



ANEXO TÉCNICO X-ROAD

BOGOTÁ, ENERO DE 2020

Contenido

Índice de ilustraciones _____	7
Índice de tablas _____	9
1. Requerimientos para la instalación de los servidores de seguridad en las entidades del estado ____	9
1.1 Instalación del Servidor de Seguridad en Sistema Operativo Ubuntu _____	10
1.1.1 Diagrama de red _____	12
1.1.2 Preparación del Sistema Operativo _____	13
1.1.3 Instalación _____	14
1.1.4 Comprobaciones posteriores a la instalación _____	18
1.1.5 Instalar el soporte para tokens de hardware (Opcional) _____	20
1.1.6 Instalación del soporte para monitoreo. _____	23
1.1.7 Manejo de errores de instalación _____	23
1.2 Instalación del Servidor de Seguridad en Sistema Operativo REDHAT _____	26
1.2.1 Diagrama de red _____	27
1.2.2 Preparación del Sistema Operativo _____	28
1.2.3 Instalación _____	30
1.2.4 Comprobaciones posteriores a la instalación _____	33
1.2.5 Instalación del soporte para tokens de hardware _____	34
1.2.6 Instalación del soporte para monitoreo. _____	34
1.2.7 Manejo de errores de instalación _____	34
2. Configuración de los servidores de seguridad en red hat y ubuntu para la integración con la plataforma de interoperabilidad-pdi _____	35
2.1 Prerrequisitos _____	35
2.2 Datos de referencia _____	35
2.3 Configuración _____	36
2.4 Anclaje de configuración _____	37
2.5 Clase de miembro, código de miembro, código de servidor de seguridad y PIN de token de software _____	38
2.6 Gestión de servicios de estampa cronológica de tiempo _____	39

2.7 Generando una clave de firma haciendo uso del certificado digital	39
2.8 Generando una solicitud de certificado digital para una clave de firma	39
2.9 Generando clave de autenticación	40
2.10 Generación de solicitud de certificado para clave de autenticación	40
2.11 Importar un certificado de firma desde un sistema de archivos local	41
2.12 Importar un certificado de firma desde un dispositivo criptográfico	42
2.13 Importar un certificado de autenticación de un sistema de archivos local	42
2.14 Registro del servidor de seguridad en la administración de X-Road.	42
2.15 Registro de un servidor de seguridad en una autoridad de gestión de X-Road (continuación)	43
2.16 Registro de un servidor de seguridad en una autoridad de gestión de X-Road (continuación)	43
2.17 Agregar un certificado de prueba a la lista de prueba de OCSP	43
2.18 Estados de disponibilidad de dispositivos clave, claves y certificados	44
2.19 Condiciones de registro de certificados	44
2.20 Firma del certificado de registro de estados.	44
2.21 Certificado de autenticación Condiciones de registro	45
2.22 Validez de los certificados.	45
2.23 Activar y desactivar certificados.	46
2.24 Cancelar el registro de autenticación	47
2.25 Eliminar certificado o solicitud de certificado	48
2.26 Borrando de la llave privada	49
2.27 Propietario y cliente del servidor de seguridad	50
2.28 Estados del cliente del servidor de seguridad	51
2.29 Adicionar un cliente al servidor de seguridad	52
2.30 Configure una clave de firma y un certificado para un cliente de servidor de seguridad	52
2.31 Registro del cliente del servidor de seguridad en la administración de X-Road.	52
2.32 Registro de cliente del servidor de seguridad	53
2.33 Cancelación del registro de clientes y eliminación de clientes	53
2.34 Cancelación de registro de cliente	53
2.35 Cancelación del registro de clientes (continuación)	54
2.36 Borrando un cliente	55
2.37 Administración de servicios de datos.	56

