

Instalación y requisitos para agregar un Security Server en la plataforma X-Road ASI

Versión de X-Road 7.3.2

HISTORIA DE DOCUMENTO

Fecha	Versión	Modifica:	Revisado:	Detalle
2023/11/06	1.0	Ivan Bua	Ivan Bua	Primera versión
2024/01/09	1.1	Ivan Bua	Ivan Bua	Cambios en las dependencias y puertos
2024/03/07	1.2	Ivan Bua	Ivan Bua	Cambios en configuración
2024/05/02	1.3	Martinez Tullio Joaquin Roberto	Ivan Bua	Documentación base de datos externa
2024/08/01	1.4	Ivan Bua	Ivan Bua	Cambios en puertos

ÍNDICE

1 Propósito de este documento – Alcance y límites	3
1.1 Referencias	3
2 Prerrequisitos de Recursos Security Server	4
3 Habilitaciones del Security Server:	4
4 Instalación	6
Habilitación de puertos - firewall	10
5 Consideraciones al finalizar la instalación:	12
Una vez finalizada la instalación del SS:	12

1 Propósito de este documento – Alcance y límites

Esta documentación está orientada para que sea recibida por el área de Operaciones / Infraestructura de la ASI para ambientes de Producción, Homologación y QA.

Se recomienda tener conocimiento en instalaciones y administración en SO Linux o RHEL .
Se dejará en “Referencias” la documentación necesaria para comenzar la instalación.

Requisitos para considerar :

- 1- VM con Sistema operativo RHEL versión 8 - Red Hat Enterprise Linux release 8.7 o superior
- 2- Tener usuario admin/sudo del Security Server.
- 3- Tener conectividad hacia los puertos necesarios para establecer comunicación con el Servidor Central y Servidor de Management de la ASI (**Visto en el tópico 3**)
- 4- Acceso a las dependencias y repositorios para la instalación. (**Visto en el tópico 3**)
- 5- Tener permisos de navegación a internet del Server para su instalación.

1.1 Referencias

Links de documentación Oficial de X-Road

Link	Tema
https://nordic-institute.atlassian.net/wiki/spaces/XRDKB/pages/223903798/X-Road+v7.3.2+Release+Notes	Documentación Oficial Dependencias X-Road
https://github.com/nordic-institute/X-Road/blob/develop/doc/Manuals/ig-ss_x-road_v6_security_server_installation_guide_for_rhel.md	Instalación Security Server
https://github.com/nordic-institute/X-Road/blob/develop/doc/Manuals/ug-ss_x-road_6_security_server_user_guide.md	Configuración Plataforma SS

2 Requisitos de Recursos Security Server

SO: Red Hat Enterprise Linux (RHEL) versión 8

Red Hat Enterprise Linux release 8.7 o superior

CPU: 64-bit dual-core

Disco: 60 gb

Memoria RAM : 4 GB

Red: Tarjeta de interfaz de red de 100 Mbps

3 Habilitaciones del Security Server:

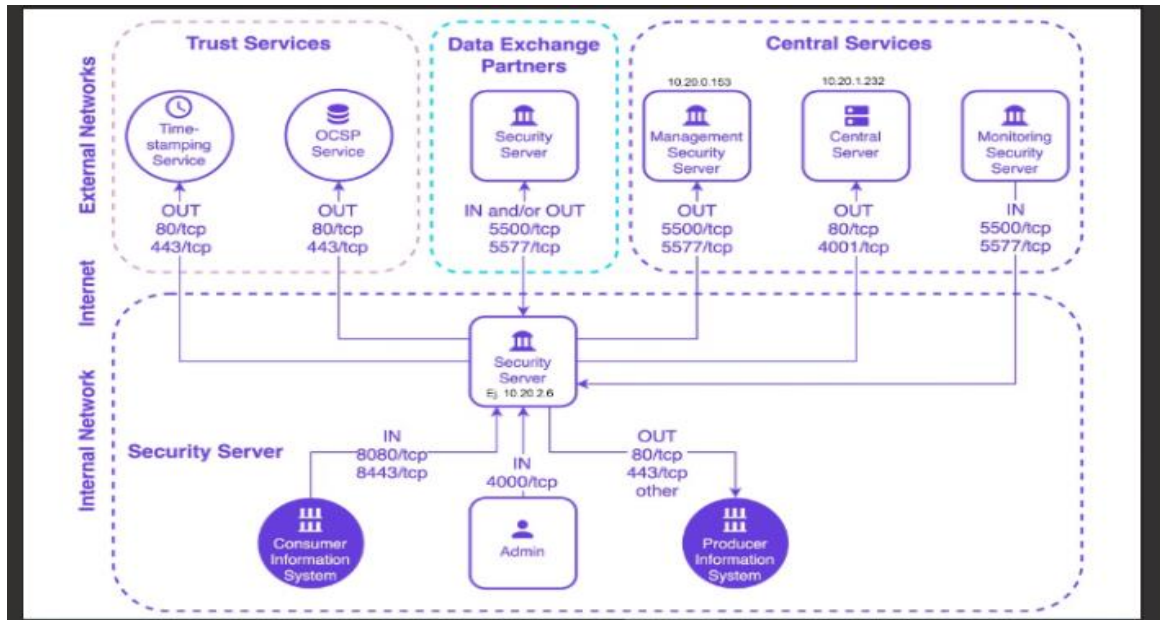
Consideraciones: tener conectividad al **Central Server**, al **Management Server** y a los **Security Server** con los cuales se intercambiará información por los puertos que se indican a continuación:

- Salida a internet para instalación
- TCP 5500 / 5577 Message Traffic - OCSP Responses ALL
- TCP 4001 / 80 Central server

Dominios del Sistema X-Road de ASI a continuación

Name Server	DNS	Environment
Central Server	xroad-central-qa.gcba.gob.ar	QA
Management Server	xroad-mss-qa.gcba.gob.ar	QA
Central Server	xroad-central-hml.gcba.gob.ar	Homologación
Management Server	xroad-mss-hml.gcba.gob.ar	Homologación
Central Server	xroad-central.buenosaires.gob.ar	Producción
Management Server	xroad-mss.buenosaires.gob.ar	Producción

Gráfico arquitectura X-Road



Dependencias y repositorios para la instalación del Security Server :

tsa.buenosaires.gob.ar	puerto:	443
http://ar.archive.ubuntu.com/ubuntu	puerto:	443
https://artifactory.niis.org/api/gpg/key/public	puerto:	443
https://artifactory.niis.org/xroad-release-deb	puerto:	443
https://adoptopenjdk.jfrog.io/adoptopenjdk/api/gpg/key/public	puerto:	443
https://adoptopenjdk.jfrog.io/adoptopenjdk/deb	puerto:	443
https://dl.fedoraproject.org	puerto:	332
https://pki.buenosaires.gob.ar/va	puerto:	443

4 instalación

4.1 Preparar OS

agregar linea en /etc/environment :

```
vim /etc/environment
```

agregar LC_ALL=en_US.UTF-8 y guardar el archivo

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

4.2 Preparar repositorios para instalación X-Road

```
RHEL_MAJOR_VERSION=$(source /etc/os-release;echo ${VERSION_ID%.*})
```

```
sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-\${RHEL\_MAJOR\_VERSION}.noarch.rpm
```

```
sudo yum-config-manager --add-repo https://artifactory.niis.org/xroad-release-rpm/rhel/\${RHEL\_MAJOR\_VERSION}/7.3.2/
```

```
sudo rpm --import https://artifactory.niis.org/api/gpg/key/public
```

4.3 Base de datos

La instalación de la base de datos puede realizarse tanto interna como externa. A continuación, se mencionan los detalles, ventajas y desventajas de cada opción.

Base de datos externalizada

Requisitos mínimos para tener la base de datos externalizada:

Postgresql server 13 +

Postgresql contrib (misma versión que server

Ventajas base de datos externalizada

Escalabilidad: El beneficio principal de tener la base de datos externalizada es la escalabilidad ya que la base de datos está vinculada a la capacidad de almacenamiento de la VM o host. Al necesitar más espacio es más seguro agregar espacio en disco.

Buenas prácticas: Es una costumbre de buenas prácticas tener separadas las plataformas de sus bases de datos para evitar posibles conflictos si falla uno u otro.

Mayor resiliencia: Si la aplicación o la VM fallan, la base de datos sigue siendo accesible desde otras ubicaciones o servidores, lo que mejora la disponibilidad del servicio.

Desventajas

Mayor complejidad de configuración inicial: Configurar una base de datos externalizada puede requerir más tiempo y esfuerzo, especialmente en términos de configuración de red y seguridad.

Posibles costos adicionales: Externalizar la base de datos puede implicar costos adicionales, como tarifas de servicio de alojamiento, ancho de banda de red y almacenamiento.

Dependencia de la conectividad de red: La base de datos externalizada depende de una conexión de red estable y de alta velocidad. Problemas de conectividad o interrupciones en la red pueden causar latencia en el acceso a los datos y aumentar el riesgo de tiempo de inactividad.

Base de datos interna (misma vm)

Ventajas base de datos interna

Rendimiento local: El acceso a la base de datos es más rápido debido a la menor latencia de red.

