



El futuro digital
es de todos

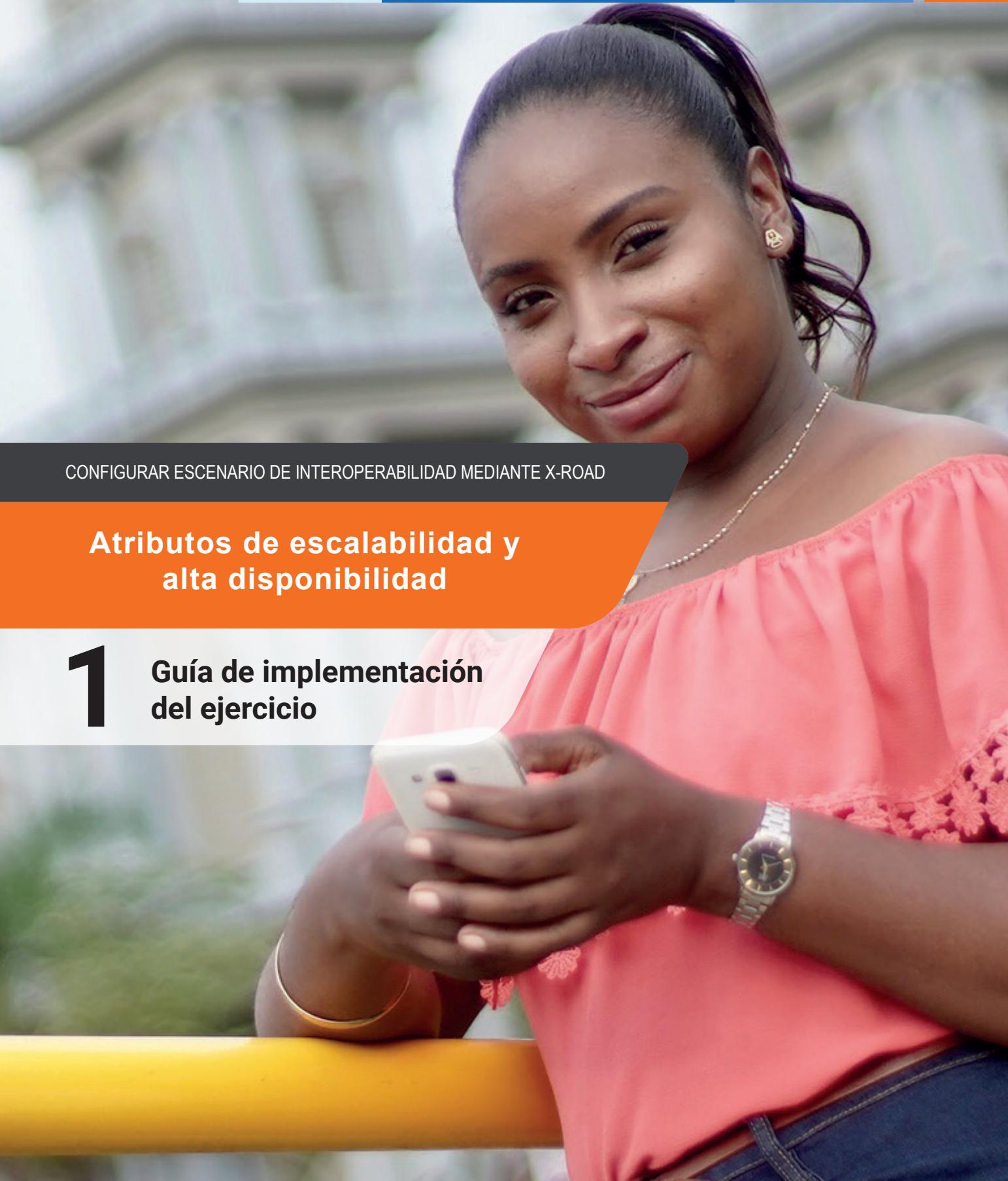
MinTIC



CONFIGURAR ESCENARIO DE INTEROPERABILIDAD MEDIANTE X-ROAD

Atributos de escalabilidad y alta disponibilidad

1 Guía de implementación del ejercicio





Contexto

Este ejercicio de escalabilidad y alta disponibilidad consiste en que el **Departamento de Tránsito** ha recibido reportes constantes de demora y fallas por *timeout* por parte del **Departamento de Tecnología**, quien gestiona las licencias en línea y debe consultar en su sistema de información si un ciudadano identificado por su tipo de documento (alias: `type`) y el número de documento (alias: `document`), posee un registro. El intercambio de información se realiza a través del ecosistema **X-Road**.