2.38 Añadiendo WSDL O REST	56
2.39 Actualizar WSDL o REST	56
2.40 Activar y desactivar Servicios Web	57
2.41 Cambiar la dirección WSDL o REST	57
2.42 Borrando WSDL o REST	57
2.43 Modificar parámetros de servicio.	58
2.44 Protocolos de comunicación con el sistema de información del cliente.	58
2.45 Conectar un servidor de intranet en el rol de un usuario de servicio	59
2.46 Conexión de un servidor de intranet en la función de un proveedor de servicios	60
2.47 Adición de un certificado TLS de red interna	60
2.48 Gestionando el Certificado Intranet TLS	61
2.49 Cambiar la clave TLS y el certificado para la intranet.	61
2.50 Validación de la instalación	62
2.51 Sujetos de derechos de acceso.	63
2.52 Gestión de derechos de acceso.	64
2.53 Cambiar los derechos de acceso al servicio.	64
2.54 Añadir un cliente de servicio	64
2.55 Cambio de los derechos de acceso del cliente de servicio.	65
2.56 Grupos con derechos de acceso locales y globales.	65
2.57 Añadiendo un grupo local	66
2.58 Ver y editar miembros del grupo local	66
2.59 Cambiar la descripción del grupo local	67
2.60 Eliminar un grupo local	67
2.61 Necesidad de monitoreo del servidor de seguridad	67
2.62 Comandos de monitoreo del servidor de seguridad	68
2.63 Comando superior	68
2.64 Comando de tiempo de actividad	70
2.65 Comando "ps"	70
2.66 Comando free	73
2.67 Comando df	73
2.68 Comando "lstat"	74

2.69 Comando mpstat	75
2.70 Comando "netstat"	75
2.71 Comando iptraf	76
2.72 Comando iftop	77
2.73 Aplicaciones de monitoreo	78
2.74 Vista de la interfaz de usuario del servidor de seguridad de respaldo	78
2.75 Copia de seguridad de la configuración del servidor de seguridad	79
2.76 Cargar y eliminar un archivo de copia de seguridad de configuración	79
2.77 Restaurar la configuración de la interfaz de usuario	79
2.78 Restaura la configuración desde la línea de comandos	79
2.79 Importancia de archivar los registros de mensajes	80
2.80 Cambiar la configuración de archivo de la configuración del registro de mensajes	80
2.90 Parámetros de sellado de tiempo	81
2.91 Transferencia de archivos de un servidor de seguridad	81
3. Intervención a los servicios web soap y rest (framework desarrollo pdi 1.0)	82
3.1 Los campos de encabezado obligatorios de X-Road son los siguientes:	82
3.2 Los campos de encabezado adicionales no obligatorios de X-Road son los siguientes:	83
3.3 Creación de un servicio de datos X-Road y un cliente basado en WSDL (en la plataforma Java)	83
3.4 Configuración del servicio de datos X-Road	86
3.5 Creación de la aplicación de cliente Java X-Road	89
3.6 SERVICIOS REST	90
3.7 Interfaz REST	91
3.8 Redirecciones HTTP	96
3.9 Uso de los parámetros de consulta	97
3.10 Manejo de errores	97
3.11 Seguridad	101
3.12 Servicios	102
3.12.1 Describiendo servicios	102
3.12.2 Ejemplos	102
3.12.2.1 General	102
3.12.2.2 Solicitud y respuesta GET	102

3.12.2.3 PUT solicitud y respuesta _____	104
3.12.2.4 Solicitud y respuesta POST _____	106
3.12.2.5 BORRAR Solicitud y Respuesta _____	107
3.12.2.6 Definición del Servicio de Ejemplo _____	108
4. Despliegue de Servidor de Seguridad para Ambiente de Desarrollo sin entorno de servicios de confianza y servidor central _____	131
5 Notas de la versión de X-Road v6.21.0 integrada a la PDI de Colombia. _____	132

