

# Security Server Installation Guide

This manual is currently reference document.  
Officially, please check the Japanese one.

## Contents

Target Audience .....	2
Skill set .....	2
About trademark.....	2
Supported Platforms: .....	3
Network requirements .....	3
Setting up for Ubuntu. ....	5
Pre-create administration user .....	5
Add apt-key and package repository server .....	5
Preparing OS:.....	6
Setting up for RHEL. ....	7
Add package repository: .....	7
Preparing OS:.....	7
Installation for Ubuntu. ....	9
Post-Installation Checks.....	13
Installation for RHEL. ....	14
Post-Installation Checks.....	15
Prerequisites .....	16
Reference Data .....	16
Generating an Authentication Key .....	20
Generating a Signing Key .....	22
Generating a Certificate Signing Request for an Authentication Key .....	25
Generating a Certificate Signing Request for a Signing Key .....	27
Sending CSR to Planetway .....	29
Importing an Authentication Certificate from the Local File System .....	29
Importing a Signing Certificate from the Local File System .....	30
Register timestamping Server.....	33

## Introduction

---

### Target Audience

This Security Server installation & user guide is aimed at PlanetCross security server system administrators for installing, operating and maintaining PlanetCross software.

### Skill set

This document is intended for readers with a moderate knowledge of Linux server management, computer networks, and the PlanetCross working principles.

### About trademark

- Amazon Web Services, Logo of "Powered by Amazon Web Services" are the registered trademark of Amazon.com, Inc in the U.S. and other countries.
- UNIX is the registered trademark of The Open Group in the U.S. and other countries.
- Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
- Red Hat, Red Hat Enterprise Linux are trademarks of Red Hat, Inc., registered in the United States and other countries.
- Ubuntu is a trademark of Canonical Ltd and is used under license from Canonical Ltd.
- PostgreSQL is trademark or registered trademark of PostgreSQL of the U.S. in the U.S. and/or other countries.
- Nginx is trademark or registered trademark of Nginx Software Inc. of the U.S. in the U.S. and/or other countries.
- Intel is trademark or registered trademark of Intel Corporation of the U.S. in the U.S. and/or other countries.
- AMD is trademarks of Advanced Micro Devices, Inc.
- X-Road is the registered trademark of Estonian Information System Authority and Estonia.
- Planetway, PlanetCross are trademarks of Advanced Planetway Japan K.K.
- All other brand or product names may be trademarks or registered trademarks of their respective companies or organizations.

## Security Server Installation

---

### Supported Platforms:

All Security Server version support following OS and need following resources.

#### Ubuntu

Operating System	Ubuntu 16.04 x86-64
CPU	2 core
RAM	4GB
Free disk space	20GB

Red Hat Enterprise Linux is supported after Security Server version v6.20.2.

#### Red Hat Enterprise Linux

Operating System	RHEL7.2 x86-64
CPU	2 core
RAM	4GB
Free disk space	10GB: OS partition 20-40GB: /var partition
Network	100Mbps (Network Interface Card)

The server's hardware (motherboard, CPU, network interface cards, storage system) must be supported by RHEL7 in general;  
A 64-bit dual-core Intel, AMD or compatible CPU; AES instruction set support is highly recommended;

### Network requirements

Inbound – ports for inbound connections (from the external network to the security server)

TCP 5500	Message exchange between security servers
TCP 5577	Querying of OCSP (Online Certificate Status Protocol) responses between security servers

Outbound – ports for outbound connections (from the security server to the external network)

TCP 5500	Message exchange between security servers
TCP 5577	Querying of OCSP (Online Certificate Status Protocol) responses between security servers
TCP 4001	Communication with the central server
TCP 80	Downloading global configuration
TCP 80,443	Most common OCSP and time-stamping services

Local access

### Ubuntu

TCP 4000	User interface
TCP 80	Connections from information systems
TCP 80,443	Connections from information systems

### RHEL

TCP 4000	User interface
TCP 8080	Connections from information systems
TCP 8080,443	Connections from information systems

## Preparing before installation.

### Setting up for Ubuntu.

If you encounter error "sudo: unable to resolve {your-host-name}: Resource temporarily unavailable" on AWS, Please add following line to /etc/hosts.

```
127.0.1.1    {your-host-name}
```

(You can change your host name with command like "sudo hostnamectl set-hostname {server-host-name}")

You can run below commands for configuring hostname

```
sudo echo 127.0.1.1 {your-host-name} | sudo tee -a /etc/hosts  
  
sudo hostnamectl set-hostname {your-host-name}
```

### Pre-create administration user

User management is carried out on command line in root user permissions. Create user before starting to install the software. You will be asked for user, during the installation.

To add a new user, enter the command:

# Enter one line.

```
sudo adduser --disabled-password --no-create-home --gecos "{username},,,",  
{username}  
  
echo "{username}:{password}" | sudo chpasswd
```

### Add apt-key and package repository server

Add Planetway's package repository to the machine.

The username and password part will be provided by your Planetway sales representative.

```
sudo sh -c 'echo "deb [arch=amd64] https://@deb.dev.planetcross.net/planetx  
trusty non-free" > /etc/apt/sources.list.d/planetx.list'  
  
sudo sh -c 'echo "deb http://ppa.launchpad.net/nginx/stable/ubuntu trusty main"  
>> /etc/apt/sources.list.d/planetx.list'
```

```
sudo sh -c 'echo "deb http://ppa.launchpad.net/openjdk-r/ppa/ubuntu trusty main" >> /etc/apt/sources.list.d/planetx.list'
```

NB: After 20.01.2020, don't have to enter {username} and {password}.

You can check with this command.

```
cat /etc/apt/sources.list.d/planetx.list
```

example output

```
deb [arch=amd64] https://@deb.dev.planetcross.net/planetx trusty non-free
deb http://ppa.launchpad.net/nginx/stable/ubuntu trusty main
deb http://ppa.launchpad.net/openjdk-r/ppa/ubuntu trusty main
```

Add Planetway's package signing key to the machine.

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
731E775DF768EF67

sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
00A6F0A3C300EE8C

sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
EB9B1D8886F44E2A
```

## Preparing OS:

Set the operating system locale. Add "LC\_ALL=en\_US.UTF-8" to the /etc/environment file.

```
$ sudo sh -c 'echo "LC_ALL=en_US.UTF-8" >> /etc/environment'
```

You can check with this command

```
$ cat /etc/environment
```

## Sample output

```
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games"
```

```
LC_ALL=en_US.UTF-8
```

## Install software-properties-common

```
$ sudo apt-get install locales software-properties-common
```

## Ensure that the locale is available

```
$ sudo locale-gen en_US.UTF-8
```

## Setting up for RHEL.

### Add package repository:

Make /etc/yum.repos.d/planetx.repo and add the following parameters.  
The username and password part will be provided by your Planetway sales representative.

#### Stable

```
[planetx]

name=PlanetCross for RHEL/CentOS

baseurl=https://rpm.planetcross.net/7/

enabled=1

gpgcheck=1

gpgkey=https://static.planetcross.net/prod/gpgkey.asc
```

NB: After 20.01.2020, don't have to enter {username} and {password}.

### Preparing OS:

Edit /etc/environment file and add the following parameter.

```
LC_ALL=en_US.UTF-8
```

Edit /etc/hosts and /etc/hostname and set the hostname and FQDN to be short (less than 64 char).

Add pairs of IP address and hostname in the /etc/hosts.

```
{private IP Address} {hostname}
```

```
{global IP Address} {hostname}
```

Modify the /etc/hostname.

```
{hostname}
```

Note: It is also necessary to modify /etc/cloud/cloud.cfg and add the following line when you use a EC2 instance in AWS.

```
preserve_hostname: true
```

Confirm hostname and FQDN are modified.

```
$ hostname  
$ hostname -f
```

Install yum-utils, a collection of utilities that integrate with yum to extend its native features.

```
$ sudo yum install yum-utils
```

If /tmp directory is mounted using noexec switch, the admin UI does not start, because it uses /tmp directory. Check is /tmp directory mounted using noexec switch:

```
$ mount | grep /tmp
```

If there is the output contain /tmp and noexec like the following

```
/dev/loop0 on /tmp type ext3 (rw,noexec,nosuid,nodev)
```

noexec switch must be removed modifying /etc/fstab file. In addition, the directory must be mounted again to make the changes effective immediately.

Run the following command.

```
$ mount -o remount,exec /tmp
```



## Installation

### Installation for Ubuntu.

To install the PlanetCross security server software, follow these steps from the command line.

You can check the version list.

```
$ sudo apt-get update  
  
$ sudo apt show -a xroad-securityserver-planetway={version} ¥
```

You can install the PlanetCross package using following command.

```
$ sudo apt-get install xroad-securityserver-planetway={version} ¥
```

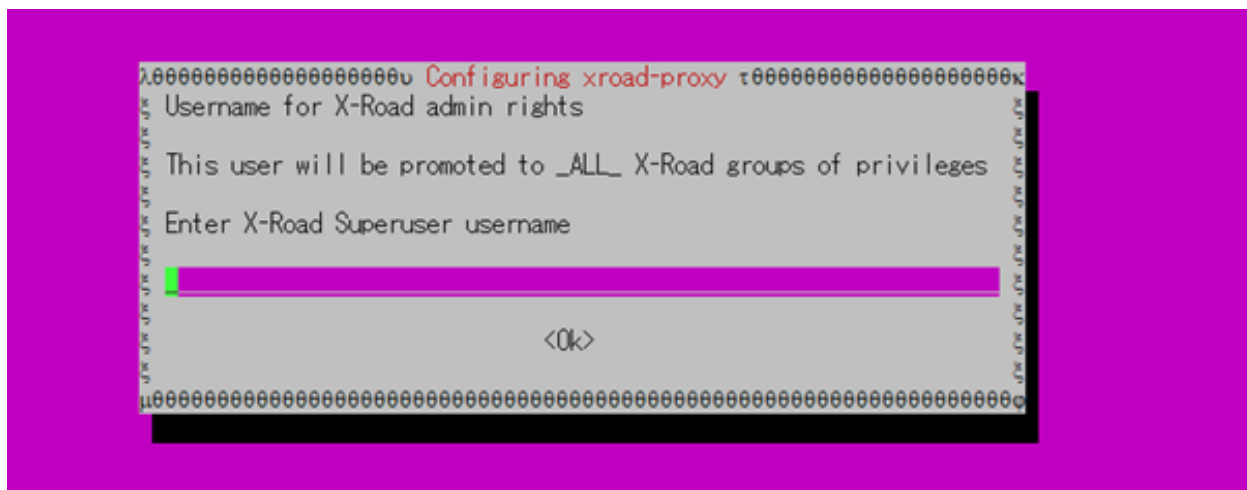
```
xroad-securityserver={version} ¥  
  