Facilidad de configuración: Al tener la base de datos en la misma máquina virtual (VM), la configuración y el mantenimiento pueden ser más simples.

Menor complejidad de administración: Gestionar una sola VM para el servidor de seguridad y la base de datos puede ser más sencillo y requerir menos recursos administrativos en comparación con la gestión de múltiples entornos separados.

Desventajas

Escalabilidad: Si el servidor de seguridad tiene mucho tráfico lo más probable es que se llene la base de datos y eso resulte en complicaciones ya que el host debe compartir los recursos entre el servidor y la base de datos.

También si en un futuro quisieran externalizar la base de datos si tienen más de un servidor de seguridad podría desembocar en problemas futuros debido a la nomenclatura de las bases de datos, si se externaliza en un cluster de base de datos solo un servidor podrá ser externalizado ya que no pueden repetirse los nombres, esquemas y usuarios administradores de las bases de datos. Esto es muy importante a tener en cuenta.

Mayor riesgo de fallos: Si la VM experimenta problemas de hardware o software, tanto la aplicación como la base de datos pueden verse afectadas, lo que aumenta el riesgo de tiempo de inactividad.

Menor resiliencia: Si la VM falla, tanto la aplicación como la base de datos pueden volverse inaccesibles hasta que se restaure la VM, lo que puede afectar la disponibilidad del servicio.

Mayor carga de mantenimiento: Administrar y mantener tanto la aplicación como la base de datos en la misma VM puede aumentar la carga de trabajo de administración y el riesgo de errores.

Instalación PostgreSQL en VM RHEL 8 :

Esta parte de la configuración se realiza en la VM o host donde estará albergada la base de datos.

Instalar el RPM del repositorio:

```
sudo dnf install -y
```

```
https://download.postgresql.org/pub/repos/yum/reporepms/EL-8-x86\_64/pgdg-redhat-repo-latest.noarch.rpm
```

Deshabilitar el módulo PostgreSQL integrado:

```
sudo dnf -qy module disable postgresql
```

Instalar PostgreSQL:

```
sudo dnf install -y postgresql13-server
```

```
sudo dnf install -y postgresql13-contrib
```

Opcionalmente inicializar la base de datos y habilitar el inicio automático:

```
sudo /usr/pgsql-13/bin/postgresql-13-setup initdb
```

```
sudo systemctl enable postgresql-13
```

```
sudo systemctl start postgresql-13
```

Habilitación de conexión

Una vez instalado y andando debemos habilitar **postgresql** para que acepte conexiones de "afuera".

Esto lo hacemos modificando los archivos `"/var/lib/pgsql/13/data/pg_hba.conf"` y `"/var/lib/pgsql/13/data/postgresql.conf"`

Hacemos:

```
vim "/var/lib/pgsql/data/pg_hba.conf"
```

y agregamos la línea:

```
host all all 0.0.0.0/0 md5
```

```
# TYPE      DATABASE         USER            ADDRESS          METHOD
# "local" is for Unix domain socket connections only
local      all              all             peer
# IPv4 local connections:
host       all              all             127.0.0.1/32     ident
# IPv6 local connections:
host       all              all             ::1/128          ident
# Allow replication connections from localhost, by a user with the
# replication privilege.
local      replication     all             peer
host       replication     all             127.0.0.1/32     ident
host       replication     all             ::1/128          ident
host       all              all             0.0.0.0/0        md5
```

Una vez modificado guardamos los cambios y modificamos

`"/var/lib/pgsql/12/data/postgresql.conf"` haciendo:

```
vim "/var/lib/pgsql/13/data/postgresql.conf"
```

Acá lo que tenemos que hacer es descomentar borrando el numeral y dejar
`listen_addresses = '*'`

```
# - Connection Settings -  
listen_addresses = '*' # what IP address(es) to listen on;  
                        # comma-separated list of addresses;  
                        # defaults to 'localhost'; use '*' for all  
                        # (change requires restart)  
#port = 5432           # (change requires restart)
```

Haciendo esto finalizamos el proceso que permite a la base de datos recibir conexiones externas.

Reiniciamos el servicio de postgresql:

```
systemctl restart postgresql
```

Configuración Usuario postgres

```
[devadmin@cloudformsadmin-x-road-securityserver1-dev-9186a3 ~]$ sudo su  
[root@cloudformsadmin-x-road-securityserver1-dev-9186a3 devadmin]# su - postgres  
Last login: Thu Nov  2 15:12:54 -03 2023 on pts/0  
[postgres@cloudformsadmin-x-road-securityserver1-dev-9186a3 ~]$ psql  
psql (10.23)  
Type "help" for help.  
  
postgres=#
```

una vez que estemos en este punto corremos el comando de sql:

```
ALTER USER postgres PASSWORD 'nueva_contraseña';
```

Esta contraseña que elegimos es la que nos va a solicitar cuando intentemos conectarnos la base de datos desde la VM del Security Server X-ROAD.