Índice de ilustraciones

Figura 1: Diagrama de red Ubuntu.....	12
Figura 2: Agregar usuario	13
Figura 3: Configuración de la Zona Horaria.....	13
Figura 4: Configuración regional.....	14
Figura 5: instalación del paquete “locale” y “software-properties-common”	14
Figura 6: Disponibilidad de la configuración regional	14
Figura 7: Agregar X-ROAD a lista de claves confiables	15
Figura 8: Repositorio de paquetes de X-Road	15
Figura 9: Instalar los paquetes del servidor de seguridad paso 1	15
Figura 10: Instalar los paquetes del servidor de seguridad paso 2	16
Figura 11: Configuración inicial paso 1.....	16
Figura 12: Configuración inicial paso 2.....	17
Figura 13: Configuración inicial paso 3.....	18
Figura 14: Estado de X-Road tras la instalación	19
Figura 15: Interfaz de usuario a través de navegador web.....	20
Figura 16: Configuración inicial.....	20
Figura 17: Diagrama de red REDHAT	28
Figura 18: Configuración regional REDHAT.....	28
Figura 19: Instalación de utilidades que se integran con yum	29
Figura 20: Zona horaria REDHAT.....	30
Figura 21: Agregar el repositorio de paquetes X-Road paso 1 REDHAT	30
Figura 22: Agregar el repositorio de paquetes X-Road paso 2 REDHAT	31
Figura 23: Agregar la clave de firma del repositorio de X-Road a la lista de claves confiables REDHAT....	31
Figura 24: características en el repositorio REDHAT.....	32
Figura 25: instalar los paquetes del servidor de seguridad REDHAT.....	32
Figura 26: Añadir un nuevo usuario REDHAT	33
Figura 27: Interfaz de usuario a través de navegador web.....	34
Figura 28: Anclaje de configuración	38
Figura 29: Estado de certificados OCSP	46
Figura 30: Activar y desactivar certificados OCSP	47
Figura 31: Cancelar el registro de autenticación.....	48
Figura 32: Eliminar certificado o solicitud de certificado	49
Figura 33: Borrar llave privada	50
Figura 34: Clientes del servidor de seguridad.....	51
Figura 35: Detalles cliente servidor de seguridad	54
Figura 36: Confirmación para eliminar cliente.....	55
Figura 37: Conectar un servidor de intranet en el rol de un usuario de servicio.....	59
Figura 38: Conexión de un servidor de intranet en la función de un proveedor de servicios.....	60
Figura 39: Parámetros del sistema	62
Figura 40: Validación de la instalación.....	63

Figura 41: Comando "Top"	69
Figura 42: Comando "uptime"	70
Figura 43: Comando "ps"	71
Figura 44: Comando "ps axjf"	71
Figura 45: Comando "ps auxw"	72
Figura 46: Comando "ps -auxf sort -nr -k 4 head -10"	72
Figura 47: Comando "ps -auxf sort -nr -k 3 head -10"	73
Figura 48: Comando "free"	73
Figura 49: Comando "df -h"	74
Figura 50: Comando "iostat"	74
Figura 51: Comando "iostat -d -x 5 3"	75
Figura 52: Comando "mpstat"	75
Figura 53: Comando "netstat"	76
Figura 54: Comando "IPTraff"	77
Figura 55: Comando "iftop"	77
Figura 56: Interfaz copia de seguridad y restauración	78
Figura 57: Comprobación del servicio SOAP	89

Índice de tablas

Tabla 1: Requerimientos para instalación Ubuntu	10
Tabla 2: Agencia Nacional Digital IP's	12
Tabla 3: Parámetros configurables del token	21
Tabla 4: Requerimientos para instalación REDHAT	26
Tabla 5: Datos de referencia	35
Tabla 6: Opciones comando "Top"	69
Tabla 7: Secuencia de comandos para transferencia de archivos de un servidor de seguridad	81
Tabla 8: Método GET	102
Tabla 9: Método PUT	104
Tabla 10: Método POST	106
Tabla 11: Método DELETE	107
Tabla 12: Notas de la versión de X-Road v6.21.0	132
Tabla 13: Tipos de problemas: corrección (corrección de errores), mejora (mejora de una característica existente), nueva (una nueva característica)	134
Tabla 14: Dependencias nuevas / actualizadas	138
Tabla 15: Repositorio de paquetes	139
Tabla 16: Ubuntu Bionic	139
Tabla 17: Ubuntu Trusty	141
Tabla 18: RHEL 7	143

1. Requerimientos para la instalación de los servidores de seguridad en las entidades del estado

1.1 Instalación del Servidor de Seguridad en Sistema Operativo Ubuntu

La entidad deberá configurar los siguientes requerimientos:

Tabla 1: Requerimientos para instalación Ubuntu

Ítem	Requisito	Explicación
1.0	https://artifactory.niis.org/xroad-release-deb	Repositorio de paquetes X-Road
1.1	https://artifactory.niis.org/api/gpg/key/public	La clave del repositorio
1.2	Conexiones entrantes	Puerto para conexiones entrantes (desde la red externa al servidor de seguridad)
	TCP 5500	Intercambio de mensajes entre servidores de seguridad. Se recomienda utilizar el filtrado de IP (en la lista blanca solo de AND IP y Nodos).
	TCP 5577	Consulta de respuestas OCSP entre servidores de seguridad. Se recomienda utilizar el filtrado de IP (en la lista blanca solo de AND IP y Nodos)
	TCP 9011	Puerto de escucha JMX del demonio de monitoreo de datos operativos
	TCP 9999	Puerto de escucha JMX del demonio de monitoreo ambiental
1.5	Conexiones salientes	Puertos para conexiones salientes (desde el servidor de seguridad a la red externa)
	TCP 5500	Intercambio de mensajes entre servidores de seguridad.
	TCP 5577	Consulta de respuestas OCSP entre servidores de seguridad.
	TCP 4001	Comunicación con el servidor central.
	TCP 2080	Puertos para conexiones salientes (desde el servidor de seguridad a la red interna) Intercambio de mensajes entre el servidor de seguridad y el demonio de monitoreo de

Ítem	Requisito	Explicación
		datos operativos (de forma predeterminada en localhost)
	TCP 80	Descarga de la configuración global desde el servidor central.
	TCP 80,443	Los servicios de OCSP y de sellado de tiempo más comunes.
1.6	TCP 4000	Interfaz de usuario (red local). ¡No debe ser accesible desde internet!
1.7	TCP 80, 443	Puntos de acceso al sistema de información (en la red local). ¡No debe ser accesible desde internet!
	TCP 2080	Intercambio de mensajes entre el servidor de seguridad y el Proceso de monitoreo de datos operativos (de forma predeterminada en localhost)
	TCP 9011	Puerto de escucha JMX del demonio de monitoreo de datos operacionales
1.8	Direcciones IP	Direcciones IP internas de servidor de seguridad y nombre (s) de host
1.9	Dirección Ip Servidor de Seguridad	Servidor de seguridad, dirección IP pública, dirección NAT.
1.10	<de forma predeterminada, las direcciones IP y los nombres del servidor se agregan al campo del Nombre Distinguido (DN) del Certificado Digital>	Información sobre el certificado TLS de la interfaz de usuario.
1.11	<de forma predeterminada, las direcciones IP y los nombres del servidor se agregan al campo del Nombre Distinguido (DN) del Certificado Digital>	Información sobre los servicios del certificado TLS.
1.12	TCP 2552	Puerto para comunicaciones entre los xroad-proxy y xroad-monitoring
1.13	IP PÚBLICA	Monitoreo de seguridad del servidor IP en instancia de Gobierno

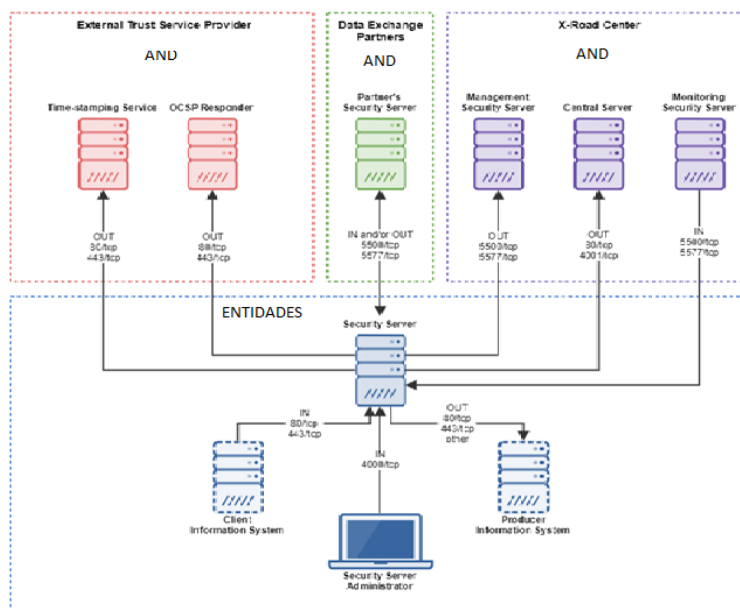
Fuente: Corporación Agencia Nacional de Gobierno Digital