xroad-addon-opmonitoring={version} ¥  
  
xroad-proxy={version} ¥  
  
xroad-addon-metaservices={version} ¥  
  
xroad-addon-messagelog={version} ¥  
  
xroad-addon-proxymonitor={version} ¥  
  
xroad-addon-wsdlvalidator={version} ¥  
  
xroad-jetty9={version} ¥  
  
xroad-confclient={version} ¥  
  
xroad-nginx={version} ¥  
  
xroad-signer={version} ¥  
  
xroad-base={version} ¥  
  
xroad-opmonitor={version} ¥  
  
xroad-monitor={version}
```

If you encounter this error, you can contact Planetway administrator

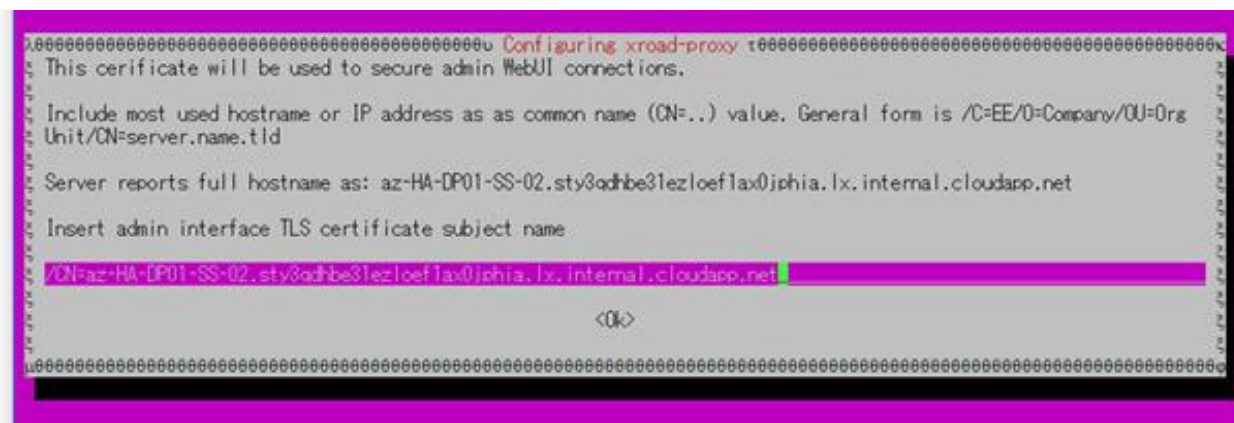
```
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package xroad-securityserver-planetway
```

Upon the first installation of the packages, the system asks for the following information.

- Account name for the user who will be granted the rights to perform all activities in the user interface.

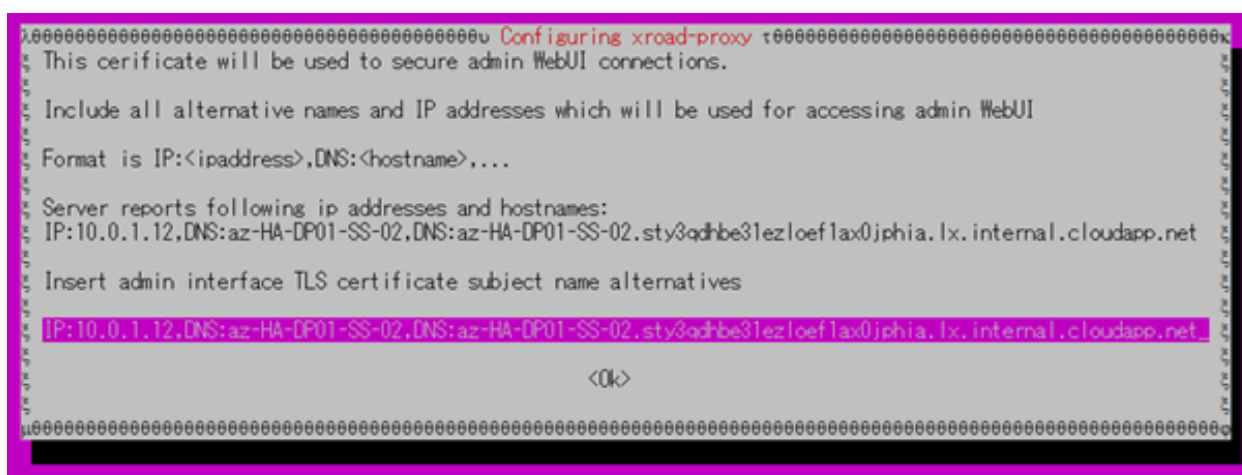


- The Distinguished Name of the owner of the user interface's self-signed TLS certificate ( Subject DN ) and its alternative names ( subjectAltName ). The certificate is used for securing connections to the user interface. The name and IP addresses detected from the operating system are suggested as default values.
  - The Subject DN must be entered in the format:  
  
/CN=server.domain.tld



- All IP addresses and domain names in use must be entered as alternative names in the format:

IP:1.2.3.4,IP:4.3.2.1,DNS:servername,DNS:servername2.domain.tld



- The Distinguished Name of the owner of the TLS certificate that is used for securing the HTTPS access point of information systems. The name and IP addresses detected from the system are suggested as default values.
  - The Subject DN must be entered in the format:

```
/CN=server.domain.tld
```

[illegible]

- All IP addresses and domain names in use must be entered as alternative names in the format:

IP:1.2.3.4,IP:4.3.2.1,DNS:servername,DNS:servername2.domain.tld

[illegible]

The meta-package `xroad-securityserver` also installs `metaservices` module `xroad-addon-metaservices` , `messagelog` module `xroad-addon-messagelog` and `WSDL` validator module `xroad-addon-wsdlvalidator` . The meta-package `xroad-securityserver-ee` installs operational data monitoring module `xroad-addon-opmonitoring` .

## Post-Installation Checks

The installation is successful if system services are started and the user interface is responding.

- Ensure from the command line that X-Road services are in the loaded/active state (example output follows):

```
$ sudo systemctl status xroad-* | grep "Loaded¥|Active"

Loaded: loaded (/lib/systemd/system/xroad-confclient.service; enabled;
vendor preset: enabled)

Active: active (running) since Fri 2018-08-10 09:30:39 UTC; 2 months 5 days
ago

Loaded: loaded (/lib/systemd/system/xroad-signer.service; enabled; vendor
preset: enabled)

Active: active (running) since Tue 2018-10-09 13:52:44 UTC; 5 days ago

Loaded: loaded (/lib/systemd/system/xroad-jetty.service; enabled; vendor
preset: enabled)

Active: active (running) since Tue 2018-10-09 14:10:32 UTC; 5 days ago

Loaded: loaded (/lib/systemd/system/xroad-proxy.service; enabled; vendor
preset: enabled)

Active: active (running) since Fri 2018-08-10 09:30:45 UTC; 2 months 5 days
ago

Loaded: loaded (/lib/systemd/system/xroad-opmonitor.service; enabled; vendor
preset: enabled)

Active: active (running) since Tue 2018-10-09 13:47:04 UTC; 5 days ago

Loaded: loaded (/lib/systemd/system/xroad-monitor.service; enabled; vendor
preset: enabled)

Active: active (running) since Tue 2018-10-09 13:46:55 UTC; 5 days ago
```

Ensure that the security server user interface at <https://SECURITYSERVER:4000/> (where SECURITYSERVER is the security server internal IP address or host-name) can be opened in a Web browser. To log in, use the account name chosen during the installation.

## Installation for RHEL.

To install the X-Road security server software on RHEL7 operating system, follow these steps.

### Add Extra Packages for Enterprise Linux (EPEL) repository.

```
$ sudo yum install  
https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

The following packages are fetched from EPEL.

crudini, rlwrap and nginx.

```
$ sudo yum install crudini  
$ sudo yum install rlwrap  
$ sudo yum install nginx
```

Issue the following command to install the security server packages.

```
$ sudo yum install xroad-securityserver-planetway
```

Add system user whom all roles in the user interface are granted. Add a new user with the command.

```
$ sudo xroad-add-admin-user <username>
```

Once the installation is completed, start the security server.

```
$ sudo systemctl start xroad-proxy
```

## Post-Installation Checks

The installation is successful if system services are started and the user interface is responding.

Ensure from the command line that X-Road services are in the running state (example output follows):

```
$ sudo systemctl | grep xroad  
  
xroad-confclient.service loaded active running X-Road confclient  
  
xroad-jetty9.service loaded active running X-Road Jetty server  
  
xroad-monitor.service loaded active running X-Road Monitor  
  
xroad-opmonitor.service loaded active running X-Road opmonitor daemon  
  
xroad-proxy.service loaded active running X-Road Proxy  
  
xroad-signer.service loaded active running X-Road signer
```

Ensure from the command line that nginx services are in the running state (example output follows):

```
$ sudo systemctl status nginx
```

Ensure that the security server user interface at <https://SECURITYSERVER:4000> can be opened in a Web browser. To log in, use the account name chosen during the installation. While the user interface is still starting up, the Web browser may display the “502 Bad Gateway” error.

If you can't access to <https://SECURITYSERVER:4000>, please check the network requirements are met in Security Groups, firewalld or so.

## Security Server Initial Configuration

During the security server initial configuration, the server's PlanetCross membership information and the software token's PIN are set.

### Prerequisites

Configuring the security server assumes that the security server owner is a member of the PlanetCross.

### Reference Data

ATTENTION: Reference items 1.1 - 1.3 in the reference data are provided to the security server owner by the PlanetCross central's administrator.

The security server code and the software token's PIN will be determined during the installation at the latest, by the person performing the installation.

