



**El futuro digital
es de todos**

MinTIC



CONFIGURAR ESCENARIO DE INTEROPERABILIDAD MEDIANTE X-ROAD

Escenario Básico de Interoperabilidad

4

**Guía de configuración
de X-Road**



Servidor Central

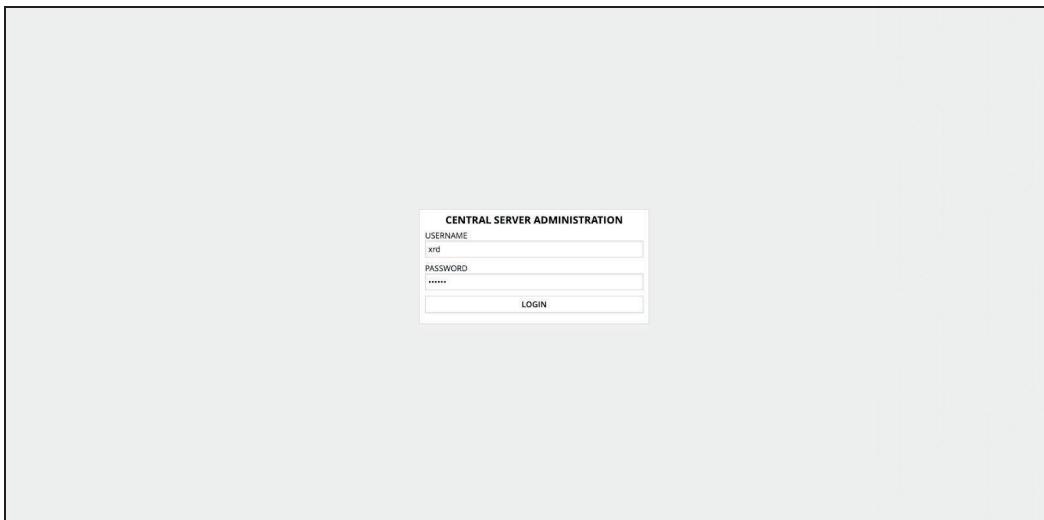
(Government)

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

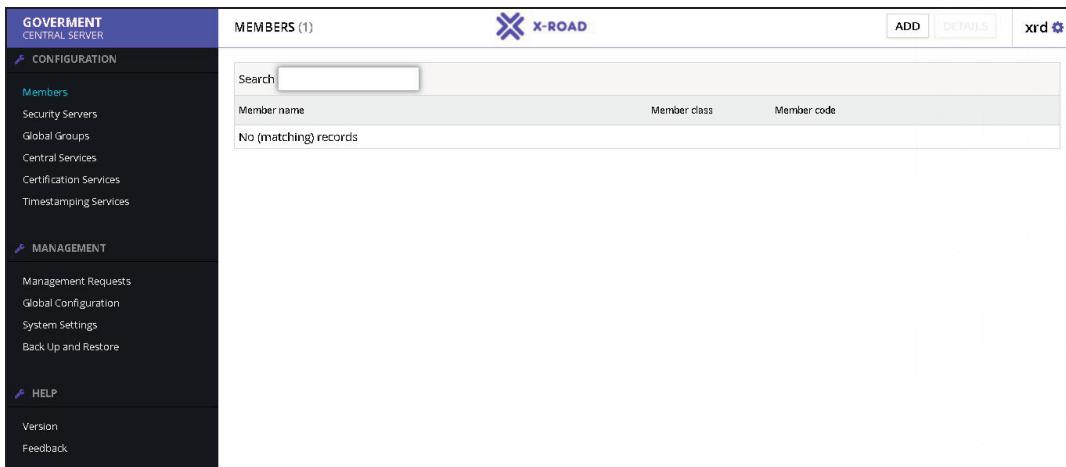
Username: xrd
Password: secret



A large rectangular placeholder box intended for displaying the 'CENTRAL SERVER ADMINISTRATION' login interface. The interface itself is shown as a smaller inset at the bottom left of the placeholder.

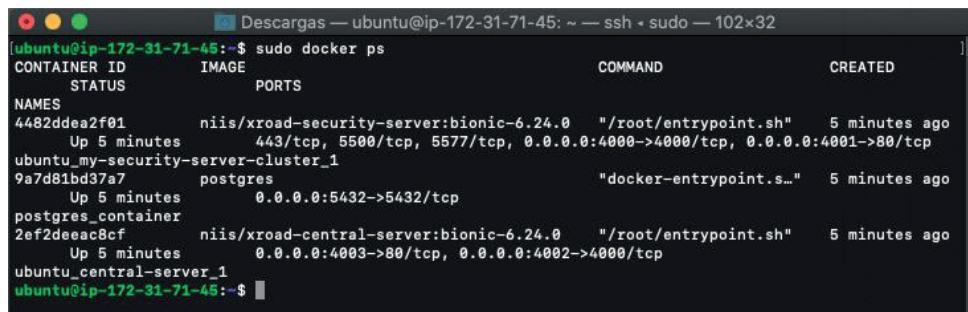
CENTRAL SERVER ADMINISTRATION	
USERNAME	xrd
PASSWORD	*****
<input type="button" value="LOGIN"/>	

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:

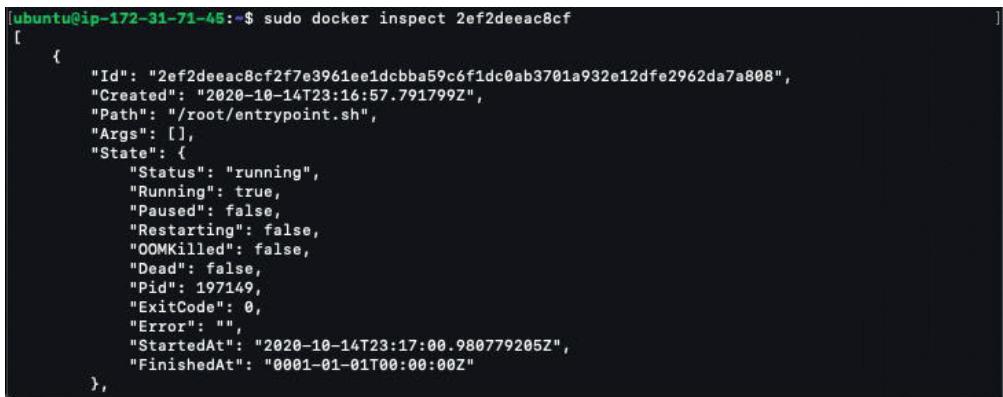
```
sudo docker ps
```



```
ubuntu@ip-172-31-71-45:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS
NAMES
4482ddea2f01      niis/xroad-security-server:bionic-6.24.0   "/root/entrypoint.sh"   5 minutes ago
                   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..."   5 minutes ago
                   Up 5 minutes   0.0.0.0:5432->5432/tcp
postgres_container
2ef2deeac8cf      niis/xroad-central-server:bionic-6.24.0   "/root/entrypoint.sh"   5 minutes ago
                   Up 5 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:~$
```

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

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



```
ubuntu@ip-172-31-71-45:~$ sudo docker inspect 2ef2deeac8cf
[{"Id": "2ef2deeac8cf2f7e3961ee1dcba59c6f1dc0ab3701a932e12dfe2962da7a808", "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"}]
```

- 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.