1.1.1 Diagrama de red

El siguiente diagrama de red es un ejemplo de una configuración simple e independiente del Servidor de seguridad. La entidad deberá garantizar que no existan configuraciones erróneas (por ejemplo, la exposición del puerto 80/TCP a la Internet pública) esto puede ocasionar que el servidor sea vulnerable.

Permitir las conexiones entrantes desde el servidor de monitoreo del servidor de seguridad en los puertos 5500/TCP y 5577/TCP es necesario para que X-Road Center pueda monitorear el ecosistema y brindar estadísticas y apoyo a los Nodos.

Figura 1: Diagrama de red Ubuntu



Fuente: Corporación Agencia Nacional de Gobierno Digital

Tabla 2: Agencia Nacional Digital IP's

Agencia Nacional Digital IP's para listas blancas	EE - producción	EE -prueba	EE - dev
Servidor central	Se enviará a la Entidad Pública	Se enviará a la Entidad Pública	Se enviará a la Entidad Pública
Servidor de Monitoreo Central	Se enviará a la Entidad Pública	Se enviará a la Entidad Pública	Se enviará a la Entidad Pública

Fuente: Corporación Agencia Nacional de Gobierno Digital

1.1.2 Preparación del Sistema Operativo

Posterior a la instalación del sistema operativo base:

- Agregar usuario del sistema a los que se otorgan todos los roles en la interfaz de usuario. Añadir un nuevo usuario con el comando.

```
sudo adduser <username >
```

Figura 2: Agregar usuario

```
root@srvsecolimserv:/home/usrand# adduser ssolim
Adding user `ssolim' ...
Adding new group `ssolim' (1001) ...
Adding new user `ssolim' (1001) with group `ssolim' ...
Creating home directory `/home/ssolim' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for ssolim
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
root@srvsecolimserv:/home/usrand# █
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

Este usuario será el que permitirá ingresar a la plataforma

- Configuración de la Zona Horaria, es necesario validar que la zona horaria del servidor se encuentre correctamente definida en Bogotá Colombia y en caso de que no sea así modificarla.

```
timedatectl set-timezone America/Bogota
```

Figura 3: Configuración de la Zona Horaria

```
root@srvcentolim:~# timedatectl set-timezone America/Bogota
root@srvcentolim:~#
root@srvcentolim:~#
root@srvcentolim:~# timedatectl
          Local time: Tue 2020-01-21 17:38:10 -05
          Universal time: Tue 2020-01-21 22:38:10 UTC
             RTC time: Tue 2020-01-21 22:38:10
             Time zone: America/Bogota (-05, -0500)
System clock synchronized: yes
systemd-timesyncd.service active: yes
                   RTC in local TZ: no
root@srvcentolim:~#
root@srvcentolim:~#
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

- Establecer la configuración regional del sistema operativo. Agregue la siguiente línea al archivo `/etc/environment`.

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

Figura 4: Configuración regional

```
root@srvsecolimserv:/home/usrand# echo "LC_ALL=en_US.UTF-8" >> /etc/environment
root@srvsecolimserv:/home/usrand# cat /etc/environment
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games"
LC_ALL=en_US.UTF-8
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

- Es necesario realizar la instalación del paquete “locale” y “software-properties-common”

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

Figura 5: instalación del paquete “locale” y “software-properties-common”