Your MemberClass is `COM`

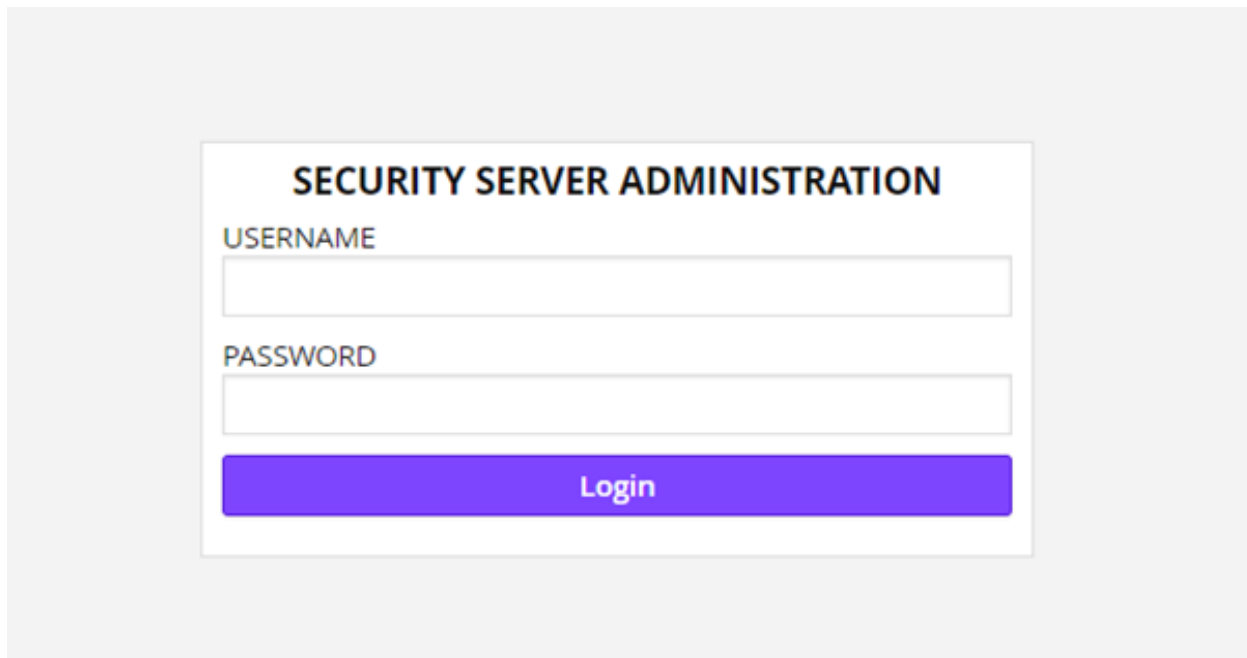
Ref		Explanation
1.1	For Test <a href="http://static.planetcross.net/test/configuration_anchor.xml">http://static.planetcross.net/test/configuration_anchor.xml</a> For Production <a href="http://static.planetcross.net/prod/configuration_anchor.xml">http://static.planetcross.net/prod/configuration_anchor.xml</a>	Global configuration anchor file is available here for download
1.2	GOV - government <b>COM - commercial</b>	Member class of the security server's owner.
1.3	<security server owner register code>	<b>Member code</b> of the security server's owner will be provided to you
1.4	<choose security server identifier name>	Security server's code
1.5	<choose PIN for software token>	Software token's PIN



## Configuration

To perform the initial configuration, open the address

<https://SECURITYSERVER:4000/> in a Web browser. To log in, use the account name chosen during the installation.



The screenshot shows a web browser window displaying the 'SECURITY SERVER ADMINISTRATION' login page. The page has a white background with a light gray border. At the top, the title 'SECURITY SERVER ADMINISTRATION' is centered in bold black text. Below the title, there are two input fields: 'USERNAME' and 'PASSWORD', both with light gray borders. Below the password field is a large blue button with the text 'Login' in white. The entire form is centered on the page.

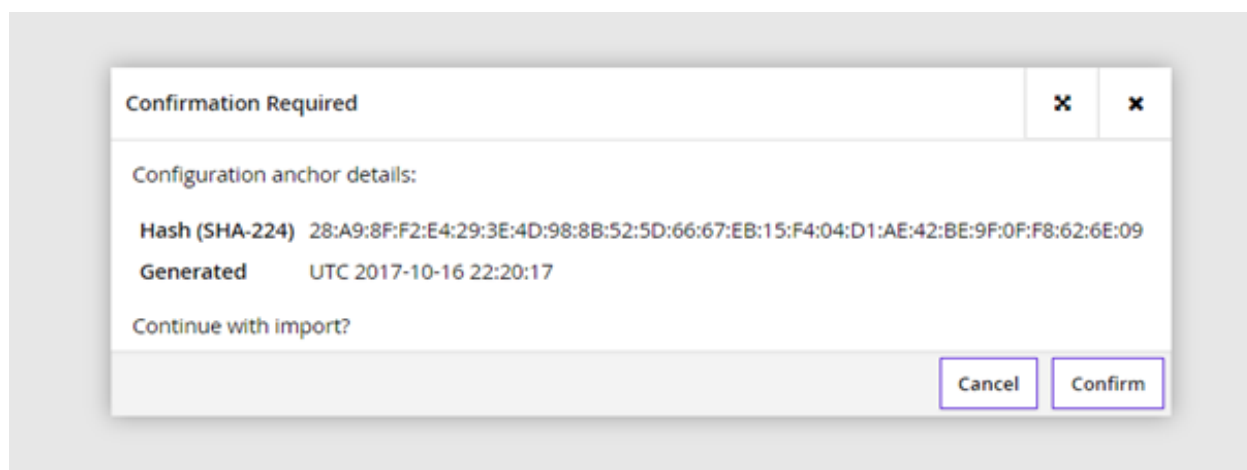
Upon first log-in, the system asks for the following information.

- The global configuration anchor file (reference data: 1.1 ).



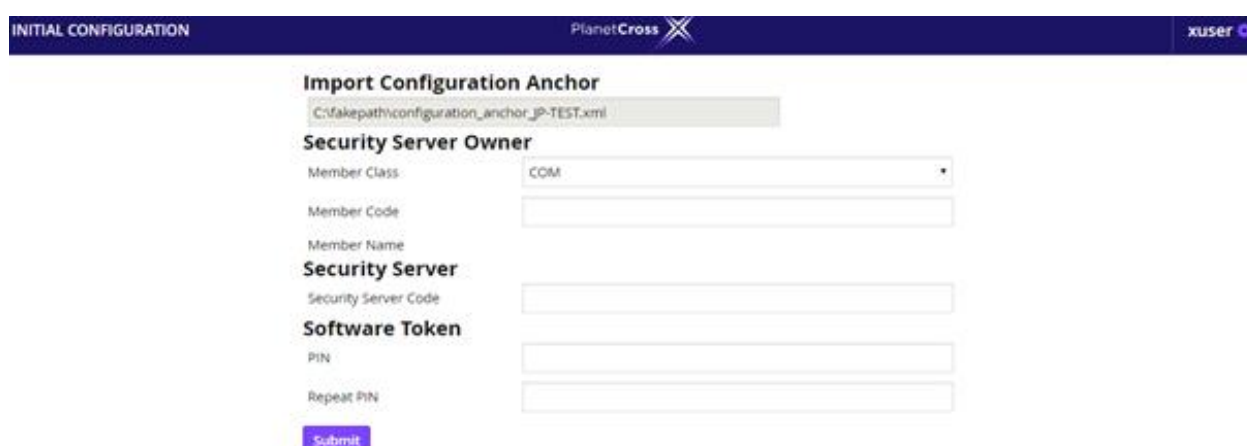
The screenshot shows the 'INITIAL CONFIGURATION' page of the Security Server Administration interface. The page has a dark blue header bar with the text 'INITIAL CONFIGURATION' on the left, the 'PlanetCross' logo in the center, and a 'xuser' profile icon on the right. Below the header, the main content area is white. It features a section titled 'Import Configuration Anchor' with a light gray input field. To the right of the input field are two buttons: 'Browse' and 'Import'.

You can confirm it now.

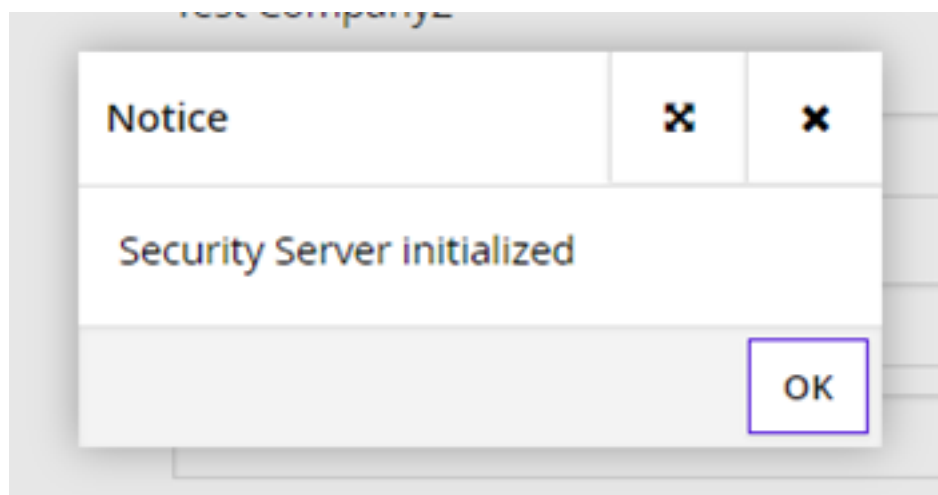


If the configuration is successfully downloaded, the system asks for the following information.

- The security server owner's member class (reference data: 1.2).
- The security server owner's member code (reference data: 1.3). If the member class and member code are correctly entered, the system displays the security server owner's name as registered in the PlanetCross center.
- Security server code (reference data: 1.4), which is chosen by the security server administrator and which has to be unique across all the security servers belonging to the same PlanetCross member.
- Software token's PIN (reference data: 1.5). The PIN will be used to protect the keys stored in the software token. The PIN must be stored in a secure place, because it will be no longer possible to use or recover the private keys in the token once the PIN has been lost.

The "INITIAL CONFIGURATION" screen of the PlanetCross system. The header bar is dark blue with "INITIAL CONFIGURATION" on the left, the "PlanetCross" logo in the center, and a "xuser" profile icon on the right. The main content area is white and titled "Import Configuration Anchor". Below the title is a text box containing the file path "C:\fakepath\configuration\_anchor JP-TEST.xml". The form is divided into three sections: "Security Server Owner" with fields for "Member Class" (a dropdown menu showing "COM") and "Member Code"; "Security Server" with a field for "Security Server Code"; and "Software Token" with fields for "PIN" and "Repeat PIN". A blue "Submit" button is located at the bottom left of the form.

