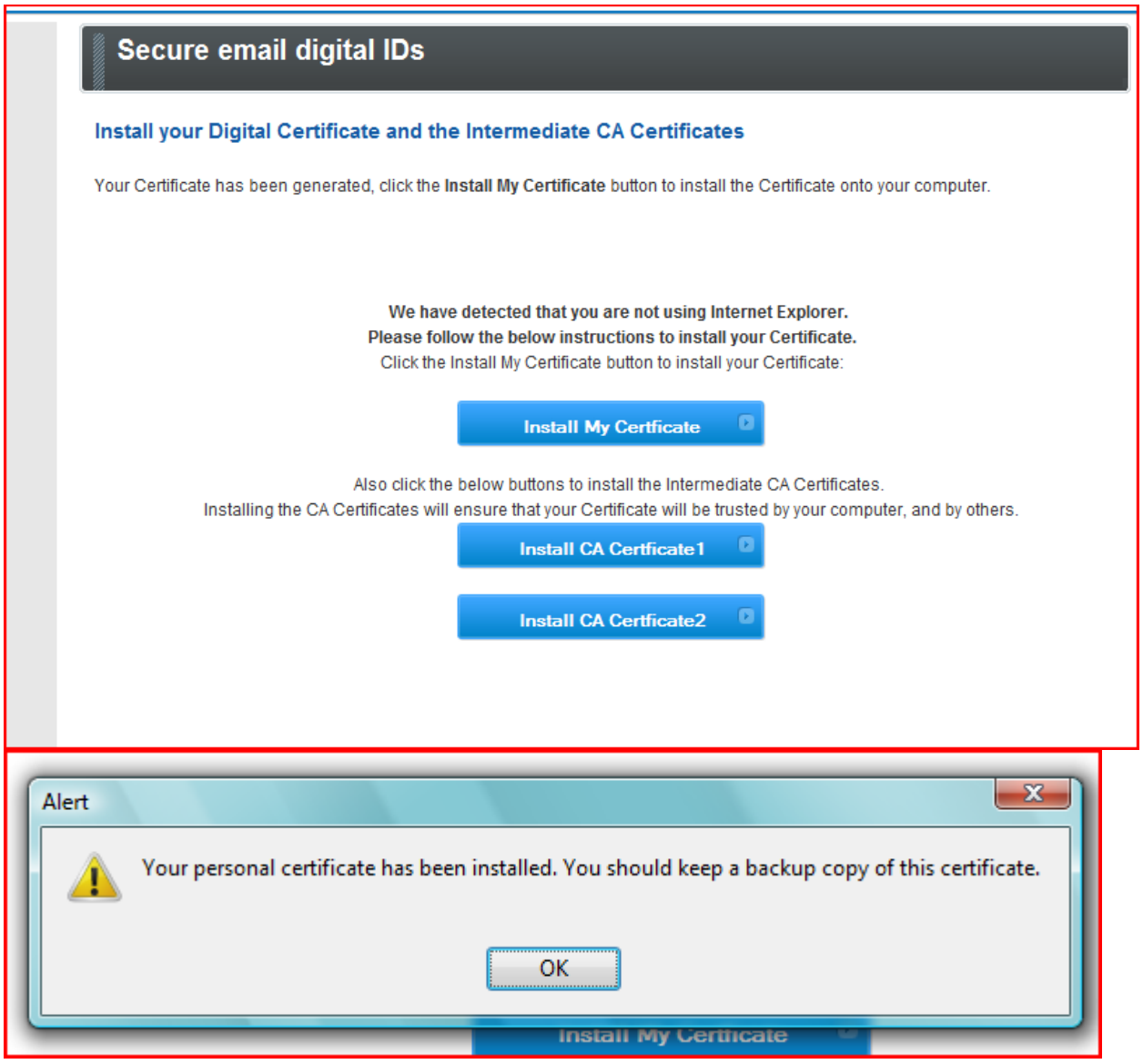
Clicking on the Certificate Pick up URL will direct the subscriber to several additional steps depending on specific product configuration selected by the ePKI Administrator. Following is an example of a PersonalSign Pro certificate enrollment using a standard browser key generation method.






ePKI related subscriber agreements
GlobalSign Subscriber Agreement for PersonalSign Certificates Version 1.3
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED
GlobalSign CPS is incorporated by reference hereto and is available at www.globa
1. Definitions
Digital Certificate A collection of electronic data consisting of a Public Key,
I AGREE TO THE SUBSCRIBER AGREEMENT
Please click Next and wait. Do not click Next again and do not close the browser, the process may take a few minutes.
Next


Choose Token Dialog
Please choose a token.
Software Security Device
OK
Cancel

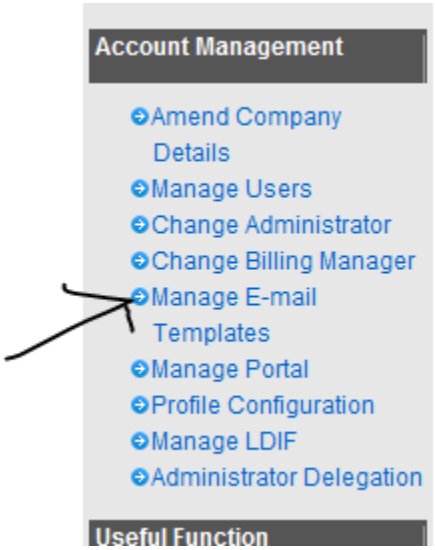


Please consult PersonalSign and DocumentSign Product specific guides for additional details http://www.globalsign.com/support/index.php.

Bulk Provisioning

BEFORE YOU BEGIN:

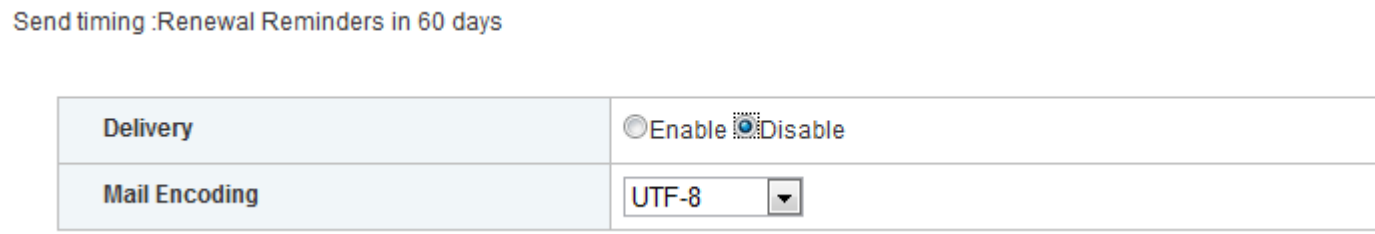
1. There is a 200 record limit (3.2M) and depending on key size selected, the ZipFile containing PKCS12s may take up to 40 minutes to process.
2. Disable all renewal messages to prevent system generated email reminders from going directly to your end user. You can do this by:
    a. Disable Renewal reminder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



b) And “edit” any template that is marked “True”

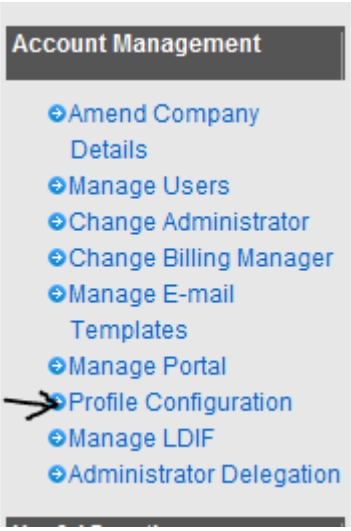
Renewal Reminders Today	true	Edit
Renewal Reminders	true	Edit
Renewal Reminders in 7 days	true	Edit
Renewal Reminders in 14 days	true	Edit
Renewal Reminders in 21 days	true	Edit
Renewal Reminders in 30 days	true	Edit
Renewal Reminders in 60 days	false	Edit
Renewal Reminders in 90 days	false	Edit

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



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”