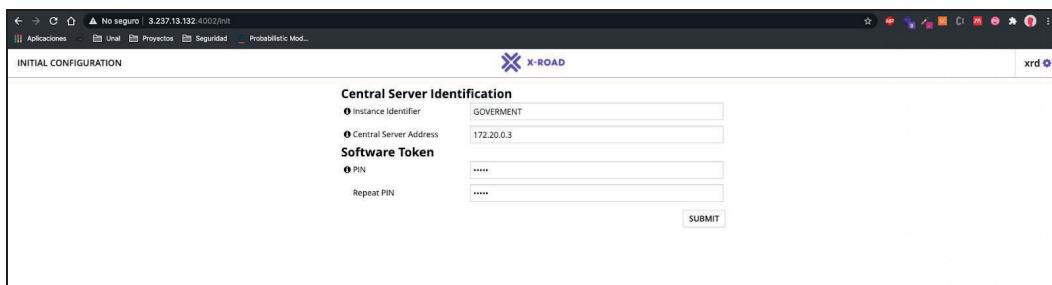
```

"Aliases": [
    "central-server",
    "2ef2deac8cf"
],
"NetworkID": "cd030c8488f0258a7bf9efabec2374e1e41c3c782977056310d3377eecdd4807",
"EndpointID": "0dbca5dc9e2feec2b65b28a6af7b4b8a846a6e6e17e7654602564c77c0b0bfd",
"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
]

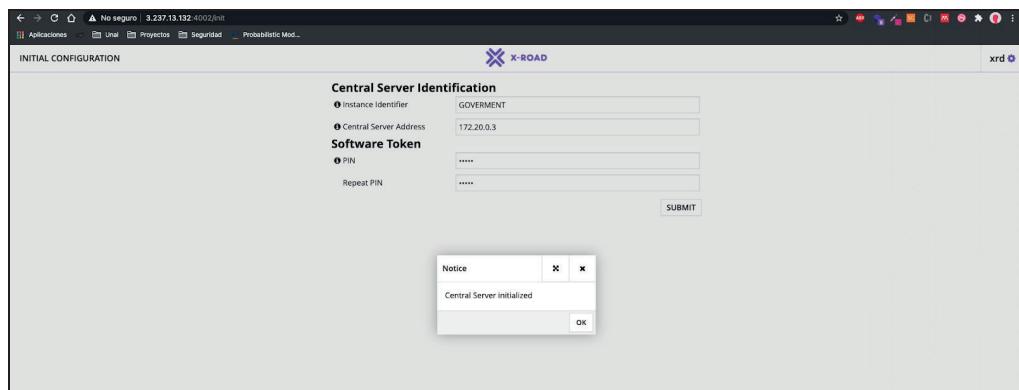
```

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

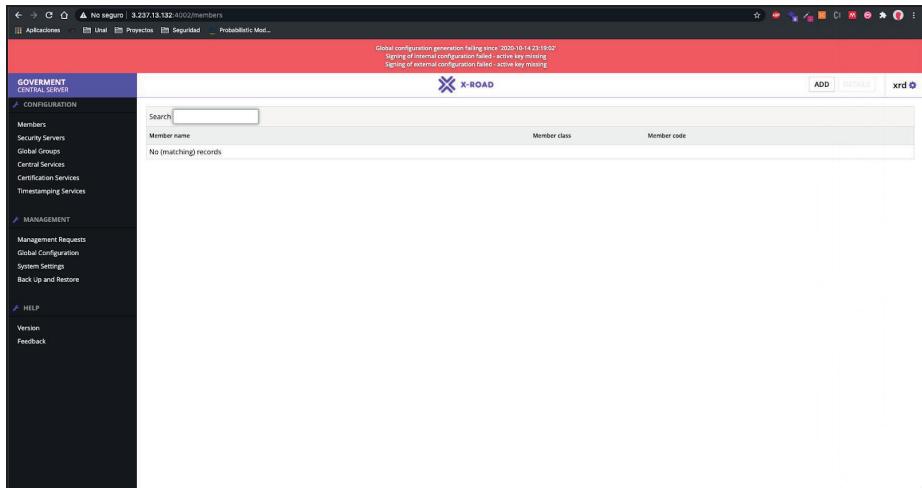
Instance Identifier: GOVERNMENT
Central Server Address: IP del contenedor
PIN: 12345
Repeat PIN: 12345



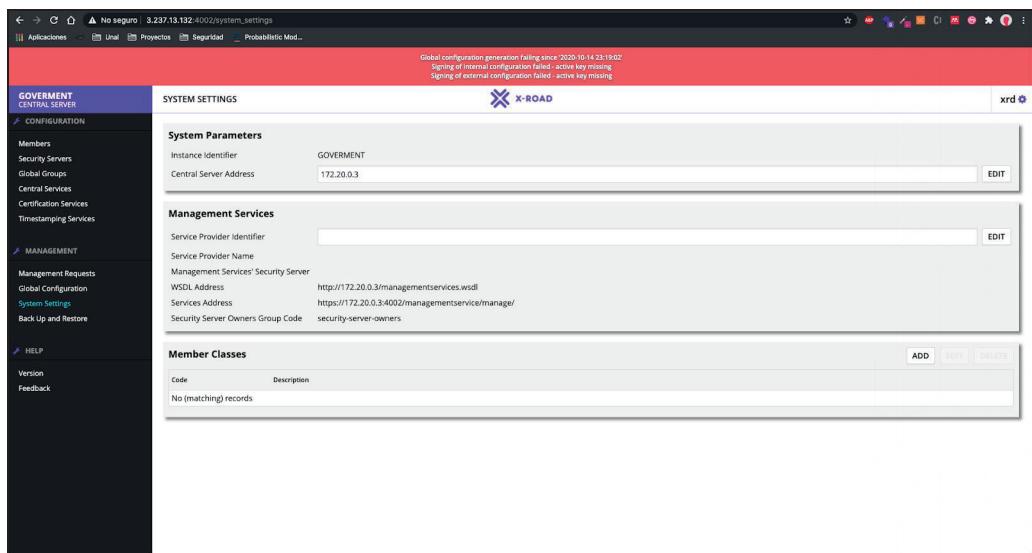
- Al hacer clic en el botón **Submit**, aparecerá un mensaje de confirmación, donde se indica que el Servidor Central ha sido instalado correctamente.



9. 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.



10. Dirigirse a la opción *System Settings*:



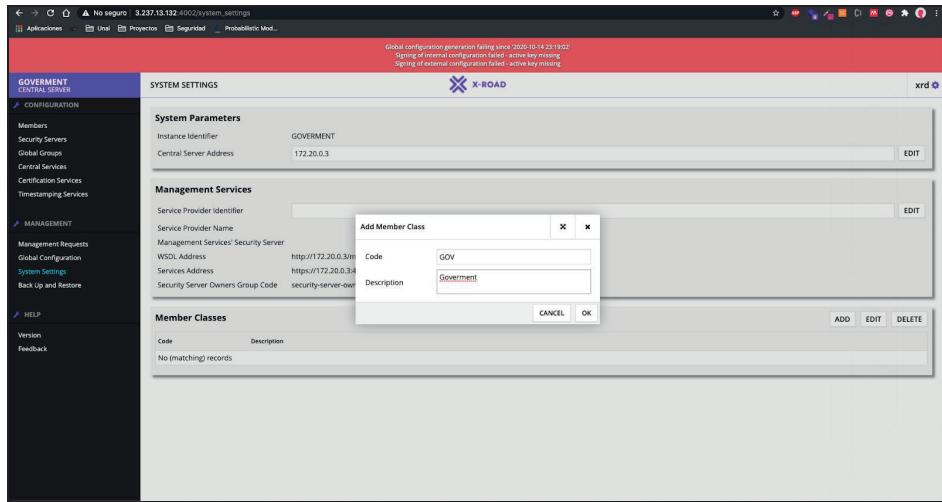
11. En la sección *Member Classes*, hacer clic sobre el botón *Add* agregar un miembro de las clases.



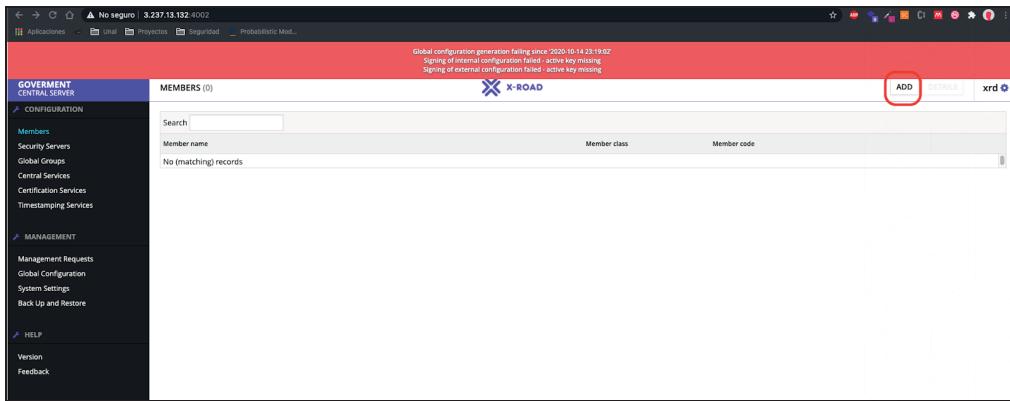
12. En la pestaña que aparecerá, agregar un *Member Class*:

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**.