This security server is initialized and click ok to proceed.



## Security Server Registration

To use a security server for mediating (exchanging) messages, the security server and its owner must be certified by a certification service provider approved by the PlanetCross governing authority, and the security server has to be registered in the PlanetCross governing authority.

### Configuring the Signing Key and Authentication Key and Certificates for the Security Server Owner

The signing keys used by the security servers for signing PlanetCross messages can be stored on software or hardware based (a Hardware Security Module or a smartcard) security tokens, according to the security policy of the PlanetCross instance.

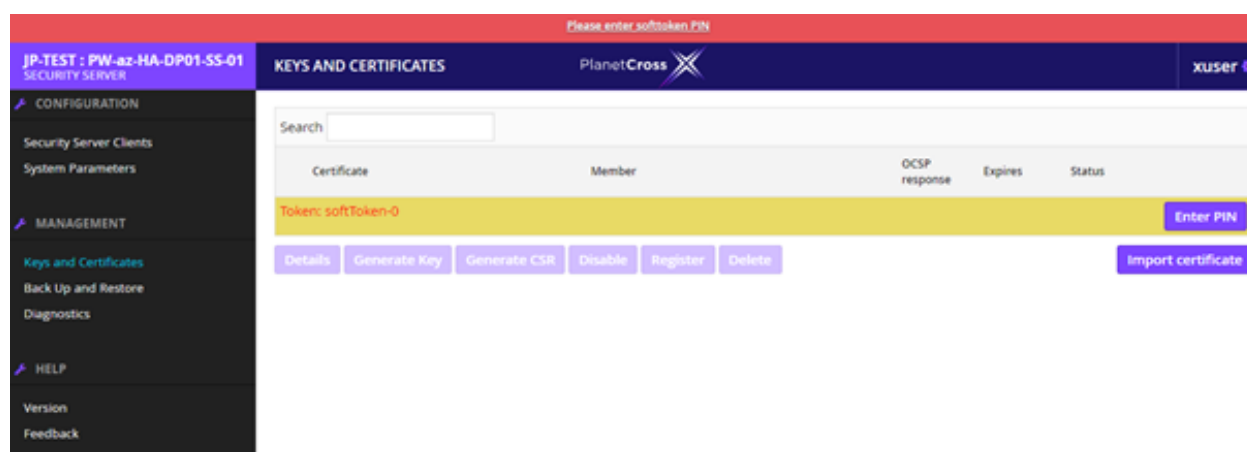
### Generating an Authentication Key

Access rights

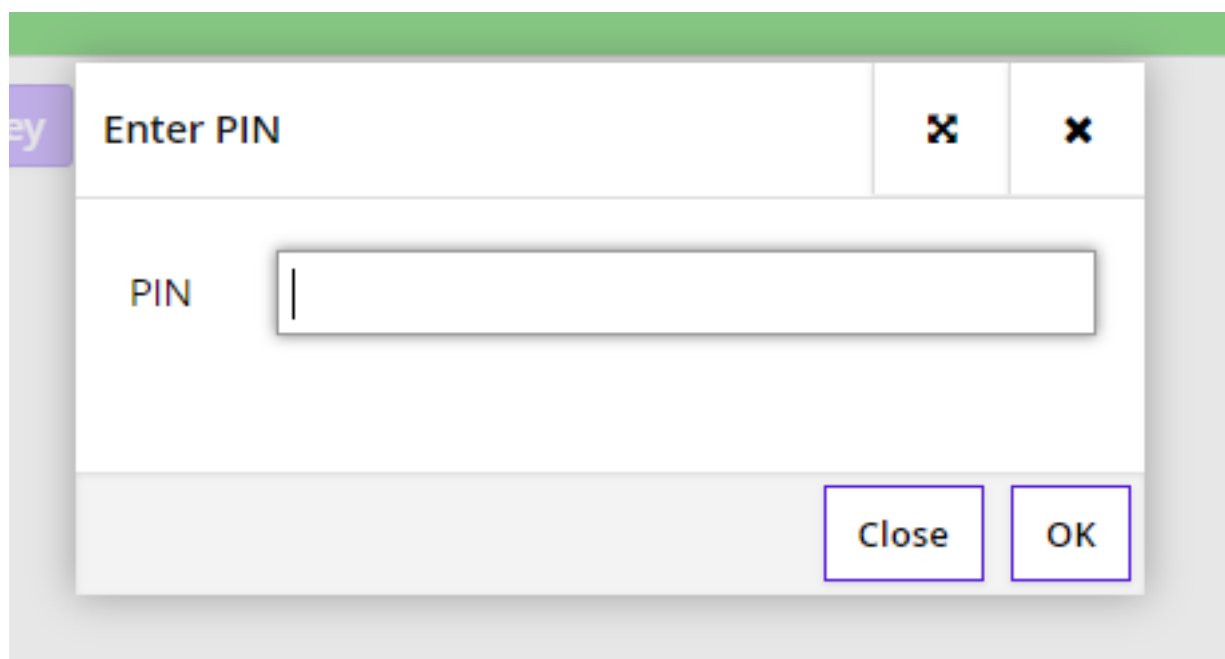
- All activities: [Security Officer](#)

The security server's authentication keys can only be generated on software security tokens.

1. On the Management menu, select Keys and Certificates.

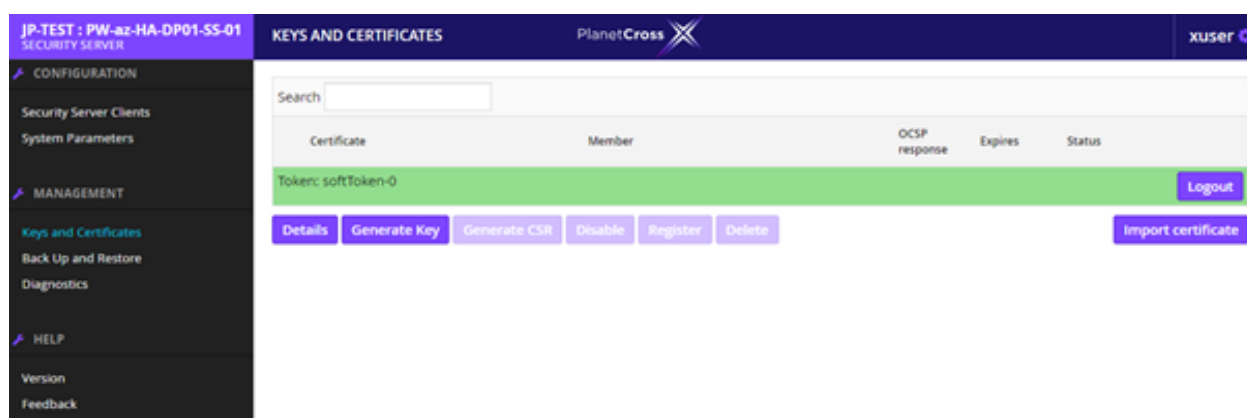


2. To log in to the software token, click Enter PIN on the token's row in the table and enter the token's PIN code. Once the correct PIN is entered, the Enter PIN button changes to Logout.



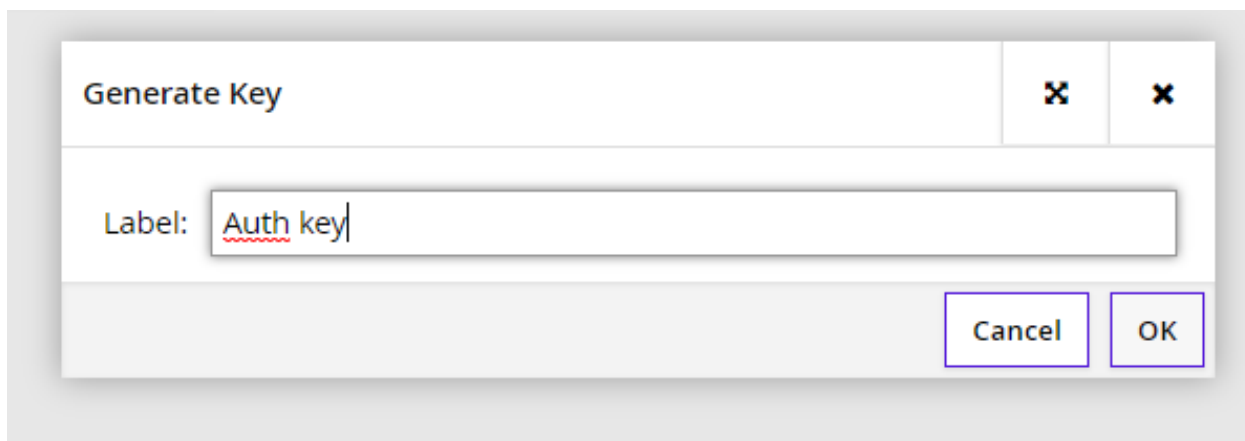
A dialog box titled "Enter PIN" with a close button (X) in the top right corner. Below the title is a text input field labeled "PIN" with a vertical cursor. At the bottom right are two buttons: "Close" and "OK".

3.To generate an authentication key, select the software token from the table by clicking the respective row, and click Generate key. Enter the label value for the key and click OK.

