GlobalSign Customers

Enterprise PKI Client Authentication User Guide

Employing authentication as an additional security layer to the EPKI platform
TABLE OF CONTENTS

I. Background information ........................................................................................................... 3

II. EPKI administrator certificate issuance .................................................................................. 3
   Step 1: log in to the Gcc ............................................................................................................. 3
   Step 2: select EPKI tab ............................................................................................................... 3
   Step 3: enroll for EPKI administrator certificate ...................................................................... 4
   Step 4: install certificate .......................................................................................................... 5
   Step 5: import certificate ......................................................................................................... 5
   Step 6: download certificate ..................................................................................................... 7
   Step 7: certificate issued .......................................................................................................... 8
   Step 8: secure area accessed via client authentication ............................................................ 8
   Step 8: access full EPKI functions ........................................................................................... 9

III. Lost EPKI administrator certificates ...................................................................................... 9
    Step 1: cancel old certificate .................................................................................................. 9
    Step 2: establish certificate pick-up password ...................................................................... 10
    Step 3: install replacement certificate .................................................................................. 10
    Step 4: import certificate ....................................................................................................... 11
    Step 5: download certificate .................................................................................................. 11

IV. Getting Help ........................................................................................................................... 13
I. BACKGROUND INFORMATION

GlobalSign has implemented client authentication as the method to access areas within EPKI requiring enhanced protection. Certificate management functions reside in a secure area that requires client authentication with a GlobalSign EPKI Administrator Certificate. All other functions are accessible without authentication. EPKI Administrator certificates will be automatically issued at initial log-in to the EPKI tab found in the GlobalSign Certificate Center (GCC).

II. EPKI ADMINISTRATOR CERTIFICATE ISSUANCE

STEP 1: LOG IN TO THE GCC

Go to [https://system.globalsign.com/au/signon/gacp/usernamePasswordLogin.do](https://system.globalsign.com/au/signon/gacp/usernamePasswordLogin.do) and enter your current username and password.

![Login screen](image.png)

STEP 2: SELECT EPKI TAB

To obtain your EPKI Administrator Certificate, click the View Admin Menu Options link under My Certificates in the left hand menu to start the enrollment process.
STEP 3: ENROLL FOR EPKI ADMINISTRATOR CERTIFICATE

Click on the **Next** button to begin the enrollment process.

The EPKI Administrator enrolls for the certificate by assigning a minimum 12 character alphanumeric certificate password (also known as the PKCS12 private key password). **You will need to remember this password for step 5 – Certificate Installation.**
STEP 4: INSTALL CERTIFICATE
You will be sent an enrollment email containing an installation link. Click the link inside your enrollment email to begin the installation process.

![Image of enrollment email]

The enrollment period will expire:
- 06/12/2011

Click on the link below to initiate the Certificate generation and installation process.
https://dev4gecp.globalsign.co.jp/c/public/certificate/install.do?pf=6afe13c4789fb4f67e2:89f76c58c36d3a81ab237

Make sure the above link is unbroken and complete. Copy and Paste the entire link into your browser if necessary.

Contact your ePIK Administrator for additional information.

Oooo o
yoshinao.kuwae@globalsign.co.jp
Web:http://www.globalsign.com

GlobaSign - Over 10 years of securing Identities, Web Sites and Transactions

STEP 5: IMPORT CERTIFICATE
First you will be prompted to enter the previously established Certificate pick-up password (from step 3).

![Image of Certificate import process]

Next you will need to establish the PKCS12 Private Key password and accept the Subscriber Agreement.

Reminder: the PKCS12 password must be alphanumeric and 12 characters long. You will need to remember this password to install your certificate.
Certificate Password: ****************
Certificate Password (re-enter): ****************

GlobalSign Subscriber Agreement
GlobalSign Subscriber Agreement PersonalSign: Version 1.3 1 of 6
GlobalSign Subscriber Agreement for PersonalSign Certificates Version 1.3

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED
GlobalSign CDP is incorporated by reference herein and is available at www.globalsign.com

I agree to the Subscriber Agreement

Next
STEP 6: DOWNLOAD CERTIFICATE
Click the **Download My Certificate** button.

Select **open** when the **File Download** window appears.

Enter the PKCS12 password (from Step 5) when the **Certificate Import Wizard** window appears.
Note: You can mark the key as exportable if you wish to use the certificate on a different machine and/or browser.

**STEP 7: CERTIFICATE ISSUED**

Note your EPKI Administrator Certificate will include the following identity elements:

- **CN** = Your PAR_Username (your username when you log in to the GCC)
- **Email** = The Administrator’s email
- **O** = GlobalSign EPKI Administrator Certificate (your organization name is removed)
- **OU** = Email control validated by GlobalSign – authenticated by LRA

The EPKI Administrator Certificate will have a validity period of 1 year from the date it was issued.