Una vez instalado configurar los puertos de ambos servidores.

Ambas Máquinas Virtuales (VMs) deben tener abierto el puerto 5432. Asegúrate de que **firewalld** está instalado y habilitado.

Si no está instalado, puedes instalarlo y habilitarlo con los siguientes comandos:

Habilitación de puertos - firewalld

```
sudo yum install firewalld  
sudo systemctl enable firewalld  
sudo systemctl start firewalld  
sudo firewall-cmd --zone=public --add-port=5432/tcp --permanent  
sudo firewall-cmd --reload  
sudo firewall-cmd --list-ports
```

Lado XROAD – Configuración bases de datos (externa).

Esta parte de la configuración se realiza en la VM donde se va a instalar el servidor de seguridad.

```
sudo yum install xroad-database-remote
```

```
sudo touch /etc/xroad.properties
```

```
sudo chown root:root /etc/xroad.properties
```

```
sudo chmod 600 /etc/xroad.properties
```

Agregar las credenciales sudo de la BD en xroad.properties:

```
Vim /etc/xroad.properties
```

```
postgres.connection.password = <database superuser password>
postgres.connection.user = <database superuser name, postgres by default>
```

```
sudo touch /etc/xroad/db.properties
```

```
sudo chmod 0640 /etc/xroad/db.properties
```

```
sudo chown xroad:xroad /etc/xroad/db.properties
```

```
serverconf.hibernate.jdbc.use_streams_for_binary = true

serverconf.hibernate.dialect = ee.ria.xroad.common.db.CustomPostgreSQLDialect

serverconf.hibernate.connection.driver_class = org.postgresql.Driver

serverconf.hibernate.connection.url = jdbc:postgresql://10.9.11.105:5432/serverconf_dev02 (IP BASE DE DATOS :
PUERTO / NOMBRE DE BASE DE DATOS SERVERCONF)

serverconf.hibernate.hikari.dataSource.currentSchema = serverconf_dev02,public (NOMBRE DEL
ESQUEMASERVERCONF,public)

serverconf.hibernate.connection.username = serverconf_dev02 (NOMBRE SERVERCONF_DBADMIN)

serverconf.hibernate.connection.password = s3cr3t (PASS SERVERCONF_DBADMIN)

messagelog.hibernate.jdbc.use_streams_for_binary = true

messagelog.hibernate.connection.driver_class = org.postgresql.Driver

messagelog.hibernate.connection.url = jdbc:postgresql://10.9.11.105:5432/messagelog_dev02 (IP BASE DE DATOS :
PUERTO / NOMBRE DE BASE DE DATOS MESSAGELOG)

messagelog.hibernate.hikari.dataSource.currentSchema = messagelog_dev02,public (NOMBRE DEL ESQUEMA
MESSAGELOG,public)

messagelog.hibernate.connection.username = messagelog_dev02 (NOMBRE MESSAGELOG_DBADMIN)

messagelog.hibernate.connection.password = s3cr3t (PASS MESSAGELOG_DBADMIN)
```

```
op-monitor.hibernate.jdbc.use_streams_for_binary = true

op-monitor.hibernate.connection.driver_class = org.postgresql.Driver

op-monitor.hibernate.connection.url = jdbc:postgresql://10.9.11.105:5432/opmonitor_dev02 (IP BASE DE DATOS :
PUERTO / NOMBRE DE BASE DE DATOS OPMONITOR)

op-monitor.hibernate.hikari.dataSource.currentSchema = opmonitor_dev02,public (NOMBRE DEL ESQUEMA
OPMONITOR,public)

op-monitor.hibernate.connection.username = opmonitor_dev02 (NOMBRE OPMONITOR_DBADMIN)

op-monitor.hibernate.connection.password = s3cr3t (PASS OPMONITOR_DBADMIN)
```

```
serverconf.hibernate.jdbc.use_streams_for_binary = true
serverconf.hibernate.dialect = ee.ria.xroad.common.db.CustomPostgreSQLDialect
serverconf.hibernate.connection.driver_class = org.postgresql.Driver
serverconf.hibernate.connection.url = jdbc:postgresql://10.9.11.105:5432/serverconf_dev02
serverconf.hibernate.hikari.dataSource.currentSchema = serverconf_dev02,public
serverconf.hibernate.connection.username = serverconf_dev02
serverconf.hibernate.connection.password = s3cr3t
messagelog.hibernate.jdbc.use_streams_for_binary = true
messagelog.hibernate.connection.driver_class = org.postgresql.Driver
messagelog.hibernate.connection.url = jdbc:postgresql://10.9.11.105:5432/messagelog_dev02
messagelog.hibernate.hikari.dataSource.currentSchema = messagelog_dev02,public
messagelog.hibernate.connection.username = messagelog_dev02
messagelog.hibernate.connection.password = s3cr3t
op-monitor.hibernate.jdbc.use_streams_for_binary = true
op-monitor.hibernate.connection.driver_class = org.postgresql.Driver
op-monitor.hibernate.connection.url = jdbc:postgresql://10.9.11.105:5432/opmonitor_dev02
op-monitor.hibernate.hikari.dataSource.currentSchema = opmonitor_dev02,public
op-monitor.hibernate.connection.username = opmonitor_dev02
op-monitor.hibernate.connection.password = s3cr3t
~
~
~
```