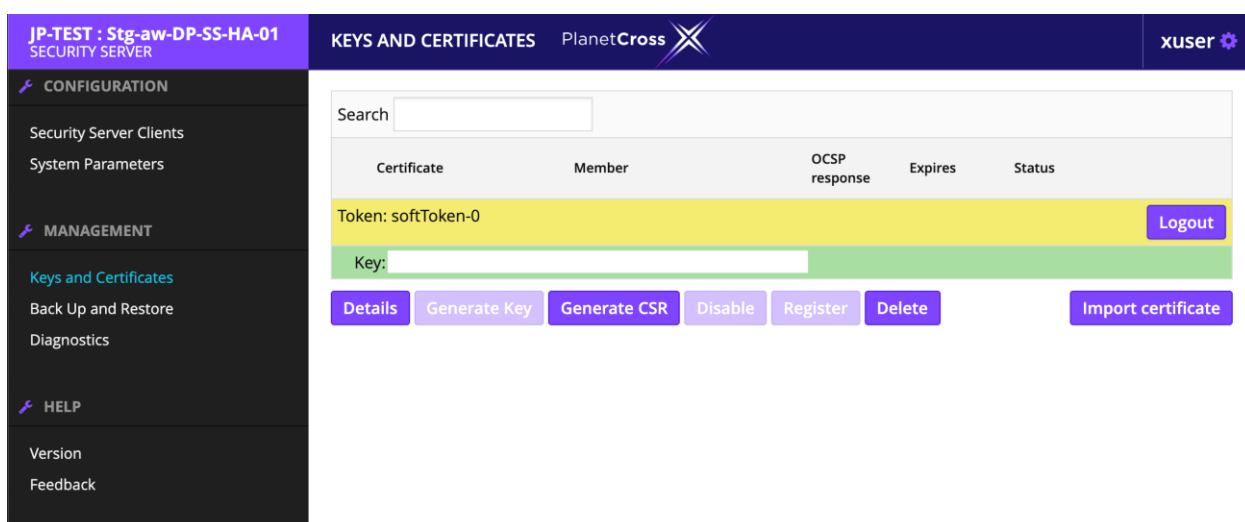


The screenshot shows the PlanetCross "KEYS AND CERTIFICATES" interface. The left sidebar contains navigation links: CONFIGURATION (Security Server Clients, System Parameters), MANAGEMENT (Keys and Certificates, Back Up and Restore, Diagnostics), and HELP (Version, Feedback). The main area has a search bar and a table with columns: Certificate, Member, OSCP response, Expires, and Status. A row is highlighted with the token "Token: softToken-0". Below the table are buttons: Details, Generate Key, Generate CSR, Disable, Register, Delete, and Import certificate. A "Logout" button is also present.

4.The generated key appears under the token's row in the table. The label value is displayed as the name of the key.



Keys appears like this



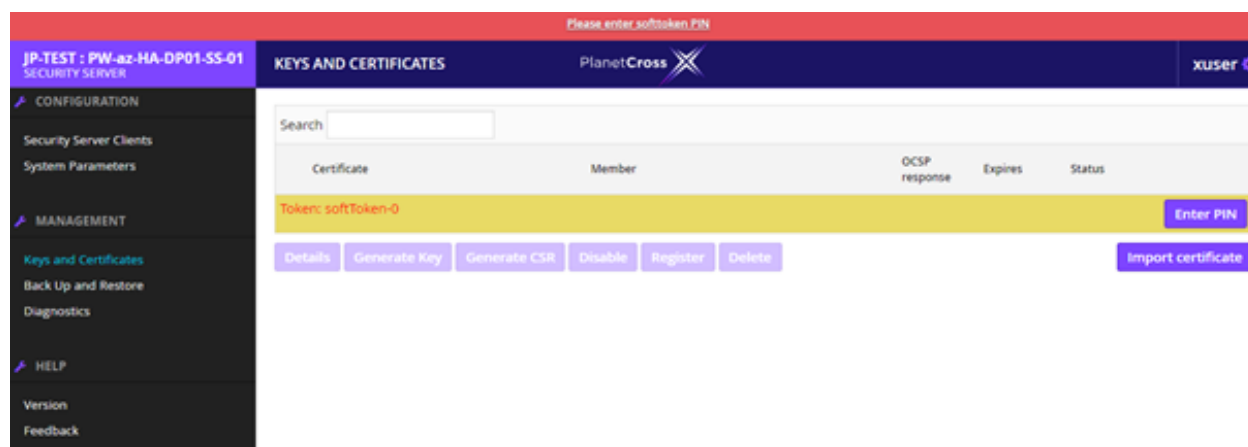
## Generating a Signing Key

Access rights:

- All activities: [Security Officer](#)
- All activities except logging into the key device: [Registration Officer](#)

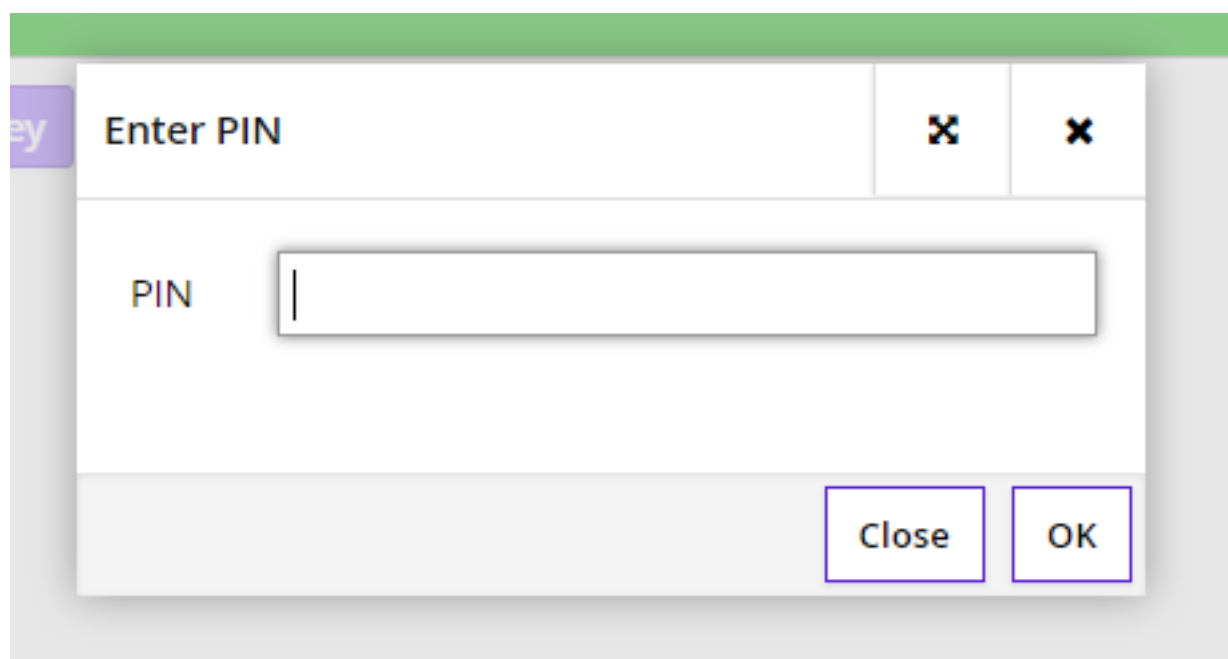
To generate a signing key, follow these steps.

1. On the Management menu, select Keys and Certificates.

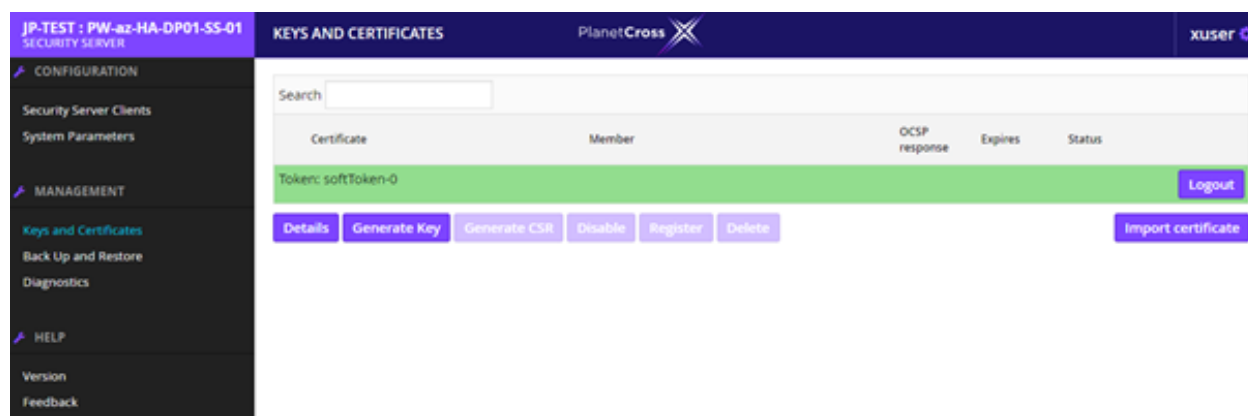


2.If you are using a hardware security token, ensure that the device is connected to the security server. The device information must be displayed in the Keys and Certificates table.

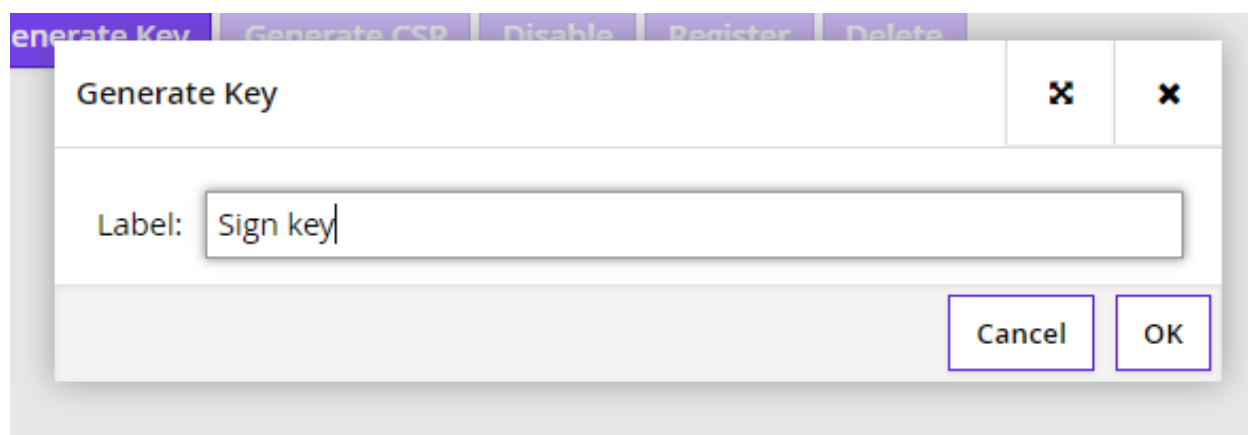
3.To log in to the token, click Enter PIN on the token's row in the table and enter the PIN code. Once the correct PIN is entered, the Enter PIN button changes to Logout.