Guía de Implementación

Este escenario de escalabilidad y alta disponibilidad consiste en que usted como el actor **Departamento de Tránsito** ha recibido reportes constantes de demora y fallas por *timeout* por parte del **Departamento de Tecnología**, quien gestiona las licencias online y debe consultar en su sistema de información si un ciudadano identificado por su tipo de documento (alias: `type`) y el número de documento (alias: `document`) tiene un registro. El intercambio de información se realiza a través del ecosistema **X-Road**.

Antes de comenzar esta práctica, es necesario realizar todas las configuraciones previas de los diferentes componentes que pertenecen al escenario de interoperabilidad (ver Secciones 2.3 y 3.1).

Descargar o clonar el siguiente repositorio:

<https://github.com/DiplomadoXRoadUNAL2020/high-availability-xroad>

Ubicarse en el directorio raíz `high-availability-xroad/`. Allí se encontrará un archivo **docker-compose.yaml**, y una carpeta con el proyecto del sistema de información del Departamento de Tránsito.

A continuación se listan las variables necesarias para las configuraciones de cada uno de los servidores del ecosistema X-Road. Se encuentran separados de acuerdo con su funcionalidad dentro del ambiente y contienen los parámetros requeridos para que el escenario de prueba funcione correctamente.

Configuración del Servidor Central

SERVIDOR CENTRAL	
Propiedad	Valor
INSTANCE IDENTIFIER	DEV
IP Interna del Contenedor	172.25.0.2
Puerto host de la interfaz gráfica principal del servidor	4000



Puerto host de los servicios expuestos por el servidor	4001
Puerto de la interfaz gráfica, que permite realizar las firmas de los certificados de los servidores de seguridad.	4002
Puerto de la interfaz gráfica que permite descargar los certificados ca, ocsp y tsa	4003
Member Class Code	GOV
Member Class Description	Government

Tabla 1. Configuración del Servidor Central**Configuración del Servidor de Seguridad - Tecnología**

SERVIDOR DE SEGURIDAD - TECNOLOGÍA	
Propiedad	Valor
Server name	TECNOLOGIA-SS
IP Interna del Contenedor	172.25.0.3
Puerto host de la interfaz gráfica principal del servidor	4100
Puerto host de los servicios expuestos por el servidor	4101
Member name	TECNOLOGIA
Member class	GOV
Member code	TECNOLOGIA
Subsystem Code	MANAGEMENT
Subsystem Code	CONSUMER

Tabla 2. Configuración del Servidor de Seguridad - Tecnología**Configuración del Servidor de Seguridad No. 1 - Tránsito**

SERVIDOR DE SEGURIDAD - TRÁNSITO 1	
Propiedad	Valor
Security Server Code	TRANSITO-SS1
IP Interna del Contenedor	172.25.0.4
Puerto host de la interfaz gráfica principal del servidor	4200

Puerto host de los servicios expuestos por el servidor	4201
Member name	TRANSITO
Member class	GOV
Member code	TRANSITO
Subsystem Code	MANAGEMENT
Subsystem Code	PROVIDER

Tabla 3. Configuración del Servidor de Seguridad - Tránsito 1**Configuración del Servidor de Seguridad No. 2 - Tránsito**

SERVIDOR DE SEGURIDAD - TRÁNSITO 2	
Propiedad	Valor
Security Server Code	TRANSITO-SS2
IP Interna del Contenedor	172.25.0.5
Puerto host de la interfaz gráfica principal del servidor	4300
Puerto host de los servicios expuestos por el servidor	4301
Member name	TRANSITO
Member class	GOV
Member code	TRANSITO
Subsystem Code	MANAGEMENT
Subsystem Code	PROVIDER

Tabla 4. Configuración del Servidor de Seguridad - Tránsito 2**Configuración del Sistema de Información - Tránsito**

SISTEMA DE INFORMACIÓN - TRÁNSITO	
Propiedad	Valor
IP de acceso al contenedor	IP
Puerto de acceso al servicio del contenedor	1002

Tabla 5. Configuración del Sistema de Información - Tránsito



- Para iniciar con la parametrización, es necesario subir todos los servicios con el siguiente comando:

```
sudo docker-compose up -d
```

Confirmar que los servicios descritos entre las *tablas 1 y 4* fueron correctamente inicializados. Se deberá observar una salida como la siguiente:

```
Creating network "x-road-network" with driver "bridge"
Creating transito_ss2 ... done
Creating transito_ss1 ... done
Creating xroad_cs      ... done
Creating tecnologia_ss ... done
```

- Configurar el Servidor Central con los siguientes miembros y sus respectivos subsistemas (consultar toda la información en las tablas 2 al 5):

Departamento de Tránsito

Member name	TRANSITO
Member class	GOV
Member code	TRANSITO
Subsystem Code	MANAGEMENT
Subsystem Code	PROVIDER

Tabla 6. Configuración de miembro del Departamento de Tránsito.

