

Diplomado en Interoperabilidad de Sistemas de Información mediante X-Road

Sección 2.3

Escenario Básico de Interoperabilidad

4

Guía de Configuración de X-Road

Servidor Central

(Government)

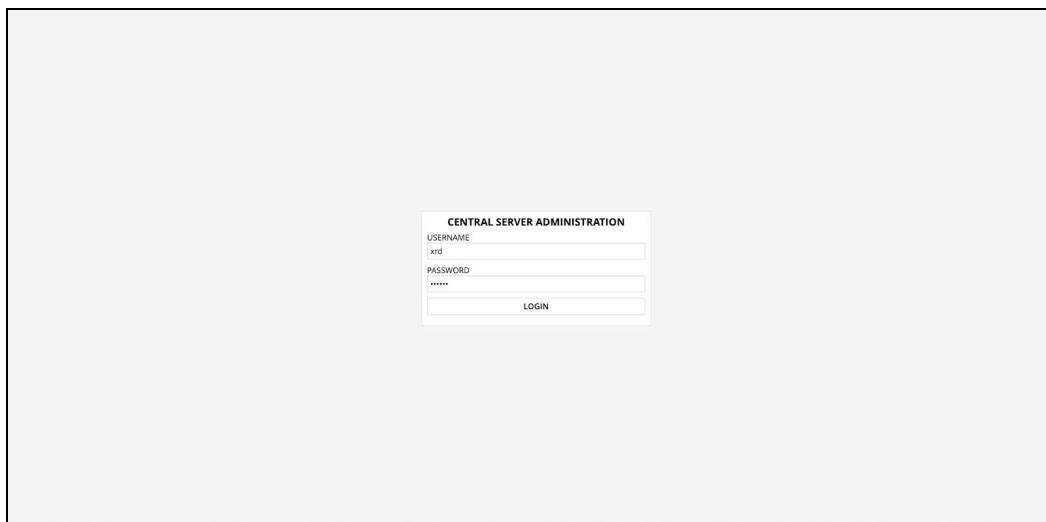
Antes de interactuar con el ecosistema de X-Road, es necesario establecer una configuración preliminar que permita interoperar entre las diferentes entidades del sistema, específicamente en uno de sus componentes, el servidor central. Para este proceso es necesario parametrizar un conjunto de certificados y llaves de seguridad con el fin brindar una comunicación a través de protocolos estándares y seguros.

1. Verificar que todos los contenedores Docker se encuentren en ejecución.
2. Acceder al panel de configuración del **Servidor Central**:

«IP del contenedor»:4000

Username: xrd

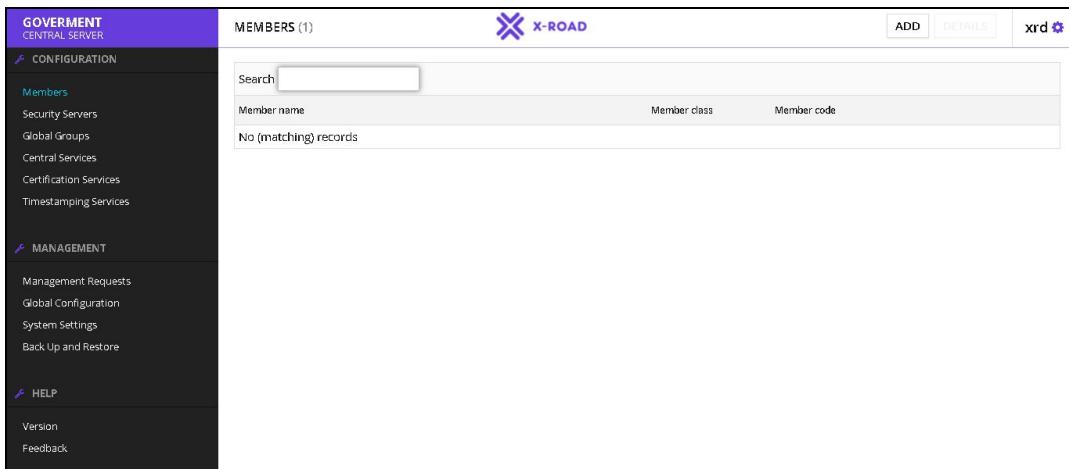
Password: secret



A large rectangular placeholder box intended for displaying a screenshot of the 'CENTRAL SERVER ADMINISTRATION' login page. The page features a header, two input fields for 'USERNAME' and 'PASSWORD', and a 'LOGIN' button.

CENTRAL SERVER ADMINISTRATION	
USERNAME	xrd
PASSWORD	*****
LOGIN	

3. Al ingresar, aparecerá la siguiente pantalla:



4. Es necesario verificar las direcciones IP de los contenedores que están desplegados, para ingresar la dirección IP en un paso posterior. Esto se puede hacer inicialmente ejecutando el comando que lista los contenedores con su respectiva información:

```
sudo docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED
4482ddea2f01	niis/xroad-security-server:bionic-6.24.0	"/root/entrypoint.sh"	5 minutes ago
9a7d81bd37a7	postgres	"docker-entrypoint.s..."	5 minutes ago
2ef2deeac8cf	niis/xroad-central-server:bionic-6.24.0	"/root/entrypoint.sh"	5 minutes ago
ubuntu_my-security-server-cluster_1	0.0.0.0:5432->5432/tcp		
ubuntu_my-security-server-cluster_1	0.0.0.0:4003->80/tcp, 0.0.0.0:4002->4000/tcp		

5. Con el siguiente comando, es posible inspeccionar o detallar la información del contenedor.