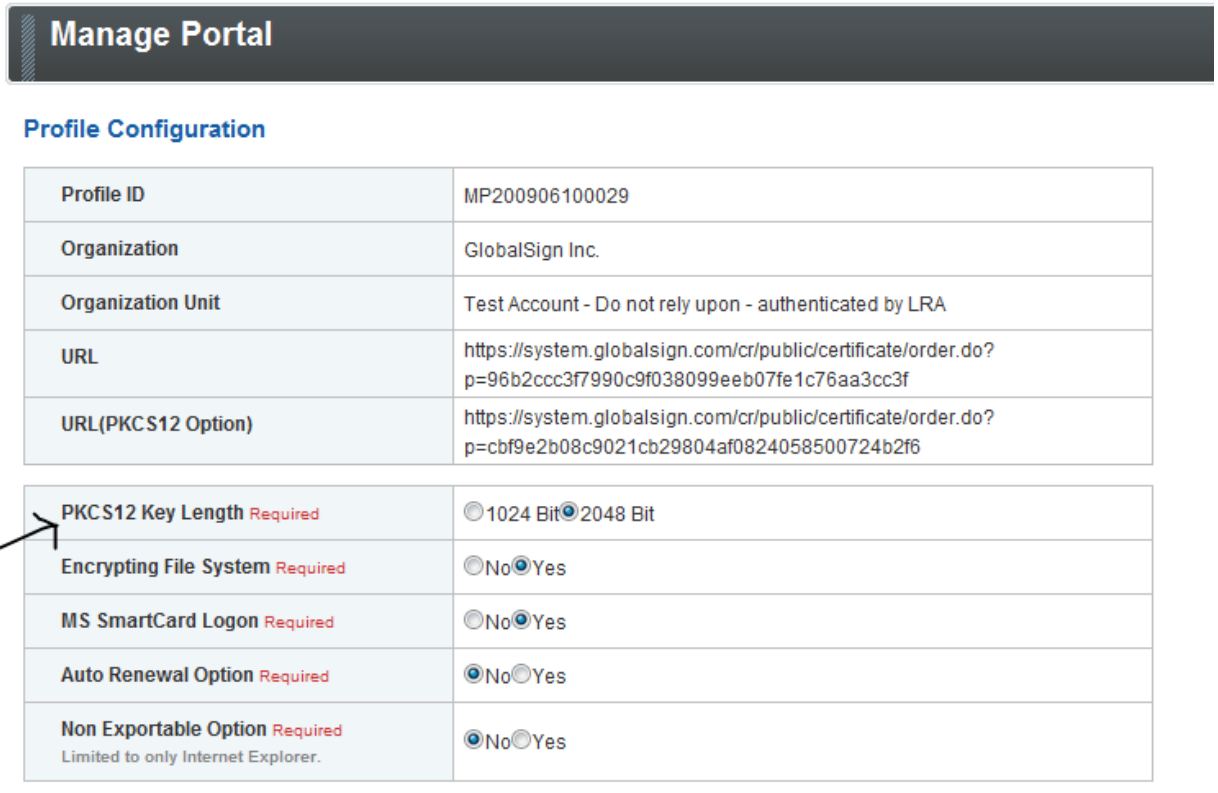


b) If you have more than a single Profile, click on the radio button next to the Profile you wish to configure and then Click Next.

○	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	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

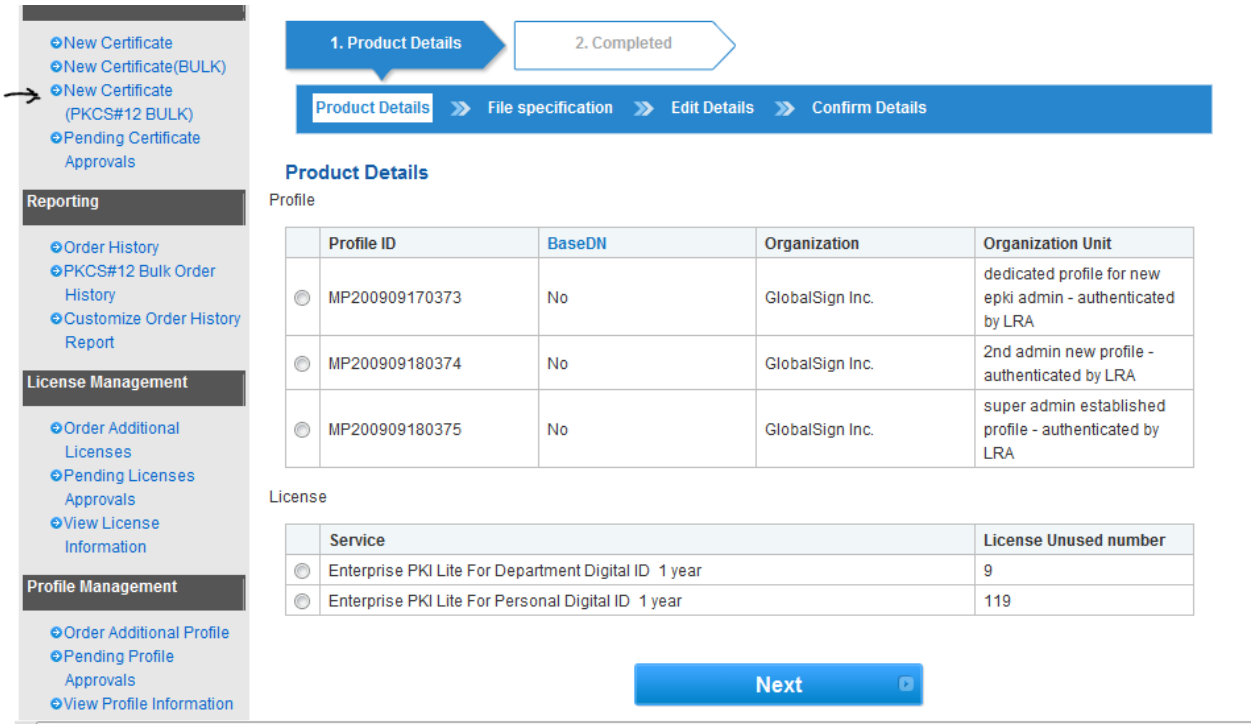
c) Select desired key size.



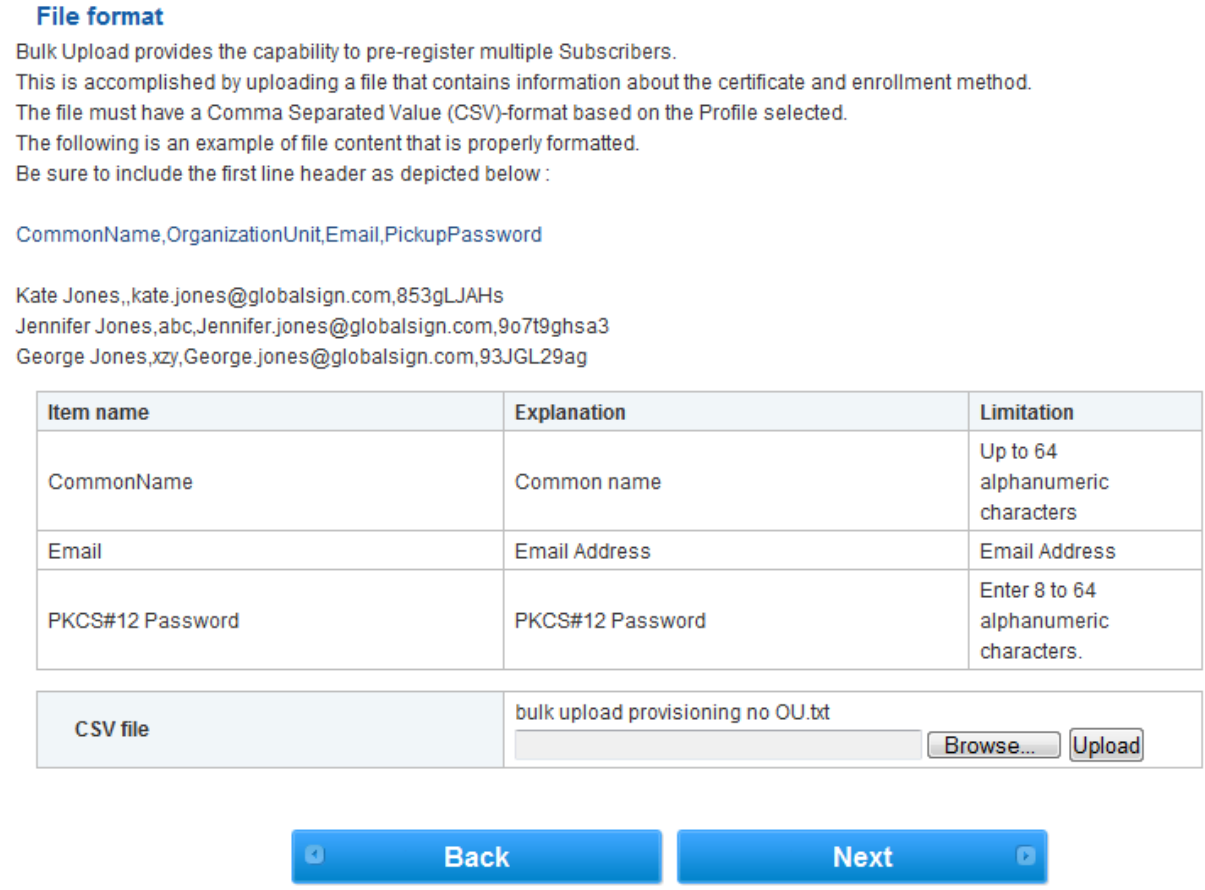
Bulk provisioning provides an alternative to bulk enrollment in that the enrollment steps perform by the end user are minimized or in some cases totally eliminated. The bulk provisioning feature provides the following benefits:

- 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



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 :

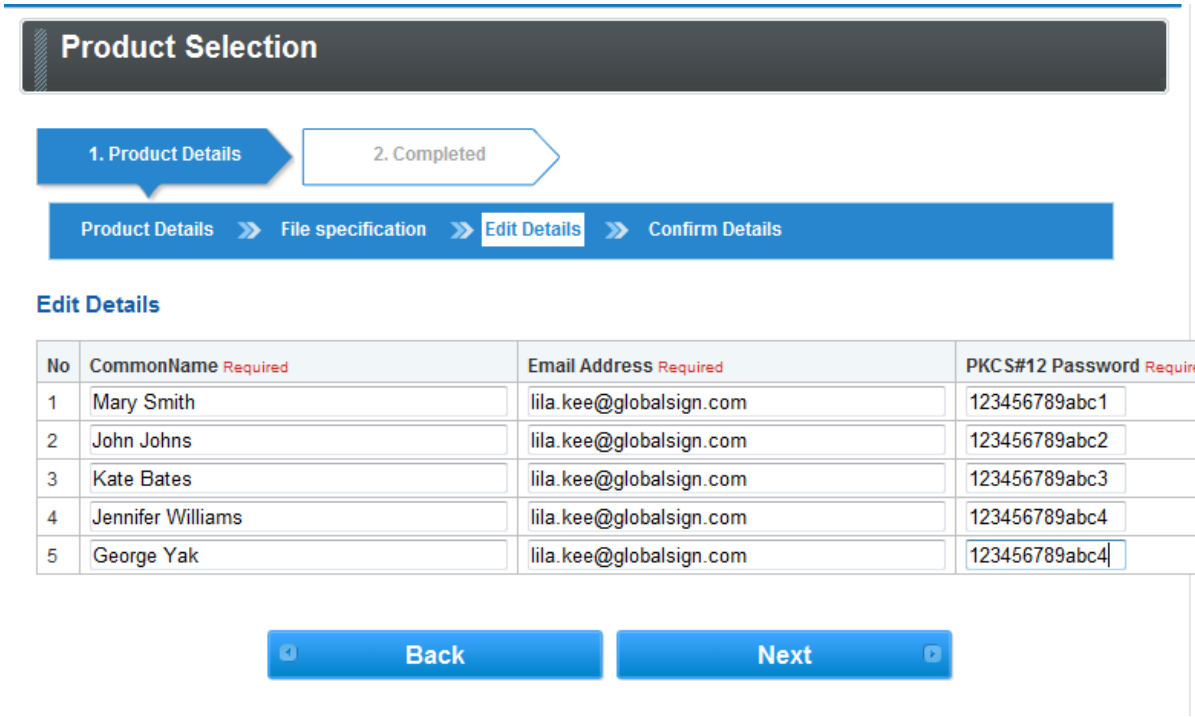
CommonName,OrganizationUnit,Email,PickupPassword

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

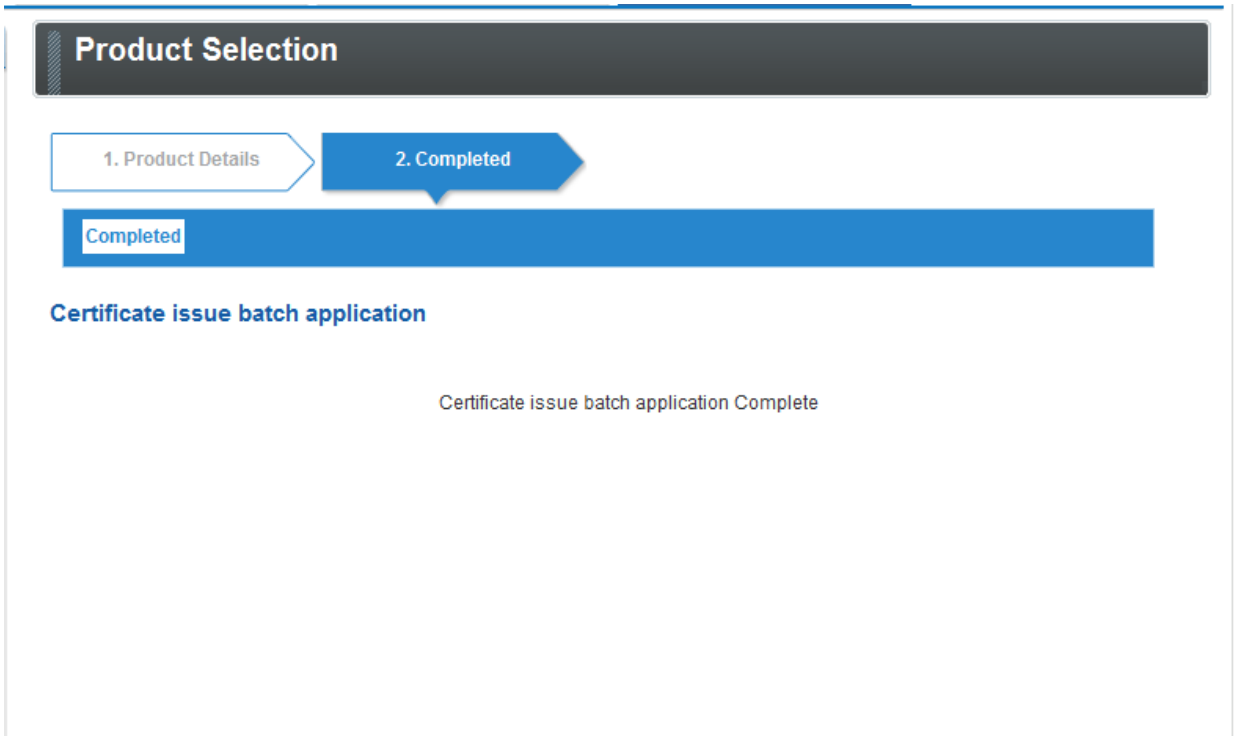
Item name	Explanation	Limitation
CommonName	Common name	Up to 64 alphanumeric characters
Email	Email Address	Email Address
PKCS#12 Password	PKCS#12 Password	Enter 8 to 64 alphanumeric characters.

CSV file	bulk upload provisioning no OU.txt Browse... Upload

Back Next

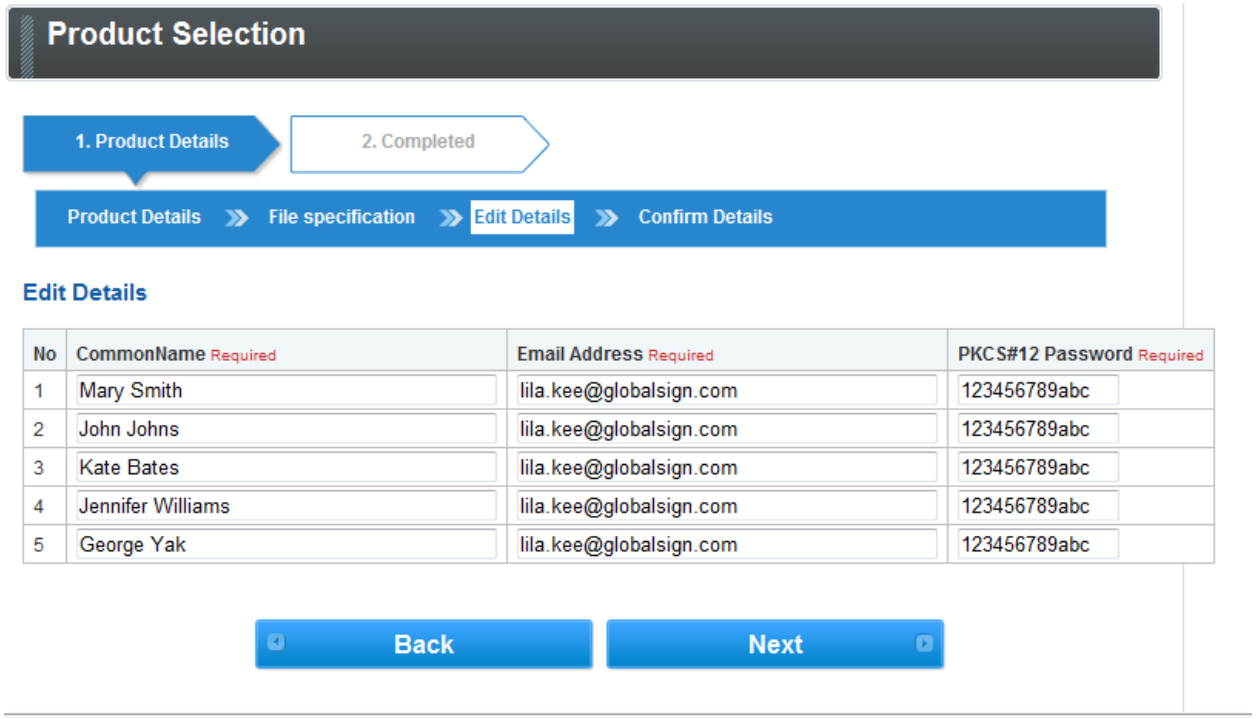


4. Certificate generation complete



5.