Departamento de Tecnología

Member name	TECNOLOGIA
Member class	GOV
Member code	TECNOLOGIA
Subsystem Code	MANAGEMENT
Subsystem Code	CONSUMER

Tabla 7. Configuración de miembro del Departamento de Tecnología

Es muy importante recordar que se pueden descargar los certificados ca.cert.pem,



`ocsp.cert.pem` y `tsa.cert.pem` a través de la interfaz gráfica en la IP del contenedor del servidor de seguridad (por defecto configurada en <http://172.25.0.2:8888/testca/certs/>).

3. Iniciar la configuración de los tres servidores de seguridad con base en la información presentada en las tablas 3 y 4.
4. En cada uno de los servidores de seguridad del punto anterior, crear las llaves de firma y autenticación (Sign - Authentication), con la siguiente información:

Llave Sign

Key Label	sign
Usage	SIGNING
Client	DEV:GOV:TRANSITO
Certification Service	Customized Test CA CN
CSR Format	DER
Organization Name (O)	TRANSITO

Tabla 8. Configuración de la llave de firma

Llave Authentication

Key Label	auth
Usage	AUTHENTICATION
Certification Service	Customized Test CA CN
CSR Format	DER
Organization Name (O)	TRANSITO
Server DNS name (CN)	<<IP interna del Contenedor>>

Tabla 9. Configuración de la llave de autenticación

Firmar las llaves en el servicio expuesto en el servidor central (se puede hacer mediante la configuración por defecto para este ejercicio, a través de la IP interna del contenedor <http://172.25.0.2:9998> o por el puerto host <http://localhost:4002>).

Se recomienda hacer una a una la creación y firma para evitar confusiones. Cuando se realice la asociación de los servidores al miembro TRANSITO, se debe completar el *Service Code* correspondiente para cada uno de los registros en el servidor de seguridad.

Al finalizar el proceso se debe observar en el servidor central, en **CONFIGURATION > Members**, los servidores de seguridad asociados a **TRANSITO**, en la pestaña **Owned Servers**.

Member Details

Member Details	Owned Servers	Global Group Membership	Subsystems	Used Servers	Management Requests
Server					
<u>TRANSITO-SS1</u>					
<u>TRANSITO-SS2</u>					

CLOSE

- Una vez asociados los servidores, se debe realizar el registro del subsistema de administración. Para esto, hay que dirigirse a la sección **MANAGEMENT > Systems Settings > Management Services**. Luego, se debe seleccionar el subsistema **Management** del miembro **TRANSITO** en el campo **Service Provider Identifier** y hacer clic en el botón de **REGISTER**.

Management Services

Service Provider Identifier	SUBSYSTEM:DEV/GOV/TRANSITO/ MANAGEMENT	EDIT
Service Provider Name	TRANSITO	
Management Services' Security Server	REGISTER	
WSDL Address	http://172.25.0.2/managementservices.wsdl	
Services Address	https://172.25.0.2:4002/managementservice/manage/	
Security Server Owners Group Code	security-server-owners	

Buscar y seleccionar el servidor de seguridad con código TRANSITO-SS1. Validar la correcta selección del servidor de seguridad. Se debe observar en la sección de **Management Services**, lo siguiente:

Management Services

Service Provider Identifier	SUBSYSTEM:DEV/GOV/TRANSITO/ MANAGEMENT	EDIT
Service Provider Name	TRANSITO	
Management Services' Security Server	SERVER:DEV/GOV/TRANSITO/TRANSITO-SS1	
WSDL Address	http://172.25.0.2/managementservices.wsdl	
Services Address	https://172.25.0.2:4002/managementservice/manage/	
Security Server Owners Group Code	security-server-owners	

- Realizar en el servidor de seguridad, la inscripción del subsistema **MANAGEMENT** con código **TRANSITO-SS1**. Este proceso se puede realizar haciendo clic en **Add Subsystem**, el cual se encuentra al mismo nivel de **TRANSITO (Owner)**, luego hacer clic en **SELECT SUBSYSTEM** y



seleccionar el subsistema correspondiente a **MANAGEMENT**. Este proceso es similar al realizado en los escenarios anteriores.

7. Añadir el WSDL del subsistema, modificar la URL de los servicios con el valor del **Service Address** suministrado en el paso anterior, y añadir los privilegios al miembro **Security server owners**.

The screenshot shows a table listing four service codes with their URLs and timeouts. The columns are Service Code, URL, and Timeout. The rows are:

Service Code	URL	Timeout
authCertDeletion	https://172.25.0.2:4002/managementservice/manage/	60
clientDeletion	https://172.25.0.2:4002/managementservice/manage/	60
clientReg	https://172.25.0.2:4002/managementservice/manage/	60
ownerChange	https://172.25.0.2:4002/managementservice/manage/	60

La siguiente imagen se podrá observar cuando se accede a cada uno de los **Service Code** (authCertDeletion, clientDeletion, clientReg, ownerChange).