```
root@srvsecandadmin:/home/usrand# apt-get install locales software-properties-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
locales is already the newest version (2.27-3ubuntu1).
The following packages will be upgraded:
  python3-software-properties software-properties-common
2 upgraded, 0 newly installed, 0 to remove and 191 not upgraded.
Need to get 33.6 kB of archives.
After this operation, 13.3 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 software-properties-common all 0.96.24.32.12 [10.0 kB]
Get:2 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python3-software-properties all 0.96.24.32.12 [23.6 kB]
Fetched 33.6 kB in 1s (46.9 kB/s)
(Reading database ... 67539 files and directories currently installed.)
Preparing to unpack .../software-properties-common_0.96.24.32.12_all.deb ...
Unpacking software-properties-common (0.96.24.32.12) over (0.96.24.32.7) ...
Preparing to unpack .../python3-software-properties_0.96.24.32.12_all.deb ...
Unpacking python3-software-properties (0.96.24.32.12) over (0.96.24.32.7) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Setting up python3-software-properties (0.96.24.32.12) ...
Processing triggers for dbus (1.12.2-1ubuntu1) ...
Setting up software-properties-common (0.96.24.32.12) ...
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

- Asegúrese de que la configuración regional esté disponible.

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

Figura 6: Disponibilidad de la configuración regional

```
root@srvsecolimserv:/home/usrand# locale-gen en_US.UTF-8
Generating locales (this might take a while)...
  en_US.UTF-8... done
Generation complete.
root@srvsecolimserv:/home/usrand# █
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

1.1.3 Instalación

Para instalar el software del servidor de seguridad X-Road, siga estos pasos.

- Agregue la clave de firma del repositorio de X-Road a la lista de claves confiables

```
curl https://artifactory.niis.org/api/gpg/key/public | sudo apt-key add -
```

Figura 7: Agregar X-ROAD a lista de claves confiables

```
root@srvsecolimserver:/home/usrand# curl https://artifactory.niis.org/api/gpg/key/public | sudo apt-key add -
% Total    % Received % Xferd  Average Speed   Time    Time     Time
           Dload  Upload  Total   Spent    Left     Speed
100  988    0  988    0    0    990    0  --:--:--  --:--:--  --:--:--  989
OK
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

- Agregue el repositorio de paquetes de X-Road

```
sudo apt-add-repository -y "deb https://artifactory.niis.org/xroad-release-deb $(lsb_release -sc)-current
main"
```

Figura 8: Repositorio de paquetes de X-Road

```
root@srvsecolimserver:/home/usrand# apt-add-repository -y "deb https://artifactory.niis.org/xroad-release-deb $(lsb_release -sc)-current main"
Hit:1 http://archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Ign:3 https://artifactory.niis.org/xroad-release-deb bionic-current InRelease
Get:4 https://artifactory.niis.org/xroad-release-deb bionic-current Release [1,885 B]
Get:5 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:6 http://archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:7 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [833 kB]
Get:8 https://artifactory.niis.org/xroad-release-deb bionic-current Release.gpg [475 B]
Get:9 https://artifactory.niis.org/xroad-release-deb bionic-current/main amd64 Packages [15.4 kB]
Get:10 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1,044 kB]
Fetched 2,146 kB in 4s (477 kB/s)
Reading package lists... Done
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

- Ejecute los siguientes comandos para instalar los paquetes del servidor de seguridad:

```
sudo apt-get update
```

Figura 9: Instalar los paquetes del servidor de seguridad paso 1

```
root@srvsecolimserver:/home/usrand# apt-get update
Hit:1 http://archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
Ign:3 https://artifactory.niis.org/xroad-release-deb bionic-current InRelease
Get:4 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Hit:5 https://artifactory.niis.org/xroad-release-deb bionic-current Release
Get:7 http://archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Fetched 163 kB in 2s (78.8 kB/s)
Reading package lists... Done
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

```
sudo apt-get install xroad-securityserver
```