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



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

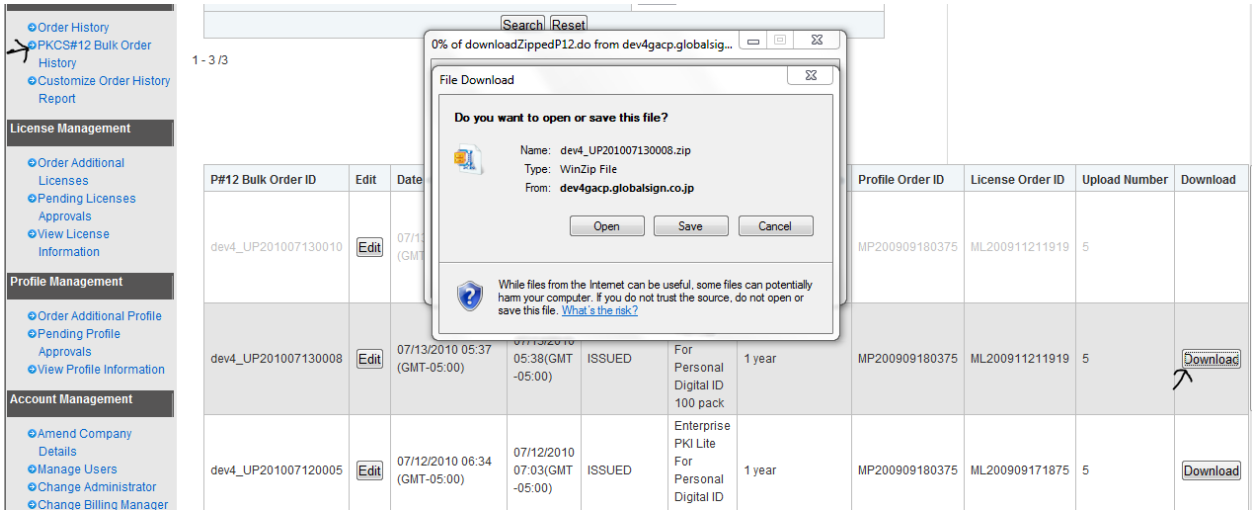
Kate Jones,,kate.jones@globalsign.com,853gLJAHs
Jennifer Jones,abc,Jennifer.jones@globalsign.com,9o7t9ghsa3
George Jones,xzy,George.jones@globalsign.com,93JGL29ag

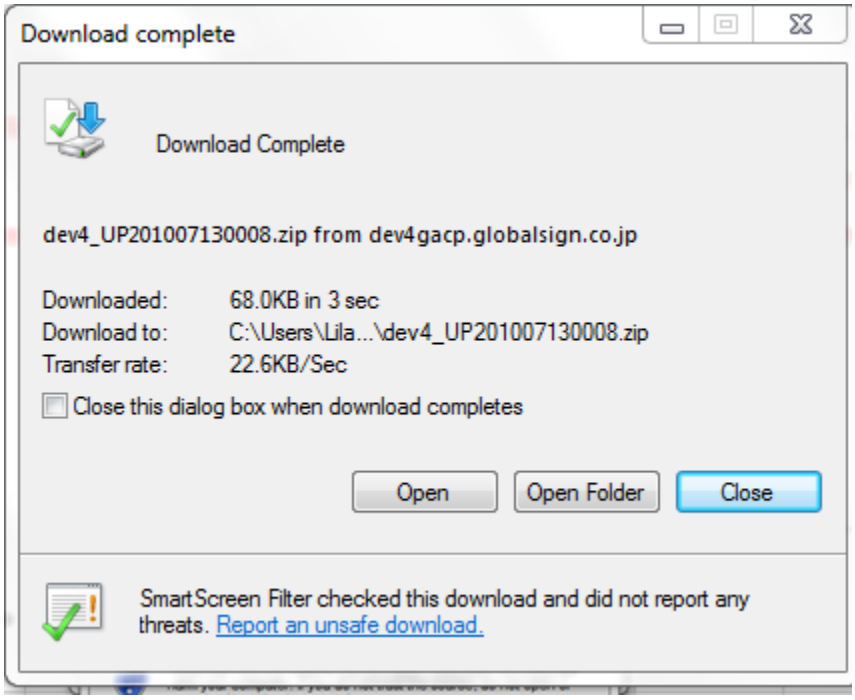
Item name	Explanation	Limitation
CommonName	Common name	Up to 64 alphanumeric characters
Email	Email Address	Email Address
PKCS#12 Password	PKCS#12 Password	Enter 8 to 64 alphanumeric characters.

CSV file	Browse... Upload

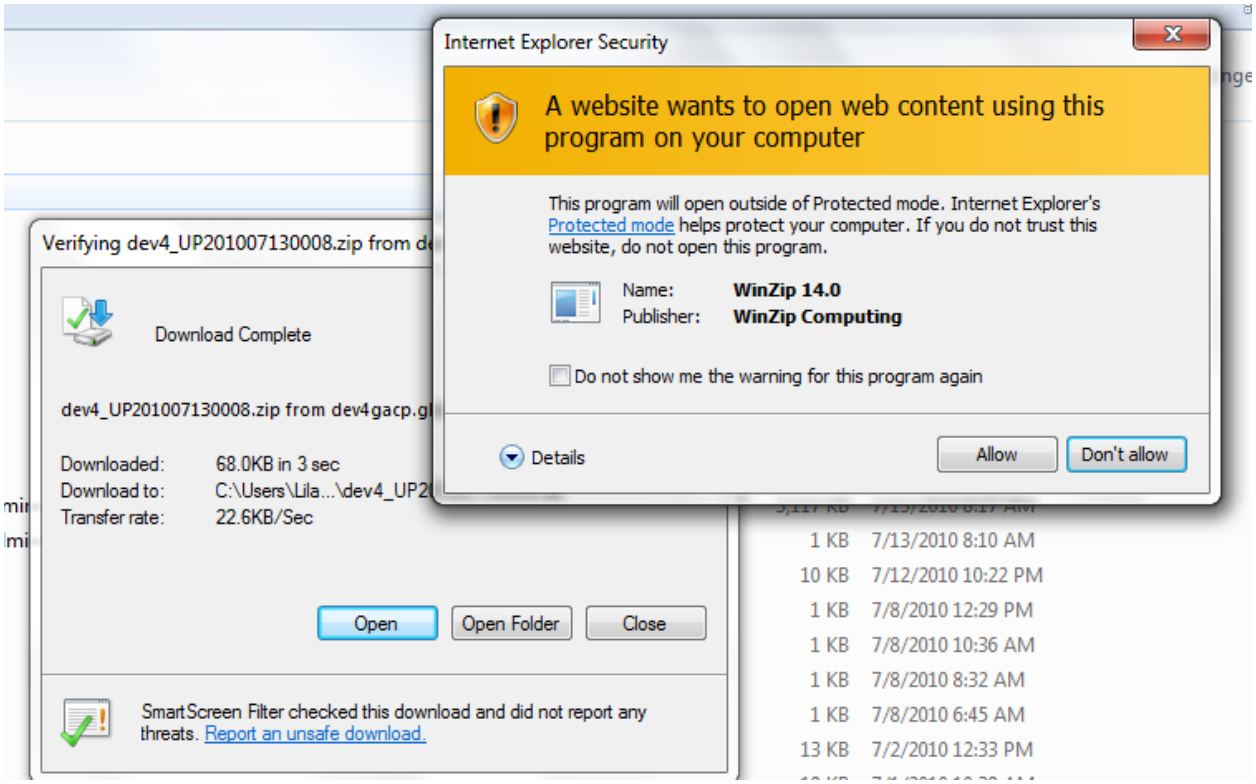
Back Next

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).