The screenshot shows a table of access rights. The columns are Member name / Group description, ID / Group code, Type, and Access Rights given. There is one entry:

Member name / Group description	ID / Group code	Type	Access Rights given
Security server owners	DEV:security-server-owners	GLOBALGROUP	2020-11-12 00:17

8. Realizar la suscripción del subsistema de administración en el servidor de seguridad con código **TRANSITO-SS2** tal como se realizó en el paso anterior (por el momento, omitir la inscripción del WSDL y los servicios). Al enviar la solicitud se podrá observar lo siguiente (presar atención al estado reportado en el lado derecho):

The message indicates that the registration for the MANAGEMENT subsystem is in progress.

9. Para terminar el registro, ir al servidor central en la sección **CONFIGURATION > Security Servers** y añadir el servidor de seguridad **TRANSITO-SS2** como cliente del subsistema **MANAGEMENT** del miembro **TRANSITO**.

DEV 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

SECURITY SERVERS (2)

X-ROAD

Search		DETAILS	xrd 
Server Code	Owner Name	Owner Class	Owner Code
TRANSITO-SS1	TRANSITO	GOV	TRANSITO
TRANSITO-SS2	TRANSITO	GOV	TRANSITO

Security Server Details

ADD **DELETE** **x** **x**

Security Server Details			
Clients			
Authentication Certificates			
Management Requests			
Name	Class	Code	Subsystem Code
No (matching) records			

CLOSE

Buscar el servidor de seguridad requerido, como se evidencia a continuación:

New Client Registration Request

CLIENT INFORMATION

SEARCH

Name	<input type="text"/>
Class	<input type="text"/>
Code	<input type="text"/>
Subsystem Code	<input type="text"/>



Search Member					
<input type="text" value="Search"/> X X					
Name	Code	Class	Subsystem	Instance	Type
TECNOLOGIA	TECNOLOGIA	GOV		DEV	MEMBER
TECNOLOGIA	TECNOLOGIA	GOV	MANAGEMENT	DEV	SUBSYSTEM
TECNOLOGIA	TECNOLOGIA	GOV	CONSUMER	DEV	SUBSYSTEM
TRANSITO	TRANSITO	GOV		DEV	MEMBER
TRANSITO	TRANSITO	GOV	MANAGEMENT	DEV	SUBSYSTEM
TRANSITO	TRANSITO	GOV	PROVIDER	DEV	SUBSYSTEM

CANCEL SELECT

10. Luego de realizado el proceso anterior, en la sección **MANAGEMENT > Management Requests** se podrá observar como pendientes de aprobación, la solicitud del servidor de seguridad realizada en el paso 7 y la solicitud realizada en el paso anterior:

Request ID	Created	Request Type	Source	Server Owner Name	Server Owner Class	Server Owner Code	Server Code	Status
7	2020-11-12 05:44:36	Client registration	X-Road center	TRANSITO	GOV	TRANSITO	TRANSITO-SS2	SUBMITTED FOR APPROVAL
6	2020-11-12 05:22:35	Client registra...	Security server	TRANSITO	GOV	TRANSITO	TRANSITO-SS2	SUBMITTED...
5	2020-11-12 04:50:13	Client registra...	X-Road center	TRANSITO	GOV	TRANSITO	TRANSITO-SS1	APPROVED
4	2020-11-12 04:40:53	Certificate reg...	X-Road center	TRANSITO	GOV	TRANSITO	TRANSITO-SS2	APPROVED
3	2020-11-12 04:40:31	Certificate reg...	Security server	TRANSITO	GOV	TRANSITO	TRANSITO-SS2	APPROVED
2	2020-11-12 04:29:15	Certificate reg...	X-Road center	TRANSITO	GOV	TRANSITO	TRANSITO-SS1	APPROVED
1	2020-11-12 04:27:21	Certificate reg...	Security server	TRANSITO	GOV	TRANSITO	TRANSITO-SS1	APPROVED

Aceptar una de las dos solicitudes.