```
sudo docker inspect <<ID_CONTENEDOR>>
```

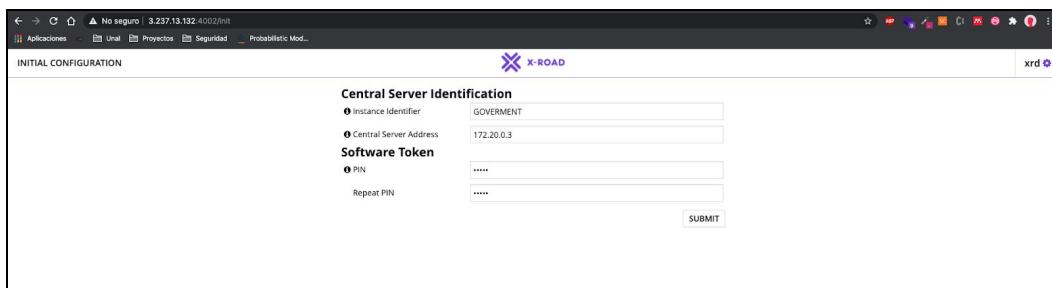
```
[{"Id": "2ef2deeac8cf2f7e3961ee1dcdba59c6f1dc0ab3701a932e12dfe2962da7a808", "Created": "2020-10-14T23:16:57.791799Z", "Path": "/root/entrypoint.sh", "Args": [], "State": { "Status": "running", "Running": true, "Paused": false, "Restarting": false, "OOMKilled": false, "Dead": false, "Pid": 197149, "ExitCode": 0, "Error": "", "StartedAt": "2020-10-14T23:17:00.980779205Z", "FinishedAt": "0001-01-01T00:00:00Z" }}
```

6. La terminal imprimirá toda la información correspondiente al contenedor específico. En una de estas propiedades se encuentra la dirección IP del contenedor (**IPAddress**), que está resaltada dentro del recuadro rojo en la siguiente imagen.

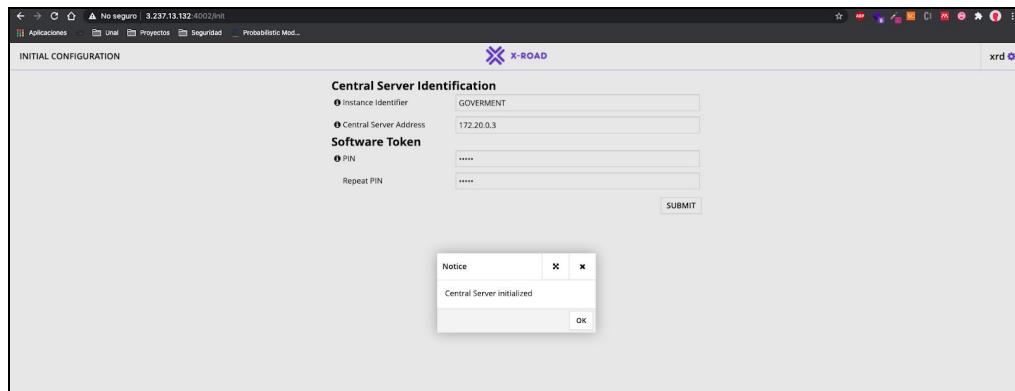
```
"Aliases": [
    "central-server",
    "2ef2deac8cf"
],
"NetworkID": "cd030c8488f0258a7bf9efabec2374e1e41c3c782977056310d3377eecdd4807",
"EndpointID": "0dbca5dc9e2feec2b65b28a6af7b4b8a846a6e6e17e7654602564c77c0b0bfde",
"Gateway": "172.20.0.1",
"IPAddress": "172.20.0.3",
"IPPrefixLen": 16,
"IPv6Gateway": "",
"GlobalIPv6Address": "",
"GlobalIPv6PrefixLen": 0,
"MacAddress": "02:42:ac:14:00:03",
"DriverOpts": null
```

7. Posterior al paso anterior, regresar a la pantalla de configuración inicial del servidor central, donde se deben poner los siguientes campos:

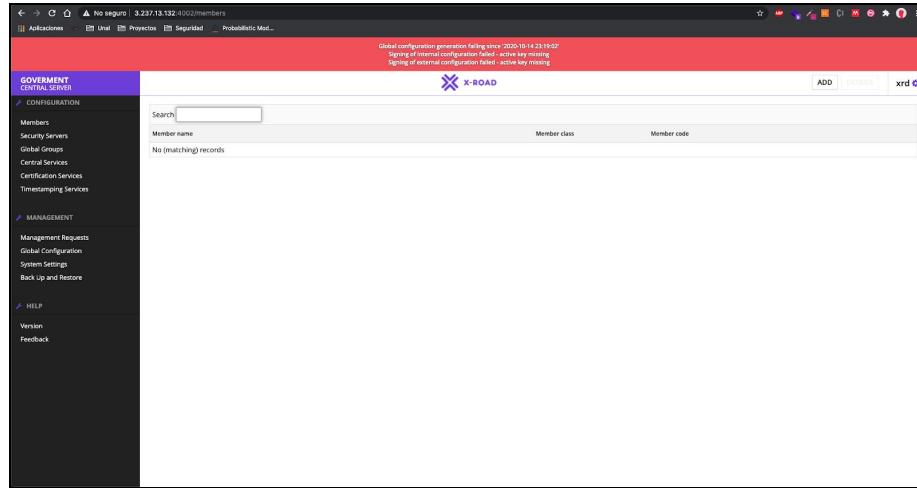
Instance Identifier: GOVERNMENT
Central Server Address: IP del contenedor
PIN: 12345
Repeat PIN: 12345



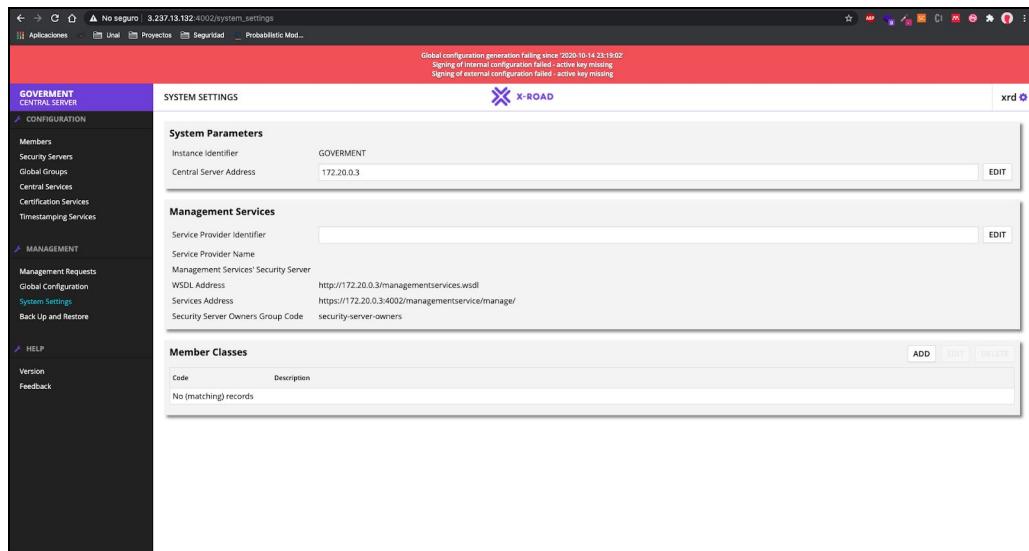
8. Al hacer clic en el botón **Submit**, aparecerá un mensaje de confirmación, donde se indica que el Servidor Central ha sido instalado correctamente.



- A continuación, aparecerá una pantalla similar a la que se muestra en la siguiente imagen, donde en la parte superior se muestran unos mensajes de alerta que se eliminan hasta que algunos pasos de la configuración hayan sido completados.



- Dirigirse a la opción *System Settings*:

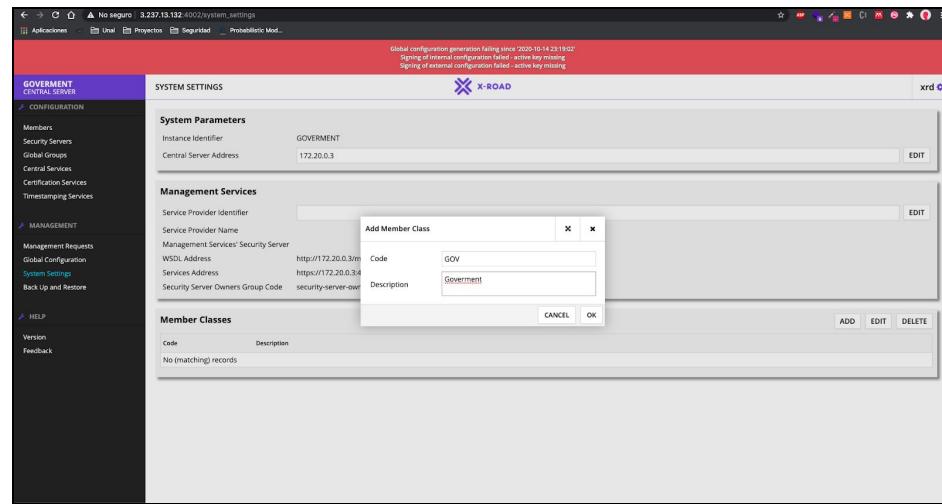


- En la sección *Member Classes*, hacer clic sobre el botón *Add* agregar un miembro de las clases.

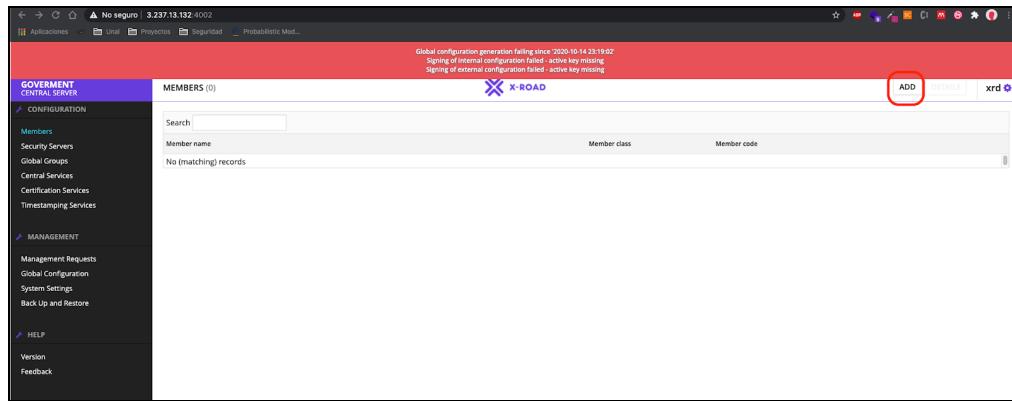


- En la pestaña que aparecerá, agregar un *Member Class*:

Code: GOV
Description: Government

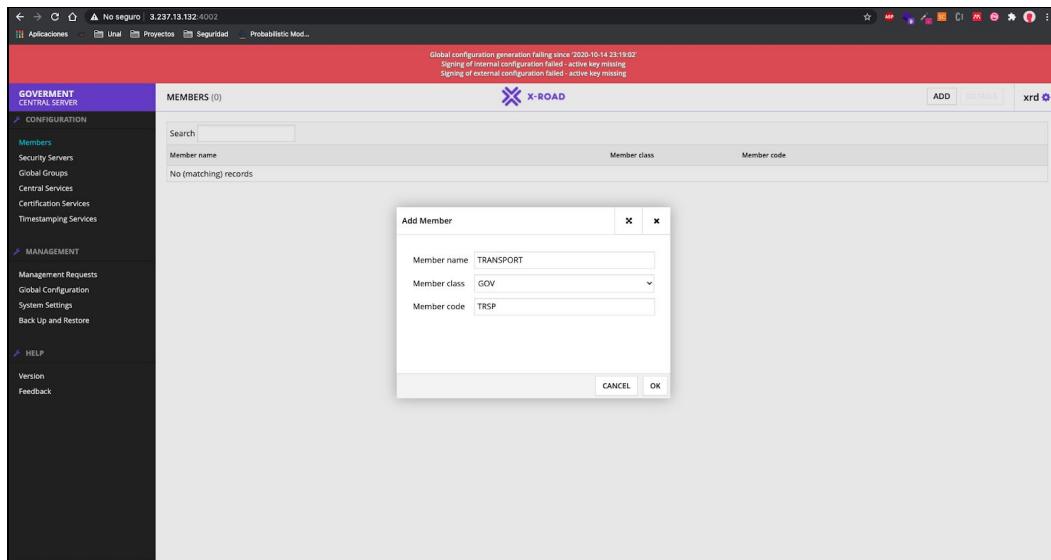


13. Ir a la opción **Members** para agregar uno de los miembros que va a tener acceso e integración dentro del sistema. Hacer clic en el botón **Add**.

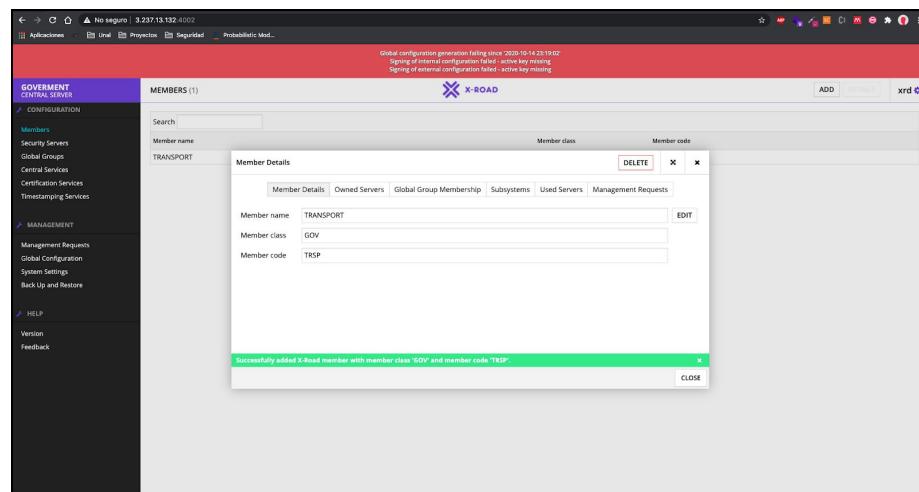


14. Especificar los siguientes datos del miembro:

Member name: Transport
Member class: GOV
Member code: TRSP

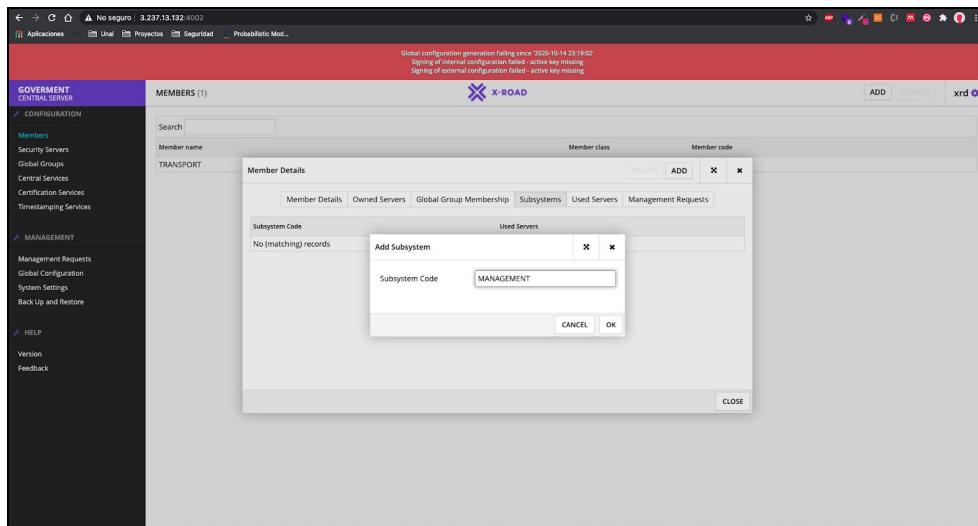


15. Luego de hacer clic en el botón OK, se mostrará un mensaje de confirmación en verde anunciando la creación exitosa del miembro.



16. Ingresar a la pestaña *Subsystems* para agregar el código del subsistema:

Subsystem Code: MANAGEMENT

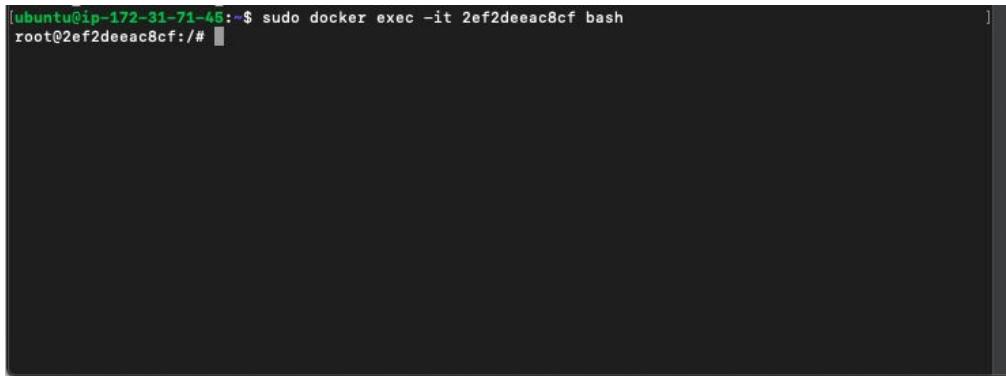


17. Después de realizar la configuración de los miembros o las entidades encargadas de interactuar con el sistema, es necesario realizar la configuración de los certificados que harán parte del ecosistema X-Road.

18. Ubicarse en el contenedor del servidor central a través del comando:

```
sudo docker exec -it <<ID CONTENEDOR>> bash
```

```
ubuntu@ip-172-31-71-45:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS
NAMES
4482dde2f01        niis/xroad-security-server:bionic-6.24.0   "/root/entrypoint.sh"   21 minutes ago
                   Up 20 minutes          443/tcp, 5500/tcp, 5577/tcp, 0.0.0.0:4000->4000/tcp, 0.0.0.0:4001->80/tcp
ubuntu_my-security-server-cluster_1
9a7d81bd37a7        postgres             "docker-entrypoint.s..."   21 minutes ago
                   Up 21 minutes          0.0.0.0:5432->5432/tcp
postgres_container
2ef2deecac8cf       niis/xroad-central-server:bionic-6.24.0    "/root/entrypoint.sh"   21 minutes ago
                   Up 20 minutes          0.0.0.0:4003->80/tcp, 0.0.0.0:4002->4000/tcp
ubuntu_central-server_1
ubuntu@ip-172-31-71-45:~$
```

A screenshot of a terminal window with a black background. At the top left, there is some very small, illegible text. The rest of the window is entirely black, indicating no output or a blank screen.

19. Una vez ubicado en la carpeta, hay que dirigirse a la siguiente ruta **/home/ca/CA/certs**, donde se encontrarán los certificados que permitirán validar parte del proceso:

```
cd /home/ca/CA/certs
```

20. Para confirmar la existencia de los certificados, es necesario listar los archivos en la carpeta mediante el comando:

```
ls
```

A screenshot of a terminal window showing the output of the 'ls' command. The terminal title is 'Descargas — root@2ef2deeac8cf:/home/ca/CA/certs — ssh + sudo — 102x32'. The command 'ls' was run, and it returned three files: 'ca.cert.pem', 'ocsp.cert.pem', and 'tsa.cert.pem'. The terminal has a dark background with light-colored text.

21. Cuando se compruebe que estos certificados se encuentran allí (que se generan por defecto una vez se cuenta con el contenedor), es necesario descargar los certificados a la máquina local con el fin de utilizarlos en pasos posteriores. Este proceso se puede realizar copiando el archivo ubicado en el contenedor:

```
sudo docker cp <>IDContenedor>>:/home/ca/CA/certs/archivoACopiar .
```

Especificamente, para los tres certificados, ejecutar:

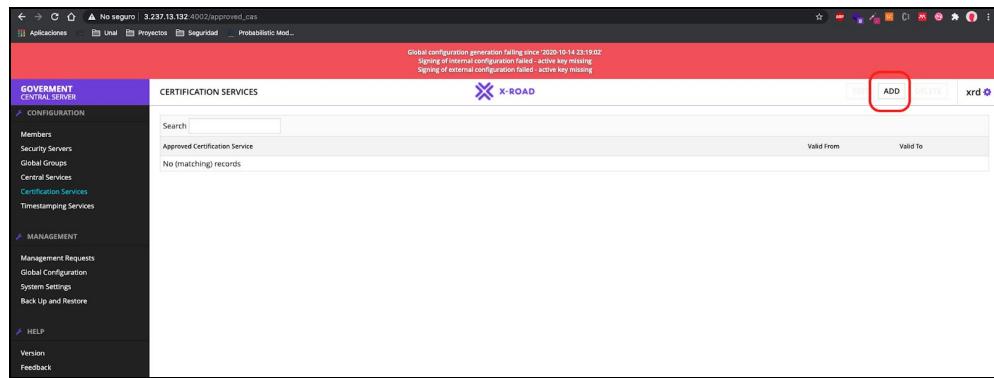
- sudo docker cp <>ID Contenedor>>:/home/ca/CA/certs/ca.cert.pem .
- sudo docker cp <>ID Contenedor>>:/home/ca/CA/certs/ocsp.cert.pem .
- sudo docker cp <>ID Contenedor>>:/home/ca/CA/certs/tsa.cert.pem .

22. Después de ejecutar estos comandos, es necesario revisar que los archivos estén ubicados en la máquina local a través del comando:

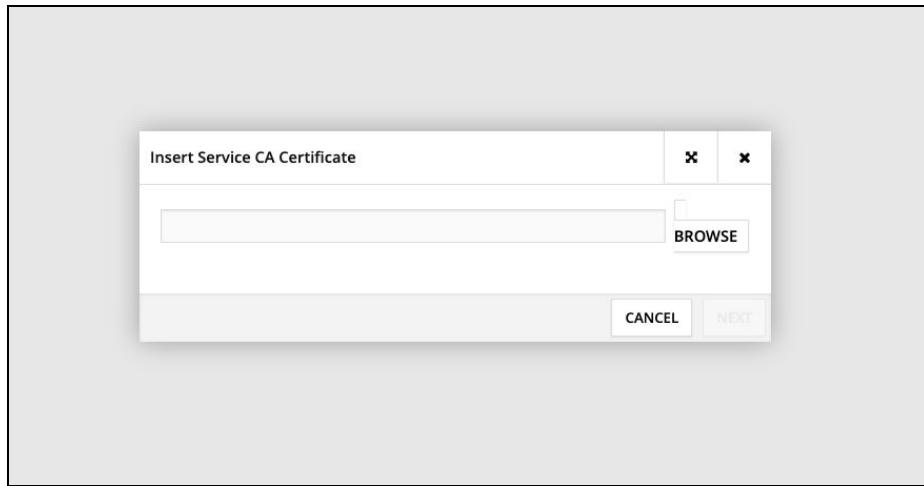
```
ls
```