Figura 10: Instalar los paquetes del servidor de seguridad paso 2

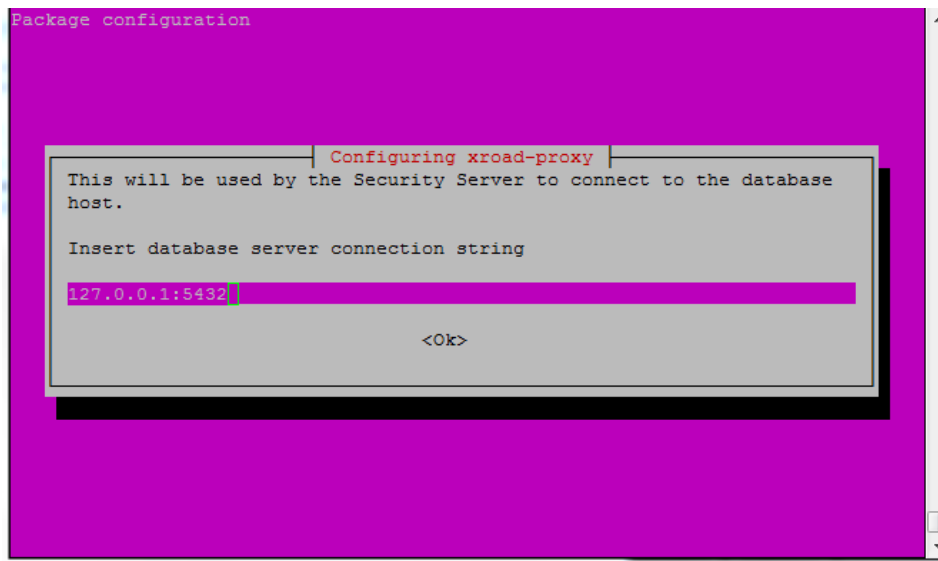
```
root@srvsecolimserv:/home/urand# apt-get install xroad-securityserver
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
ca-certificates-java crudini fontconfig-config fonts-dejavu-core java-common libavahi-client3 libavahi-common-data libavahi-common3 libcups2 libfontconfig1
libjpeg-turbo8 libjpeg8 liblcms2-2 libnginx-mod-http-echo libnsspr4 libnss3 libpoco1.10 libpq5 libpython-stdlib libpython2.7-minimal libpython2.7-stdlib libsensors4
libx11 libxrender1 libxtst6 nginx-common nginx-light openjdk-8-jre-headless postgresql postgresql-10 postgresql-client-10 postgresql-client-common postgresql-common
postgresql-contrib python python-iniparse python-minimal python-six python2.7 python2.7-minimal x11-common x11-xkb-utils x11-xfont-utils x11-xserver-utils x11-common
xroad-addon-metaseervices xroad-addon-proxymonitor xroad-addon-wsdlvalidator xroad-base xroad-confclient xroad-jetty9 xroad-monitor xroad-nginx xroad-proxy
xroad-signer
Suggested packages:
default-jre cups-common liblcms2-utils pcsd lm-sensors foglwrap nginx-doc libnss-mdns fonts-dejavu-extra fonts-ipafont-gothic fonts-ipafont-mincho
fonts-wqy-microhei fonts-wqy-zenhei fonts-indic postgresql-doc locales-all postgresql-doc-10 libjson-perl python-doc python-tk python2.7-doc binutils binfmt-support
openssl-blacklist isag
The following NEW packages will be installed:
ca-certificates-java crudini fontconfig-config fonts-dejavu-core java-common libavahi-client3 libavahi-common-data libavahi-common3 libcups2 libfontconfig1
libjpeg-turbo8 libjpeg8 liblcms2-2 libnginx-mod-http-echo libnsspr4 libnss3 libpoco1.10 libpq5 libpython-stdlib libpython2.7-minimal libpython2.7-stdlib libsensors4
libx11 libxrender1 libxtst6 nginx-common nginx-light openjdk-8-jre-headless postgresql postgresql-10 postgresql-client-10 postgresql-client-common postgresql-common