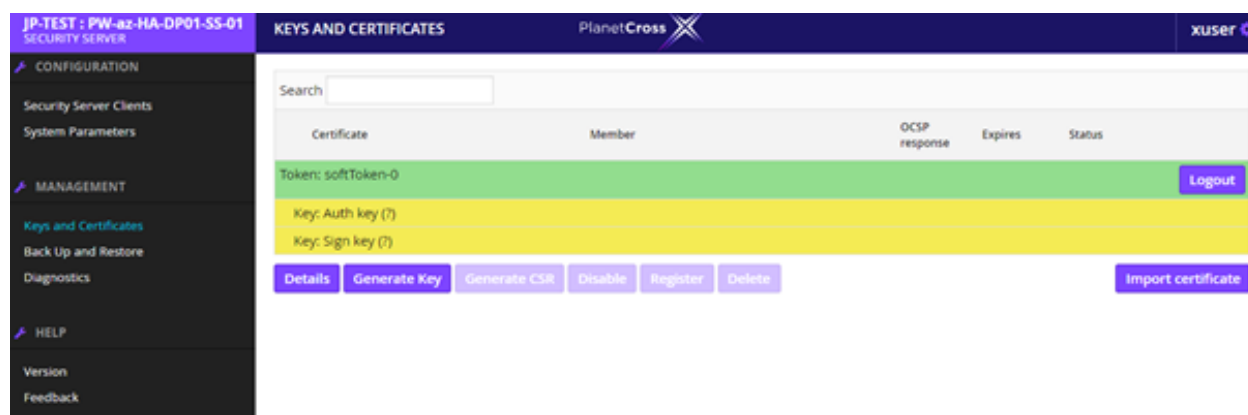
4.To generate a signing key, select the token from the table by clicking the respective row and click Generate key.



5. Enter the label value for the key and click OK. The generated key appears under the token's row in the table. The label value is displayed as the name of the key.



key appears like this



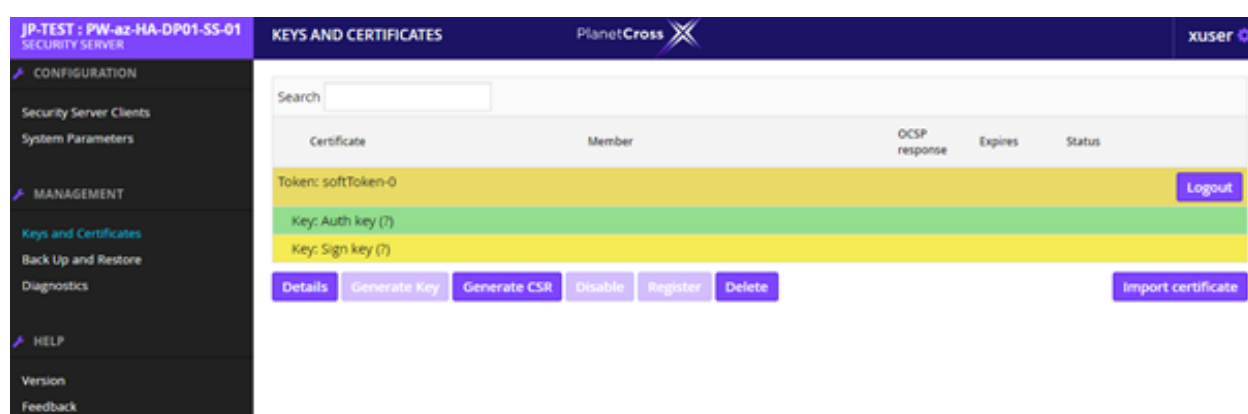


## Generating a Certificate Signing Request for an Authentication Key

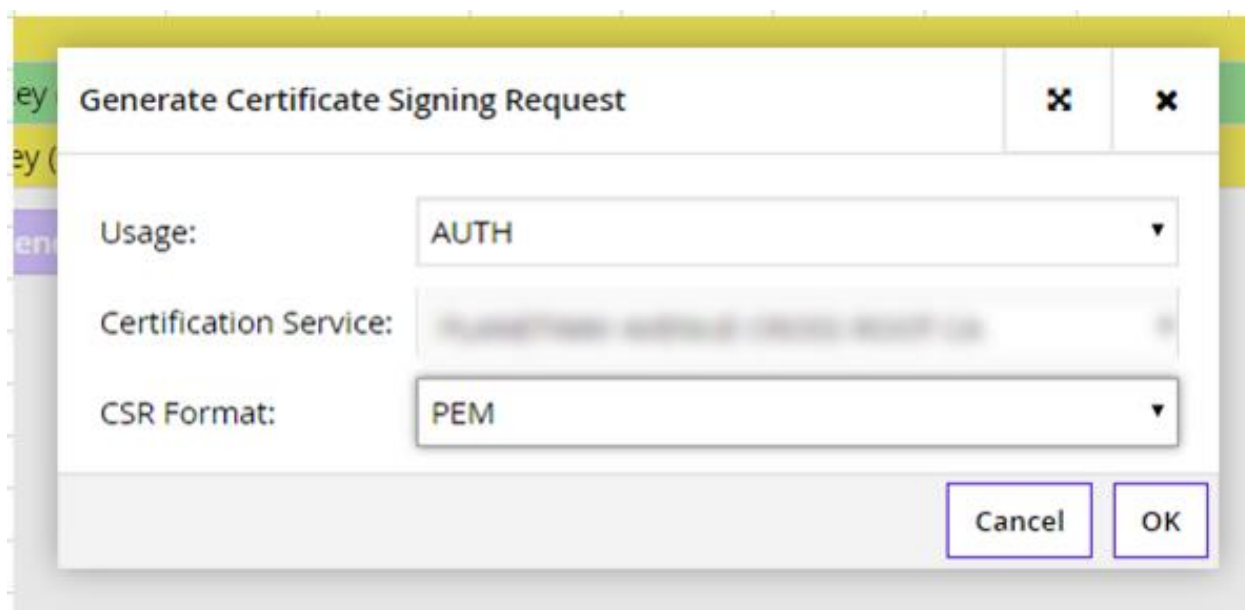
Access rights: [Security Officer](#)

To generate a certificate signing request (CSR) for the authentication key, follow these steps.

1. On the Management menu, select Keys and Certificates.
2. Select the authentication key from the table and click Generate CSR. In the dialog that opens

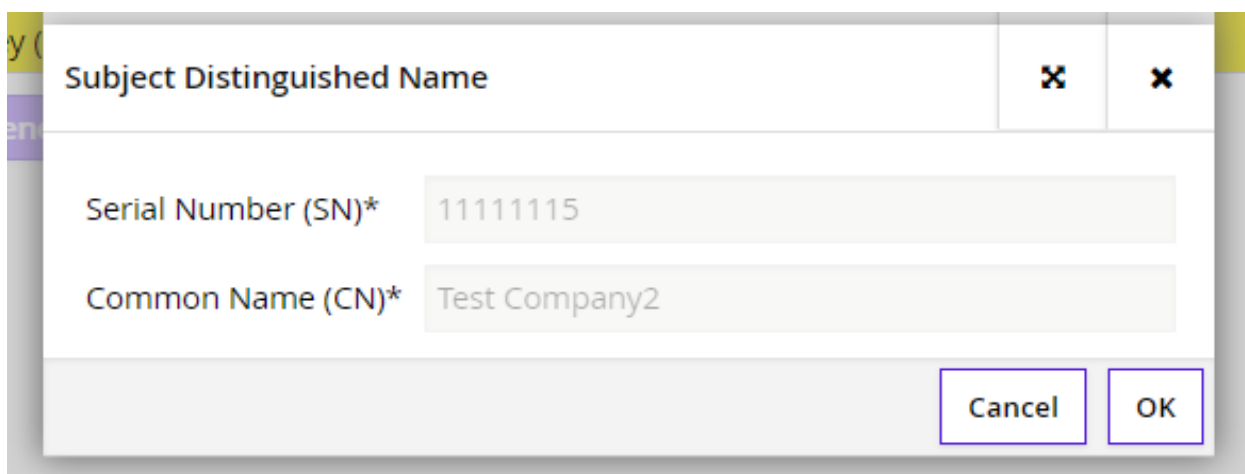


- a. Select the certificate usage policy from the Usage drop down list (AUTH for authentication certificates);
- b. Select the issuer of the certificate from the Certification Service drop-down list;
- c. Select the **PEM** format of the certificate signing request (PEM or DER), according to the certification service provider's requirements
- d. Click OK;



The screenshot shows a dialog box titled "Generate Certificate Signing Request". It has three input fields: "Usage:" with a dropdown menu showing "AUTH", "Certification Service:" with a text field containing "PLANETWAY JAPAN CONFIDENTIAL", and "CSR Format:" with a dropdown menu showing "PEM". At the bottom right, there are "Cancel" and "OK" buttons.

3. In the form that opens, review the information that will be included in the CSR and fill in the empty fields, if needed.



The screenshot shows a dialog box titled "Subject Distinguished Name". It has two input fields: "Serial Number (SN)\*" with a text field containing "11111115" and "Common Name (CN)\*" with a text field containing "Test Company2". At the bottom right, there are "Cancel" and "OK" buttons.

4. Click OK to complete the generation of the CSR and save the prompted file to the local file system.

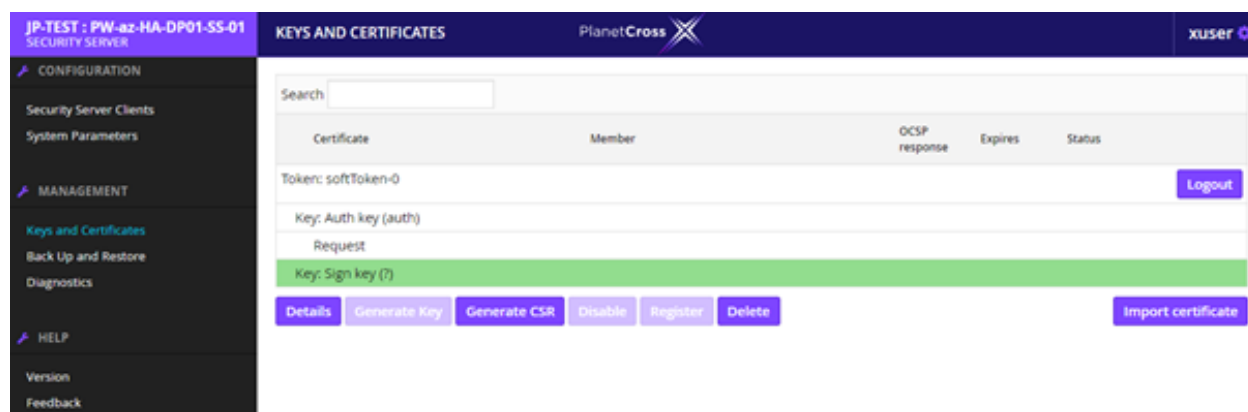
After the generation of the CSR, a "Request" record is added under the key's row in the table, indicating that a certificate signing request has been created for this key. The record is added even if the request file was not saved to the local file system. (take note of the location that the file is save)

## Generating a Certificate Signing Request for a Signing Key

Access rights: [Security Officer](#) , [Registration Officer](#)

To generate a certificate signing request (CSR) for the signing key, follow these steps.