11. Pasados unos minutos, se podrá observar en el servidor de seguridad con código **TRANSITO-SS2** el estado **REGISTERED** para el subsistema **MANAGEMENT**:

	MANAGEMENT	DEV:GOV:TRANSITO:MANAGEMENT	● REGISTERED
--	-------------------	-----------------------------	---

De igual forma, se podrá observar en el servidor central, en la sección **MANAGEMENT > System Settings** la siguiente información:



Management Services

Service Provider Identifier	SUBSYSTEM:DEV/GOV/TRANSITO/MANAGEMENT	EDIT
Service Provider Name	TRANSITO	
Management Services' Security Server	SERVER:DEV/GOV/TRANSITO/TRANSITO-SS1; SERVER:DEV/GOV/TRANSITO/TRANSITO-SS2	
WSDL Address	http://172.25.0.2/managementservices.wsdl	
Services Address	https://172.25.0.2:4002/managementservice/manage/	
Security Server Owners Group Code	security-server-owners	

Revisar que en el campo **Management Services' Security Server** se encuentren registrados los dos servidores de seguridad dispuestos para el sistema de información de Tránsito.

12. En el servidor de seguridad con código **TRANSITO-SS2**, añadir los servicios de administración del subsistema **MANAGEMENT** con el WSDL (completar los pasos que se omitieron en el punto 7).

▼ [WSDL \(http://172.25.0.2/managementservices.wsdl\)](http://172.25.0.2/managementservices.wsdl)

Last refreshed: 2020-11-12 00:14 [Refresh](#)

Service Code	URL	Timeout
authCertDeletion	https://172.25.0.2:4002/managementservice/manage/	60
clientDeletion	https://172.25.0.2:4002/managementservice/manage/	60
clientReg	https://172.25.0.2:4002/managementservice/manage/	60
ownerChange	https://172.25.0.2:4002/managementservice/manage/	60

13. Ahora, para los dos servidores de seguridad (**TRANSITO-SS1** y **TRANSITO-SS2**) añadir el subsistema **PROVIDER**, que permitirá exponer los servicios del sistema de información del departamento de Tránsito. Para este punto puede guiarse de los pasos ejecutados anteriormente (del punto 7 al punto 10)

Al finalizar, se deberá observar lo siguiente:



Name ↑	ID	Status
TRANSITO (Owner)	DEV:GOV:TRANSITO	● REGISTERED
MANAGEMENT	DEV:GOV:TRANSITO:MANAGEMENT	● REGISTERED
PROVIDER	DEV:GOV:TRANSITO:PROVIDER	● REGISTERED

14. Para finalizar la configuración, se deben añadir los servicios al subsistema **PROVIDER**.

Recordar que el sistema de información de Tránsito posee dos servicios REST. El primero de ellos permite consultar mediante un GET si un ciudadano ya se encuentra registrado dentro del sistema. El segundo permite crear un ciudadano en el sistema mediante una petición POST. El detalle se encuentra consolidado en la siguiente tabla.

Servicio	Método	URL de acceso
<i>hasRegistry</i>	GET	http://IP:1002/citizen/runt-registry
<i>createRegistry</i>	POST	http://IP:1002/citizen/transit-registry/create

Tabla 10. Información del servicio del sistema de información de Tránsito.

Para la configuración, acceder al subsistema de **PROVIDER** haciendo clic en él. Acceder a la sección de **SERVICES** y hacer clic al botón **ADD REST**:

The screenshot shows the 'PROVIDER (subsystem)' configuration page. At the top, there are tabs for 'CLIENTS', 'KEYS AND CERTIFICATES', 'DIAGNOSTICS', and 'SETTINGS'. Below these, there is a 'UNREGISTER' button. A horizontal navigation bar includes 'DETAILS', 'SERVICE CLIENTS', 'SERVICES' (which is highlighted with a yellow box), 'INTERNAL SERVERS', and 'LOCAL GROUPS'. Under the 'SERVICES' tab, there is a search bar labeled 'Service' and a 'Q' icon. Below the search bar, it says 'No matching records'. To the right of the search bar are two buttons: 'ADD REST' (highlighted with a red box) and 'ADD WSDL'.

Crear los servicios de acuerdo con la siguiente información. Reemplazar los campos **URL** y **Service Code** de la tabla 11 con los valores correspondientes de la tabla 10.



URL type	REST API Base Path
URL	<<URL de acceso>>
Service Code	<<Servicio>>

Tabla 11. Configuración de los servicios REST.

Al finalizar, se debe observar lo que se presenta en la siguiente imagen.