```
[ubuntu@ip-172-31-71-45:~$ ls  
ca.cert.pem docker-compose.yml ocsp.cert.pem tsa.cert.pem
```

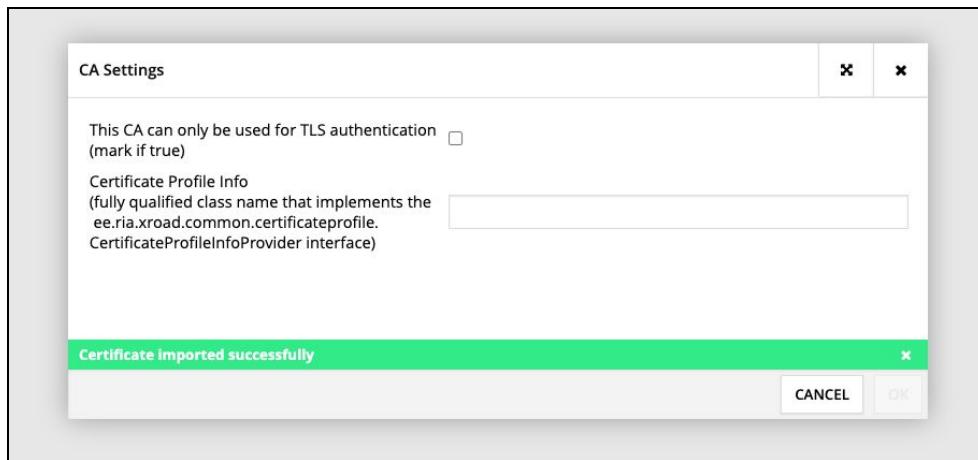
23. Después de realizar esta verificación, ir a la interfaz gráfica de los certificados con el fin de agregarlos como parte de la configuración del servidor central.
24. En la interfaz, ir al enlace “Certification Services” y agregar el certificado **ca.cert.pem** con el botón “Add”.



25. Aparecerá una ventana donde se podrá agregar el certificado **CA** que se descargó anteriormente, específicamente el certificado *ca.cert.pem*.

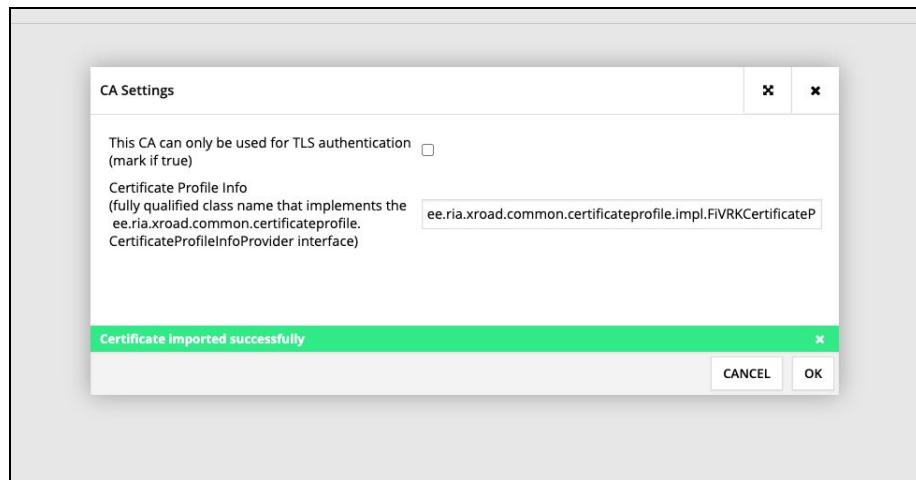


26. Después de cargar el certificado aparecerá la siguiente pantalla, donde aparecerá una ventana con el título de “CA Settings” con un mensaje en color verde confirmando el cargue exitoso del certificado.

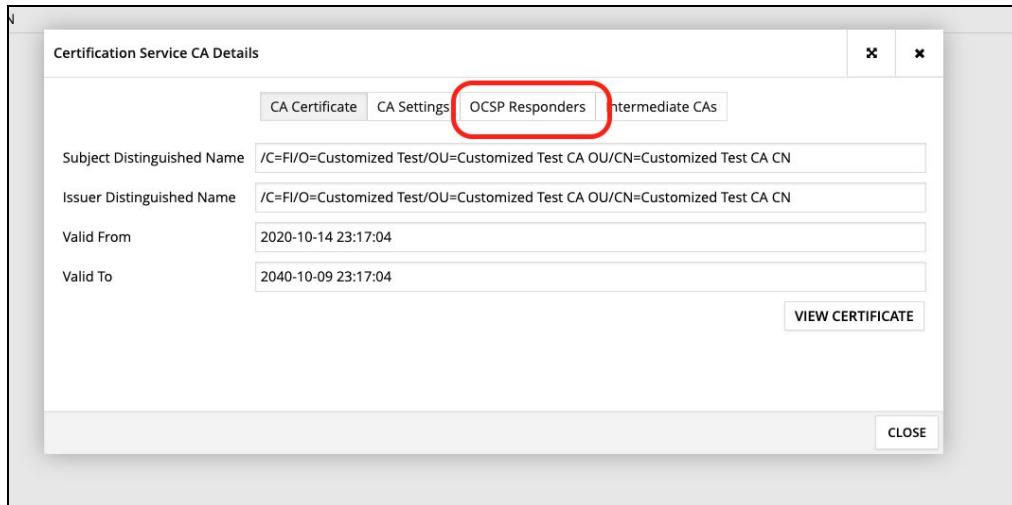


27. Allí también será necesario agregar una ruta preestablecida por el servidor central en el campo "Certificate Profile Info", y la opción "TLS authentication" se deberá dejar tal como esté.

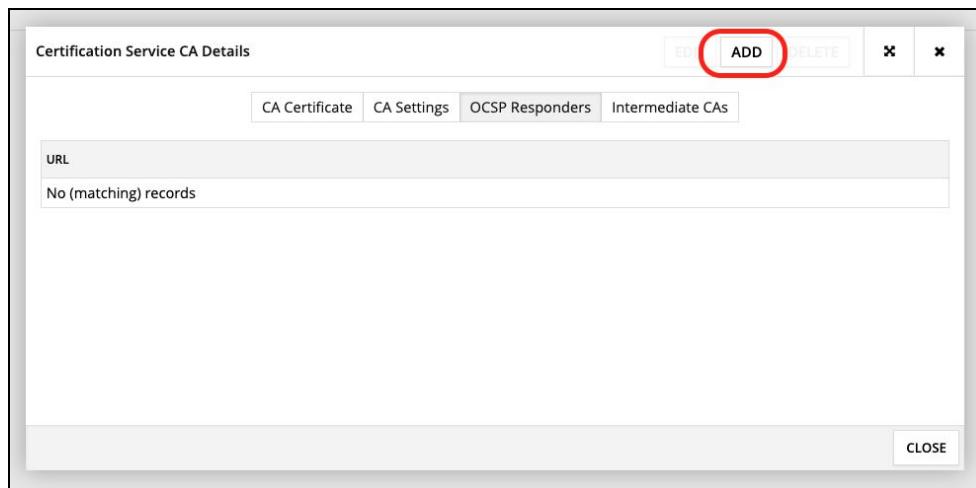
`ee.ria.xroad.common.certificateprofile.impl.FiVRKCertificateProfileInfoProvider`



28. Luego de haber agregado la ruta, se desplegará una ventana con los detalles del certificado creado, allí es necesario ir a la pestaña *OCSP Responders*.

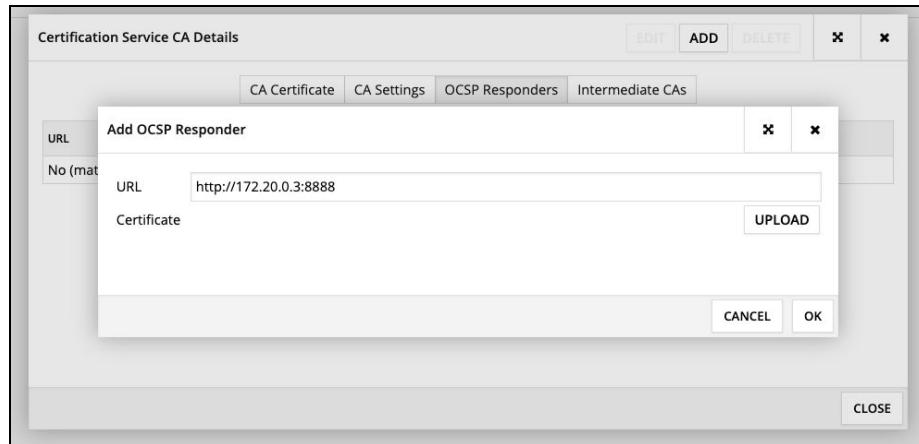


29. Después de llegar a esa pestaña, hacer clic sobre el botón *Add* para agregar el protocolo de vigencia del certificado (OCSP Responder) agregado anteriormente:

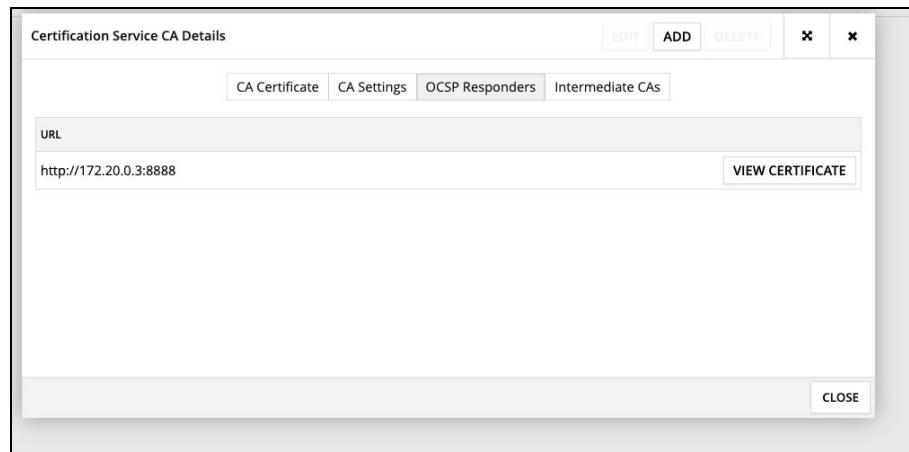


30. En la pestaña que aparecerá, agregar la especificación del *Responder*, donde se deberá agregar la URL del servidor OCSP, donde irá la IP del Contendor de Docker + el puerto, que generalmente se despliega sobre el puerto 8888.

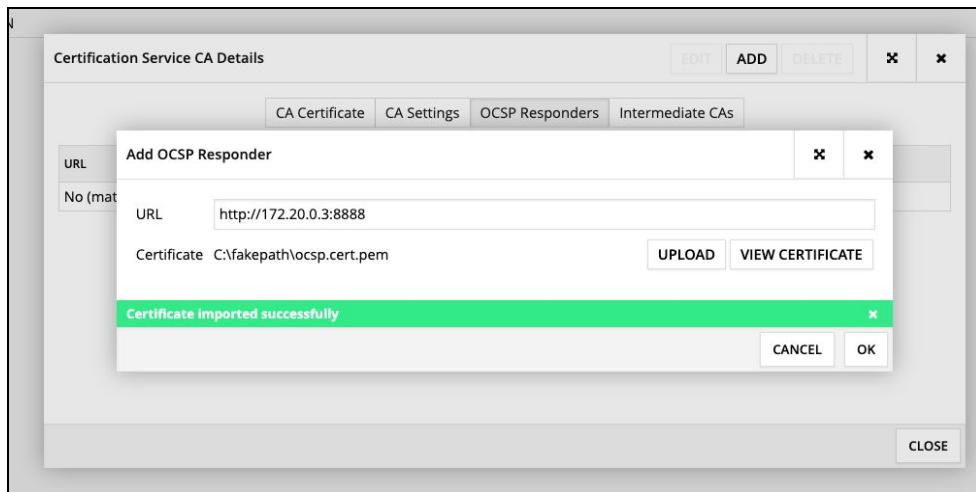
URL: <IP DOCKER>:8888



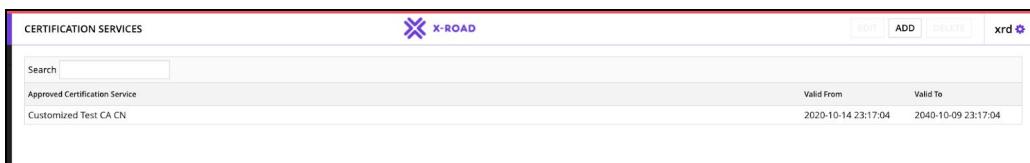
31. Cargar el certificado *ocsp.cert.pem* haciendo clic sobre el *View Certificate*, allí se desplegará una ventana que permitirá cargar el archivo desde el computador.



32. Cuando el certificado haya sido cargado exitosamente, aparecerá un mensaje de confirmación indicando el éxito de la acción.

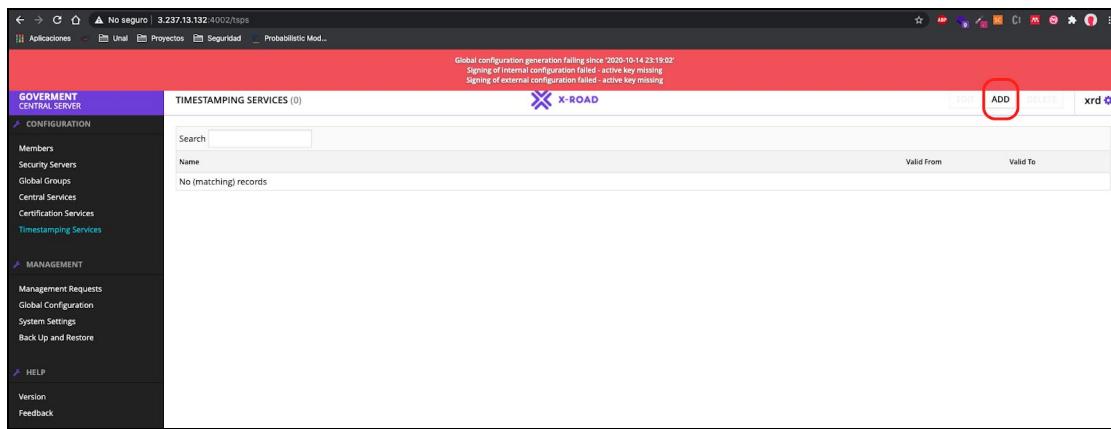


33. Después del mensaje de confirmación, se observará en la opción *Certification Services*, que el certificado ha sido agregado exitosamente.



Timestamping Services

34. Ahora será necesario agregar los servicios de Timestamping que permitirán tener un mayor control de la integración del sistema.



35. Ir a la opción *Timestamping Services*, en el botón Add, allí se deberá agregar la URL que es será la IP del Contenedor + el puerto 8899.

URL: `http://<<IP CONTENEDOR>>:8899`

Add Timestamping Service

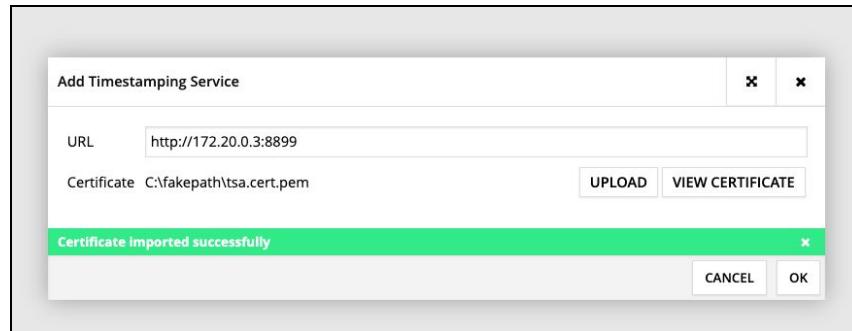
URL

Certificate

UPLOAD

CANCEL OK

36. Cargar el certificado **tsa.cert.pem** con el botón **UPLOAD**. Cuando el certificado haya sido cargado, saldrá un mensaje de confirmación.



37. Configurar las llaves en el módulo *Global Configuration* ubicado en el panel izquierdo de la configuración general.

GOVERNMENT CENTRAL SERVER

CONFIGURATION

Members
Security Servers
Global Groups
Central Services
Certification Services
Timestamping Services

MANAGEMENT

Management Requests
Global Configuration
System Settings
Back Up and Restore

HELP

Version
Feedback

GLOBAL CONFIGURATION

X-ROAD

Anchor
Hash (SHA-256): Anchor file not found
Generated: Anchor file not found

Download URL
http://172.20.0.3/internalconf

Signing Keys
Device ID: Key ID
No (matching) records

RE-CREATE DOWNLOAD DATA

INTERNAL CONFIGURATION

External Configuration Trusted Anchors

Configuration Parts

File	Content Identifier	Version	Updated
fetchinterval-params.xml	FETCHINTERVAL	All Versions	
monitoring.params.xml	MONITORING	All Versions	
nextupdate.params.xml	NEXTUPDATE	All Versions	
private-params.xml	PRIVATE-PARAMETERS	0	
shared-params.xml	SHARED-PARAMETERS	0	

38. Para agregar una llave, hacer clic sobre el botón **NEW KEY**, en la sección *Signing Keys*:

Global configuration generation failing since: 2020-10-14 23:19:02
Signing of internal configuration failed - active key missing