**STEP 8: SECURE AREA ACCESSED VIA CLIENT AUTHENTICATION**

The certificate management area of the EPKI portal is accessed via client authentication. When you try to access the *My Certificates* menu items, you will be prompted to select a certificate – choose the one that includes your PAR_Username.

![Select a Certificate](image)

Note: There is only one active EPKI Administrator per PAR_Username. Any additional EPKI Administrators will be issued unique Administrator Certificates.
STEP 8: ACCESS FULL EPKI FUNCTIONS
After selecting your certificate, you will have full access to all areas of the EPKI portal.

Note the expanded left menu in the screen image below.

III. LOST OR EXPIRED EPKI ADMINISTRATOR CERTIFICATES
In the event you have lost or expired your EPKI Certificate you may enroll for a replacement certificate. Replacement certificates will make previous Administrator Certificates inactive.

STEP 1: CANCEL OLD CERTIFICATE
Simply click cancel when prompted to authenticate to a secured area of the EPKI portal (i.e., View Admin Menu Options). Then click next on the following screen to begin the replacement certificate registration process.
STEP 2: ESTABLISH CERTIFICATE PICK-UP PASSWORD

The replacement certificate process requires the creation of a pick-up password. The password must be alphanumeric and a minimum of 8 characters.

Note: This is not the same as the PKCS12 password.

STEP 3: INSTALL REPLACEMENT CERTIFICATE

You will be sent an enrollment email containing an installation link. Click the link inside your enrollment email to begin the installation process.
**STEP 4: IMPORT CERTIFICATE**

First you will be prompted to enter the previously established Certificate pick-up password (from step 2).

Next you will need to establish the PKCS12 Private Key password and accept the Subscriber Agreement. Reminder: the PKCS12 password must be alphanumeric and 12 characters long. You will need to remember this password to install your certificate.

**STEP 5: DOWNLOAD CERTIFICATE**

Click the Download My Certificate button.
Select open when the File Download window appears.

![File Download](image1)

Enter the PKCS12 password (from Step 4) when the Certificate Import Wizard window appears.

![Certificate Import Wizard](image2)

Note: You can mark the key as exportable if you wish to use the certificate on a different machine and/or browser.
**IV. GETTING HELP**

Every GlobalSign EPKI customer has a dedicated Account Manager who is on hand to help with any questions you may have regarding the EPKI portal. GlobalSign urges EPKI Administrators to browse the GlobalSign support pages and user guides for product-specific guidance.

- EPKI support site: [https://www.globalsign.com/support/EnterprisePKI.php](https://www.globalsign.com/support/EnterprisePKI.php)

If you can’t find the answer to your questions, please open a support ticket [http://www.globalsign.com/help/](http://www.globalsign.com/help/). GlobalSign also provides technical support through our Client Service departments around the world.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GlobalSign Americas</strong></td>
<td><strong>GlobalSign EU</strong></td>
<td><strong>GlobalSign UK</strong></td>
</tr>
<tr>
<td>Tel: 1-877-775-4562</td>
<td>Tel: +32 16 891900</td>
<td>Tel: +44 1622 766766</td>
</tr>
<tr>
<td><a href="http://www.globalsign.com">www.globalsign.com</a></td>
<td><a href="http://www.globalsign.eu">www.globalsign.eu</a></td>
<td><a href="http://www.globalsign.co.uk">www.globalsign.co.uk</a></td>
</tr>
<tr>
<td><a href="mailto:sales-us@globalsign.com">sales-us@globalsign.com</a></td>
<td><a href="mailto:sales@globalsign.com">sales@globalsign.com</a></td>
<td><a href="mailto:sales@globalsign.com">sales@globalsign.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>GlobalSign FR</strong></td>
<td><strong>GlobalSign DE</strong></td>
<td><strong>GlobalSign NL</strong></td>
</tr>
<tr>
<td>Tel: +33 1 82 88 01 24</td>
<td>Tel: +49 30 8878 9310</td>
<td>Tel: +31 20 8908021</td>
</tr>
<tr>
<td><a href="http://www.globalsign.fr">www.globalsign.fr</a></td>
<td><a href="http://www.globalsign.de">www.globalsign.de</a></td>
<td><a href="http://www.globalsign.nl">www.globalsign.nl</a></td>
</tr>
<tr>
<td><a href="mailto:ventes@globalsign.com">ventes@globalsign.com</a></td>
<td><a href="mailto:verkauf@globalsign.com">verkauf@globalsign.com</a></td>
<td><a href="mailto:verkoop@globalsign.com">verkoop@globalsign.com</a></td>
</tr>
</tbody>
</table>

---

[GlobalSign Logo]