

GlobalSign ePKI for iOS Authentication Solution Guide v1.0

Table of Contents

Introduction:	3
Establishing an ePKI Account	3
Configuring iOS Devices	5
Assigning a Configuration Profile to an iOS Identity Certificate	5
Register end-users for iOS Certificates using ePKI	
Certificate Installation	6
iOS Certificate Management	8

Appendix

Customizing iOS Identity Certificate enrollment emails:	12
Appendix A- Configuration Profiles	12
Appendix B- Obtaining Device IDs for the iPhone, iPad, & iPod	13
Appendix C - Configuring access control using Digital Certificates	14

Introduction:

With the adoption of digital certificate technology, Apple iOS devices (such as iPhones, iPads, and iPods) are proving to be a viable and secure method to remotely access internal networks via the Enterprise. GlobalSign's iOS Identity Certificates are Digital Certificates designed specifically for iOS devices to permit access control to corporate business services such as Exchange ActiveSync, VPNs, WPA2, and Enterprise Wi-Fi networks.

GlobalSign ePKI for iOS Authentication provides a fast, easy, scalable, and low cost method to provision these Identity Certificates onto iOS devices using the SCEP and over the air enrollment protocol.

Step 1: Establishing an ePKI Account

If you do not already have a GlobalSign ePKI Account, you will need to enroll for an ePKI account and setup a Certificate Profile. A Certificate Profile will serve as a pre-vetted organization template containing the organization's identity records (such as organization name, city, state, etc) that end user certificate requests will be issued from. Verifying the organization's identity associated with a profile typically takes between 2 and 3 days.

If you already have an ePKI Account, please proceed to Step 2- Configuring iOS Devices

If you do not already have an ePKI Account, please follow the instructions below:

1. Navigate to <http://www.globalsign.com/ios-authentication/> and click Buy Now.
2. Register for an ePKI accounts by entering your account details.

Account Details
Please specify details for your account. Your account contact will receive notices regarding your Certificate application and will be the main contact associated with your GlobalSign Certificate Center (GCC) account. If you are applying on behalf of someone else, enter their details, and you can specify an additional Technical Contact for yourself later in the application process.

First Name <i>Required</i>	<input type="text"/>
Middle Name or Initial	<input type="text"/>
Last Name <i>Required</i>	<input type="text"/>
Email Address <i>Required</i>	<input type="text"/> <small>Please check email is accurate. This email address will be used in the application process.</small>
Phone Number <i>Required</i>	<input type="text"/> <small>e.g. 603-670-7000 or 01422 700700</small>
Fax Number	<input type="text"/> <small>e.g. 603-670-7000 or 01422 662266</small>
Organization Name <i>Required</i>	<input type="text"/> <small>Specify the Organization Registered Name in full, including Inc, Ltd, NV, Plc etc</small>
Department	<input type="text"/>
Street Address 1 <i>Required</i>	<input type="text"/> <small>e.g. Two International Drive</small>
Street Address 2	<input type="text"/> <small>e.g. Suite 200</small>
City <i>Required</i>	<input type="text"/>
State / County <i>Required</i>	<input type="text"/>

3. Choose a username and password and click **next** to continue.

GlobalSign Certificate Center (GCC) Login Details
Your GCC account allows you to manage all your GlobalSign Certificates and provides fast access to ordering additional products and renewing, reissuing and revoking current Certificates. Please create a memorable Username and Password.

Username <i>Required</i>	<input type="text"/> <small>Username is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9).</small>
Password <i>Required</i>	<input type="password"/> <small>Password is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9).</small>
Password(re-enter) <i>Required</i>	<input type="password"/>

[Next](#)