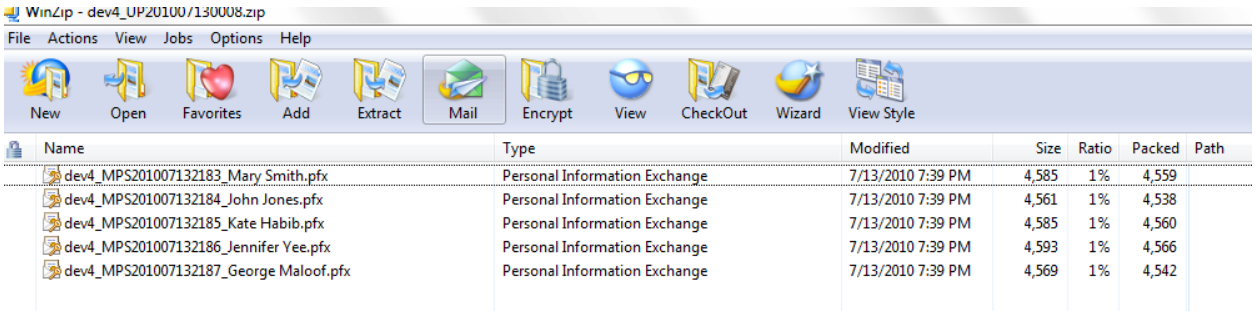




When download is complete, Click open and if prompted “Allow” IE security warning.:

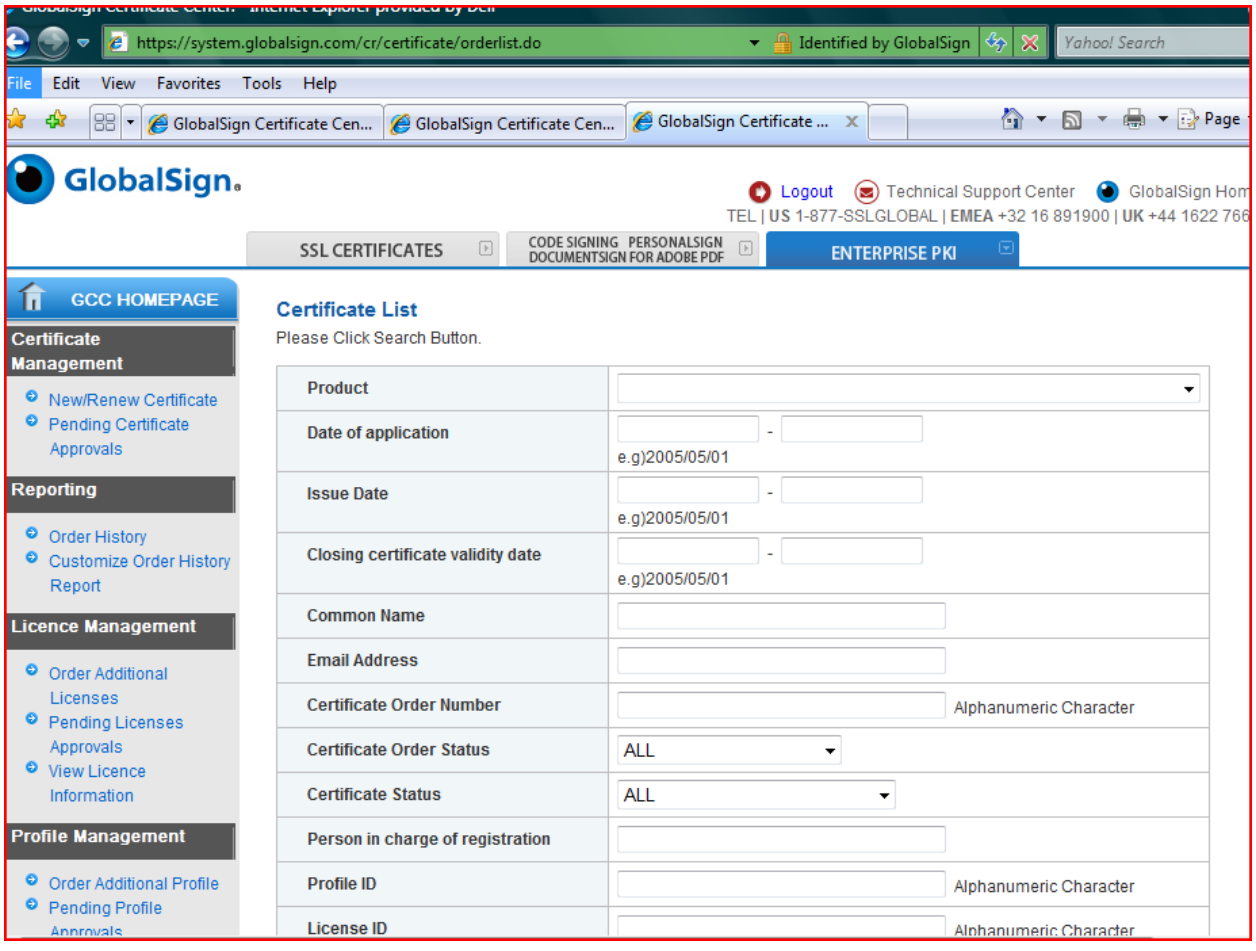


Note, individual file names will be identified using the common name of the certificate specified at registration. Also note, you will need the P12 passphrase also established at Registration to install the certificate.

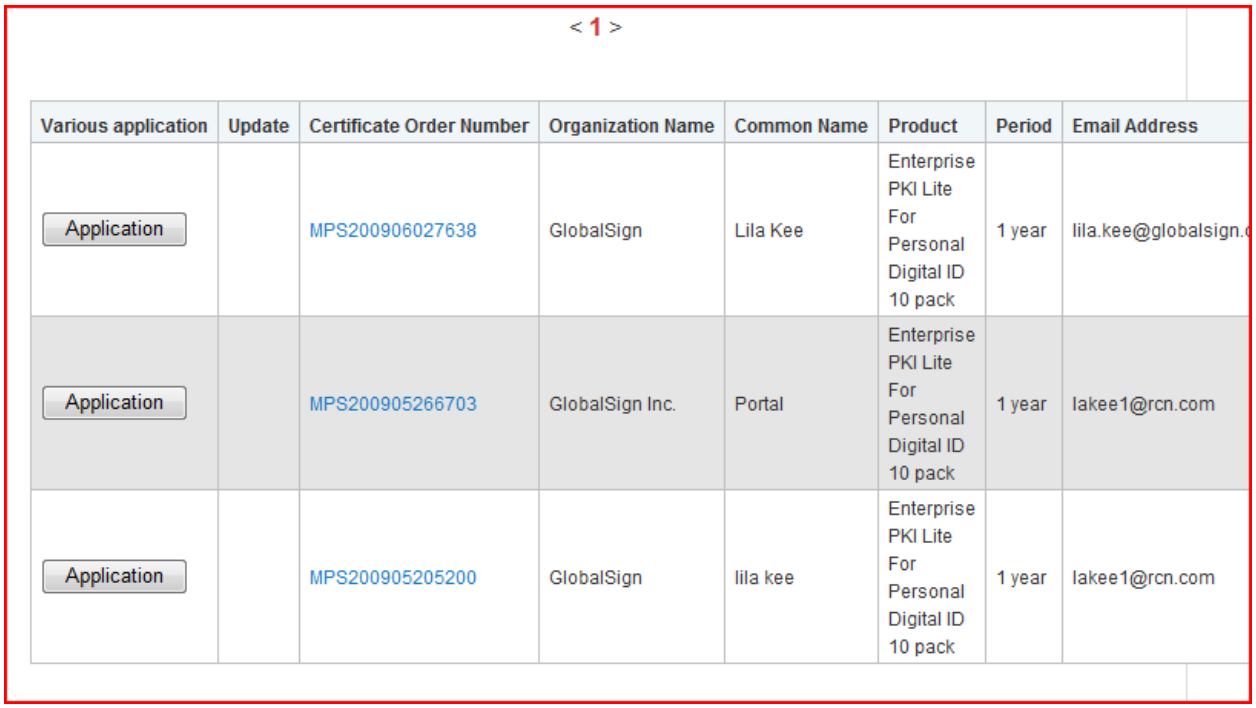


Reporting

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.



Then click “Application” next to the order you wish to review.