(ejemplo de archivo /etc/xroad/db.properties)

4.4 Instalación Security Server

```
sudo yum install xroad-securityserver
```

```
sudo xroad-add-admin-user <username> (usuario para la plataforma)
```

```
sudo yum install xroad-addon-opmonitoring
```

```
sudo yum install xroad-autologin
```

4.5 Configurar archivo Local.ini para balanceo de cargas

De la siguiente manera definiremos puertos para que pasen por el 80 y 443.

Si no colocamos nada por defecto nos utilizará el 8080 y 8443.

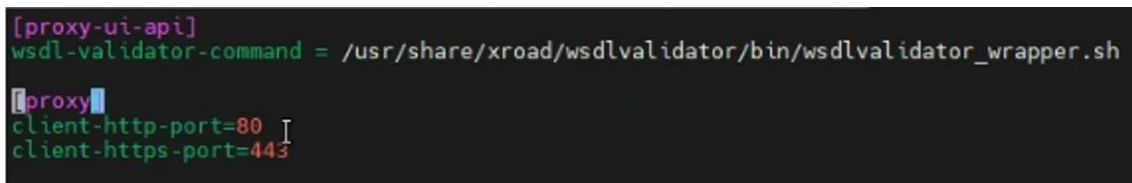
Necesitamos ir al siguiente directorio y modificar el archivo de texto

- **cd /etc/xroad/conf.d**
- **vim local.ini** (puede hacerse con otro editor de texto)
- ingresar la siguiente declaración como se muestra en la imagen :

[proxy]

client-http-port=80

client-https-port=443



```
[proxy-ui-api]
wsdl-validator-command = /usr/share/xroad/wsdlvalidator/bin/wsdlvalidator_wrapper.sh

[proxy]
client-http-port=80
client-https-port=443
```

4.6 Iniciar Security Server

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

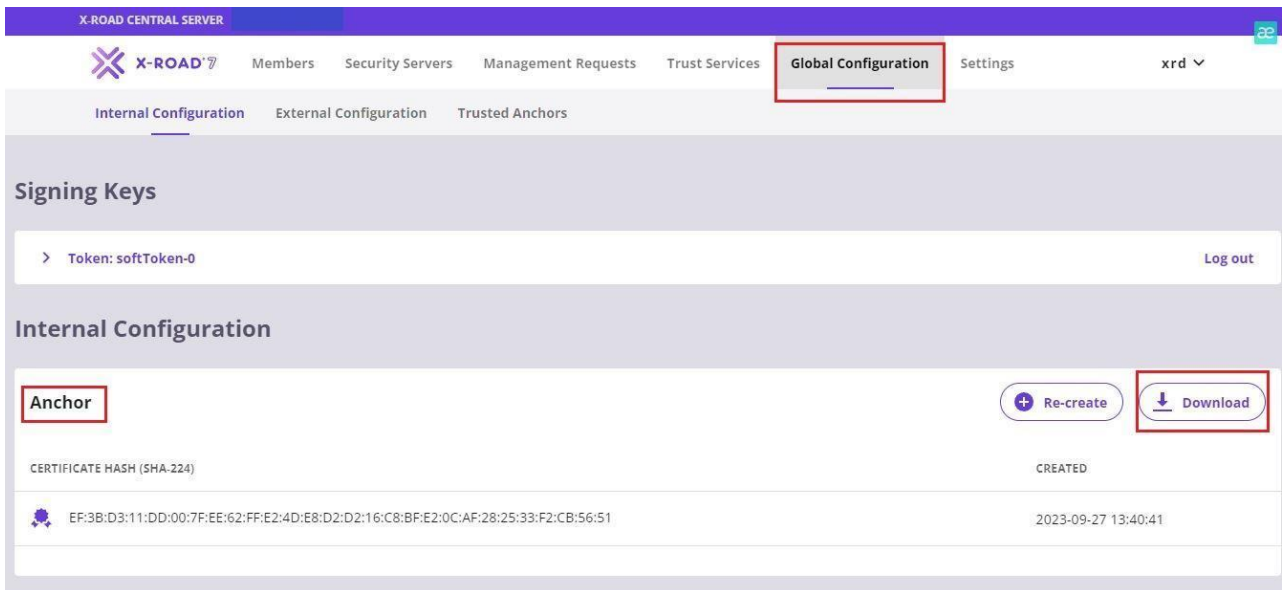
4.7 Check post-instalación de servicios X-Road

```
sudo systemctl list-units "xroad-*
```