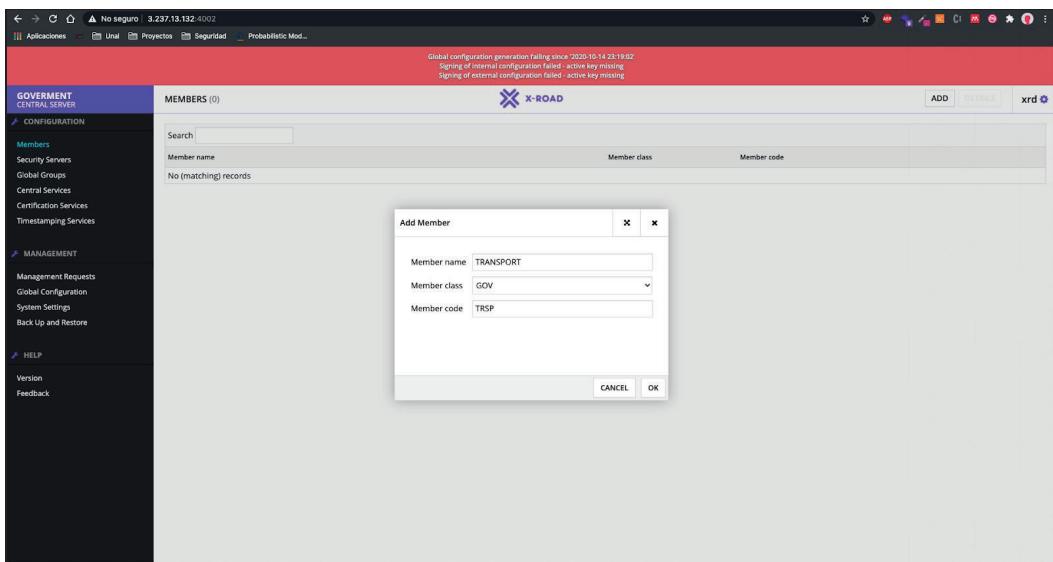


14. Especificar los siguientes datos del miembro:

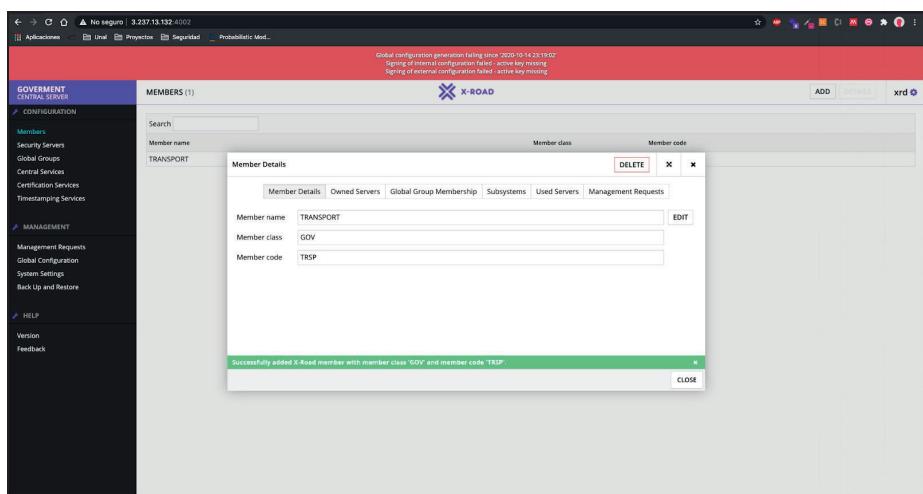
Member name: Transport

Member class: GOV

Member code: TRSP

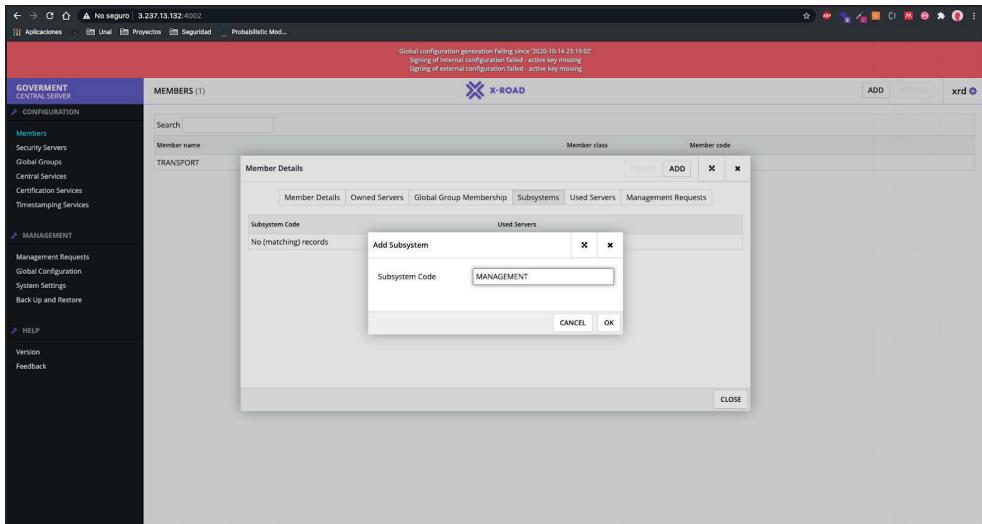


15. Luego de hacer clic en el botón OK, se mostrará un mensaje de confirmación en verde anunciando la creación exitosa del miembro.



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:~$
```



```
[ubuntu@ip-172-31-71-45:~$ sudo docker exec -it 2ef2deeac8cf bash
root@2ef2deeac8cf:/# ]
```

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