Signing of external configuration failed - active key missing

Anchor

Hash (SHA-224): Anchor file not found
Generated: Anchor file not found

Download URL
<http://172.20.0.3/internalconf>

Signing Keys

Device ID: Key ID	Generated	Actions
No (matching) records		NEW KEY

Configuration Parts

File	Content Identifier	Version	Updated
fetchinterval-params.xml	FETCHINTERVAL	All Versions	0
monitoring-params.xml	MONITORING	All Versions	0
nextupdate-params.xml	NEXTUPDATE	All Versions	0
private-params.xml	PRIVATE-PARAMETERS	All Versions	0
shared-params.xml	SHARED-PARAMETERS	All Versions	0

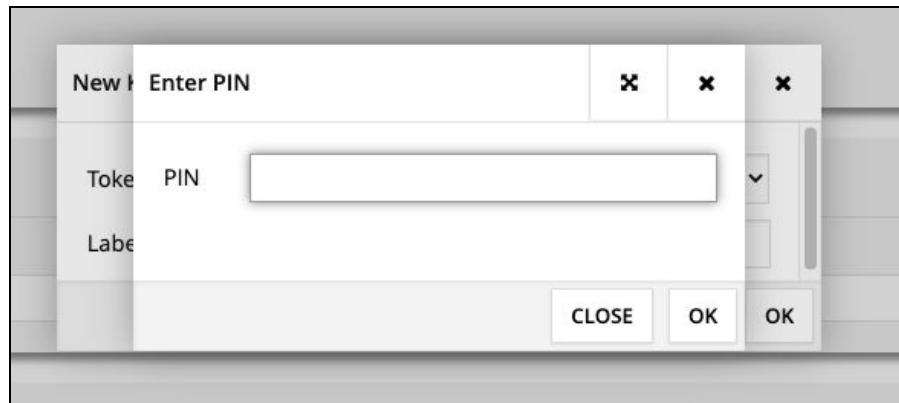
39. Como primera llave, agregar el *token* por defecto y como *label* **key1**.

Token: softToken-0

Label: key1



40. Como PIN, agregar el número 12345.



41. Luego de que la llave haya sido configurada, esta aparecerá listada en el módulo de *Global Configuration*.

The screenshot shows the X-ROAD Global Configuration interface. The top navigation bar has tabs for 'Internal Configuration' (selected), 'External Configuration', and 'Trusted Anchors'. Below the tabs, there are four main sections: 'Anchor' (Hash (SHA-224): Anchor file not found, Generated: Anchor file not found), 'Download URL' (http://172.20.0.3/internalconf), 'Signing Keys' (Device ID: Key ID, softToken-0: 7487C081EE703E7D661AF6DBC09FF500441478D, Generated: 2020-10-15 00:00:26, Logout button), and 'Configuration Parts' (File: fetchinterval-params.xml, Content Identifier: FETCHINTERVAL, Version: All Versions, Updated: MONITORING; File: monitoring-params.xml, Content Identifier: MONITORING, Version: All Versions, Updated: MONITORING).

42. Agregar nuevas configuraciones, por medio de la pestaña de *External Configuration*:

The screenshot shows the X-ROAD Global Configuration interface with the 'External Configuration' tab selected (highlighted with a red circle). The other tabs are 'Internal Configuration' and 'Trusted Anchors'. The interface displays the same sections as the internal configuration: Anchor, Download URL, Signing Keys, and Configuration Parts.

43. Agregar otra llave en la pestaña *External Configuration*, en la sección *Signing Keys*.

The screenshot shows the X-ROAD Global Configuration interface with the 'External Configuration' tab selected. The 'Signing Keys' section contains a 'NEW KEY' button, which is highlighted with a red circle. The other sections are 'Anchor', 'Download URL', and 'Configuration Parts'.

44. Después de hacer clic en el botón *New Key*, aparecerá una ventana donde se podrá agregar el token de la llave y el label, en este caso:

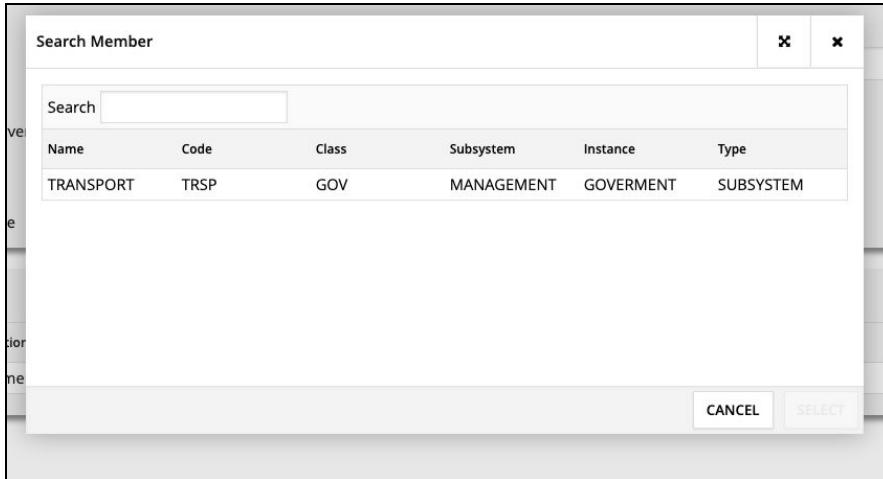
Token: softToken-0
Label: key2



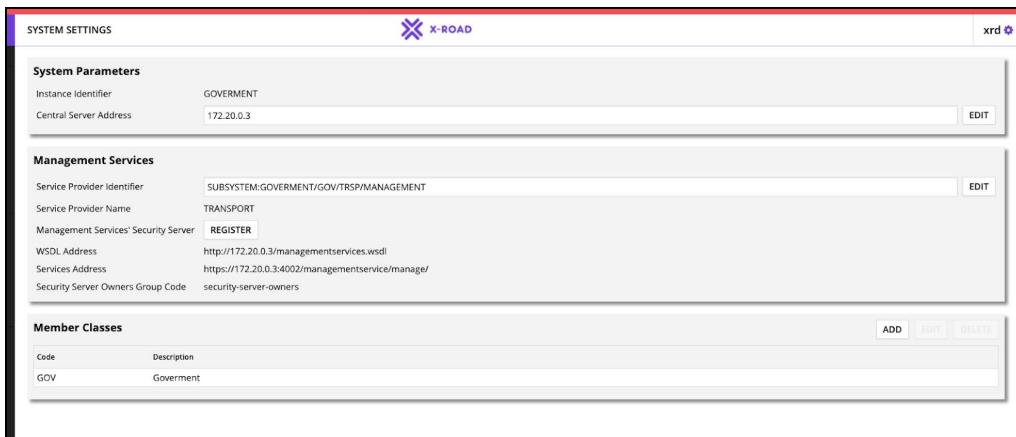
45. Para confirmar el proceso, en la sección Signing Keys estará listada la llave que se acaba de crear.

46. Dirigirse al módulo *System Settings* y hacer clic en el módulo *Management Systems*, en el botón EDIT:

47. En ese punto, seleccionar TRANSPORT y luego hacer clic en clic en el botón SELECT:



48. Hacer clic en el botón REGISTER del módulo *Global Configuration*, para hacer el registro de la configuración.



49. Luego de refrescar la interfaz gráfica o actualizar el navegador donde está la interfaz, deberán haber desaparecido todas las advertencias anteriores:

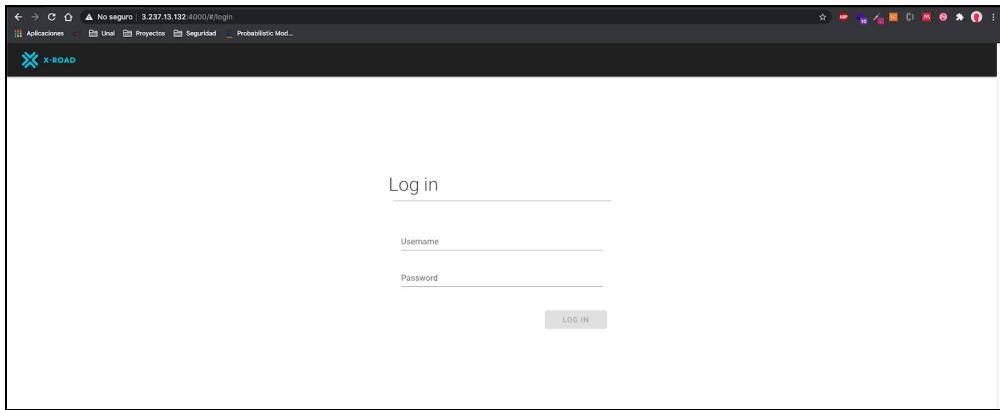
50. Tras los pasos anteriores, el servidor central estará completamente configurado. Ahora, para configurar el servidor de seguridad, será necesario ir al módulo Global Configuration, hacer clic sobre el botón RE-CREATE y luego en el botón DOWNLOAD.

Esta acción permitirá la descarga del archivo de Configuración que va a ser agregado en el Servidor posteriormente. El archivo que se guardará es *configuration_anchor_<Parametros>.xml*

Servidor de Seguridad (Security Server)

1. Así como en el servidor central, es posible acceder a la configuración del servidor de seguridad en una interfaz gráfica visible en la IP Pública del Contenedor de Docker más el puerto 4000, que es generalmente donde se despliega uno de los servidores de seguridad:

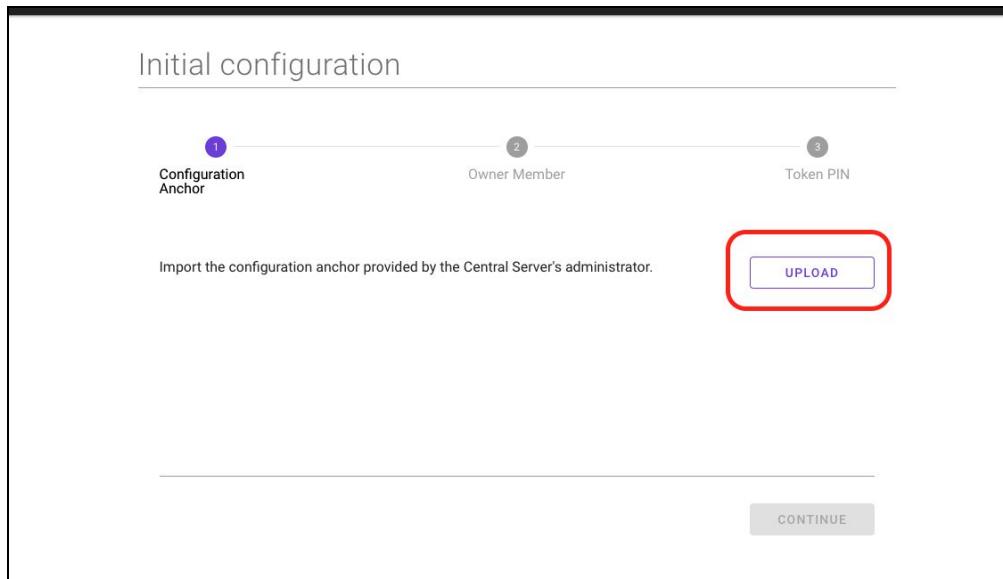
URL: <IP>:4000



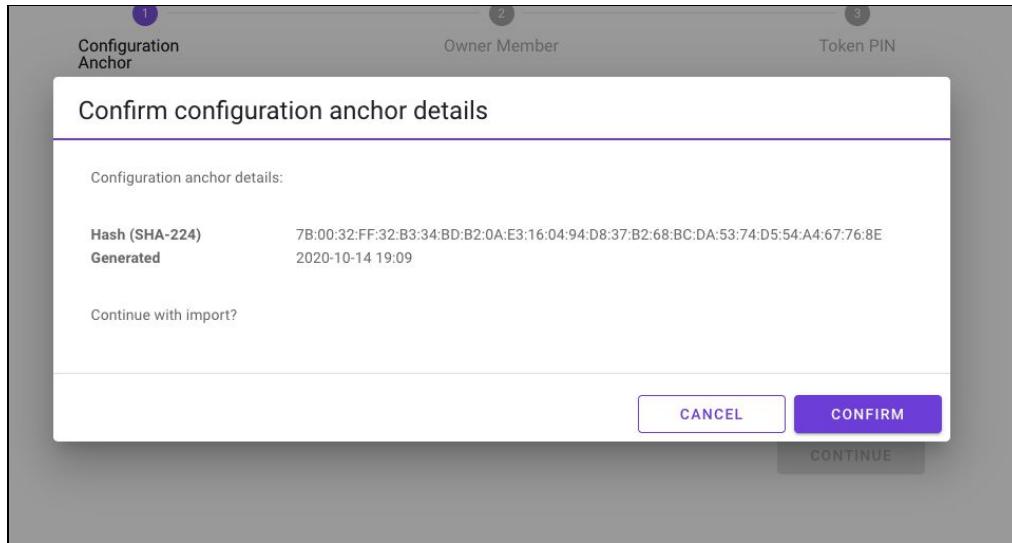