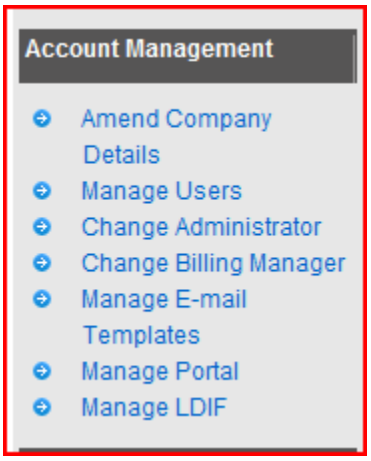


LDIF

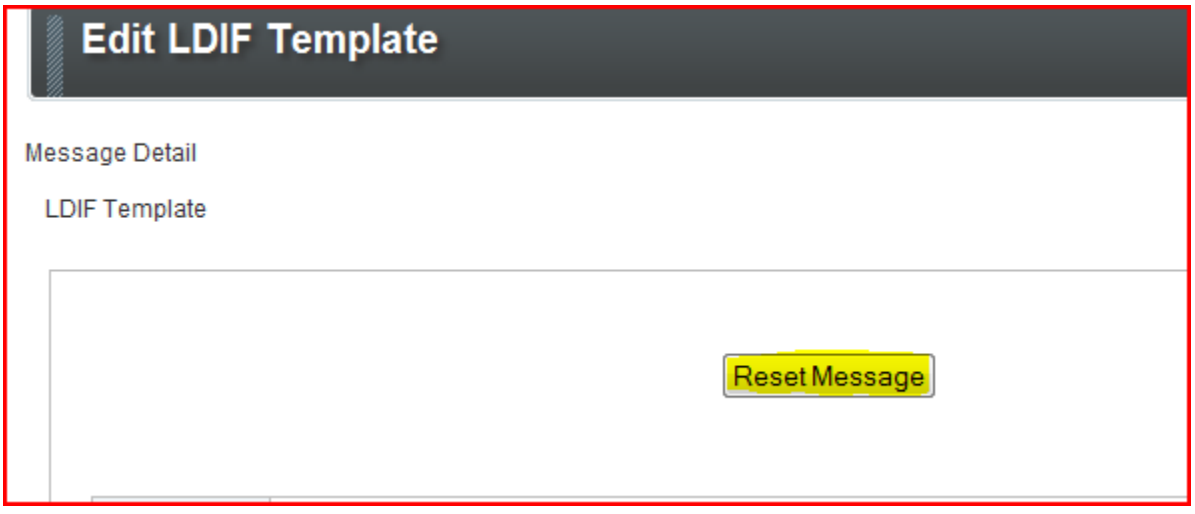
ePKI Administrators may wish to upload the public certificates associated with their ePKI service to a directory. ePKI provides a method to generate a LDIF (Lightweight Directory Access Protocol) report for upload to a LDAP directory.

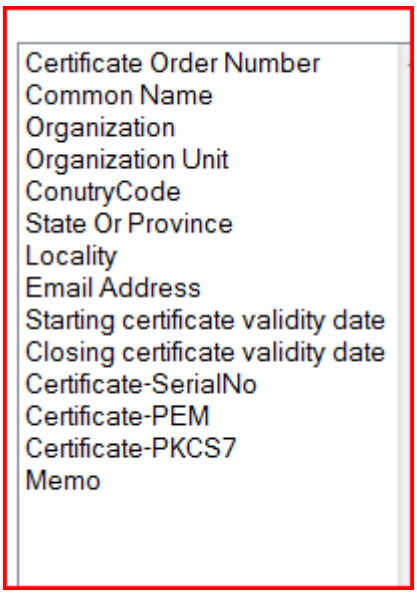
Configuring LDIF

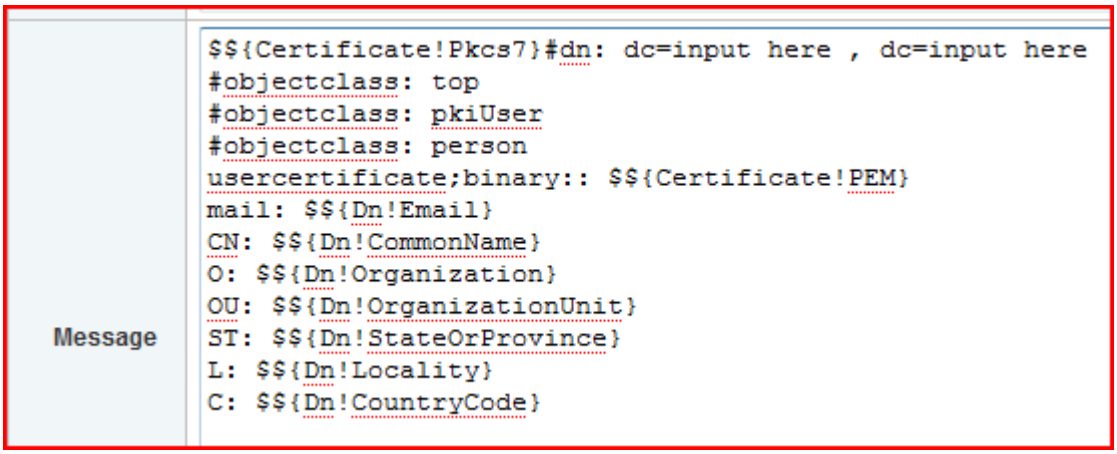
LDIF reports can be formatted by the ePKI Administrator via the "Manage LDIF" link found under "Account Management".



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:

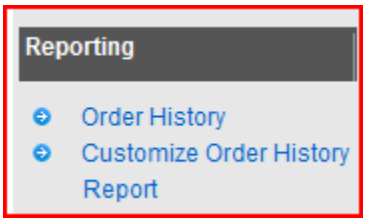




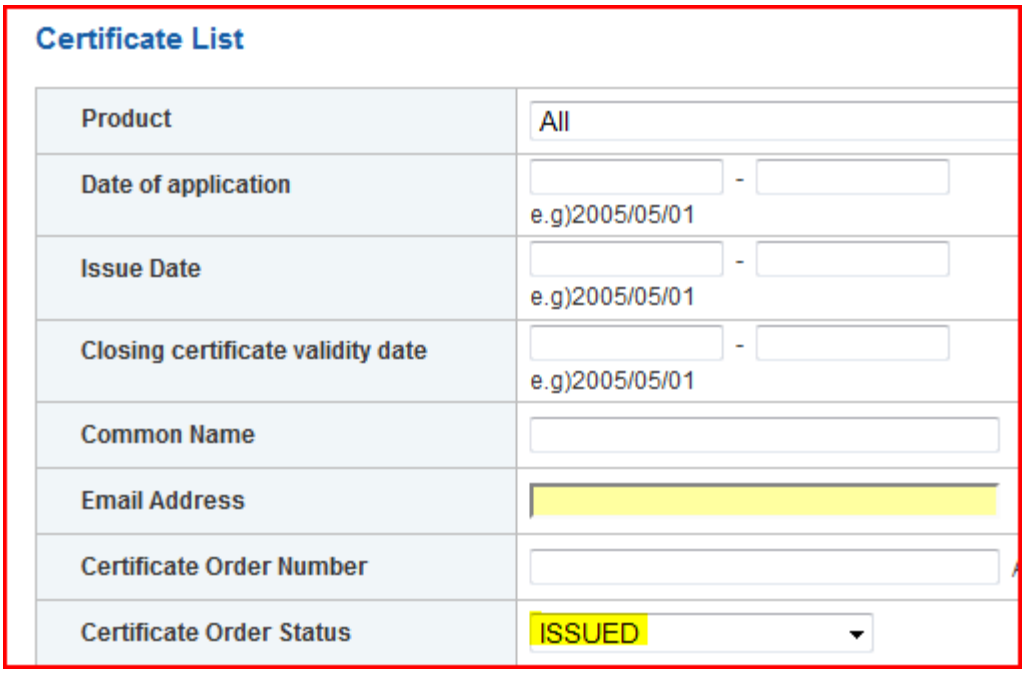


Generating a LDIF Report

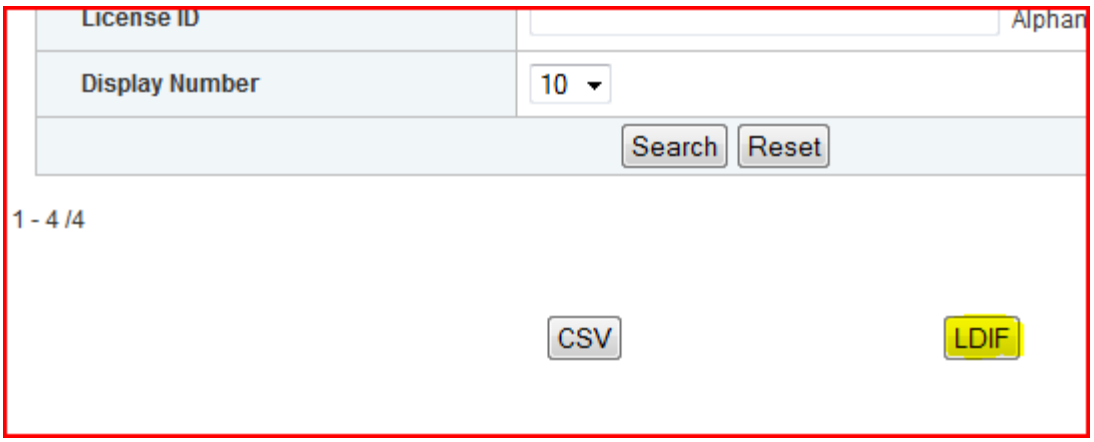
LDIF reports are generated from the “Order History” link.