```
[● ● ● Descargas — root@2ef2deeac8cf:/home/ca/CA/certs — ssh + sudo — 102x32
root@2ef2deeac8cf:/home/ca/CA/certs# ls
ca.cert.pem  ocsp.cert.pem  tsa.cert.pem
root@2ef2deeac8cf:/home/ca/CA/certs# ]
```

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:

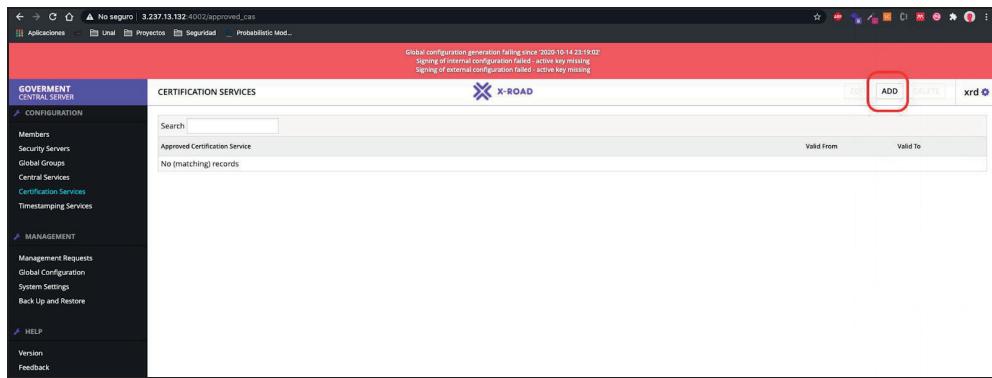
- **sudo docker cp <>ID Contenedor>>:/home/ca/CA/certs/ca.cert.pem .**
- **sudo docker cp <>ID Contenedor>>:/home/ca/CA/certs/ocsp.cert.pem .**
- **sudo docker cp <>ID Contenedor>>:/home/ca/CA/certs/tsa.cert.pem .**

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

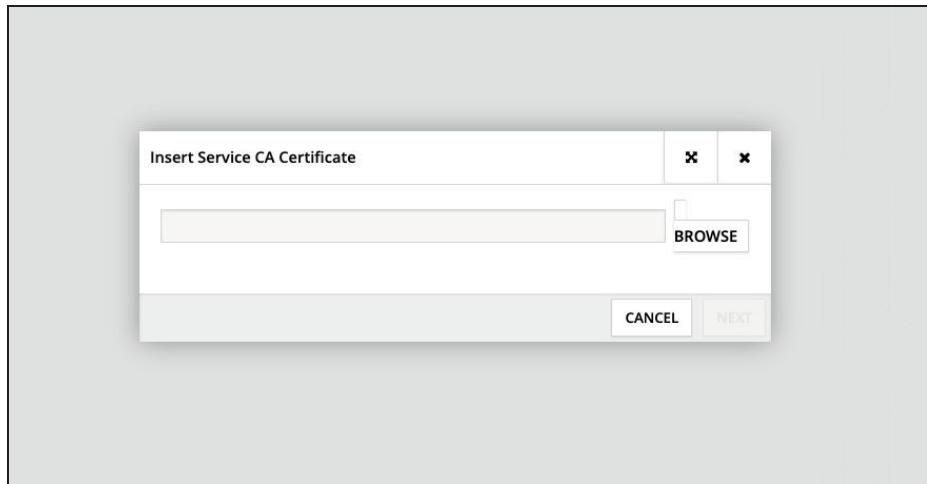
ls

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

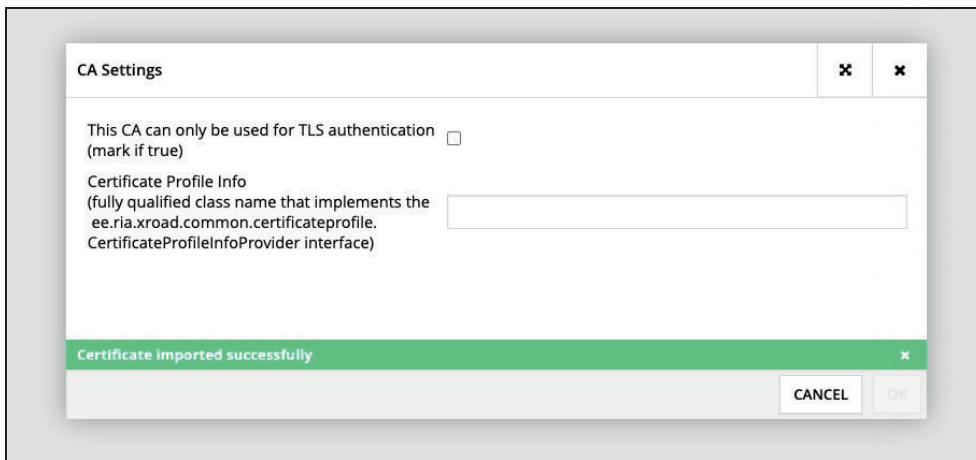
23. Después de realizar esta verificación, ir a la interfaz gráfica de los certificados con el fin de agregarlos como parte de la configuración del servidor central.
24. En la interfaz, ir al enlace “Certification Services” y agregar el certificado **ca.cert.pem** con el botón “Add”.



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

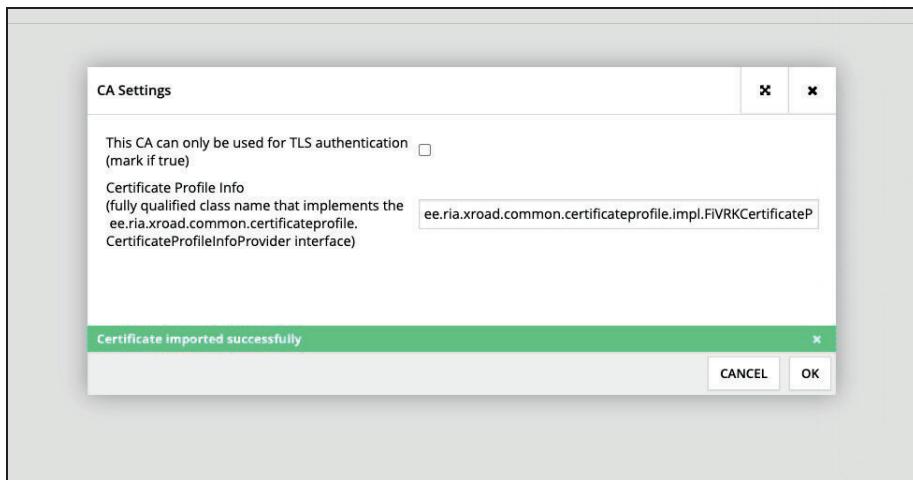


26. Después de cargar el certificado aparecerá la siguiente pantalla, donde aparecerá una ventana con el título de “CA Settings” con un mensaje en color verde confirmando el cargue exitoso del certificado.



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*.



Certification Service CA Details

	CA Certificate	CA Settings	OCSP Responders	Intermediate CAs
Subject Distinguished Name	/C=FI/O=Customized Test/OU=Customized Test CA OU/CN=Customized Test CA CN			
Issuer Distinguished Name	/C=FI/O=Customized Test/OU=Customized Test CA OU/CN=Customized Test CA CN			
Valid From	2020-10-14 23:17:04			
Valid To	2040-10-09 23:17:04			
VIEW CERTIFICATE				
CLOSE				

29. Despu s de llegar a esa pesta a, hacer clic sobre el bot n *Add* para agregar el protocolo de vigencia del certificado (OCSP Responder) agregado anteriormente:

Certification Service CA Details

	EDIT	ADD	DELETE	X	x
	CA Certificate	CA Settings	OCSP Responders	Intermediate CAs	
URL					CLOSE
No (matching) records					CLOSE

30. En la pesta a que aparecer , agregar la especificaci n del *Responder*, donde se deber  agregar la URL del servidor OCSP, donde ir  la IP del Contendor de Docker + el puerto, que generalmente se despliega sobre el puerto 8888.

URL: <IP DOCKER>:8888



Certification Service CA Details

EDIT ADD DELETE × ×

CA Certificate CA Settings OCSP Responders Intermediate CAs

Add OCSP Responder

URL http://172.20.0.3:8888

Certificate

UPLOAD

CANCEL OK

CLOSE

No (mat)

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.

Certification Service CA Details

EDIT ADD DELETE × ×

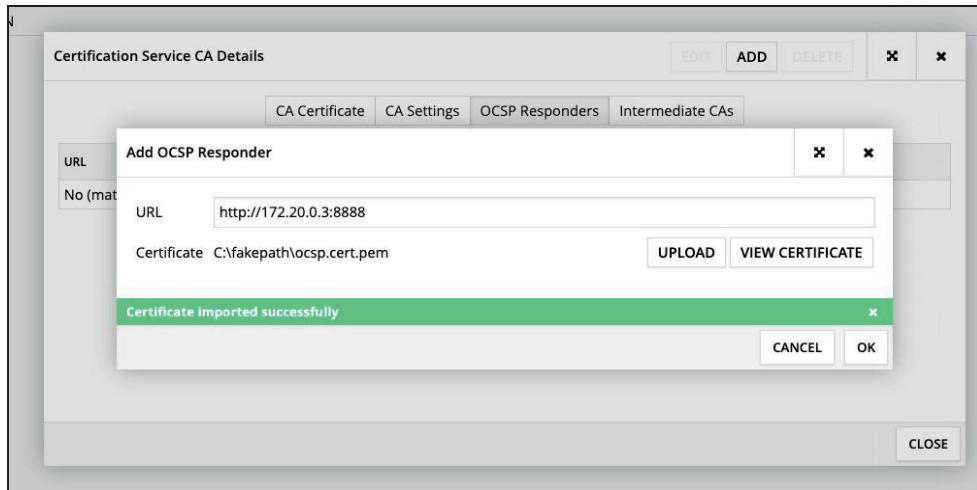
CA Certificate CA Settings OCSP Responders Intermediate CAs

URL http://172.20.0.3:8888

VIEW CERTIFICATE

CLOSE

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

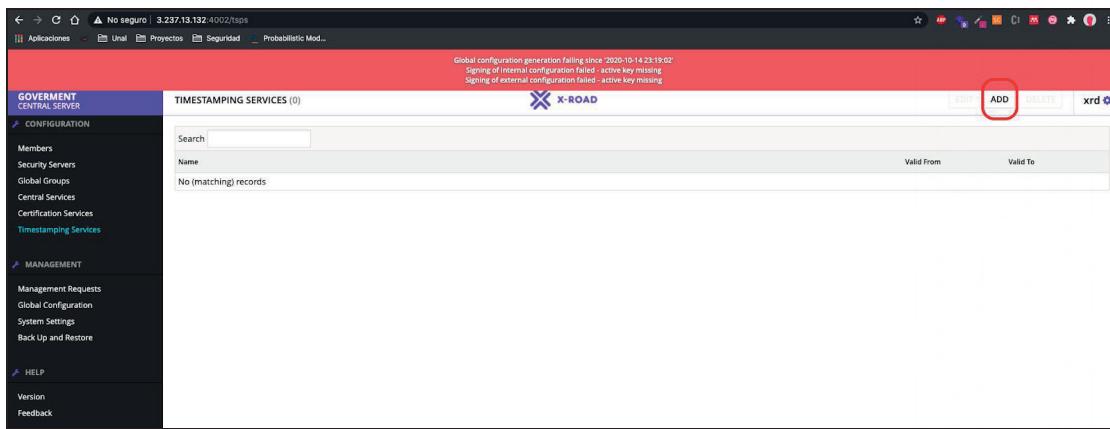


33. Después del mensaje de confirmación, se observará en la opción *Certification Services*, que el certificado ha sido agregado exitosamente.



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.



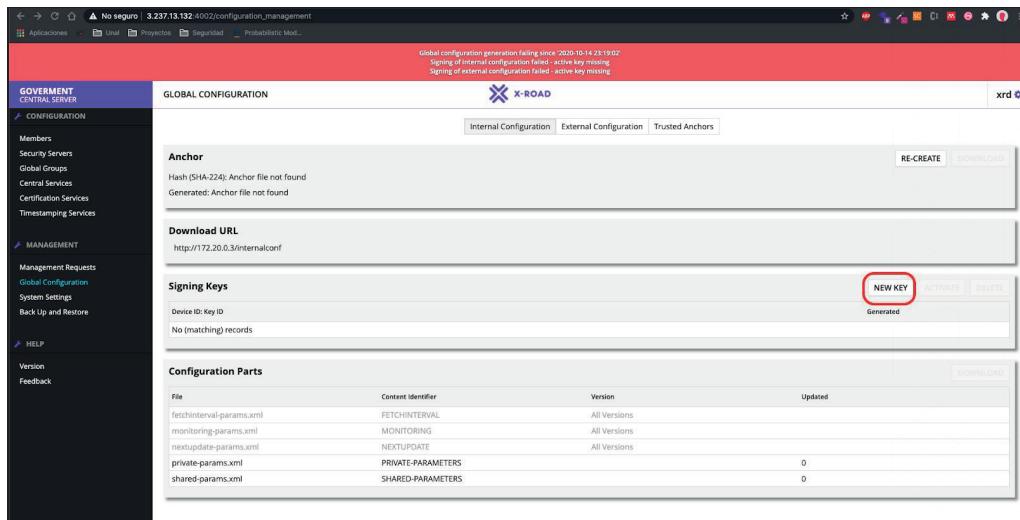