5 Consideraciones al finalizar la instalación:

Una vez finalizada la instalación del SS:

- Probar Ingreso a la Plataforma X-Road mediante la IP del server y el puerto 4000 | <https://SECURITYSERVER:4000>
- Descargar **Anchor File** desde servidor central, este es requerido para empezar a configurar la plataforma del Security Server una vez instalado para que sea reconocido por el Central Server.
- Para el caso de los Externos, pedir el **Anchor File** a la ASI. Imagen a continuación.



The screenshot shows the X-Road Central Server web interface. The top navigation bar includes 'X-ROAD CENTRAL SERVER', 'Members', 'Security Servers', 'Management Requests', 'Trust Services', 'Global Configuration' (highlighted with a red box), and 'Settings'. Below this, the 'Internal Configuration' tab is selected. The main content area is titled 'Signing Keys' and shows a token 'softToken-0' with a 'Log out' button. Under 'Internal Configuration', there is a table with one entry. The 'Anchor' column has a red box around the word 'Anchor'. The 'Re-create' and 'Download' buttons are also highlighted with red boxes. The table shows a certificate hash and a creation date.

CERTIFICATE HASH (SHA-224)	CREATED
EF:3B:D3:11:DD:00:7F:EE:62:FF:E2:4D:E8:D2:D2:16:C8:BF:E2:0C:AF:28:25:33:F2:CB:56:51	2023-09-27 13:40:41

Primer ingreso

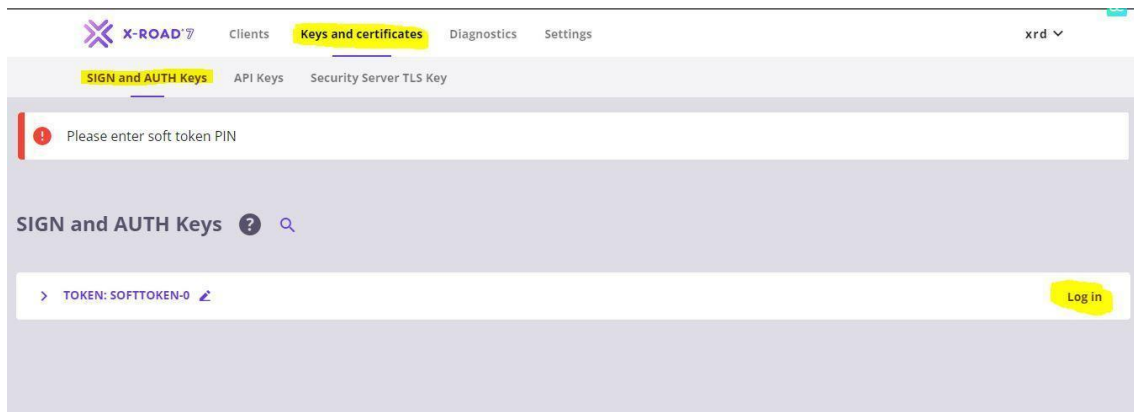
Ingresar:

- **anchor file** (se descarga desde Server Central - Será provisto por el GCBA).
- **member class** (Consultar cual seleccionar, actualmente es GOB - Será provisto por el GCBA).
- **member code** (Mismo número de miembro creado en Server Central para que lo reconozca - Será provisto por el GCBA).
- **server code** (Identificador Security Server – Será provisto por el GCBA).
- **PIN** (Guardar bien este número porque no se puede cambiar).

Al Terminar la Configuración inicial

Aparece el error de que tenemos que ingresar PIN para inicializar el server. Esto lo realizamos desde **Keys and Certificates** al clickear en **Login**, o haciendo Click directamente sobre el error.