4. Confirm your account information and review the Terms of Service Agreement and click **next** to continue.

5. Choose the license pack size of Identity Certificates you wish to purchase (5-7,500) and click **next**.

Product Details

Personal Sign

- Enterprise PKI Lite For Mobile 1 pack
- Enterprise PKI Lite For Mobile 5 pack
- Enterprise PKI Lite For Mobile 10 pack
- Enterprise PKI Lite For Mobile 25 pack
- Enterprise PKI Lite For Mobile 50 pack
- Enterprise PKI Lite For Mobile 100 pack
- Enterprise PKI Lite For Mobile 250 pack
- Enterprise PKI Lite For Mobile 500 pack
- Enterprise PKI Lite For Mobile 1,000 pack
- Enterprise PKI Lite For Mobile 10,000 pack
- Enterprise PKI Lite For Mobile 2,500 pack
- Enterprise PKI Lite For Mobile 25,000 pack
- Enterprise PKI Lite For Mobile 3,500 pack
- Enterprise PKI Lite For Mobile 5,000 pack
- Enterprise PKI Lite For Mobile 7,500 pack
- Enterprise PKI Lite For Mobile unlimited

6. Choose a validity period to be applied to your license pack (1-3 years)

Product Details - Enterprise PKI Lite For Mobile 10 pack

Certificate Validity <i>Required</i> Multi-year offers significant per annum savings	<input checked="" type="radio"/> 1 year \$428 <input type="radio"/> 2 year \$570 <input type="radio"/> 3 year \$715
Campaign Code	<input type="text"/> <input type="button" value="Redeem code"/> <small>If you have a Campaign Code please enter and click "Redeem Code". This page will be reloaded with your appropriate discount.</small>
Coupon Code	<input type="text"/> <input type="button" value="Redeem code"/> <small>If you have a one-off Coupon Code for a particular promotion please enter and click "Redeem Code". This page will be reloaded with your appropriate discount.</small>
TOTAL COST (inc. Tax)	\$ 428

7. **Optional** - Add an additional technical contact (this is commonly used when you are applying on behalf of someone else), click **next** once complete.

8. Enter the Certificate Profile Details. These details will be vetted and included as the certified identity within your issued Certificates. Click **next** to continue.

Important - make sure the details entered are correct as we will vet the details you include.

Organization <i>Required</i>	<input type="text" value="globalsign"/>
Organizational Unit <i>Optional unless locked as unique</i>	<input type="text"/> <input type="text"/> <input type="checkbox"/> Lock a unique OU
Locality <i>Optional</i>	<input type="text" value="Portsmouth"/>
State or Province <i>Optional</i>	<input type="text" value="New Hampshire"/>
Country <i>Required</i>	<input type="text" value="United States - US"/>

9. Complete the payment details

Payment Details

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

Credit Card Details & Billing Address



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

10. Confirm your order details and review the ePKI Service Agreement Click **next** when finished.

11. The next screen will display your username and information about your profile. Save this information for your records.

Application Completed

User ID	PAR57453_mobiletest
License ID	ML201111300887
Profile ID	MP201111300733

 Login to GCC 

12. Once you have successfully created an ePKI account your information will be sent to our vetting team. Vetting your organization details can take up to 2-3 days. Once the vetting process is complete, you will receive an email notification notifying you of its completion.

Once your ePKI account is setup and established, please continue to Step 2a - Configuring iOS Devices.

Step 2a - Configuring iOS Devices:

You need to decide how you'll configure each iOS device. This is influenced in part by how many devices you plan on deploying and managing over time. If the number is small, you may find that it's simpler for you or your users to manually configure each device. This involves using the physical device to configure the settings for each mail account, Wi-Fi settings, and VPN configuration information. See your device guide for further instructions.

If you plan on configuring your devices at the device level you can proceed to Step 3 - Registering end-users for Identity Certificates.

If you deploy a large number of devices, or you have a large collection of email settings, network settings, and certificates to install, then you may want to configure the devices by creating and distributing configuration profiles. Configuration profiles quickly load settings and authorization information onto a device. Some VPN and Wi-Fi settings can only be set using a configuration profile, and if you're not using Microsoft Exchange, you'll need to use a configuration profile to set device passcode policies.

View the Apple deployment guide for further details: http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

Step 2b - Assigning a Configuration Profile to an iOS Identity Certificate

iPhone Configuration profiles can be uploaded to the ePKI platform and associated with an ePKI Certificate Profile, which will then be applied to all iOS Identity Certificates issued from that Certificate Profile. For more information on Configuration Profiles, please see Appendix A.