REST (http://35.223.30.195:1002/citizen/runt-registry)		
Last refreshed: 2020-11-12 03:02		
Service Code	URL	Timeout
hasRegistry	http://35.223.30.195:1002/citizen/runt-registry	60

REST (http://35.223.30.195:1002/citizen/transit-registry/create)		
Last refreshed: 2020-11-12 03:12		
Service Code	URL	Timeout
createRegistry	http://35.223.30.195:1002/citizen/transit-registry/create	60

15. Para permitir el acceso, se debe configurar el *endpoint* y los permisos requeridos.

Ingresar al servicio haciendo clic en el valor del **Service Code** (hasRegistry o createRegistry) y seleccionar la pestaña **ENDPOINTS**:

SERVICE PARAMETERS		ENDPOINTS
		ADD ENDPOINT
HTTP Request Method		Path

Hacer clic en **ADD ENDPOINT** y seleccionar el método HTTP según corresponda. Dejar el path por defecto (/). Por ejemplo, el servicio hasRegistry utiliza el método GET, por lo tanto debería ver observarse de la siguiente manera:



Add Endpoint X

HTTP Request Method	GET
Path	/
Paths is relative to the API base path, e.g. '/pets'. The asterisk (*) can be used as a wildcard. * = match one path segment. ** = match zero or more segments, e.g. '/pets/**'. Path parameters must be replaced with an asterisk, e.g. '/pets/{id}/images' => '/pets/*/images'.	
CANCEL ADD	

(Si el método HTTP de consulta es un POST, deberá seleccionar un POST)

Luego se requiere brindar acceso a los clientes que utilizarán el Endpoint. Para ello, acceder al botón de **Access Rights**:

SERVICE PARAMETERS		ENDPOINTS	
		ADD ENDPOINT	
HTTP Request Method	Path		
GET	/	Edit	Access Rights

Buscar todos los subsistemas y los miembro especificados:

Add Subjects X

Name	Instance		
Member class	Member group code		
Subsystem code	Subject type		
SEARCH			
Member name / Group description	ID / Group code	Type	
<input type="text"/> <input type="text"/> <input type="text"/>			
		CANCEL	ADD SELECTED

Seleccionar y añadir el subsistema de **CONSUMER** del miembro **TECNOLOGIA**.

Add Subjects X

Member name / Group description	ID / Group code	Type
<input type="checkbox"/> Security server owners	DEV:security-server-owners	GLOBALGROUP
<input checked="" type="checkbox"/> TECNOLOGIA	DEV:GOV:TECNOLOGIA:CONSUMER	SUBSYSTEM
<input type="checkbox"/> TECNOLOGIA	DEV:GOV:TECNOLOGIA:MANAGEMENT	SUBSYSTEM
<input type="checkbox"/> TRANSITO	DEV:GOV:TRANSITO:MANAGEMENT	SUBSYSTEM
<input type="checkbox"/> TRANSITO	DEV:GOV:TRANSITO:PROVIDER	SUBSYSTEM
<input type="button" value="CANCEL"/> <input type="button" value="ADD SELECTED"/>		

Como resultado, se deberá observar lo siguiente:

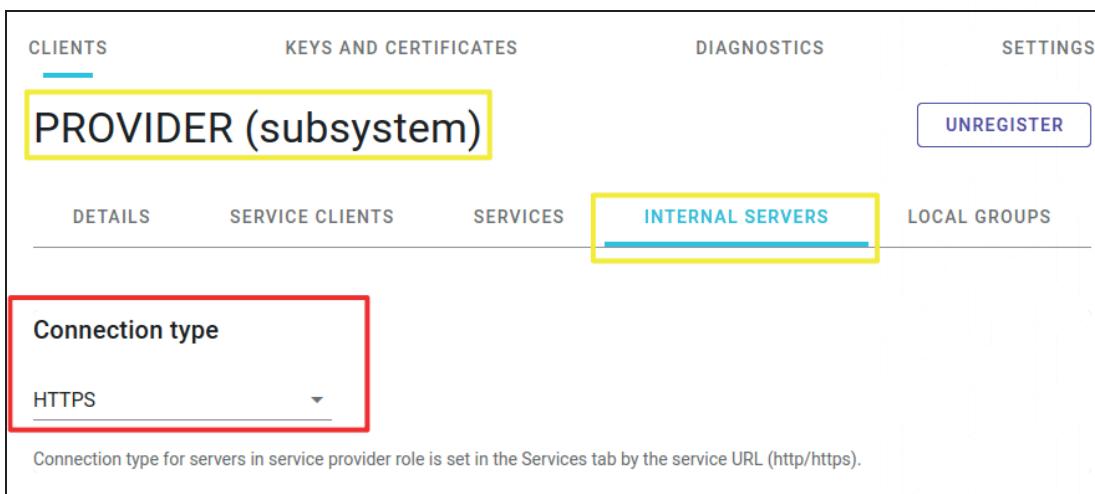
Access Rights		REMOVE ALL	ADD SUBJECTS
Member Name / Group Description	ID	Access Rights given	
TECNOLOGIA	DEV:GOV:TECNOLOGIA:CONSUMER	2020-11-12 23:30	Remove

Adicionalmente, se requiere añadir acceso al servicio general. Para ello, ubicarse al final de la pestaña **SERVICE PARAMETERS** y añadir los privilegios de acceso al subsistema **CONSUMER** del miembro **TECNOLOGIA** (este paso, es muy similar al anterior).