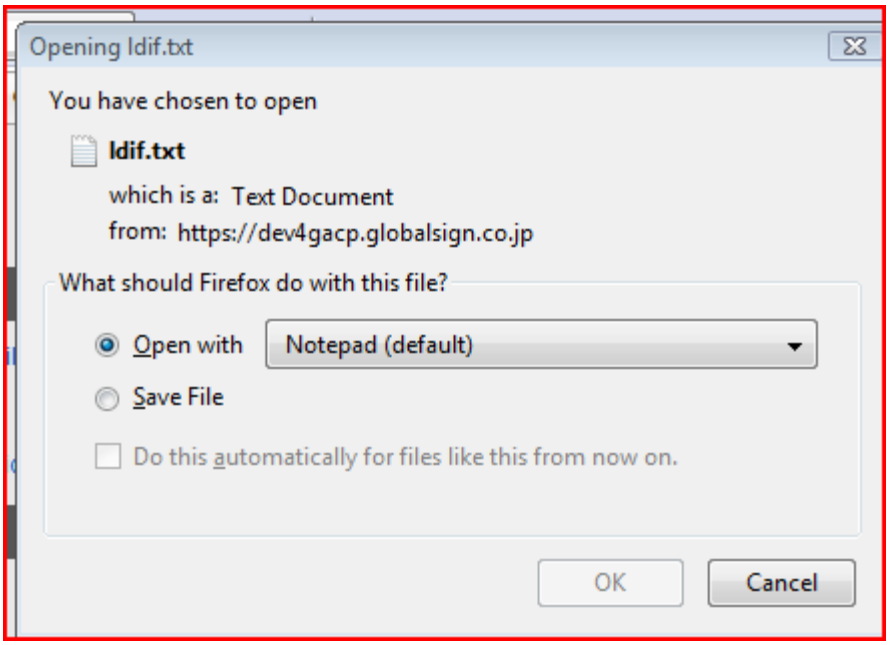
Select the appropriate date range, Profile (if you have more than 1) and set “Certificate Order Status = Issued” via the drop down menu. Note: If a certificate has been “Re-issued”, the replacement certificate will have a status = Issued and be included in the LDIF report. The original, “replaced” certificate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



Click on the “LDIF” Button:



Open the file with your prefer application.


Opening ldif.txt
You have chosen to open
ldif.txt
which is a: Text Document
from: https://dev4gacp.globalsign.co.jp
What should Firefox do with this file?
Open with
Notepad (default)
Save File
Do this automatically for files like this from now on.
OK
Cancel

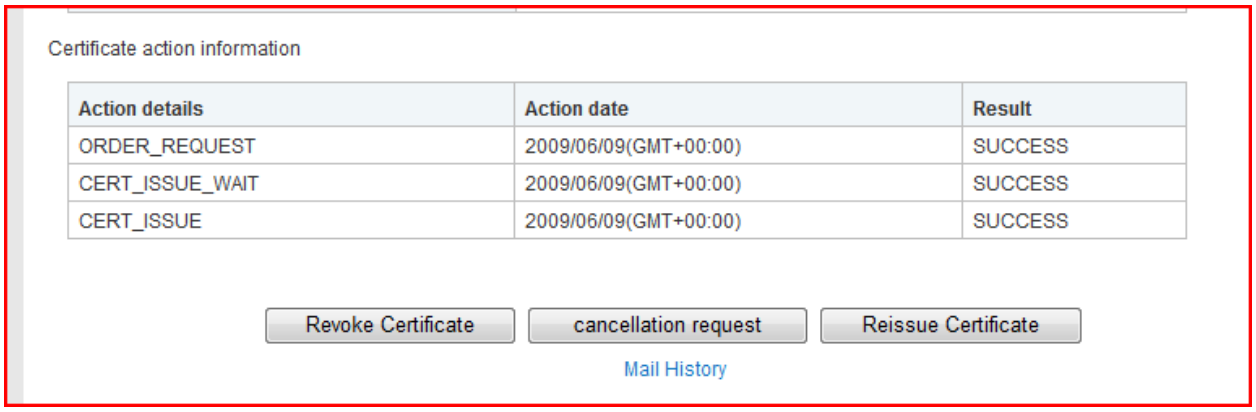
Below is an example entry:

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.



Click “Mail History” to review or resend system generated emails:

< 1 >

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.

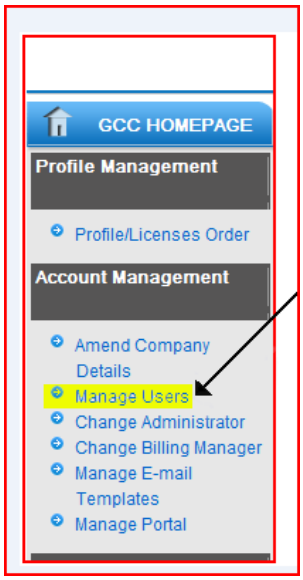
Manager

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.

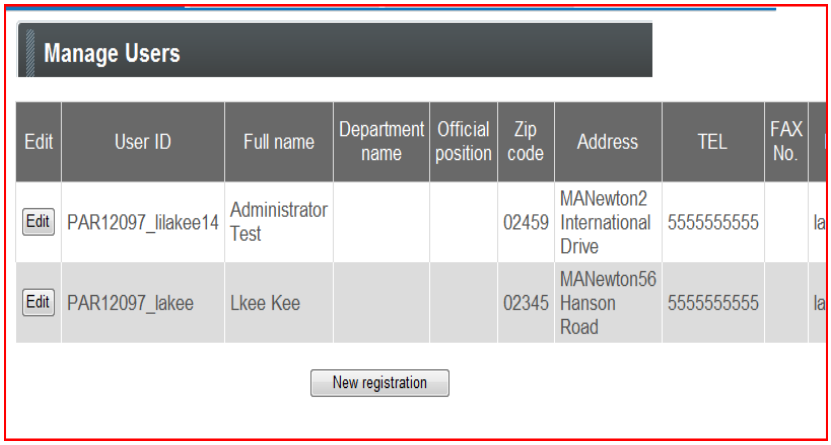
Staff in Charge

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.



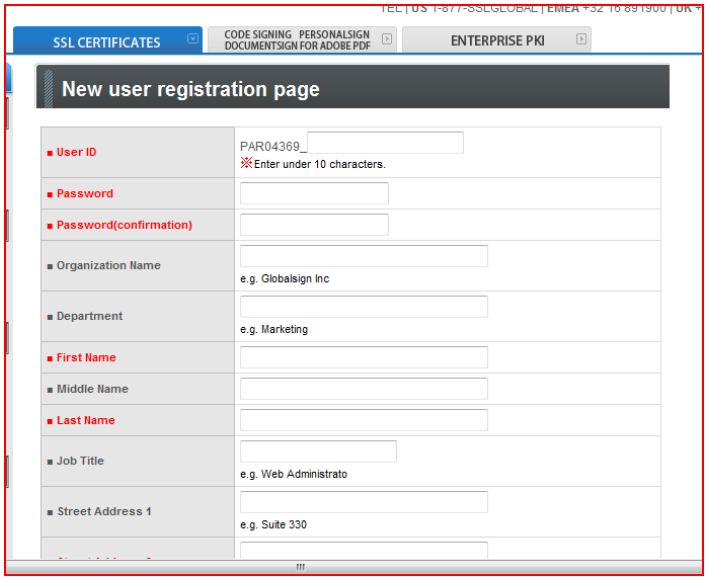
A list of active ePKI Administrators can be found under “Manage Users”. New ePKI registrations can also be created at this link.

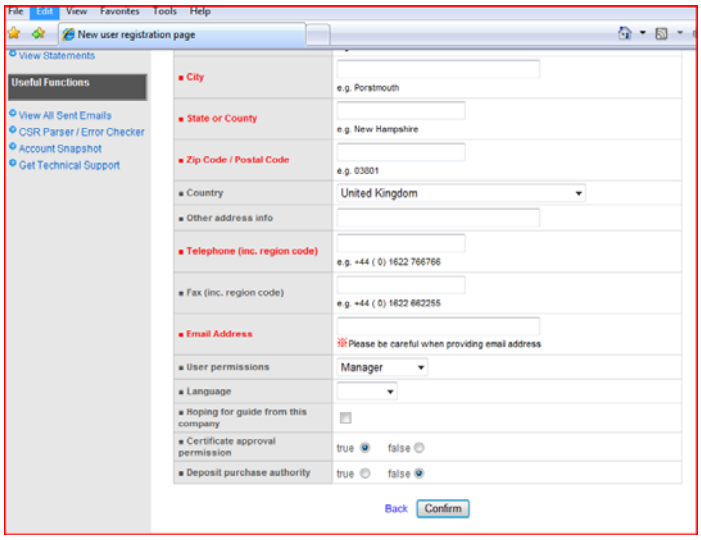


Registering additional Administrators

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.

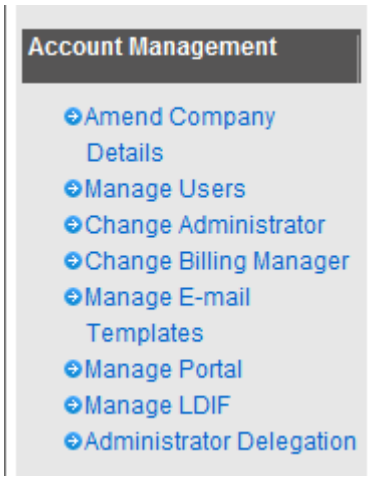
Ignore settings related to Deposit Purchase Authority.