URL: `http://<<IP CONTENEDOR>>:8899`

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.

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	

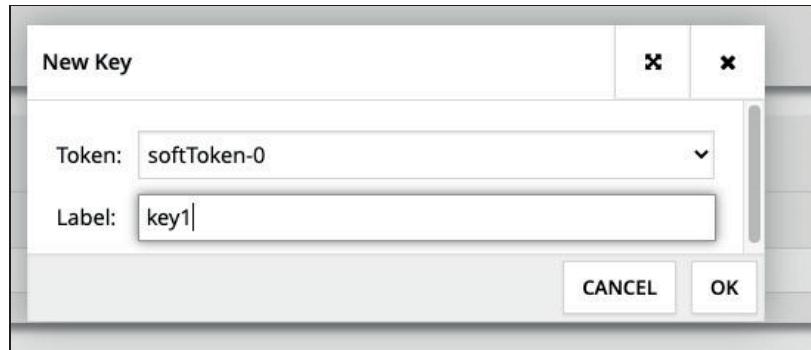
38. Para agregar una llave, hacer clic sobre el botón **NEW KEY**, en la sección *Signing Keys*:



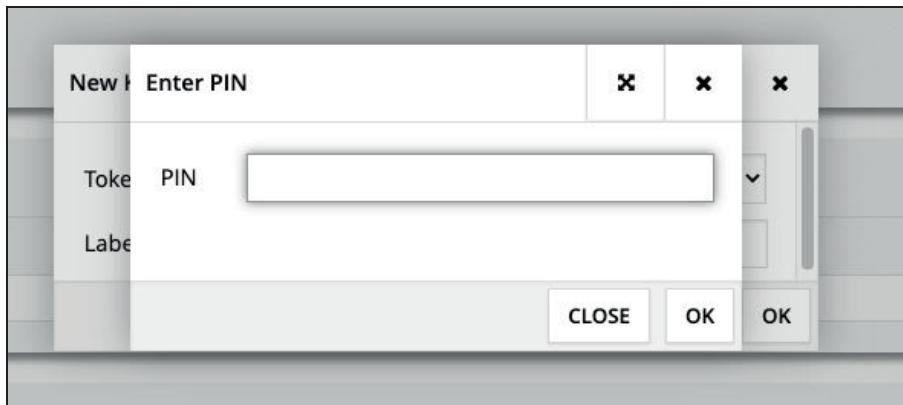
39. Como primera llave, agregar el *token* por defecto y como *label* **key1**.

Token: softToken-0

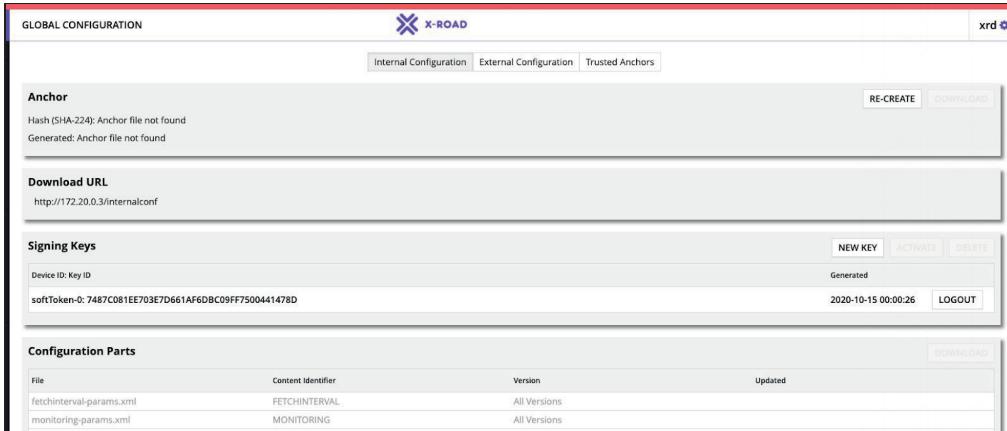
Label: key1



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*.



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

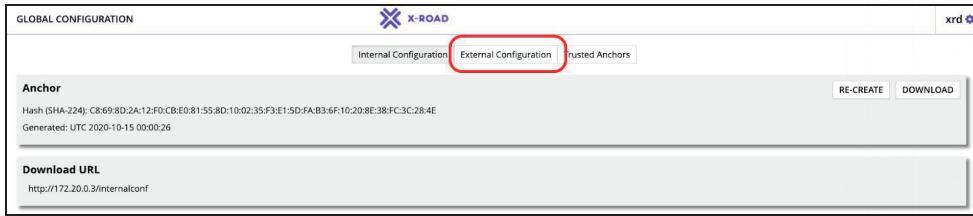
Download URL
<http://172.20.0.3/internalconf>

Signing Keys
Device ID: Key ID
softToken-0: 7487C081EE703E7D661AF6DBC09FF7500441478D
Generated: 2020-10-15 00:00:26 | Logout

Configuration Parts

File	Content Identifier	Version	Updated
fetchinterval-params.xml	FETCHINTERVAL	All Versions	
monitoring-params.xml	MONITORING	All Versions	

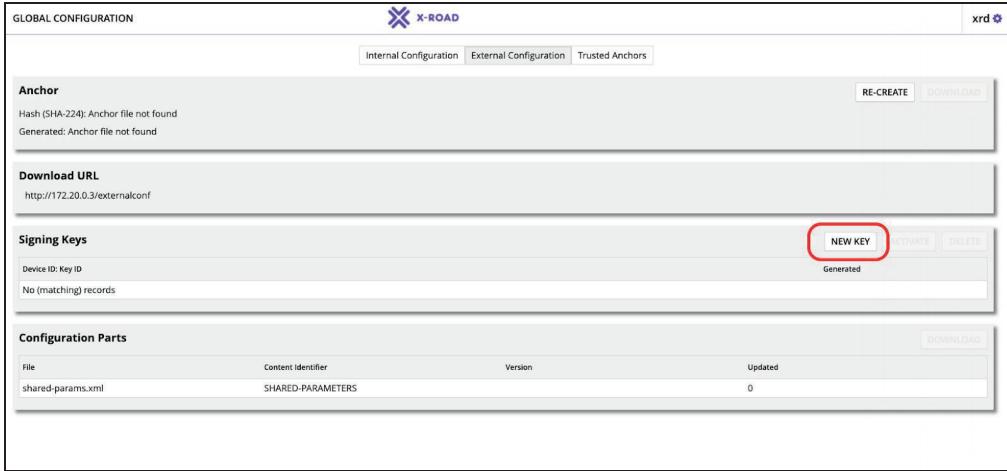
42. Agregar nuevas configuraciones, por medio de la pestaña de *External Configuration*:



Anchor
Hash (SHA-224): C8:69:8D:2A:12:F0:CB:E0:81:55:8D:10:02:35:F3:E1:5D:FA:B3:6F:10:20:8E:38:FC:3C:28:4E
Generated: UTC 2020-10-15 00:00:26

Download URL
<http://172.20.0.3/internalconf>

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



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

Download URL
<http://172.20.0.3/externalconf>

Signing Keys

Device ID: Key ID	Generated
No (matching) records	

Configuration Parts

File	Content Identifier	Version	Updated
shared-params.xml	SHARED-PARAMETERS	0	

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.

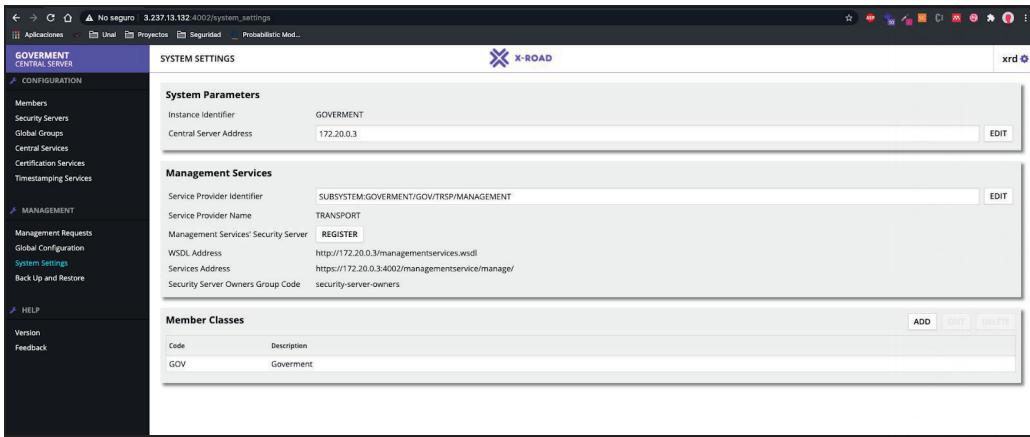
46. Dirigirse al módulo *System Settings* y hacer clic en el módulo *Management Systems*, en el botón EDIT:

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

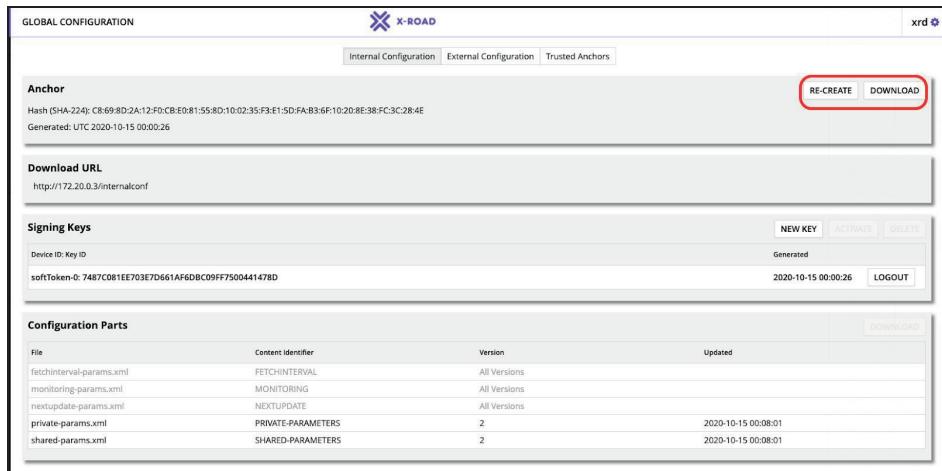
Name	Code	Class	Subsystem	Instance	Type
TRANSPORT	TRSP	GOV	MANAGEMENT	GOVERNMENT	SUBSYSTEM

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)

- 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



The screenshot shows a web browser window with the URL 3.237.13.132:4000/#/login. The page title is "Log in". It contains two input fields: "Username" and "Password", and a "LOG IN" button.

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

Username: xrd
Password: secret

- 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:

The screenshot shows the "Initial configuration" screen. It displays three numbered steps: 1. Configuration Anchor, 2. Owner Member, and 3. Token PIN. Step 1 is active. Below the steps, there is a text field with placeholder text: "Import the configuration anchor provided by the Central Server's administrator." To the right of the text field is a blue "UPLOAD" button, which is highlighted with a red rectangular border. At the bottom right of the screen is a "CONTINUE" button.

- 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.



Configuration Anchor Owner Member Token PIN

Confirm configuration anchor details

Configuration anchor details:

Hash (SHA-224) 7B:00:32:FF:32:B3:34:BD:B2:0A:E3:16:04:94:D8:37:B2:68:BC:DA:53:74:D5:54:A4:67:76:8E
Generated 2020-10-14 19:09

Continue with import?

CANCEL **CONFIRM** **CONTINUE**

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

Initial configuration

Configuration Anchor Owner Member Token PIN

Import the configuration anchor provided by the Central Server's administrator.

UPLOAD

Hash (SHA-224) 7B:00:32:FF:32:B3:34:BD:B2:0A:E3:16:04:94:D8:37:B2:68:BC:DA:53:74:D5:54:A4:67:76:8E
Generated 2020-10-14 19:09

CONTINUE

- 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

1 Configuration Anchor 2 Owner Member 3 Token PIN

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

1 Configuration Anchor 2 Owner Member 3 Token PIN

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.

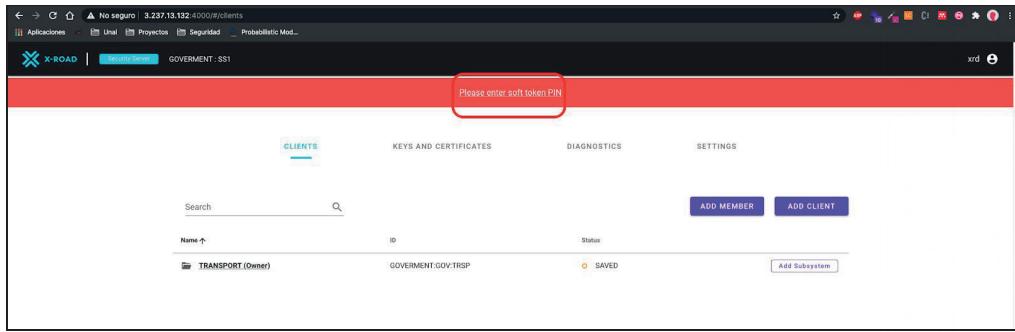
PIN
Confirm PIN

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

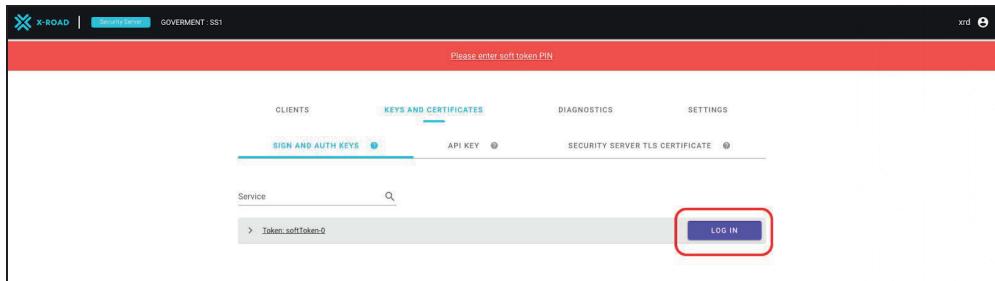
Once the initialisation is done, you must complete the Security Server configuration - simply click the Configure button in the toast notification that will appear in a few moments.

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.

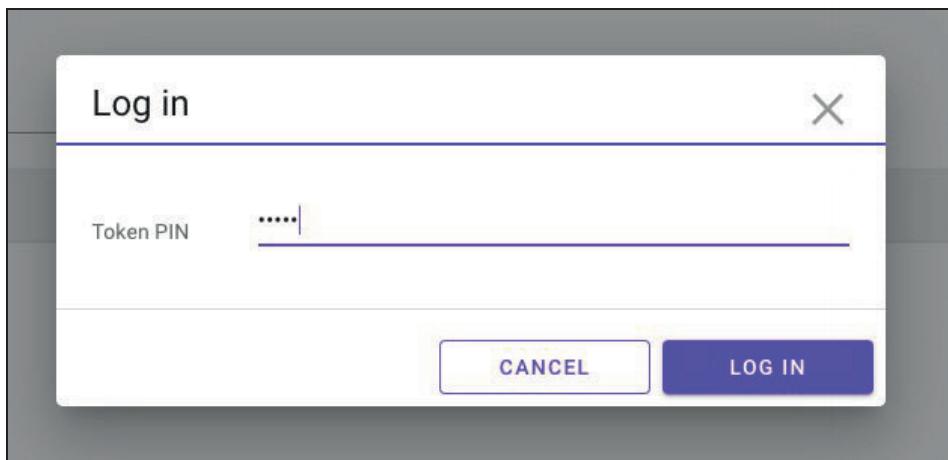


9. Ir a la pantalla **KEYS AND CERTIFICATES**, ubicada en la parte superior de la pantalla.



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

1 Key details 2 CSR details 3 Generate CSR

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

Key Label

15. 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

1 Key details 2 CSR details 3 Generate CSR

Usage AUTHENTICATION

Certification Service Customized Test CA CN

CSR Format DER

16. 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.



The screenshot shows the X-Road configuration interface with the 'KEYS AND CERTIFICATES' tab selected. At the top, there are tabs for 'CLIENTS', 'KEYS AND CERTIFICATES' (highlighted in blue), 'DIAGNOSTICS', and 'SETTINGS'. Below these are sub-tabs: 'SIGN AND AUTH KEYS' (highlighted in blue), 'API KEY', and 'SECURITY SERVER TLS CERTIFICATE'. A search bar labeled 'Service' is present. A dropdown menu shows 'Token: softToken-0'. On the right, there are 'LOG OUT', 'ADD KEY', and 'IMPORT CERT.' buttons. The main area lists 'AUTH Key and Certificate' details: ID, OCSP, Expires, Status, and a 'Generate CSR' button. One entry is shown: 'Auth' (Request) with ID '0F26547074B94FEC3CEAF88589E6550DAF51DF3A' and a 'Delete CSR' button.

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*

The screenshot shows the 'Add key' wizard. Step 1: Key details is selected. A progress bar shows three steps: 1. Key details (selected), 2. CSR details, 3. Generate CSR. A note below says 'You can define a label for the newly created SIGN key (not mandatory)'. The 'Key Label' field contains 'sign'. At the bottom are 'CANCEL' and 'NEXT' buttons.

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

1 Key details 2 CSR details 3 Generate CSR

Usage: SINGING

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

1 Key details 2 CSR details 3 Generate CSR

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-----
MIIECzCCAlmgAwIBAgIBAzANBgkqhkiG9w0BAQsFADBnMQswCQYDVQQGEwJGSTEY
```