1. On the Management menu, select Keys and Certificates.
2. Select a key from the table and click Generate CSR. In the dialog that opens



- a. Select the certificate usage policy from the Usage drop down list (SIGN for signing certificates);
- b. select the PlanetCross member the certificate will be issued for from the Client drop-down list;
- c. select the issuer of the certificate from the Certification Service drop-down list;
- d. select the format of the certificate signing request (PEM or DER), according to the certification service provider's requirements
- e. click OK;

A dialog box titled "Generate Certificate Signing Request" with a close button (X) in the top right corner. It contains four fields: "Usage:" with a dropdown menu set to "SIGN"; "Client:" with a dropdown menu set to "JP-TEST:COM:11111115:\*"; "Certification Service:" with a blurred text field; and "CSR Format:" with a dropdown menu set to "PEM". At the bottom right are "Cancel" and "OK" buttons.

Generate Certificate Signing Request

Usage: SIGN

Client: JP-TEST:COM:11111115:\*

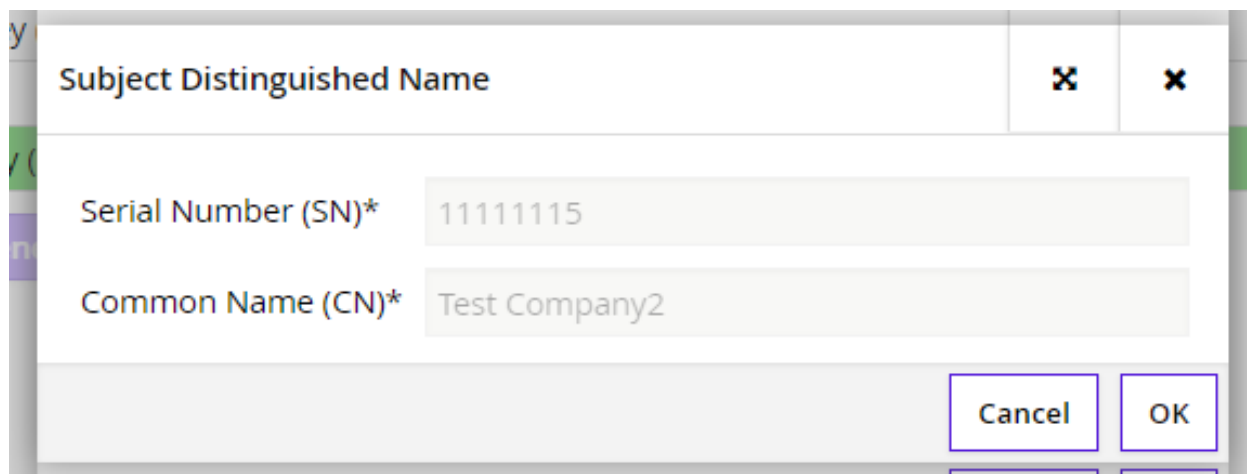
Certification Service:

CSR Format: PEM

Cancel OK

3. In the form that opens, review the certificate owner's information that will be included in the CSR and fill in the empty fields, if needed.

4. Click OK to complete the generation of the CSR and save the prompted file to the local file system.

A dialog box titled "Subject Distinguished Name" with a close button (X) in the top right corner. It contains two fields: "Serial Number (SN)\*" with the value "11111115" and "Common Name (CN)\*" with the value "Test Company2". At the bottom right are "Cancel" and "OK" buttons.

Subject Distinguished Name

Serial Number (SN)\* 11111115

Common Name (CN)\* Test Company2

Cancel OK

After the generation of the CSR, a "Request" record is added under the key's row in the table, indicating that a certificate signing request has been created for this key. The record is added even if the request file was not saved to the local file system. (take note of the location that you save the file to)

## Sending CSR to Planetway

At this step, you need send CSR file and Security Server Code to Planetway representative.

Please, send following information.

- Authentication CSR
- Signing CSR
- Securiy Server Code

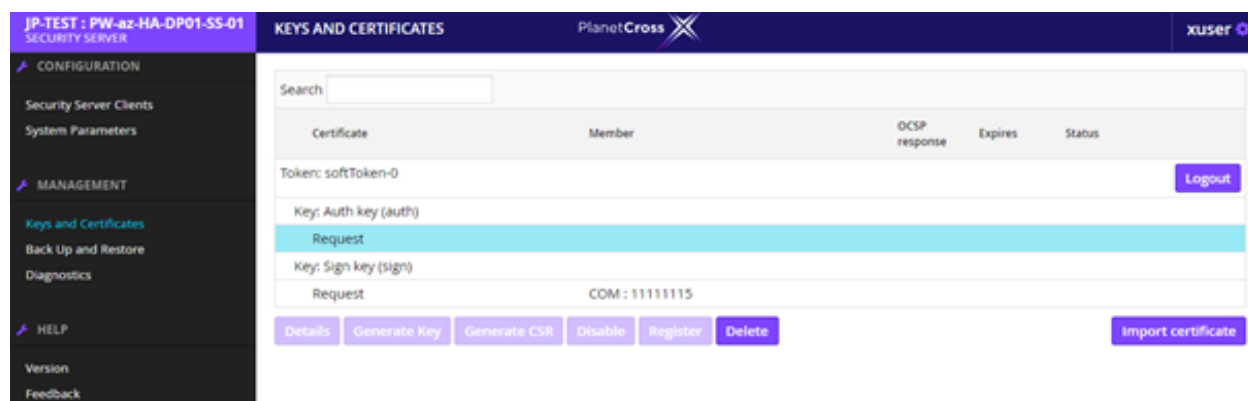
After that, Planetway will resigiter above information in Central Server and send you Authentication certificate file and Signing certificate file.

## Importing an Authentication Certificate from the Local File System

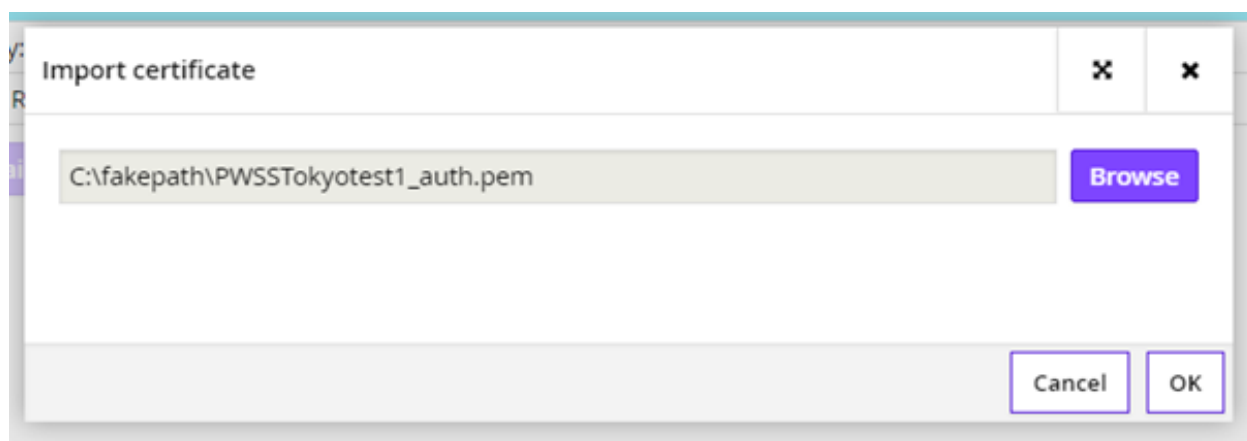
Access rights: [Security Officer](#)

To import the authentication certificate to the security server, follow these steps.

1. On the Management menu, select Keys and Certificates.
2. Click Import certificate.



3. Locate the certificate file from the local file system and click OK. After importing the certificate, the "Request" record under the authentication key's row is replaced with the information from the imported certificate. By default, the certificate is imported in the "Saved" and "Disabled" states.



## Importing a Signing Certificate from the Local File System

Access rights: [Security Officer](#) , [Registration Officer](#)

To import the signing certificate to the security server, follow these steps.

1. On the Management menu, select Keys and Certificates.
2. Click Import certificate.



3. Locate the certificate file from the local file system and click OK. After importing the certificate, the "Request" record under the signing key's row is replaced with the information from the imported certificate. By default, the signing certificate is imported in the "Registered" state.