2. Para iniciar la configuración de servidor de seguridad es necesario ingresar las credenciales predeterminadas:

Username: xrd
Password: secret

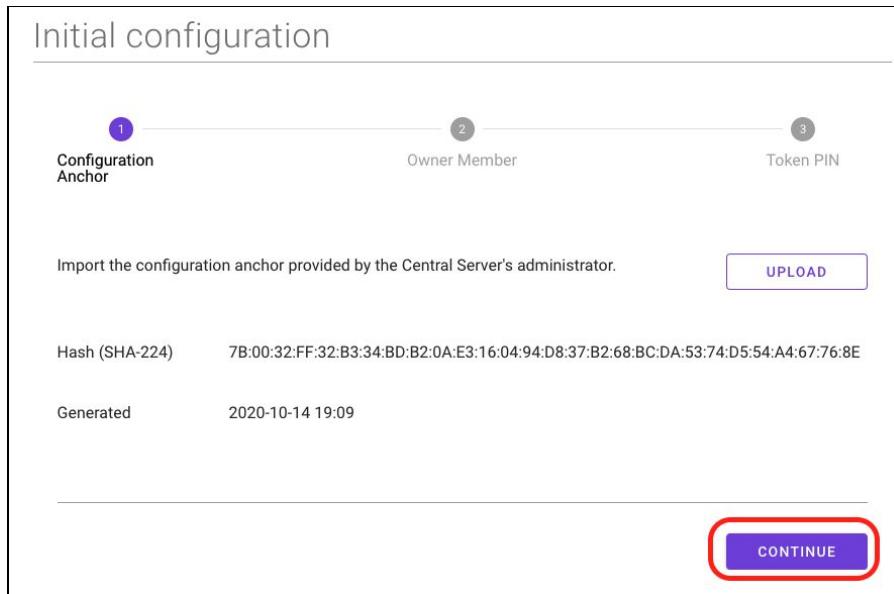
3. Después de agregar las credenciales, es necesario cargar el archivo de configuración creado en los pasos anteriores en la parametrización del servidor central. Para esto se desplegarán unos pasos iniciales donde se debe cargar el archivo (*configuration_anchor_<parametros>.xml*) en el botón UPLOAD resaltado en la siguiente imagen:



4. Después de agregar el archivo, una ventana es presentada con el código HASH generado automáticamente. En este paso hay que confirmar la carga del archivo dando clic sobre el botón de CONFIRM.



5. Pasar al siguiente paso haciendo clic en el botón *CONTINUE*.



6. En el segundo paso, hay que configurar el miembro que va a tener los permisos necesarios en el servidor central. Agregar los siguientes datos:

Member Name: TRANSPORT
Member Class: GOV
Member Code: TRSP
Security Server Code: SS1

Initial configuration

Member Name: TRANSPORT

Member Class: GOV

Member Code: TRSP

Security Server Code: SS1

PREVIOUS **CONTINUE**

- Al ingresar todos los datos se habilitará el botón de **CONTINUE** para ir al tercer paso donde se deberá ingresar un **PIN**:

PIN: 12345
Confirm PIN: 12345

Initial configuration

The software token is the place where the Security Server's AUTH keys is stored. Please define a PIN to log-in into the software token.

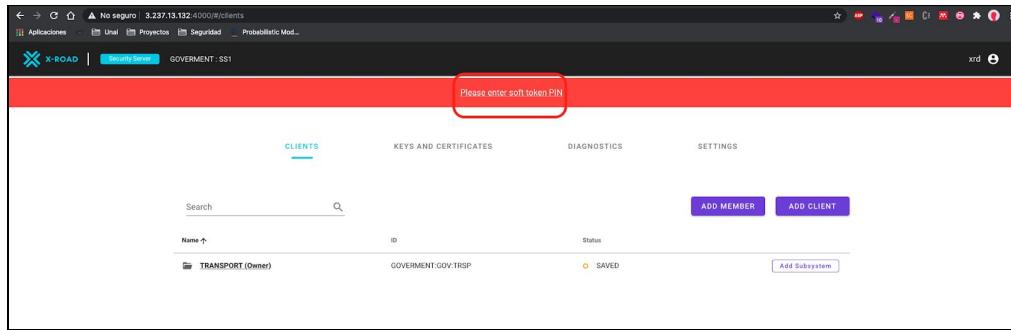
PIN:
 Confirm PIN:

All required information is collected, press the Submit button to initialise the Security Server.

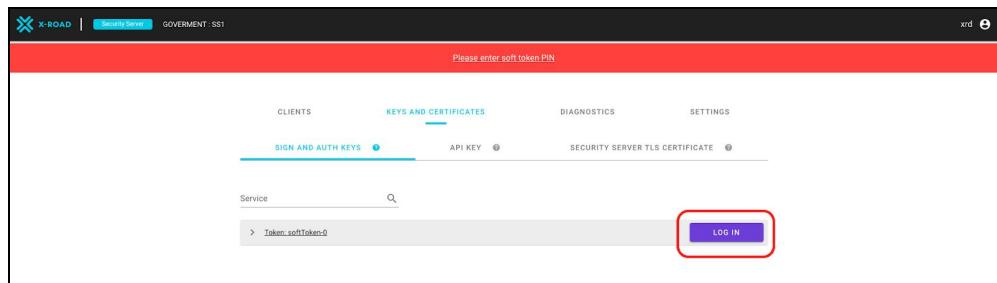
Once the initialisation is done, you must complete the Security Server configuration - simply click the Configure button in the toast notification that will appear in a few moments.

PREVIOUS **SUBMIT**

- Hacer clic en el botón **SUBMIT** para cargar todos los datos inscritos y terminar la configuración inicial. Como acción siguiente se desplegará una pantalla como se muestra en la siguiente imagen, donde se deberá ingresar el **PIN** escrito anteriormente, para que el servidor de seguridad detecte el cambio y quede configurado de forma preliminar.

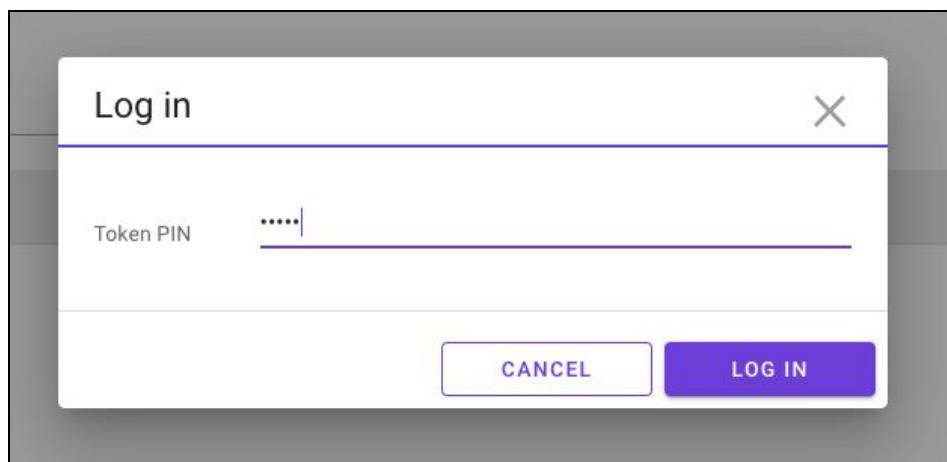


9. Ir a la pantalla *KEYS AND CERTIFICATES*, ubicada en la parte superior de la pantalla.

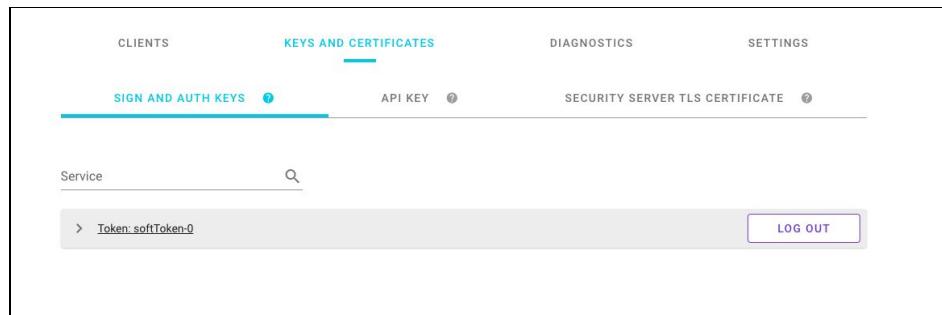


10. Despues de ingresar a esta pestaña, será necesario hacer clic sobre el botón *LOGIN* para que se muestre otra ventana donde se ingresará el PIN.

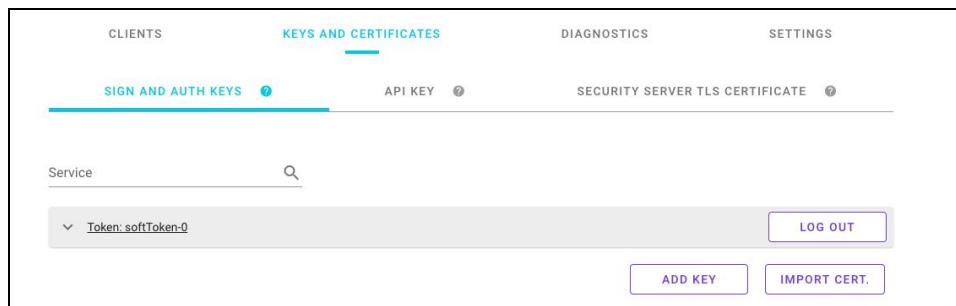
Token PIN: 12345



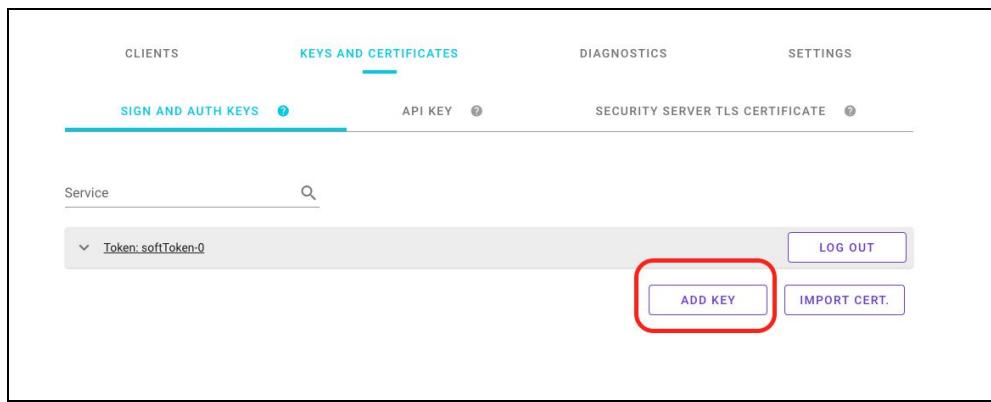
11. Despues del paso anterior, quedará registrado el Token.



12. Expandir el cuadro horizontal, haciendo clic sobre la flecha que apunta a la derecha, con el fin de visualizar detalles del Token:



13. Agregar un par de llaves como parte de la parametrización del servidor de seguridad. Este procedimiento se podrá hacer haciendo clic sobre el botón **ADD KEY** ubicado en la sección inferior derecha de la sección **Token:softToken-0**.



14. Cuando se haga clic en este botón, se abrirá una ventana donde se podrá cargar la información relativa a la llave. En el primer paso hay que indicar como nombre: *Auth* (en el campo **KeyLabel**).

Add key

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

Key Label

CANCEL **NEXT**

- Como segundo paso, se deben agregar más detalles de la llave. Por ejemplo es posible agregar los siguientes datos, **usage**, para indicar el tipo de uso o implementación que va a tener la llave, el **servicio de certificación** que en este caso se trae del servidor central, y la **extensión** o formato de la llave.:.

Usage: AUTHENTICATION
Certification Service: Customized Test CA CN
CSR Format: DER

Add key

Usage AUTHENTICATION

Certification Service Customized Test CA CN

CSR Format DER

CANCEL **PREVIOUS** **CONTINUE**

- Posterior a este procedimiento, es necesario ir a la consola de comando donde se listan los contenedores desplegados en Docker. Allí se debe ejecutar el comando **docker inspect** sobre el contenedor donde está ubicado el servidor de seguridad:

```
sudo docker inspect <<ID CONTENEDOR>>
```

17. Esto es necesario para detallar la información del contenedor y específicamente conocer la dirección IP del mismo. Para el tercer paso de creación de la llave, es necesario copiar la **IP Address** que fue extraída anteriormente y hay que ubicarla en el campo **Server DNS Name** del tercer paso.

Organization Name (O): MANAGEMENT
Server DNS Name (CN): <<IP_Servidor_Seguridad>>

Add key

Key details CSR details Generate CSR

Country Code (C) : FI

Organization Name (O) : MANAGEMENT

Serial Number : GOVERMENT/SS1/GOV

Server DNS name (CN) : 172.20.0.4

Generate a new CSR and save it into a safe place. **GENERATE CSR**

CANCEL **PREVIOUS** **DONE**

18. Una vez los datos han sido ingresados, es necesario hacer clic sobre el botón **GENERATE CSR** para descargar la llave de forma local y finalmente hacer clic sobre el botón **DONE** para finalizar el proceso.

19. Asimismo, es necesario generar otra llave que servirá como medio de firma o de autenticación en procesos posteriores de configuración. En este caso la **segunda llave** tendrá como nombre *sign*.

Key Label: sign

20. En el segundo paso, se deben agregar prácticamente los mismos datos de la primera:

Usage: SIGNING
Client: GOVERNMENT:GOV:TRSP
Certification Service: Customized Test CA CN
CSR Format: DER

Add key

Key details	CSR details	Generate CSR
Usage: SIGNING		
Client: GOVERMENT:GOV:TRSP		
Certification Service: Customized Test CA CN		
CSR Format: DER		

CANCEL **PREVIOUS** **CONTINUE**

21. Finalmente, en el tercer paso se deben agregar los siguientes datos:

Organization Name (O): MANAGEMENT
Serial Number: GOVERMENT/SS1/GOV
Member Code (CN): TRSP

Add key

Country Code (C): FI	
Organization Name (O): MANAGEMENT	
Serial Number: GOVERMENT/SS1/GOV	
Member Code (CN): TRSP	

Generate a new CSR and save it into a safe place. **GENERATE CSR**

CANCEL **PREVIOUS** **DONE**

22. Finalmente, se debe descargar la llave (botón *GENERATE CSR*) y hace clic en el botón *DONE* para terminar con la generación de la segunda llave.
23. Cuando las dos llaves hayan sido descargadas exitosamente y estén ubicadas de forma visible, es necesario realizar una firma sobre cada una de ellas en el servidor central. Para este procedimiento será necesario cargarlas al contenedor del servidor de seguridad con un comando particular en la consola de comandos. En ese sentido, hay que situarse en el directorio donde fueron descargadas las llaves (generalmente estas llaves se descargan en la carpeta raíz del computador, sin embargo, se pueden buscar en los diferentes directorios y ubicarse sobre esa ruta en particular).

Un comando útil para visualizar los archivos que hay sobre un directorio es el comando:

ls