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)

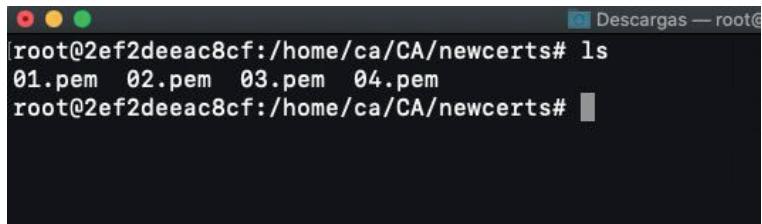
Write out database with 1 new entries
-----BEGIN CERTIFICATE-----
MIETDCCAjSgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBnMQswCQYDVQQGEwJGSTEY
MBYGA1UECgwPQ3VzdG9taXplZCBUXN0MR4wHAYDVQQLDBVdDxN0b21pemVkJFR1
c3QgQQ8gtT1UxhjAcBgNVBAMMFUN1c3RvbWl6ZWQgVGVzdCBDQSBDTjAeFw0yMDEw
MTUwMDQ2MjNaFw00MDExMTAwMDQ2MjNaME0xCzAJBgNVBAYTAkZJMRMwEQQDVQQK
```

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
```



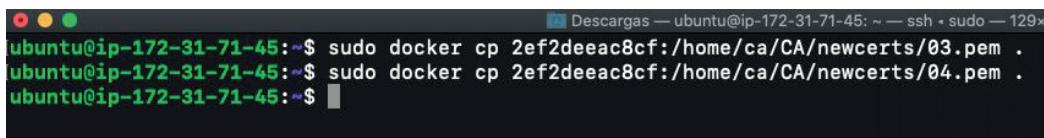
```
root@2ef2deeac8cf:/home/ca/CA/newcerts# ls
01.pem 02.pem 03.pem 04.pem
root@2ef2deeac8cf:/home/ca/CA/newcerts#
```

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**.