If you wish to upload a pre-configured iPhone profile follow the below steps:

1. In the left hand menu under **Useful Function**, click **Edit iPhone Configuration** then select **Edit**.



2. Browse for your configuration file (XML file), click **upload** and then click **next**. Then **confirm** to save changes:

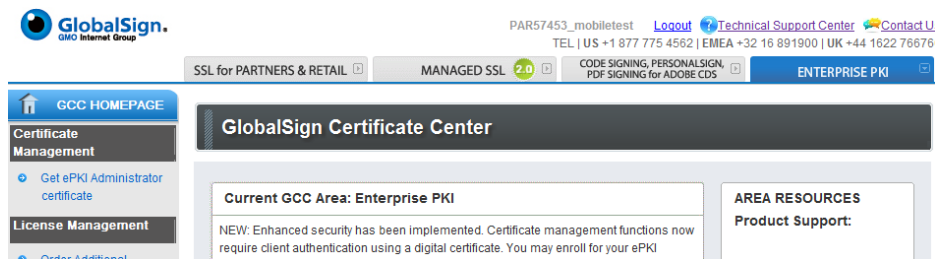


3. Once confirmed, all Identity Certificates issued from the chosen profile will contain the iPhone Configuration profile.

Step 3- Registering end-users for iOS Identity Certificates using ePKI

When you are ready to issue certificates to your end-users, please follow the below steps:

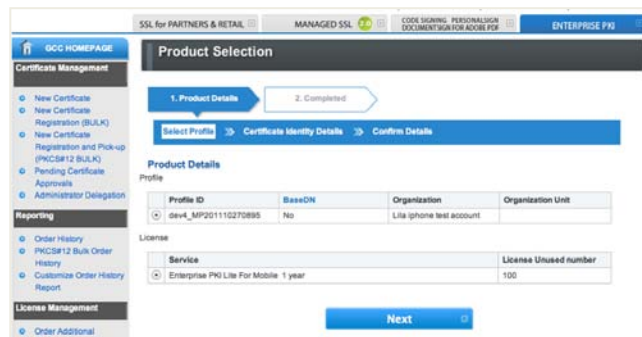
1. Login to your GlobalSign Certificate Center (GCC) account at www.globalsign.com/login/
2. Select the “Enterprise PKI” tab found at the top menu bar
3. **Please note**, if this is your first time logging in your menu options will be limited. For first time users, you will need to enroll for an “ePKI Administrator Certificate”, which is an authentication certificate needed to access secure areas of GCC such as the Certificate Management section. Please follow the steps to enroll for your administrator certificate.
 - a. Click Get ePKI Administrator Certificate link in the left hand menu to start the enrolment process
 - b. Follow the prompted steps to enrol and install your certificate.
 - c. If you need further assistance and detailed instructions on how to enroll for your ePKI Admin Certificate, please see our administrator guide located at <http://www.globalsign.com/support/ordering-guides/epki-authentication-user-guide.pdf>



4. In the left hand menu, Select **New Certificate** or **New Certificate BULK** link under **Certificate Management**



5. Next, select the **Profile** and **License** pack (in most cases there will be only one option for each area) that you want to issue the certificate from and click **Next**.



6. Provide the end-user identity details.
 - a. **Optional** - If you wish to “lock” a Identity Certificate to a specific device, you may enter a **Device Authentication ID**. This value will not be included in the Certificate itself, but instead only allow installation to an iOS device with a matching Device Authentication ID. **View Appendix B** for further instructions on finding a device’s ID.
 - b. Establish a one-time Pickup Password. **Important** - the user will need this password to install the certificate onto their device, you must deliver this Pickup Password in an out-of-band method.

- c. **Optional** - enter a reason or note associated with the registration. This note will appear in the Order History section of ePKI and may be useful for audit purposes. Click Next to continue.