SERVICE PARAMETERS		ENDPOINTS	
Service URL <small>?</small>	http://35.223.30.195:1002/citizen/runt-registry		
Timeout (s) <small>?</small>	60	<input type="button" value="▲"/> <input type="button" value="▼"/>	
Verify TLS certificate <small>?</small>	<input type="checkbox"/>		
SAVE			
Access Rights			
Member name / Group description	ID / Group code	Type	Access Rights given
CLOSE			

Se debe realizar esta configuración para los servicios **hasRegistry** y **createRegistry**

16. Ahora, se deberá habilitar el tráfico de red en texto plano HTTP para ambos servicios. Nuevamente, ubicarse sobre el subsistema **PROVIDER** seleccionar la pestaña **INTERNAL SERVERS** y visualizar el campo **Connection type**

PROVIDER (subsystem)

INTERNAL SERVERS

Connection type

HTTPS

Connection type for servers in service provider role is set in the Services tab by the service URL (http/https).

Cambiar el valor HTTPS por HTTP.

17. Para finalizar, configurar el servidor de seguridad del sistema de información de Tecnología (ver sección 2.3).

Pruebas de Alta Disponibilidad

Se realizarán las pruebas de alta disponibilidad, simulando la falla de uno de los servidores de seguridad.

1. Realizar una petición desde Postman al servidor de seguridad de Tecnología. Así como en el escenario básico de interoperabilidad, Postman simulará las peticiones del sistema de información de Tecnología.

Configurar la petición de la siguiente manera:

- Método HTTP (en la lista desplegable): método GET
- Request URL (en la entrada de texto junto al método):
`http://localhost:4101/r1/DEV/GOV/TRANSITO/PROVIDER/allowedMethods`
- Pestaña Headers (bajo la entrada de texto de la URL): añadir la siguiente cabecera HTTP:

X-Road-Client DEV/GOV/TECNOLOGIA/CONSUMER



```

1  {
2      "service": [
3          {
4              "member_class": "GOV",
5              "member_code": "TRANSITO",
6              "subsystem_code": "PROVIDER",
7              "service_code": "hasRegistry",
8              "object_type": "SERVICE",
9              "xroad_instance": "DEV"
10         },
11         {
12             "member_class": "GOV",
13             "member_code": "TRANSITO",
14             "subsystem_code": "PROVIDER",
15             "service_code": "createRegistry",
16             "object_type": "SERVICE",
17             "xroad_instance": "DEV"
18         }
19     ]
20 }
```

Si la respuesta es un error o un arreglo vacío, revisar las configuraciones realizadas en la sección anterior

2. Probar el alcance al servicio del sistema de información de Tránsito.

Configurar la petición de la siguiente manera:

- Método HTTP (en la lista desplegable): método GET
- Request URL (en la entrada de texto junto al método):
`http://localhost:4101/r1/DEV/GOV/TRANSITO/PROVIDER/hasRegistry?document=16590399020&type=1`
- Pestaña Headers (bajo la entrada de texto de la URL); añadir la siguiente cabecera HTTP:

X-Road-Client DEV/GOV/TECNOLOGIA/CONSUMER

La respuesta debe ser la siguiente:

```

1  {
2      "hasRegistry": false,
3      "registryID": 0
4 }
```

3. Una vez se haya podido verificar el alcance al servicio de Tránsito, simular la falla del servidor de seguridad de Tránsito TRANSITO-SS1. En la consola ubicarse en el directorio donde se encuentra el proyecto del presente escenario y ejecutar el siguiente comando:

```
sudo docker-compose stop transito_security_server1
```

Como resultado se deberá obtener lo siguiente:

```
Stopping transito_ss1 ... done
```



Este comando detendrá el contenedor, simulando una falla completa del servidor.

- Realizar nuevamente la petición mediante Postman. Aunque puede demorarse un poco en reaccionar la primera vez, el servicio deberá continuar respondiendo:

```

1  [
2      "hasRegistry": false,
3      "registryID": 0
4 ]