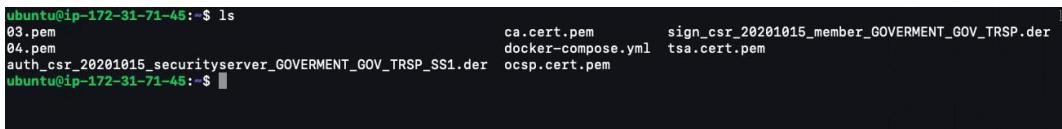
```
sudo docker cp <>ID CONTENEDOR CA>>:/home/ca/CA/newcerts/03.pem .
sudo docker cp <>ID CONTENEDOR CA>>:/home/ca/CA/newcerts/04.pem .
```



```
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*:

AUTH Key and Certificate	ID	OCSP	Expires	Status
Auth	0F26547074B94FEC3CEAF88589E6550DAF51DF3A	Generate CSR	Delete CSR	
Request				

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

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

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

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

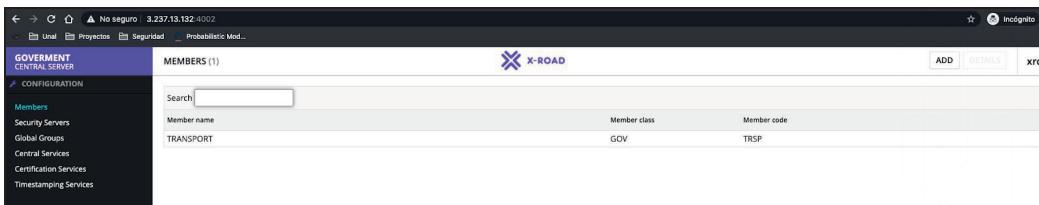
KEYS AND CERTIFICATES				
Service	ID	OCSP	Expires	Status
<input checked="" type="radio"/> Auth	Customized Test CA CN 3	Disabled	2040-10-09	<input checked="" type="radio"/> Saved
<input checked="" type="radio"/> sign	Customized Test CA CN 4	GOVERMENT.GOV:TRSP	Good	<input checked="" type="radio"/> Registered

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

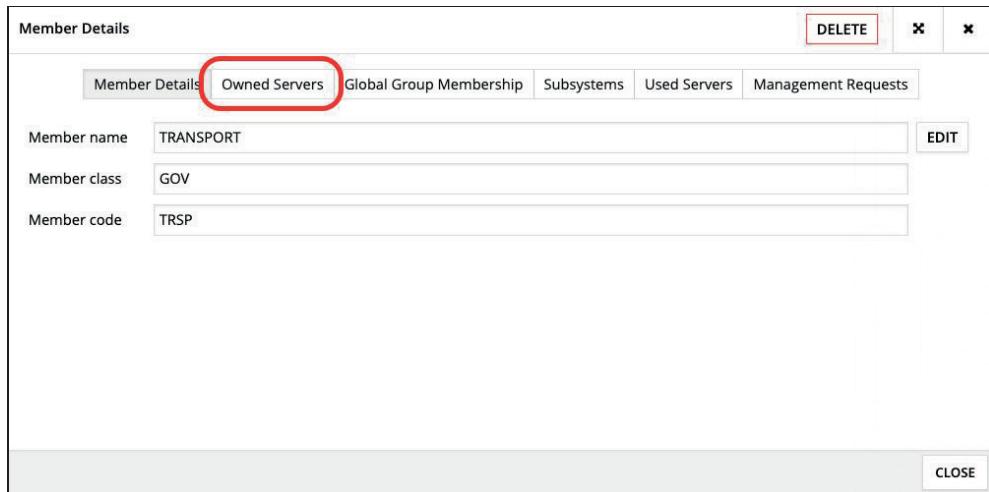
KEYS AND CERTIFICATES				
Service	ID	OCSP	Expires	Status
<input checked="" type="radio"/> Auth	Customized Test CA CN 3	Disabled	2040-10-09	<input checked="" type="radio"/> Saved
<input checked="" type="radio"/> sign	Customized Test CA CN 4	GOVERMENT.GOV:TRSP	Good	<input checked="" type="radio"/> Registered

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.

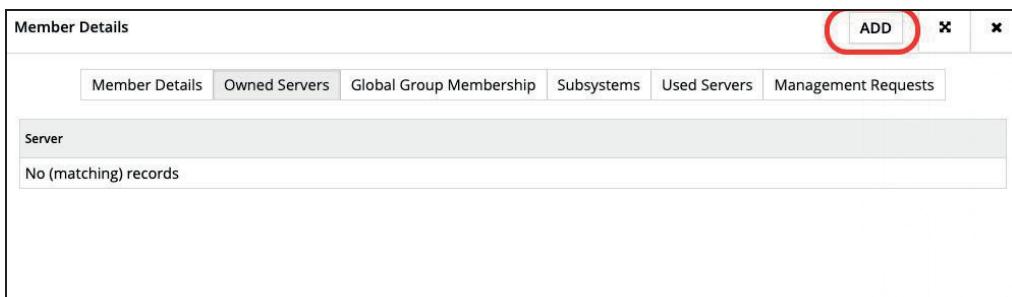
39. ir al módulo **Members** ubicado en el panel izquierdo de la pantalla.



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

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

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

AUTHENTICATION CERTIFICATE INFORMATION

UPLOAD

CA: Customized Test CA CN

Serial Number: 3

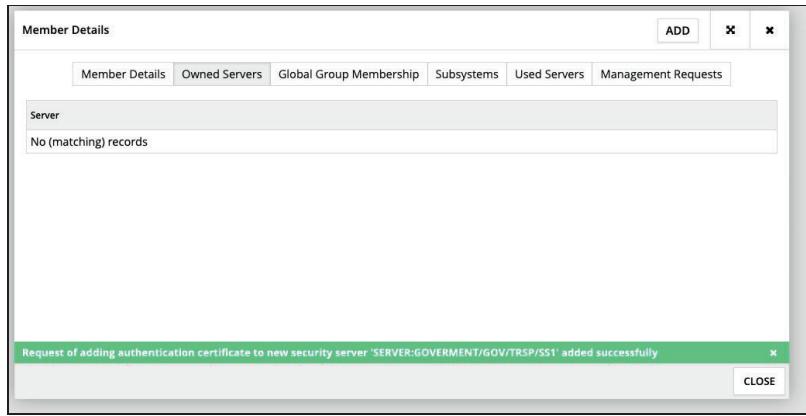
Subject: /C=FI/O=MANAGEMENT/CN=172.20.0.4/serialNumber

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:

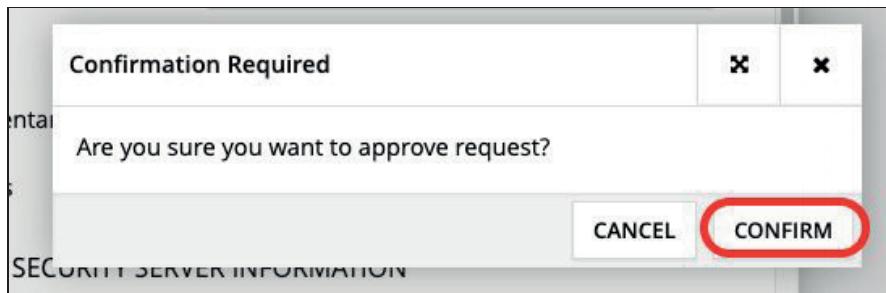
The screenshot shows the 'MANAGEMENT REQUESTS (2)' page. The left sidebar has sections for Configuration (Members, Security Servers, Global Groups, Central Services, Certification Services, Timestamping Services), Management (Management Requests, Global Configuration, System Settings, Back Up and Restore), and Help (Version, Feedback). The main area displays a table with two rows of management requests. The columns are Request ID, Created, Request Type, Source, Server Owner Name, Server Owner Class, Server Owner Code, Server Code, and Status. The data is as follows:

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 three buttons: 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**.



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	REGISTER
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	Goverment

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

Management Service Provider Registration Request

CLIENT INFORMATION

Name	TRANSPORT
Class	GOV
Code	TRSP
Subsystem Code	MANAGEMENT

SECURITY SERVER INFORMATION

Owner Name	
Owner Class	
Owner Code	
Server Code	

SEARCH

CANCEL **SUBMIT**

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

Security Servers

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

Search

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

SEARCH	<input type="button"/>
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:

The screenshot shows the 'CLIENTS' tab of the Security Server interface. It displays a list of clients with columns for Name, ID, and Status (e.g., TRANSPORT.(Owner), GOVERNMENT.GOV:TRSP, REGISTERED). At the top right, there are buttons for 'ADD MEMBER' and 'ADD CLIENT', with 'ADD CLIENT' being highlighted with a red oval.

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.*



The screenshot shows the 'MANAGEMENT (subsystem)' page with the 'SERVICES' tab selected. At the bottom right of the main area, there is a blue button labeled 'ADD WSDL' which is highlighted with a red rectangle.

The screenshot shows the 'SYSTEM SETTINGS' page with the 'Management Services' section. In the 'Management Services' table, the 'WSDL Address' row contains the URL 'http://172.20.0.3/managementservices.wsdl', which is highlighted with a red rectangle.

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.

The screenshot shows the 'MANAGEMENT (subsystem)' page with the 'SERVICES' tab selected. A modal dialog box titled 'Add WSDL' is open. Inside the dialog, there is a single input field labeled 'URL' containing the value 'http://172.20.0.3/managementservices.wsdl', which is highlighted with a red rectangle.



63. Despues 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.

The screenshot shows the 'MANAGEMENT (subsystem)' interface. At the top, there are tabs for 'CLIENTS', 'KEYS AND CERTIFICATES', 'DIAGNOSTICS', and 'SETTINGS'. Below these is a 'UNREGISTER' button. The main area has tabs for 'DETAILS', 'SERVICE CLIENTS', 'SERVICES' (which is highlighted in blue), 'INTERNAL SERVERS', and 'LOCAL GROUPS'. A search bar labeled 'Service' and a 'Refresh' button are also present. A 'WSDL' section shows the URL 'WSDL_(http://172.20.0.3/managementservices.wsdl)'. Below this is a table with columns 'Service Code', 'URL', and 'Timeout'. The listed services are:

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**:

This is a configuration dialog for the 'authCertDeletion' service. It includes fields for 'Service URL' (set to 'http://INSERT_MANAGEMENT_SERVICE_ADDRESS_HERE'), 'Timeout (s)' (set to '60'), and 'Verify TLS certificate' (checked). There is a 'SAVE' button. Below this is an 'Access Rights' section with 'REMOVE ALL' and 'ADD SUBJECTS' buttons, and a table for managing access rights.

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



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

The screenshot shows the 'System Settings' page under the 'GOVERNMENT CENTRAL SERVER' tab. In the 'Management Services' section, the 'Service Provider Identifier' is set to 'SUBSYSTEM:GOVERNMENT/GOV/TRSP/MANAGEMENT' and the 'Service Provider Name' is 'TRANSPORT'. The 'Management Services' Security Server is 'SERVER:GOVERNMENT/GOV/TRSP/SS1' and its WSDL Address is 'http://172.20.0.3/managementservices.wsdl'. The 'Services Address' field is highlighted with a red box and contains the URL 'https://172.20.0.3:4002/managementservice/manage/'. The 'Member Classes' section shows a single entry for 'GOV' with the description 'Government'.

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**.

The dialog box is titled 'authCertDeletion'. It has fields for 'Service URL' (https://172.20.0.3:4002/managementservice/manage/), 'Timeout (s)' (60), and 'Verify TLS certificate' (unchecked). There is a checkbox labeled 'Apply to all in WSDL' which is checked. At the bottom right is a large blue 'SAVE' button, which is also highlighted with a red box. Below the dialog is a section titled 'Access Rights' with buttons for 'REMOVE ALL' and 'ADD SUBJECTS'.

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: <https://172.20.0.3:4002/managementservice/manage/>

Timeout (s): 60

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

		Apply to all in WSDL								
Service URL	https://172.20.0.3:4002/managementservice/manage/	<input checked="" type="checkbox"/>								
Timeout (s)	60	<input checked="" type="checkbox"/>								
Verify TLS certificate	<input type="checkbox"/>	<input checked="" type="checkbox"/>								
		<input type="button" value="SAVE"/>								
Access Rights <div style="display: flex; justify-content: space-between;"> <input type="button" value="REMOVE ALL"/> <input type="button" value="ADD SUBJECTS"/> </div> <table border="1"> <thead> <tr> <th>Member name / Group description</th> <th>ID / Group code</th> <th>Type</th> <th>Access Rights given</th> </tr> </thead> <tbody> <tr> <td>Security server owners</td> <td>GOVERMENT:security-server-owners</td> <td>GLOBALGROUP</td> <td>2020-10-14 20:59</td> </tr> </tbody> </table>			Member name / Group description	ID / Group code	Type	Access Rights given	Security server owners	GOVERMENT:security-server-owners	GLOBALGROUP	2020-10-14 20:59
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="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**.