Common Name <small>Required</small>	<input type="text" value="John Smith"/>
Organization	Lila iphone test account
Organizational Unit	Marketing
Locality	Newton
State or Province	Massachusetts
Country	United States - US
Email Address <small>Required</small>	<input type="text" value="john.smith@abc.com"/>
Device Authentication ID	<input type="text"/>
Pickup Password <small>Required</small>	<input type="password" value="*****"/> <small>Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9)</small> <input type="button" value="Password Generation"/> <small>When the password automatic operation generation button is pressed, a random password automatic construction/is set.</small>
Pickup Password (re-enter) <small>Required</small>	<input type="password" value="*****"/>
Memo	<input type="text" value="User active status verified"/>

Click **Next** to continue

10. Review and confirm registration details. If satisfied, click **Next** to complete the registration.

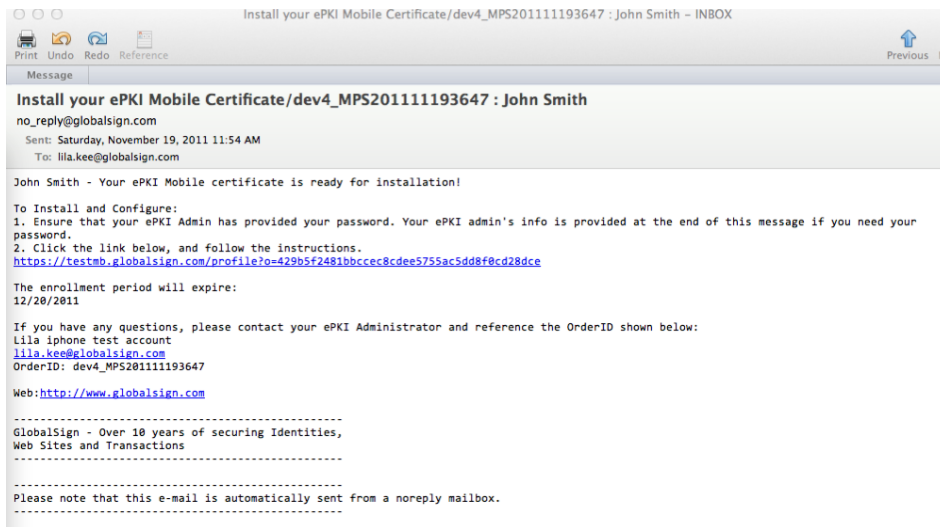
Step 4 - Certificate Installation

Certificate delivery is completed using over-the-air enrollment. The Certificate enrollment is sent directly to the end-user's iOS device and is picked up via an email that will be delivered to the email address specified at registration.

1. Pick up certificate via iOS Device. The end user will receive an email on their iOS device containing instructions on how to install their new iOS Certificate.

Sample Enrollment Email

This enrollment email can be customized for your end-users. See Appendix C on email template customization instructions.



2. The end user will be instructed to click the installation link provided in the email.
3. Next, the end user will be prompted to enter a pick up password and then click **Get Cert.**



4. Next, the SCEP certificate generation process will begin



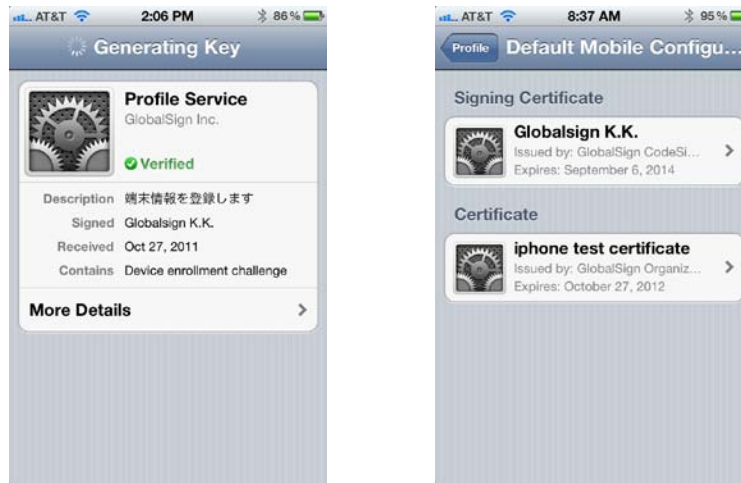
5. Once the certificate generation is complete, the user will be prompted to install the certificate.



6. Next, a dialog window will appear prompting the user to continue with the installation understanding that it will change settings on their phone. The end-user should click **Install Now** to start the Profile installation.