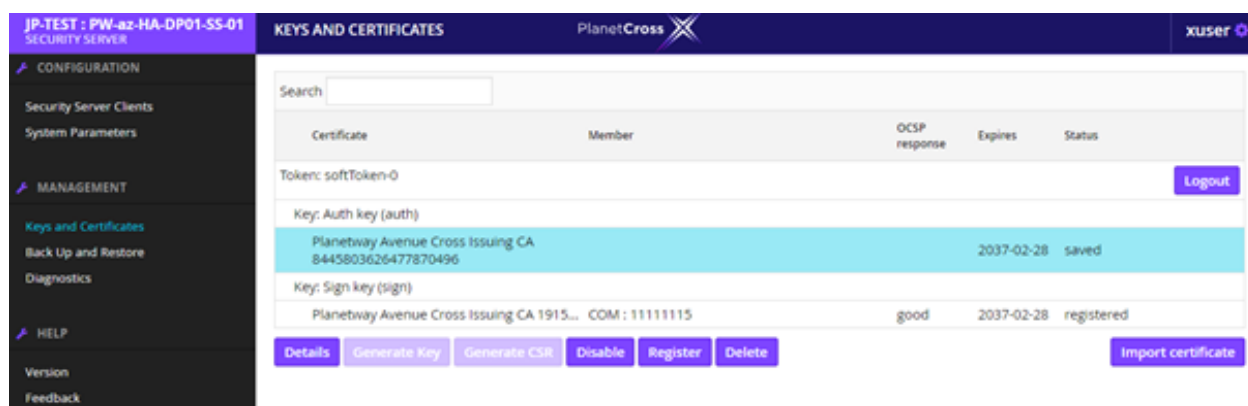
## Registering an Authentication Certificate

Access rights: [Security Officer](#)

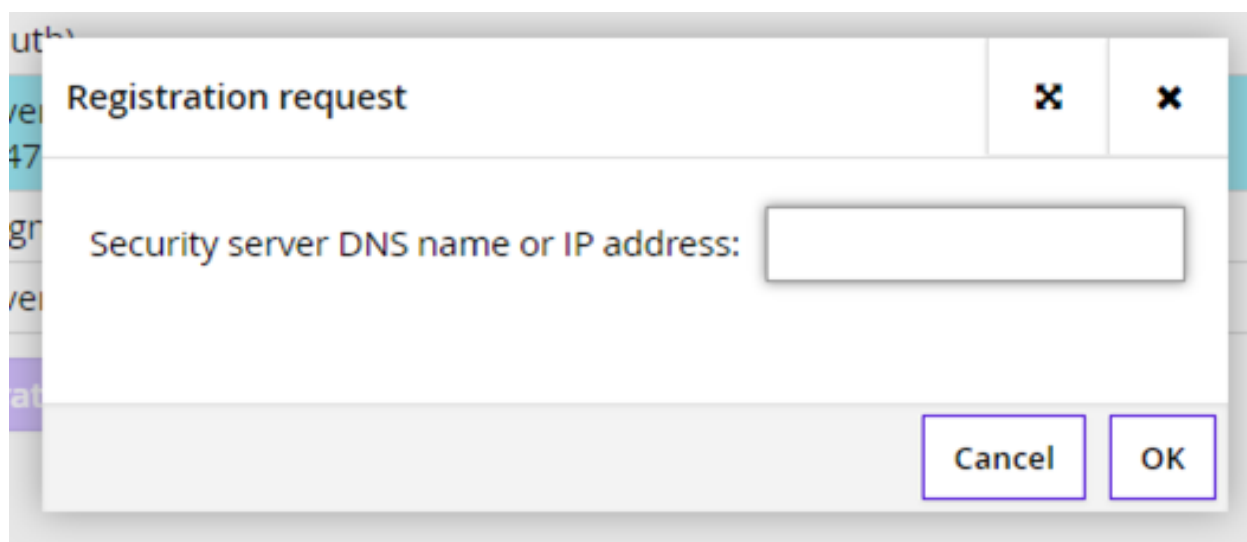
The security server's registration request is signed in the security server with the server owner's signing key and the server's authentication key. Therefore, ensure that the corresponding certificates are imported to the security server and are in a usable state (the tokens holding the keys are in logged in state and the OCSP status of the certificates is "good").

To submit an authentication certificate registration request, follow these steps.

1. On the Management menu, select Keys and Certificates.
2. Select an authentication certificate to be registered (it must be in the "saved" state) and click Register.
3. Click "Activate" button to be ready to register



3. In the dialog that opens with "Register" button, enter the security server's public DNS name or its external IP address and click OK.



(Use the DNS name not IP when registering the Security Server. e.g: sho-ss.domain.com. The reason is if your IP address is changed then some setting should be changed at the Central Server as well.)

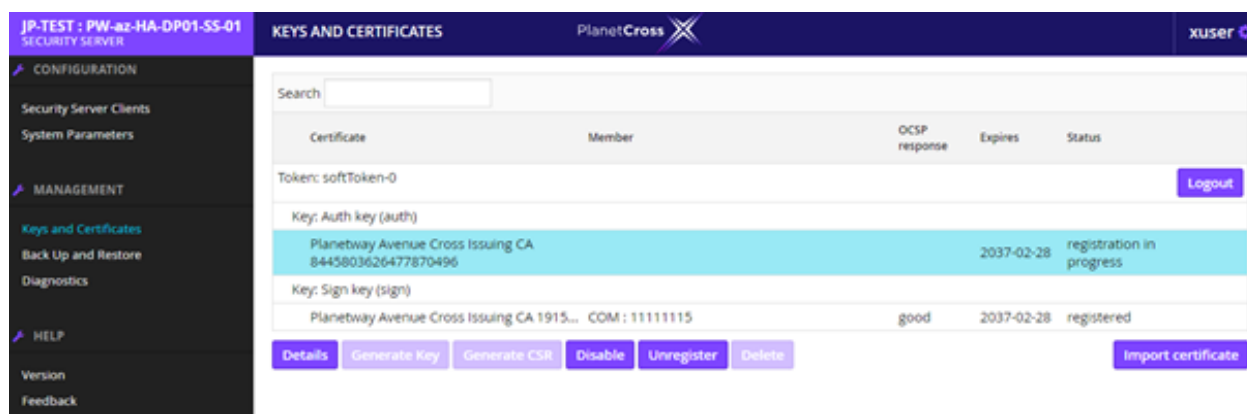
On submitting the request, the message "Request sent" is displayed, and the authentication certificate's state is set to "Registration in process".

After this step, you need to send following information to Planetway representative again.

- Security Server Code
- Authentication certificate file (pem format)

After Planetway receive these information, Planetway register these information Central Server.

Then, your request is approved so that authentication certificate is set to "Registered" and the registration process is completed.

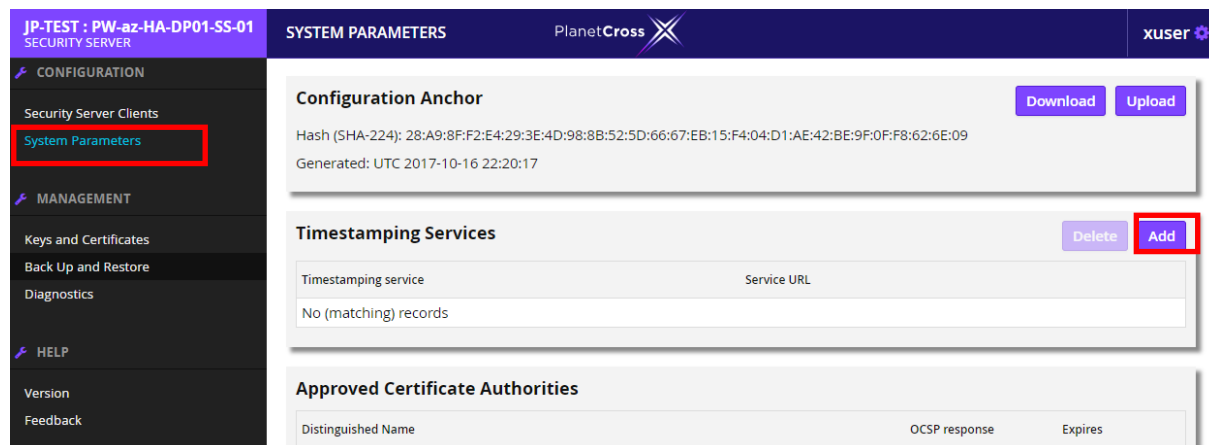




## Register timestamping Server

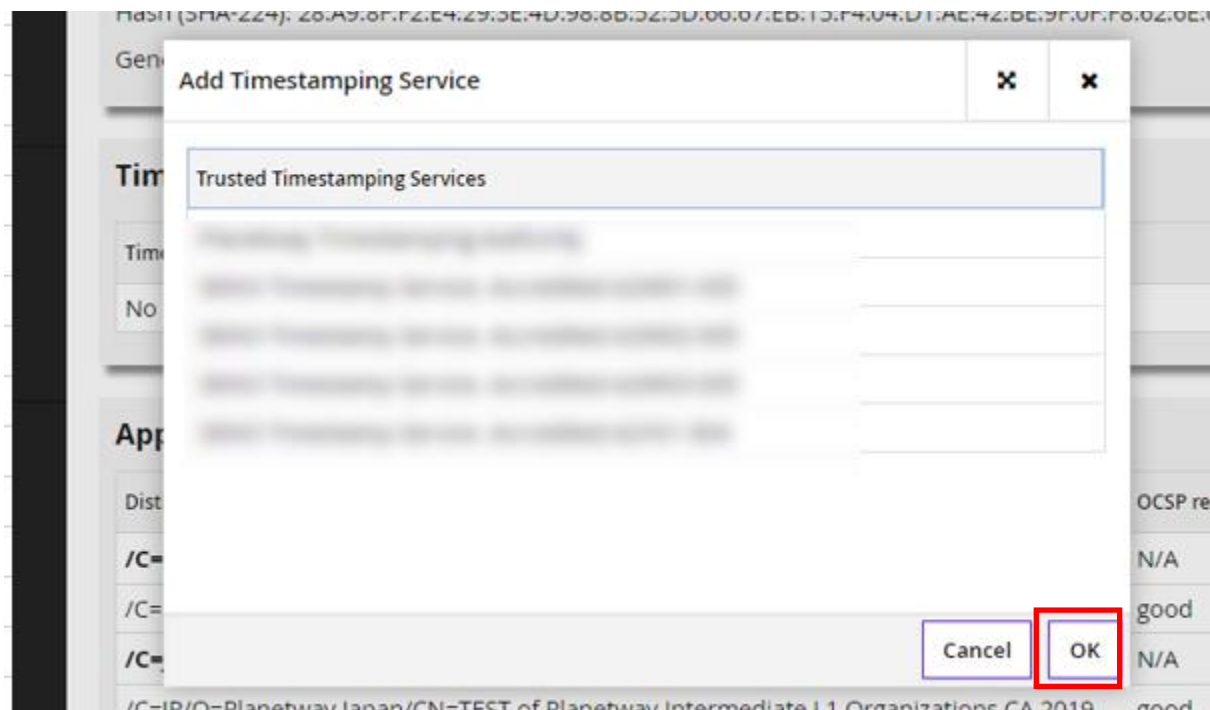
You need to register timestamping server (TSA) in your security server with following steps.

Select “System Parameters” and push “add” button in “Timestamping Services” filed.



Then, you need to select timestamping service in list,

An appropriate service has been described in “Release note”, please make sure one.



Finally, Sercurit Server Installation steps are completed.

The other document, "Security Server Setting Guide" is described how to exchange the data to with other organizations, please refer to this one as well.

## Revision History

---

Version	Date	Details
V1.6	10/02/2020	Publish first edition.