```

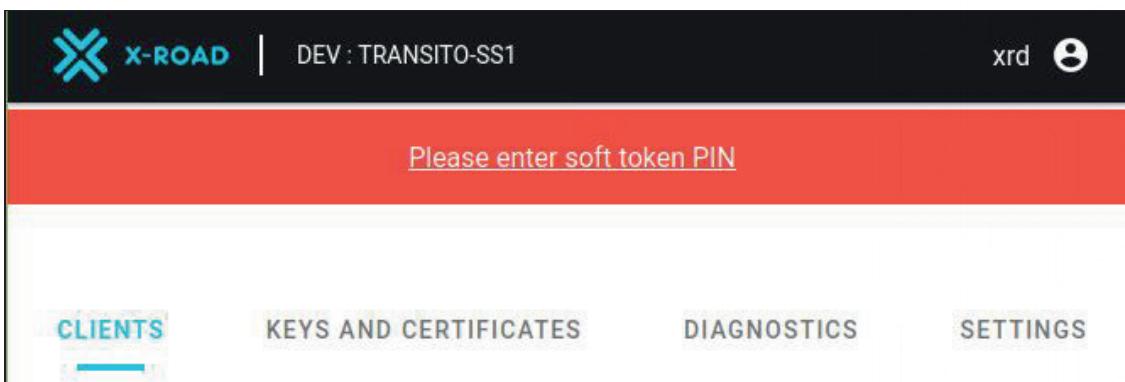
- Ahora, simular la recuperación del servidor de seguridad TRANSITO-SS1, ejecutando el siguiente comando:

```
sudo docker-compose up -d transito_security_server1
```

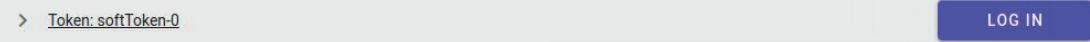
Como respuesta se deberá obtener lo siguiente:

```
Starting transito_ssl ... done
```

Adicionalmente, ingresar en la interfaz gráfica del servidor de seguridad para realizar el login del token de acceso. Notar el mensaje y hacer clic sobre él.



Hacer clic sobre el botón **LOGIN** e ingresar las credenciales asignadas para el **Token:softToken-0**



- Volver a realizar la petición y el servicio deberá seguir respondiendo a las solicitudes de forma exitosa.
- Nuevamente, se simulará una falla dentro de nuestro sistema. Esta vez, el servidor que se detendrá será **TRANSITO-SS2**.

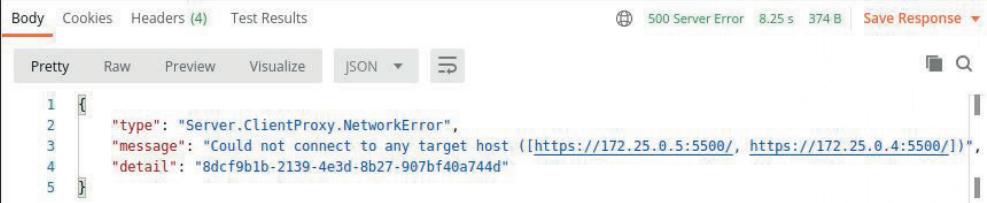
Ejecutar el siguiente comando:

```
sudo docker-compose stop transito_security_server2
```

Como respuesta, se deberá obtener lo siguiente:

```
Stopping transito_ss2 ... done
```

8. Probar nuevamente la petición hacia el servicio de Tránsito y este deberá continuar respondiendo si se pudo habilitar de forma correcta el servidor de seguridad **TRANSITO-SS1**.
9. Por último, volver a detener el servidor de seguridad **TRANSITO-SS1**, en este caso se deberá generar un error como respuesta:



The screenshot shows a REST API response in a browser-based tool. The top bar includes tabs for 'Body' (which is selected), 'Cookies', 'Headers (4)', and 'Test Results'. Below the tabs are buttons for 'Pretty', 'Raw', 'Preview', 'Visualize', and 'JSON'. The status bar at the top right indicates a '500 Server Error' with a response time of '8.25 s' and a size of '374 B', along with a 'Save Response' button. The main content area displays the following JSON error message:

```

1  {
2   "type": "Server.ClientProxy.NetworkError",
3   "message": "Could not connect to any target host ([https://172.25.0.5:5500/, https://172.25.0.4:5500/]),",
4   "detail": "8dcf9b1b-2139-4e3d-8b27-907bf40a744d"
5 }

```

¿Qué sucedió?

Cuando se tienen múltiples instancias de un servidor de seguridad que poseen la misma **organización, subsistema y código de servicio**, asociados en el administrador de servicios del servidor central, cualquiera de las instancias de los servidores de seguridad es capaz de responder la solicitud.

La manera de seleccionar cuál instancia utilizar será la del servidor de seguridad que más rápido responda una conexión TCP, esta será seleccionada de forma predeterminada para atender las solicitudes. Sin embargo, una vez el servidor de seguridad seleccionado falla por *timeout*, X-Road re-intentará realizar la petición a otra de las instancias del servidor de seguridad registradas, y así hasta completar con todas las opciones disponibles. Esta nueva configuración planteada en este ejercicio aumenta la disponibilidad del sistema X-Road, entre más instancias se posean y se apliquen técnicas como distribución geográfica entre ellas, mayor será la disponibilidad del ecosistema.