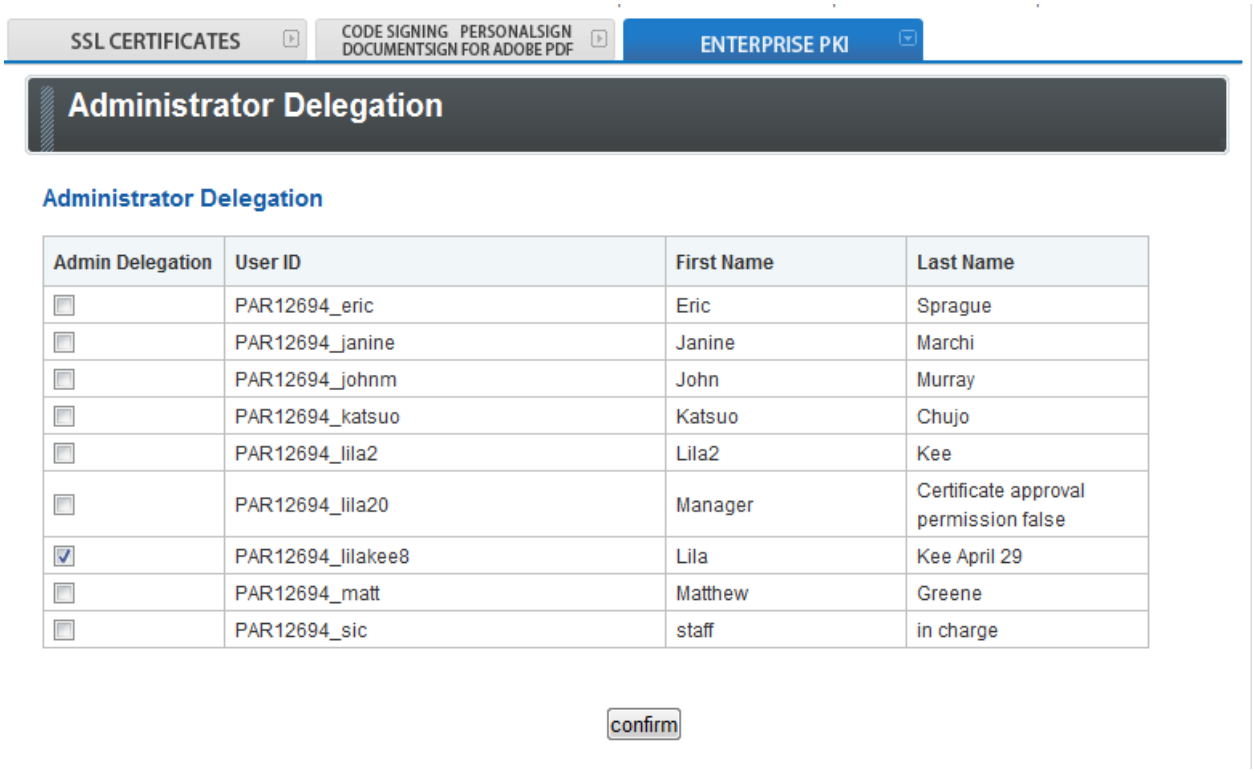


Administration Delegation

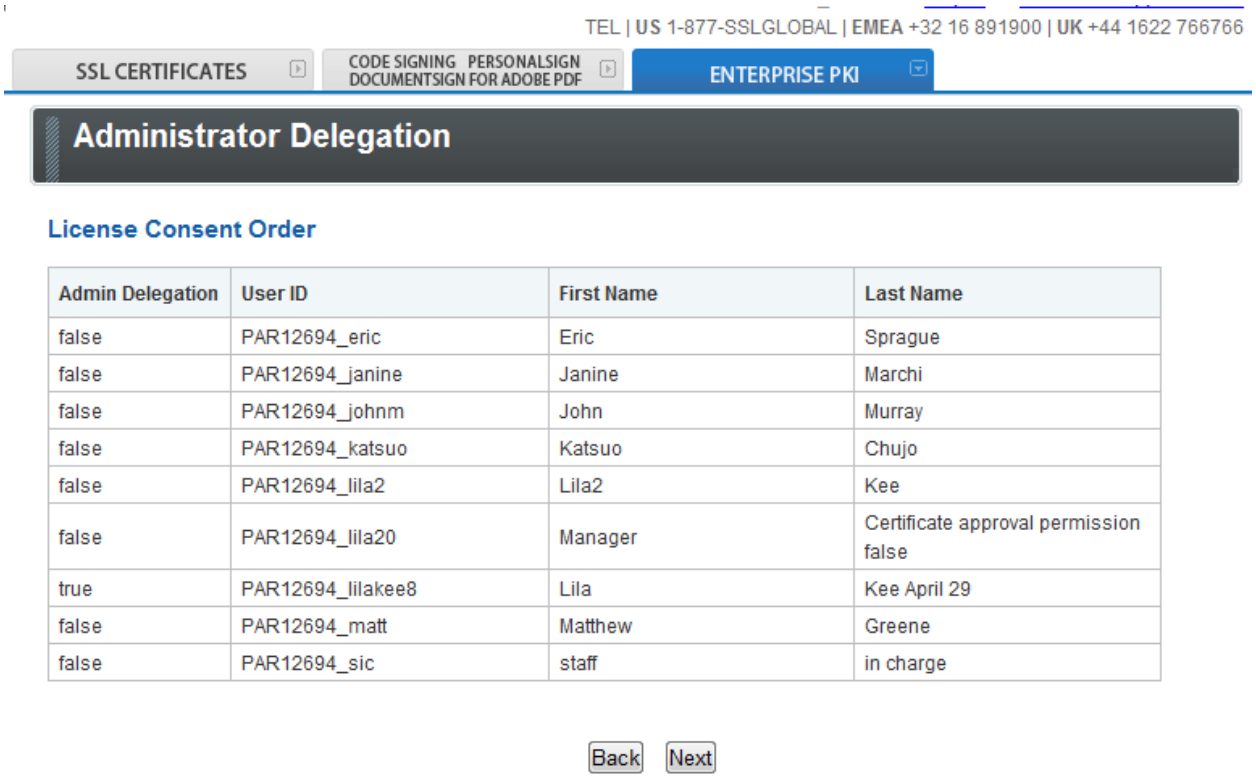
Shared administration can be established by enabling the Administration Delegation feature found on the left pane menu under Account Management:


Account Management
Amend Company Details
Manage Users
Change Administrator
Change Billing Manager
Manage E-mail Templates
Manage Portal
Manage LDIF
Administrator Delegation

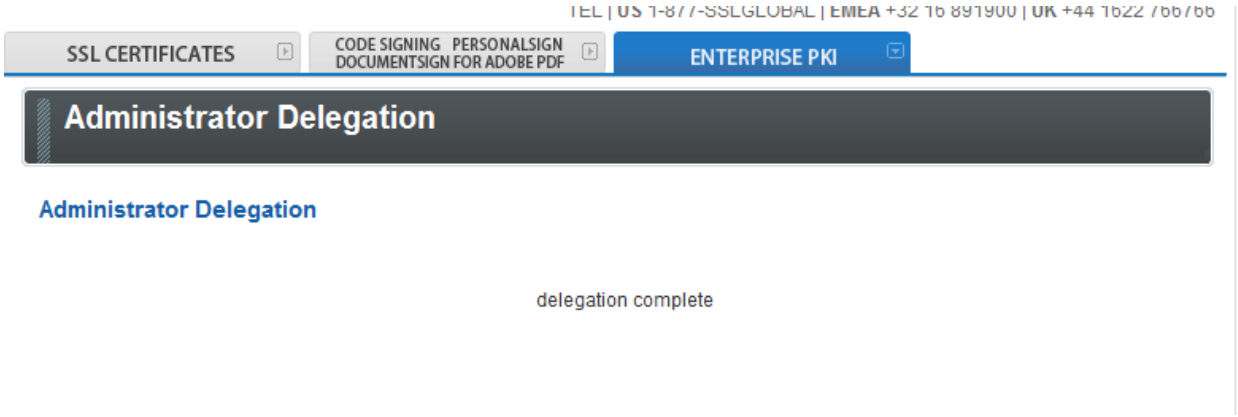
Tick off the box next to the User ID that you wish to extend full administrative rights across all profiles established. Extended rights allows the User to view, approve, cancel, reissue, and revoke certificates initiated by any other User with either Staff or Manager rights for a given PAR.



Next, confirm selection by clicking “Next”:



Note changes have been confirmed when the following screen appears:



Getting Help

Although ePKI Adminstrators 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:

GlobalSign Inc
2 International Drive
Suite 330, 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