Imagen a continuación:



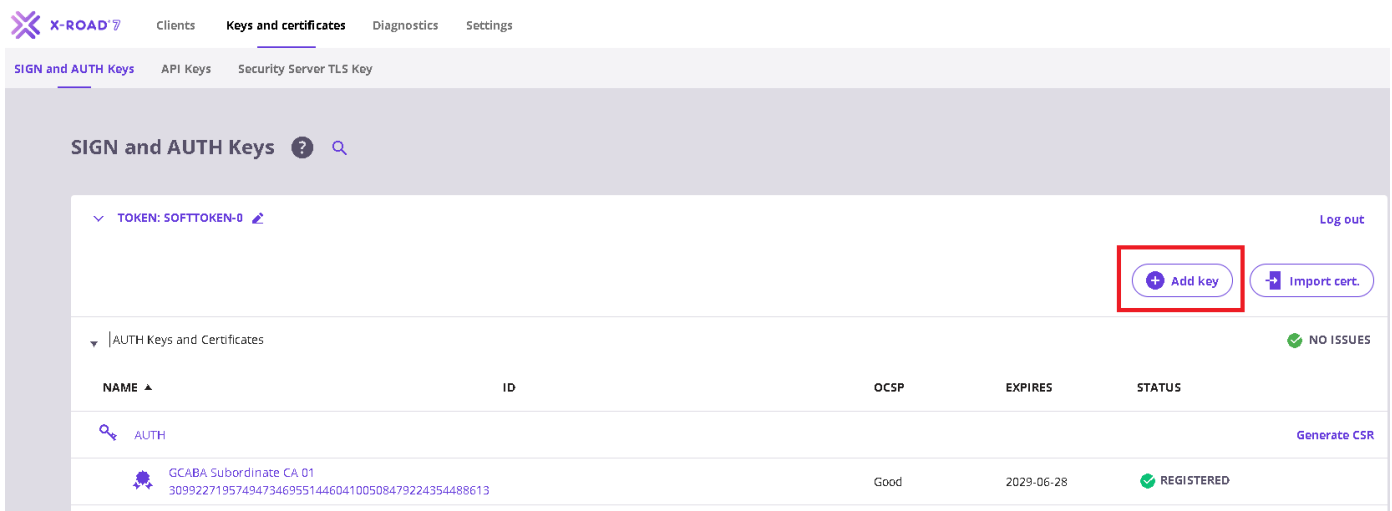
Configurar Timestamp en el SS (**Settings -> System Parameters** - seleccionar el timestamp que está configurado en Server Central).

Certificados

Una vez de habernos logeados en la sección **Keys and Certificates** de la plataforma del Security Server, es necesario generar las Keys de **SIGN** y **AUTH** para poder generar los **CSR** de tipo **DER** y que sean firmados por seguridad informática y sean aceptados por X-Road.

- crear clave AUTH (seleccionar **DER**), generar CSR
- crear clave SIGN (seleccionar **DER**), generar CSR

Se hace para ambos casos desde el siguiente lugar con el Botón **Add Key**.



The screenshot shows the X-Road Security Server interface. The top navigation bar includes 'Clients', 'Keys and certificates', 'Diagnostics', and 'Settings'. The 'Keys and certificates' section is active, showing 'SIGN and AUTH Keys'. Below this, there are tabs for 'SIGN and AUTH Keys', 'API Keys', and 'Security Server TLS Key'. The 'SIGN and AUTH Keys' tab is selected, displaying a table of keys. The table has columns for 'NAME', 'ID', 'OCSP', 'EXPIRES', and 'STATUS'. A red box highlights the 'Add key' button in the top right corner of the table area. The table contains one entry for 'GCABA Subordinate CA 01' with a status of 'REGISTERED'.

NAME	ID	OCSP	EXPIRES	STATUS
GCABA Subordinate CA 01	309922719574947346955144604100508479224354488613	Good	2029-06-28	REGISTERED

Key AUTHENTICATION

El campo **Key Label** se debe completar con **AUTH** si a continuación seleccionamos **AUTHENTICATION** en **CSR details**.

La segunda Key debe llamarse **SIGN** para luego seleccionar **SIGNING** en **CSR details**

Imagen a continuación

Add key

1

2

3

Key details

CSR details

Generate CSR

Key Label
You can define a label for the newly created SIGN key (not mandatory)

Cancel

Next

Add key

✓

2

3

Key details

CSR details

Generate CSR

Usage
Usage policy of the certificate: signing messages or authenticating Security Server.

Certification Service
Certification Authority (CA) that will issue the certificate.

CSR Format
Format of the certificate signing request according to the CA's requirements.

Cancel

Previous

Continue

Al clicar **Continue**, ya podremos generar los request del Certificado en CSR para que la firme seguridad informática.