```
[ubuntu@ip-172-31-71-45:~$ ls
auth_csr_20201015_securityserver_GOVERMENT_GOV_TRSP_SS1.der
ca.cert.pem
docker-compose.yml
ocsp.cert.pem
sign_csr_20201015_member_GOVERMENT_GOV_TRSP.der
tsa.cert.pem
ubuntu@ip-172-31-71-45:~$ ]
```

24. Luego de estar ubicados en el directorio correspondiente, es necesario ejecutar los siguientes comandos para copiar las llaves de un lugar a otro, en este caso moverlas de la máquina o el computador local al contenedor donde está desplegado el servidor central con Docker.

Copiar la llave de autorización (Auth_CSR):

sudo docker cp <>Nombre_archivo_Auth>> <>ID Contenedor>>:/root

Copiar la llave de firma (Sign_CSR):

sudo docker cp <>Nombre_archivo_Sign>> <>ID Contenedor>>:/root

```
[ 0 • 0 Descargas — ubuntu@ip-172-31-71-45: ~ — ssh - sudo — 129x32
ubuntu@ip-172-31-71-45:~$ sudo docker cp auth_csr_20201015_securityserver_GOVERMENT_GOV_TRSP_SS1.der 2ef2deea8cf:/root
ubuntu@ip-172-31-71-45:~$ sudo docker cp sign_csr_20201015_member_GOVERMENT_GOV_TRSP.der 2ef2deea8cf:/root
ubuntu@ip-172-31-71-45:~$ ]
```

25. Después de haber ejecutado los anteriores comandos, ir a la consola de comandos del contenedor para poder firmar los certificados. El comando que permite ingresar a la consola de comandos del contenedor es:

sudo docker exec -it <>ID Contenedor CA>> bash

26. Firmar cada una de las llaves ejecutando los siguientes comandos:

```
/home/ca/CA/sign.sh /root/<<Nombre_archivo_auth>>
/home/ca/CA/sign.sh /root/<<Nombre_archivo_sign>>
```

27. Cuando se hayan ejecutado los dos comandos, saldrá la información detallada de la firma tal como se muestra en las siguientes imágenes con cada una de las llaves.

Firma de archivo (*auth_csr....der*)

```
root@2ef2deac8cf:/# /home/ca/CA/sign.sh /root/auth_csr_20201015_securityserver_GOVERMENT_GOV_TRSP_SS1.der
Using configuration from CA.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 3 (0x3)
    Validity
        Not Before: Oct 15 00:45:41 2020 GMT
        Not After : Oct 10 00:45:41 2040 GMT
    Subject:
        countryName          = FI
        organizationName     = MANAGEMENT
        commonName           = 172.20.0.4
        serialNumber         = GOVERNMENT/SS1/GOV
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Key Usage: critical
            Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
        X509v3 Extended Key Usage:
            TLS Web Client Authentication, TLS Web Server Authentication
Certificate is to be certified until Oct 10 00:45:41 2040 GMT (7300 days)

Write out database with 1 new entries
-----BEGIN CERTIFICATE-----
MIIEctCCAlmgAwIBAgIBAzANBgkqhkiG9w0BAQsFADBnMQswCQYDVQQGEwJGSTEY
```

Firma de archivo (*sign_csr....der*):

```
root@2ef2deac8cf:/# /home/ca/CA/sign.sh /root/sign_csr_20201015_member_GOVERNMENT_GOV_TRSP.der
Using configuration from CA.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 4 (0x4)
    Validity
        Not Before: Oct 15 00:46:23 2020 GMT
        Not After : Oct 10 00:46:23 2040 GMT
    Subject:
        countryName          = FI
        organizationName     = MANAGEMENT
        commonName           = TRSP
        serialNumber         = GOVERNMENT/SS1/GOV
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Key Usage: critical
            Non Repudiation
Certificate is to be certified until Oct 10 00:46:23 2040 GMT (7300 days)

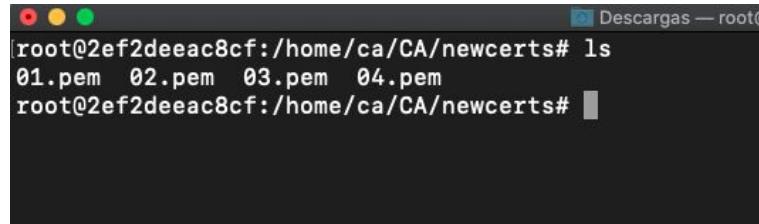
Write out database with 1 new entries
-----BEGIN CERTIFICATE-----
MIIEtDCCAjSgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBnMQswCQYDVQQGEwJGSTEY
MBYGA1UECgwPQ3VzdG9taXplZCBUZXN0MR4wHAYDVQQLDBVDbDxDN0b21pemVkJFRl
c3QgQQ0EgtT1UxhjAcBgNVBAMMFUN1c3RvbWl6ZWQgVGVzdCBDQSBDTjAeFw0yMDEw
MTUwMDQ2MjNaFw00MDExMTAwMDQ2MjNaME0xCzAJBgNVBAYTAkZJMRMwEQYDVQQK
```

28. Después de que se hayan procesado las firmas de los archivos, verificar que se hayan ejecutado bien los comandos, ingresando a la carpeta newcerts (utilizar el siguiente comando):

```
cd /home/ca/CA/newcerts/
```

29. Después de que se esté ubicado en la carpeta, validar que se encuentren los siguientes 4 archivos:

Ls



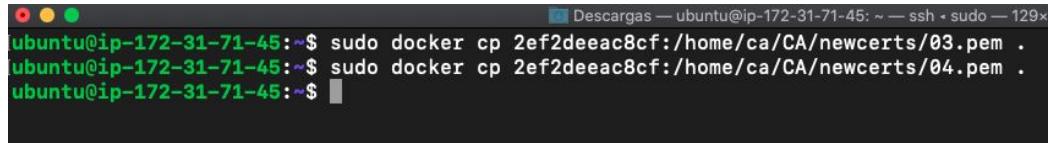
```
root@2ef2deeac8cf:/home/ca/CA/newcerts# ls
01.pem 02.pem 03.pem 04.pem
root@2ef2deeac8cf:/home/ca/CA/newcerts#
```

30. Allí deberán estar ubicados los cuatro archivos, el archivo **03.pem** corresponde al resultado de la firma del *archivo_auth* y el **04.pem** es el resultado de la firma del *archivo_sign*. Posterior a esta revisión y confirmando que en este directorio se encuentran los archivos generados, salir del contenedor con el comando:

exit

31. De la misma forma como se hizo en pasos anteriores, copiar estos archivos que están en el contenedor de CA al computador o máquina local. Esta instrucción se puede realizar ejecutando los siguientes comandos para los archivos **03.pem** y **04.pem**.

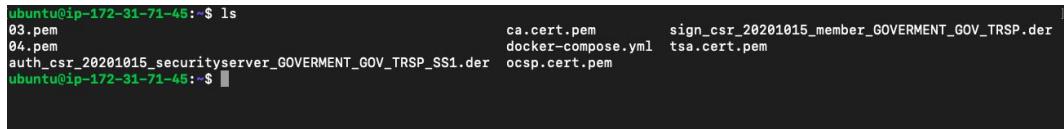
```
sudo docker cp <>ID CONTENEDOR CA>>:/home/ca/CA/newcerts/03.pem .
sudo docker cp <>ID CONTENEDOR CA>>:/home/ca/CA/newcerts/04.pem .
```



```
ubuntu@ip-172-31-71-45:~$ sudo docker cp 2ef2deeac8cf:/home/ca/CA/newcerts/03.pem .
ubuntu@ip-172-31-71-45:~$ sudo docker cp 2ef2deeac8cf:/home/ca/CA/newcerts/04.pem .
ubuntu@ip-172-31-71-45:~$
```

32. Después de que se ejecuten estos comandos, validar que los archivos se encuentren transferidos en la carpeta root del computador con exactamente el mismo nombre:

Ls