Once complete, the following screen will appear with “Verified” confirming that the certificate has been installed on the iOS device. For additional certificate details, click **more details**.



iOS Certificate Management

The ePKI platform provides several methods to manage the lifecycle of your iOS Identity Certificates.

Reissuance: Allows certificates to be reissued with exact same identity details and expiration date at no extra cost.

Revocation: Certificates may be revoked placing the serial number of the revoked certificate on the GlobalSign Certificate Revocation List (CRL).

Renewal: Not currently supported

Reissuance can be found under the “Application Details” associated with the given Order found in “Order History”

Unsupported:

Please note that ePKI for iOS Authentication does not support the following ePKI functions that are applicable to ePKI for PersonalSign users:

- PKCS12 Bulk registration
- Encrypted File System (EFS) extended key usage
- Smartcard logon extended key usage
- Renewal
- Private key exportability
- API

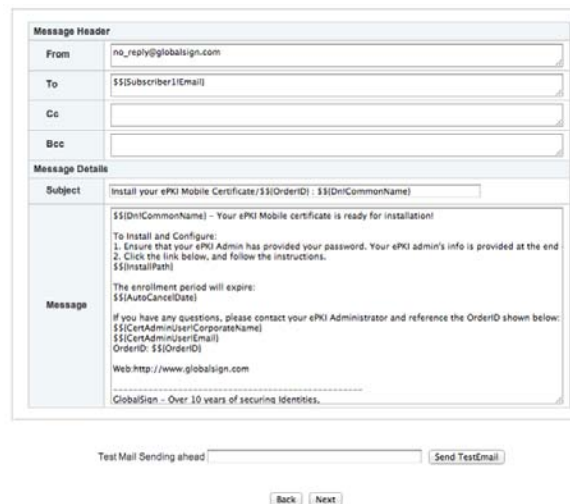
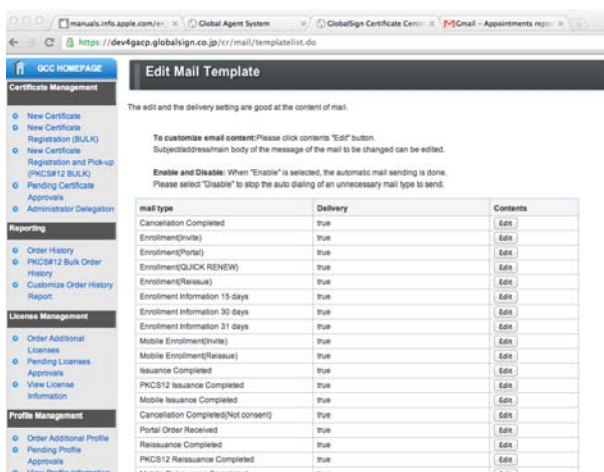
Customizing iOS Identity Certificate enrollment emails:

System generated emails are delivered automatically via the ePKI System. As the ePKI Administrator you can customize the emails your end-users receive.

The following email templates apply to the ePKI iOS Mobile Device service:

- Mobile Enrollment (Invite)
- Mobile Enrollment (Reissue)
- Mobile Issuance Completed
- Mobile Reissuance Completed
- Mobile Enrollment Information 15 days
- Mobile Enrollment Information 30 days

Customize your templates by navigating to **Manage E-mail Template** in the **Account Management** section of the left hand menu. Click **edit** next to the applicable template.