Key SIGNING

Add key

1

2

3

Key details

CSR details

Generate CSR

Key Label
You can define a label for the newly created SIGN key (not mandatory)

Cancel

Next

Add key

✓

2

3

Key details

CSR details

Generate CSR

Usage
Usage policy of the certificate: signing messages or authenticating Security Server.

Client
X-Road member the certificate will be issued for.

Certification Service
Certification Authority (CA) that will issue the certificate.

CSR Format
Format of the certificate signing request according to the CA's requirements.

Cancel

Previous

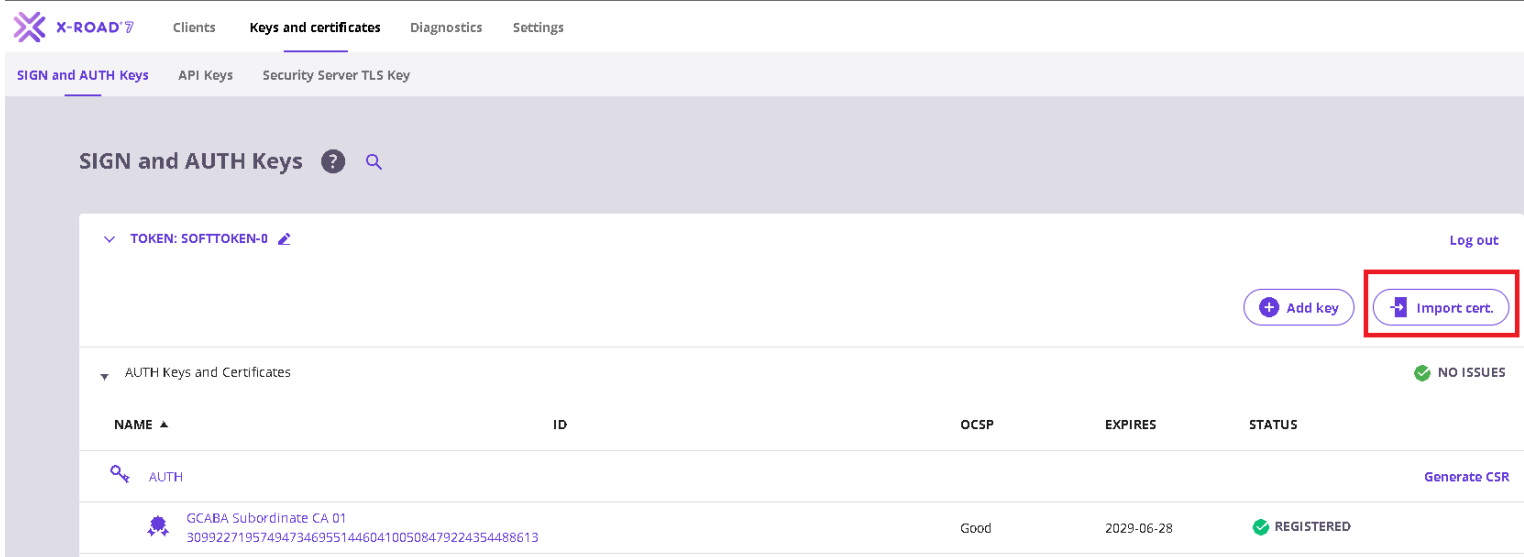
Continue

Al clicar **Continue**, ya podremos generar los request del Certificado en CSR para que la firme seguridad informática.

Estos CSR deben ser enviados a Seguridad Informática de ASI para su posterior firma.

Una vez firmado se enviará al mail del solicitante de este Security Server.

- Una vez recibidos los CSR firmados por la ASI, cargarlos en la plataforma en el apartado de **Key and Certificates > SIGN and AUTH Keys** y deben ser importados con el botón **Import Cert.** (hay que subir los .PEM)



SIGN and AUTH Keys ? 🔍

TOKEN: SOFTOKEN-0 🔗 Log out

+ Add key Import cert.

AUTH Keys and Certificates ✓ NO ISSUES

NAME ▲	ID	OCSP	EXPIRES	STATUS
 AUTH Generate CSR				
 GCABA Subordinate CA 01 309922719574947346955144604100508479224354488613		Good	2029-06-28	✓ REGISTERED

- Una vez aceptados por X-Road , Entrar a los certificados y activarlos haciendo clic sobre el nombre para ingresar a los detalles.
- Nos va a dar la posibilidad de **“Register”** al lado del certificado de AUTH o SIGN y colocar la IP o DNS del Security Server que estamos configurando.
- En el servidor central habilitar el certificado de authentication en **Management Request**.

A menos que esté activada la aprobación automática. (tarda 5 min aprox en impactar)