```
ubuntu@ip-172-31-71-45:~$ ls
03.pem          ca.cert.pem      sign_csr_20201015_member_GOVERNMENT_GOV_TRSP.der
04.pem          docker-compose.yml  tsa.cert.pem
auth_csr_20201015_securityserver_GOVERMENT_GOV_TRSP_SS1.der  ocsp.cert.pem
ubuntu@ip-172-31-71-45:~$
```

33. Cargar los archivos en el servidor de seguridad a través de la consola gráfica del servidor de seguridad (pestaña principal de **KEYS AND CERTIFICATES**), en la sub-pestaña **SIGN AND AUTH KEYS**, en el botón **IMPORT CERT**:

The screenshot shows the 'SIGN AND AUTH KEYS' tab selected in the top navigation bar. Below it, there's a search bar and a dropdown menu showing 'Token: softToken-0'. On the right, there are 'LOG OUT' and 'IMPORT CERT.' buttons, with 'IMPORT CERT.' being highlighted by a red box. The main area displays two sections: 'AUTH Key and Certificate' and 'SIGN Key and Certificate', each with a table and 'Generate CSR' and 'Delete CSR' buttons.

AUTH Key and Certificate	ID	OCSP	Expires	Status
Auth	OF26547074B94FEC3CEAF88589E6550DAF51DF3A			Generate CSR
Request				Delete CSR

SIGN Key and Certificate	ID	OCSP	Expires	Status
sign	425AA081F6FD8EE4497C841B2C9D5DFBA690D7AB			Generate CSR
Request				Delete CSR

34. Inicialmente se debe cargar el archivo **03.pem** en el selector de archivos que abre el botón **IMPORT CERT**.

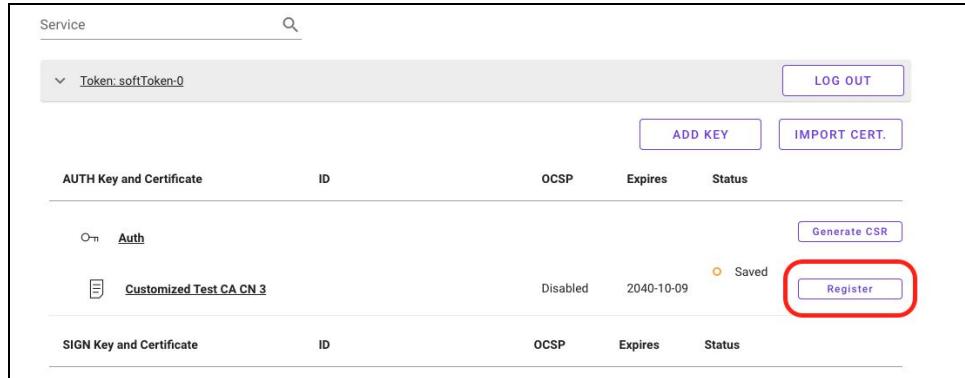
This screenshot shows the same 'SIGN AND AUTH KEYS' interface after a certificate has been imported. A new entry for 'Customized Test CA CN 3' is listed under 'AUTH Key and Certificate'. This entry includes fields for 'ID' (disabled), 'Expires' (2040-10-09), and 'Status' (Saved). There is also a 'Register' button next to the status. The rest of the interface remains the same, with the 'SIGN Key and Certificate' section below it.

AUTH Key and Certificate	ID	OCSP	Expires	Status
Auth				Generate CSR
Customized Test CA CN 3	Disabled	2040-10-09	Saved	Register
Request				

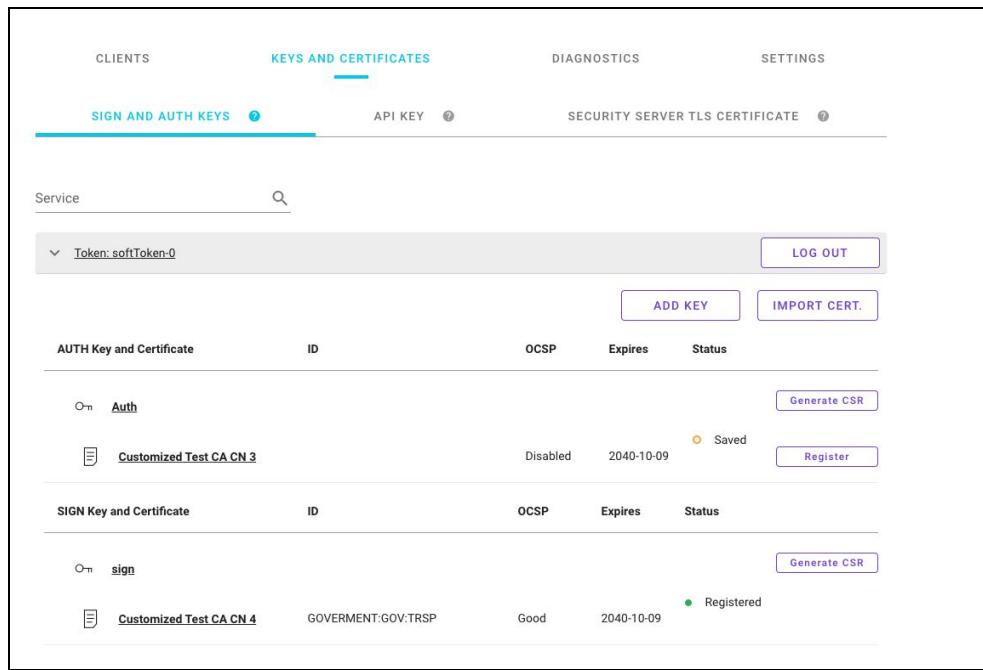
SIGN Key and Certificate	ID	OCSP	Expires	Status
sign	425AA081F6FD8EE4497C841B2C9D5DFBA690D7AB			Generate CSR
Request				Delete CSR

35. La pantalla mostrará un mensaje verde de confirmación exponiendo la carga exitosa del certificado. Igualmente dentro de la columna **Status**, se mostrará en *Saved* cuando el archivo haya sido cargado correctamente.

36. Hacer clic en el botón *Register* para guardar el certificado en el sistema.



37. Cargar el certificado **04.pem** haciendo clic en el botón *Register*:



38. Una vez hecho y confirmado que ambos certificados hayan sido cargados exitosamente (*círculo verde - Registered*) en la columna de **Status** en el Servidor de Seguridad, ir a la interfaz gráfica del Servidor Central.

39. ir al módulo **Members** ubicado en el panel izquierdo de la pantalla.

40. Hacer doble clic en *TRANSPORT*, que es el miembro creado para tener acceso. Se desplegará una ventana con los detalles de configuración de dicho miembro. Para este caso, ir a la sub-pestaña *Owned Servers* tal como se muestra en el recuadro rojo:

41. En la parte superior derecha de la ventana, hacer clic sobre el botón *ADD* para agregar un nuevo servicio.

42. Una vez se haga clic en el botón, se desplegará otra ventana con el título **Authentication Certificate Registration**. Allí agregar el código SS1:

Server Code: SS1

Authentication Certificate Registration

SECURITY SERVER INFORMATION

Owner Name	TRANSPORT
Owner Class	GOV
Owner Code	TRSP
Server Code	SS1

AUTHENTICATION CERTIFICATE INFORMATION

UPLOAD

CANCEL **SUBMIT**

43. En la sección **AUTHENTICATION CERTIFICATE INFORMATION**, cargar el archivo **03.pem** que está ubicado en el computador local correspondiente al certificado Auth. Cuando se haya cargado, es necesario hacer clic en el botón **SUBMIT** para completar los cambios. Adicionalmente, la ventana mostrará un mensaje verde de confirmación demostrando el proceso exitoso.

Authentication Certificate Registration

SECURITY SERVER INFORMATION

Owner Name	TRANSPORT
Owner Class	GOV
Owner Code	TRSP
Server Code	SS1

AUTHENTICATION CERTIFICATE INFORMATION

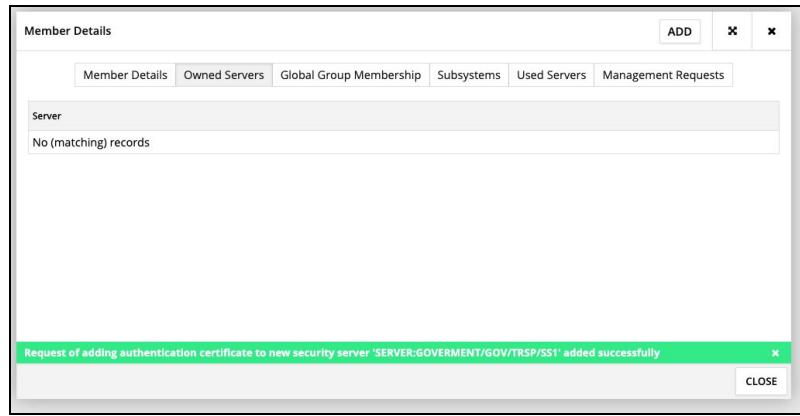
UPLOAD

CA	Customized Test CA CN
Serial Number	3
Subject	/C=FI/O=MANAGEMENT/CN=172.20.0.4/serialNumber
Expires	2040-10-10 00:45:41

Certificate imported successfully

CANCEL **SUBMIT**

44. Después de que se haya cerrado la ventana, en la sección **Member Details** saldrá un mensaje de confirmación anunciando que la solicitud de adición del nuevo certificado de autenticación ha sido enviada correctamente.



45. Dirigirse al módulo **Management Request** ubicado en el panel izquierdo de la pantalla, con el fin de validar que los certificados se encuentren registrados de la siguiente manera:

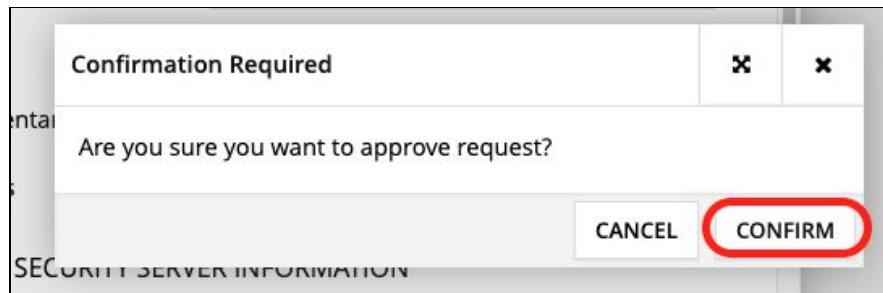
The screenshot shows the 'MANAGEMENT REQUESTS (2)' page. The left sidebar has sections for Configuration (Members, Security Servers, Global Groups, Central Services, Certification Services, Timestamping Services), Management (Management Requests, Global Configuration, System Settings, Back Up and Restore), and Help (Version, Feedback). The main area displays a table of management requests:

Request ID	Created	Request Type	Source	Server Owner Name	Server Owner Class	Server Owner Code	Server Code	Status
2	2020-10-15 01:04:37	Certificate regis...	Security server	TRANSPORT	GOV	TRSP	SS1	SUBMITTED...
1	2020-10-15 01:01:32	Certificate regis...	X-Road center	TRANSPORT	GOV	TRSP	SS1	SUBMITTED...

46. Para que se envíe y se apruebe directamente la solicitud, es necesario hacer clic sobre el registrado con (**Request ID = 2**), hacer clic en el botón **APPROVE**, ubicado en la parte inferior derecha de la ventana:

The screenshot shows the 'Authentication Certificate Registration Request Details' window. It contains two sections: 'REQUEST INFORMATION' and 'AFFECTED SECURITY SERVER INFORMATION'. The 'REQUEST INFORMATION' section includes fields for Request ID (2), Received (2020-10-15 01:04:37), Source (SECURITY_SERVER), Status (SUBMITTED FOR APPROVAL), Complementary request ID (1), and Comments. The 'AFFECTED SECURITY SERVER INFORMATION' section includes fields for Owner Name (TRANSPORT), Owner Class (GOV), Owner Code (TRSP), and Server Code (SS1). At the bottom, there are buttons for CLOSE, DECLINE, and APPROVE, with APPROVE being circled in red.

47. Allí saldrá un mensaje de confirmación, donde será necesario hacer clic sobre el botón **CONFIRM** para validar la acción.



48. Para verificar parte del proceso, ir al módulo **SECURITY SERVERS** (ubicado en el panel izquierdo), donde se detallarán los datos del servidor, enlazando la relación con el miembro **TRANSPORT**:

SECURITY SERVERS (1)				X-ROAD	DETAILS	xrd ⚙
Server Code	Owner Name	Owner Class	Owner Code			
SS1	TRANSPORT	GOV	TRSP			

49. De la misma forma, hacer la aprobación del registro con (**RequestId = 1**), dejando como resultado una tabla con la información similar a como se muestra en la siguiente imagen:

MANAGEMENT REQUESTS (2)									X-ROAD	DETAILS	xrd ⚙
Request ID	Created	Request Type	Source	Server Owner Name	Server Owner Class	Server Owner Code	Server Code	Status			
2	2020-10-15 01:04:37	Certificate registration	Security server	TRANSPORT	GOV	TRSP	SS1	APPROVED			
1	2020-10-15 01:01:32	Certificate regis...	X-Road center	TRANSPORT	GOV	TRSP	SS1	APPROVED			

50. Una vez aprobada la solicitud, dirigirse a la sección **System Settings** y hacer clic en el botón **REGISTER**, en la subsección **Management Services**.

The screenshot shows the 'System Parameters' section with 'Instance Identifier' set to 'GOVERNMENT' and 'Central Server Address' set to '172.20.0.3'. In the 'Management Services' section, under 'Management Services' Security Server', the 'REGISTER' button is highlighted with a red circle. Below it, the WSDL Address is 'http://172.20.0.3/managementservices.wsdl' and the Services Address is 'https://172.20.0.3:4002/managementservice/manage/'. The 'Member Classes' section lists 'GOV' with 'Description' 'Goverment'. There are 'ADD', 'EDIT', and 'DELETE' buttons at the top right of the member class table.

51. Aparecerá una ventana en la plataforma con el nombre **Management Service Provider Registration Request**, donde se deberá hacer clic sobre el botón **SEARCH**.

The dialog box has 'Management Service Provider Registration Request' at the top. It contains two sections: 'CLIENT INFORMATION' and 'SECURITY SERVER INFORMATION'. Under 'CLIENT INFORMATION', fields are filled with 'Name: TRANSPORT', 'Class: GOV', 'Code: TRSP', and 'Subsystem Code: MANAGEMENT'. Under 'SECURITY SERVER INFORMATION', the 'SEARCH' button is highlighted with a red circle. Below it, there are fields for 'Owner Name', 'Owner Class', 'Owner Code', and 'Server Code'. At the bottom are 'CANCEL' and 'SUBMIT' buttons.

52. Se listarán los miembros propietarios del servidor de seguridad, donde se deberá hacer clic sobre el registro **TRANSPORT** y finalmente en el botón **SELECT**, para seleccionarlo de manera correcta.

Central Server Address Book			
Security Servers			
<input type="text" value="Search"/>			
Owner Name	Owner Class	Owner Code	Server Code
TRANSPORT	GOV	TRSP	SS1

CANCEL **SELECT**

53. Finalmente, para aplicar y guardar los cambios, hacer clic en el botón **SUBMIT**.

Management Service Provider Registration Request

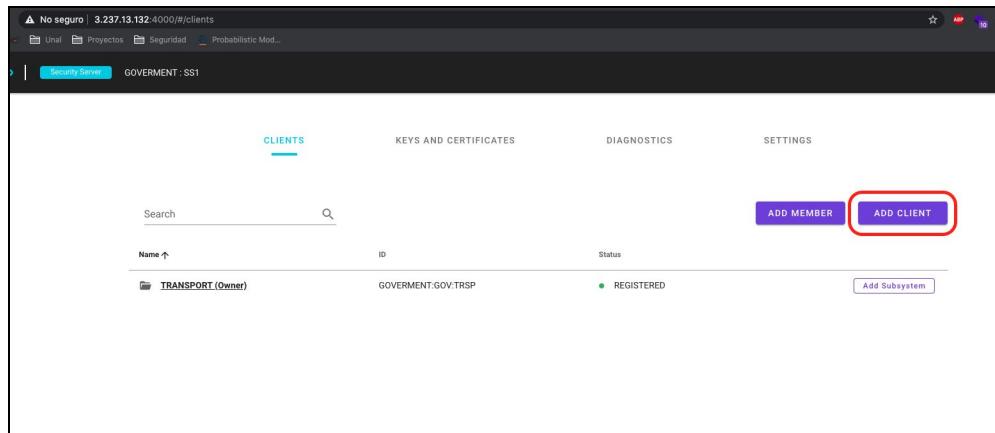
CLIENT INFORMATION	
Name	TRANSPORT
Class	GOV
Code	TRSP
Subsystem Code	MANAGEMENT
SECURITY SERVER INFORMATION	
<input type="button" value="SEARCH"/>	
Owner Name	TRANSPORT
Owner Class	GOV
Owner Code	TRSP
Server Code	SS1

CANCEL **SUBMIT**

54. De esta manera, se podrá observar en la subsección *Management Services*, la inclusión del miembro *TRSP* (propiedad *Management Services' Security Server*).

The screenshot shows the 'SYSTEM SETTINGS' page of the X-ROAD interface. It includes sections for 'System Parameters' (Instance Identifier: GOVERNMENT, Central Server Address: 172.20.0.3), 'Management Services' (Service Provider Identifier: SUBSYSTEM:GOVERNMENT/GOV/TRSP/ MANAGEMENT, Service Provider Name: TRANSPORT, Management Services' Security Server: SERVER:GOVERNMENT/GOV/TRSP/SS1, WSDL Address: http://172.20.0.3/managementservices.wsdl, Services Address: https://172.20.0.3:4002/managementservice/manage/, Security Server Owners Group Code: security-server-owners), and 'Member Classes' (Code: GOV, Description: Government). Buttons for ADD, EDIT, and DELETE are visible.

55. De esta manera, se concluye la configuración en el Servidor Central.
56. Ahora, dirigirse al Servidor de Seguridad, específicamente a la pestaña *CLIENTS*, donde se podrá visualizar un botón que permitirá agregar más clientes. Hacer clic en el botón para adicionar un cliente nuevo:



57. Cuando se despliegue la ventana, ingresar los datos como se describen a continuación:

Member Class: GOV
Member Code: TRSP
Subsystem Code: MANAGEMENT

Add a Client

1 Client details 2 Finish

Specify the details of the Client you want to add.

If the Client is already existing, you can select it from the Global list. **SELECT CLIENT**

Member Name ⓘ

Member Class GOV ⓘ

Member Code TRSP ⓘ

Subsystem Code MANAGEMENT ⓘ

CANCEL **NEXT**

58. Hacer clic en el botón **SUBMIT** para guardar la configuración del nuevo cliente.

Add a Client

1 Client details 2 Finish

All required information is collected. By clicking "Submit", the new client will be added to the Clients list and the new key and CSR will appear in the Keys and Certificates view.

In order to register the new client, please complete the following steps:

- 1) Send the CSR to a Certificate Authority for signing
- 2) Once received back, import the resulting certificate to the corresponding key
- 3) At this point you can register the new client

NOTE: if you click Cancel, all data will be lost

Register client

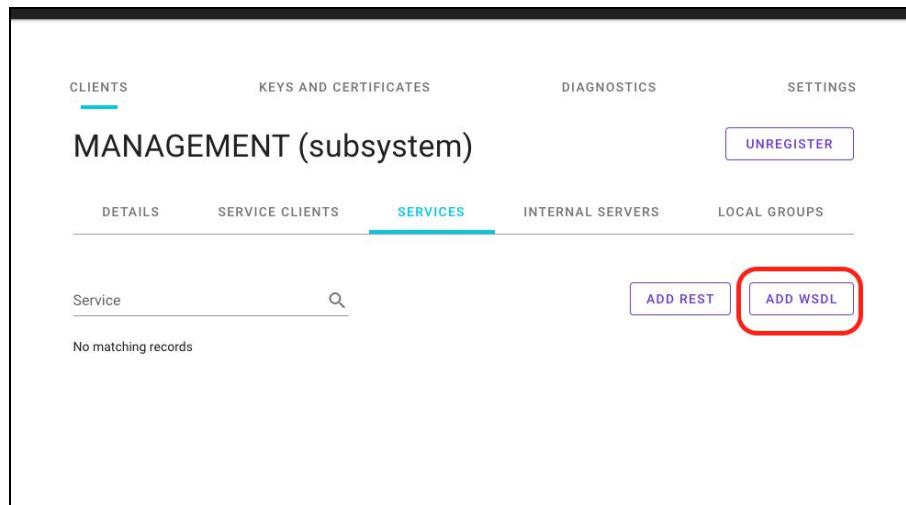
CANCEL **PREVIOUS** **SUBMIT**

59. Validar que el cliente haya sido agregado correctamente y se encuentre en estado **REGISTERED**. Si se encuentra de esta manera, hacer clic sobre el botón **MANAGEMENT**:

60. Dirigirse a la pestaña **SERVICES** para crear los servicios asociados al nuevo cliente.

61. Luego de visualizar los detalles de creación del subsistema (**MANAGEMENT**) donde se visualiza el nombre, la clase, el código del miembro, y el código del subsistema, dirigirse a la sub-pestaña **SERVICES**. Hacer clic sobre el botón **ADD WSDL** para agregar la URL correspondiente.

*Esta URL está ubicada bajo el título de WSDL Address en la sección Management Services, en el módulo de **SYSTEM SETTINGS** del Servidor Central.*



System Parameters

Instance Identifier	GOVERNMENT
Central Server Address	172.20.0.3

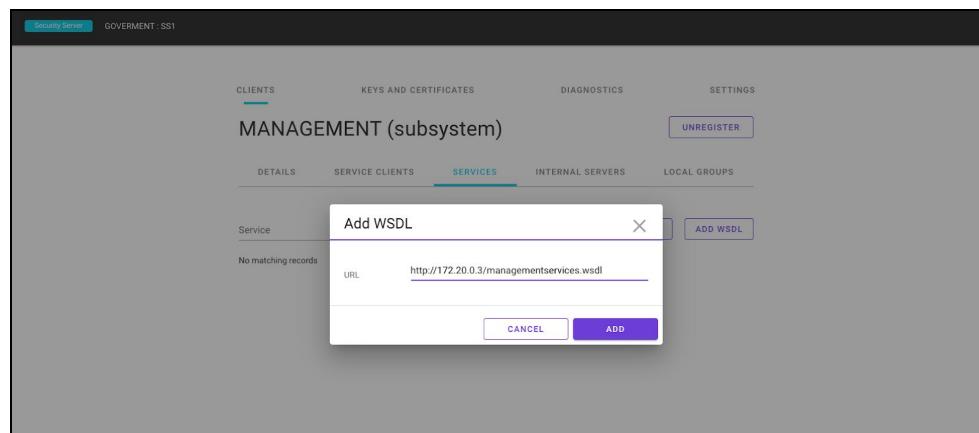
Management Services

Service Provider Identifier	SUBSYSTEM:GOVERNMENT/GOV/TRSP/MANAGEMENT
Service Provider Name	TRANSPORT
Management Services' Security Server	SERVER:GOVERNMENT/GOV/TRSP/SS1
WSDL Address	http://172.20.0.3/managementservices.wsdl
Services Address	https://172.20.0.3:4002/managementservice/manage/
Security Server Owners Group Code	security-server-owners

Member Classes

Code	Description
GOV	Government

62. Copiar la *URL* que se muestra en el campo y agregarla en el servidor de seguridad, en la ventana que se abrirá tras hacer clic en **Add WSDL**. Hacer clic en el botón **ADD** para registrar los cambios en el sistema.



63. Después de hacer clic en el botón ADD, aparecerán cuatro servicios listados dentro de la etiqueta WSDL, tal cual como se muestra en la siguiente imagen.

Service Code	URL	Timeout
authCertDeletion	http://INSERT_MANAGEMENT_SERVICE_ADDRESS_HERE	60
clientDeletion	http://INSERT_MANAGEMENT_SERVICE_ADDRESS_HERE	60
clientReg	http://INSERT_MANAGEMENT_SERVICE_ADDRESS_HERE	60
ownerChange	http://INSERT_MANAGEMENT_SERVICE_ADDRESS_HERE	60

64. Despues de verificar que se hayan listado los cuatro servicios con su respectivo código (**Service Code**), dirección URL (**URL**) y tiempo de espera (**Timeout**), hacer clic sobre el servicio **authCertDeletion**:

authCertDeletion

Service URL: http://INSERT_MANAGEMENT_SERVICE_ADDRESS_HERE

Timeout (s): 60

Verify TLS certificate:

SAVE

Access Rights

Member name / Group description **ID / Group code** **Type** **Access Rights given**

CLOSE

65. Antes de realizar cualquier cambio, dirigirse al Servidor Central y copiar la URL de los servicios (propiedad **Services Address**):

66. Dirigirse nuevamente al servidor de seguridad y modificar el atributo **Service URL** por la URL copiada en el paso anterior. Desmarcar la casilla **Verify TLS certificate** y marcar las casillas correspondiente a aplicar estos cambios a todos los métodos en el WSDL (Apply to all in WSDL). Hacer clic en el botón **SAVE**.

67. Agregar los permisos correspondientes a este método, haciendo clic en el botón **ADD SUBJECTS**:

GOVERNMENT : SS1

authCertDeletion

Apply to all in WSDL

Service URL:

Timeout (s):

Verify TLS certificate:

SAVE

Access Rights

ADD SUBJECTS (highlighted with a red box)

Member name / Group description	ID / Group code	Type	Access Rights given

CLOSE

68. Se desplegará una ventana con el título de **Add Subjects**. Antes de escribir en cualquier campo o realizar cualquier cambio, es necesario hacer clic en el botón **SEARCH**:

Add Subjects

Name

Instance

Member class Member group code

Subsystem code Subject type

SEARCH (highlighted with a red box)

Member name / Group description	ID / Group code	Type

CANCEL **ADD SELECTED**

69. Hacer clic sobre el *checkbox* correspondiente a *Security server owners*, y finalmente en el botón **ADD SELECTED**:

Add Subjects

Name	Instance	
Member class	Member group code	
Subsystem code	Subject type	
SEARCH		
Member name / Group description	ID / Group code	Type
<input checked="" type="checkbox"/> Security server owners	GOVERMENT:security-server-owners	GLOBALGROUP
<input type="checkbox"/> TRANSPORT	GOVERMENT:GOV:TRSP:MANAGEMENT	SUBSYSTEM
		<input type="button" value="CANCEL"/> <input style="border: 2px solid red; border-radius: 5px; padding: 2px 10px;" type="button" value="ADD SELECTED"/>

70. De esta manera, la configuración deberá quedar como se muestra en la siguiente imagen. Para finalizar el proceso hacer clic en el botón **CLOSE**.

authCertDeletion

Service URL <small>?</small>		https://172.20.0.3:4002/managementservice/manage/	<input checked="" type="checkbox"/> Apply to all in WSDL
Timeout (s) <small>?</small>		60	<input checked="" type="checkbox"/>
Verify TLS certificate <small>?</small>		<input type="checkbox"/>	<input checked="" type="checkbox"/> SAVE
Access Rights		<input type="button" value="REMOVE ALL"/> <input type="button" value="ADD SUBJECTS"/>	
Member name / Group description	ID / Group code	Type	Access Rights given
Security server owners	GOVERMENT:security-server-owners	GLOBALGROUP	2020-10-14 20:59 <input type="button" value="Remove"/>
<input type="button" value="CLOSE"/>			

71. Para finalizar la configuración, repetir el proceso con los 4 servicios, agregando siempre los **Security server owners** listados en la etiqueta *WSDL* en el subsistema **MANAGEMENT**.