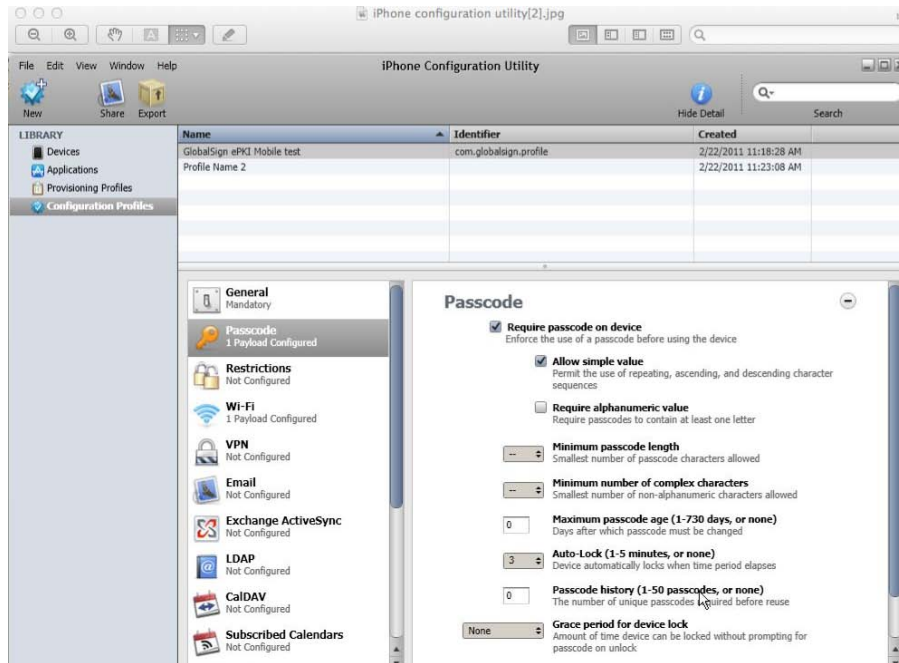
The following fields may be modified:

- Cc: Enter additional email addresses
- Bcc: Enter additional email addresses
- Subject header: Change subject header
- Subject Content: Change subject content (excluding substitution variables)

Click **Next** and then **Complete** to save changes.

Appendix A- Configuration Profiles

Configuration profiles can be generated using Apple's iPhone Configuration Utility. Below is an example of a configuration profile setup associated with an ePKI Certificate Profile.



Apple's iPhone Configuration Utilities can be found at:

- <http://support.apple.com/kb/DL1465>- Mac
- <http://support.apple.com/kb/DL1466> -Windows

Appendix B- Obtaining Device IDs for the iPhone, iPad, & iPod

During the certificate registration process, you may restrict a certificate to a specific device using the device ID (step3).

There are two main types of Device ID's.

- International Mobile Equipment Identity (IMEI): 15 number characters
- UDID 40 alphanumeric characters

Assigning a device ID to a certificate will allow users to control what device the certificate is installed on.

Obtaining a "Device ID" via your iPhone

1. Navigate to your iPhone's "About" screen. From the home screen, tap **Settings >General > About**.
2. At the About screen, you will be able to view your iPhone's Device ID (IMEI) and additional information (serial number, ICCID, MEID, etc)



Obtaining a “Device ID” via your iPad

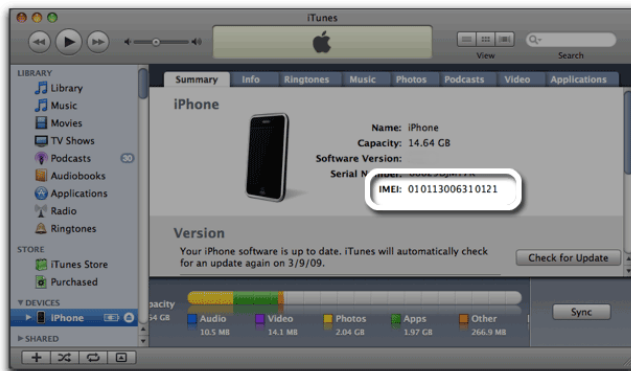
You can obtain your iPad’s Device ID one of the following ways:

- Using iTunes
- iPad About Screen
- On the back of the iPad

Obtaining a “Device ID” via iTunes for the iPod, iPhone, and iPad

You can obtain your iPod’s Device ID using your computer and iTunes

1. Connect your device to your computer and open iTunes
2. Select the device when it appears in the left-hand column
3. Click the Summary tab. Your device’s serial number will display



For detailed instructions on how to find your Device ID, please see <http://support.apple.com/kb/ht1267>

Appendix C - Configuring access control using Digital Certificates

For details and instructions on how to configure network access using certificate-based authentication, please view Apple’s Enterprise Deployment guide located at http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf



Appendix D- Additional Certificate Mangement- ePKI User Guide

For further instructions on managing your GlobalSign Certificate Center (GCC) Account, please see our ePKI User Guide <http://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf>.

GlobalSign Contact Information

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