postgresql-contrib python python-iniparse python-minimal python-six python2.7 python2.7-minimal x11-common x11-xkb-utils x11-xfont-utils x11-xserver-utils x11-common
xroad-addon-metaseervices xroad-addon-proxymonitor xroad-addon-wsdlvalidator xroad-base xroad-confclient xroad-jetty9 xroad-monitor xroad-nginx xroad-proxy
xroad-securityserver xroad-signer
0 upgraded, 56 newly installed, 0 to remove and 105 not upgraded.
Need to get 409 MB of archives.
After this operation, 553 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

Tras la primera parte de la instalación, el sistema solicita la siguiente información:

- Nombre de cuenta del usuario a la que se le otorgarán los privilegios de administración en el servidor de seguridad.
- Ruta de conexión por dirección ip y puerto de la base de datos, para el caso se instalará local, razón por la que figurará la dirección localhost con el puerto 5432

Figura 11: Configuración inicial paso 1



Fuente: Corporación Agencia Nacional de Gobierno Digital

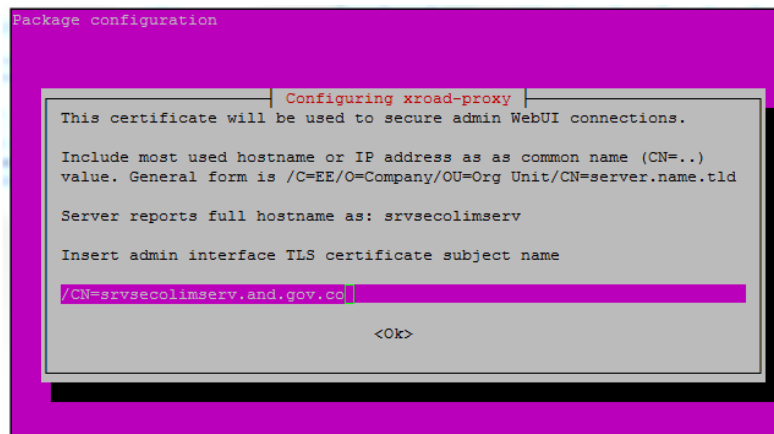
- Configuraciones propias de la plataforma

- El Distinguished Name (DN) del propietario de la interfaz de usuario y de la gestión del certificado TLS autofirmado de REST API's autofirmado TLS certificado (DN del sujeto) y sus nombres alternativos (*subjectAltName*) El certificado se utiliza para asegurar las conexiones a la interfaz de usuario. El nombre y las direcciones IP detectadas del sistema operativo se sugieren como valores predeterminados.
- El *DN de Asunto* debe ser ingresado en el formato:

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

Para la configuración se recomienda por ejemplo el nombre del hostname del servidor acompañado por el subdominio correspondiente a la entidad.

Figura 12: Configuración inicial paso 2



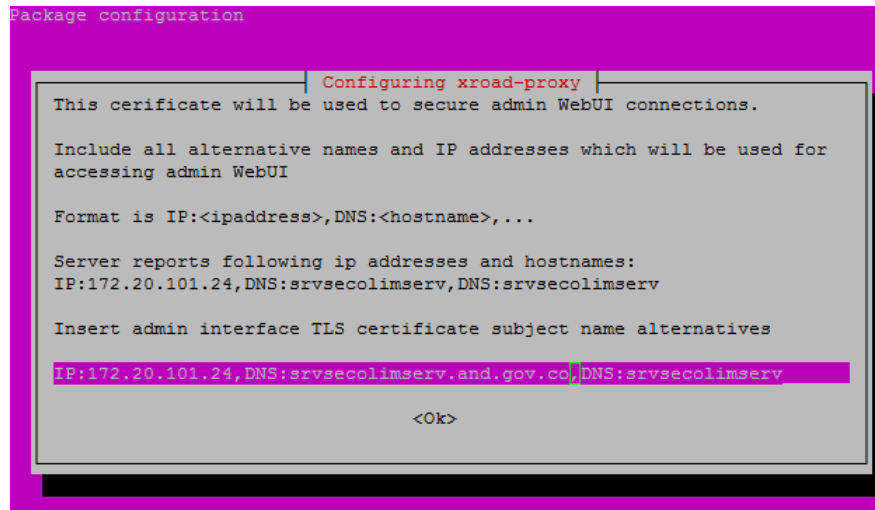
Fuente: Corporación Agencia Nacional de Gobierno Digital

- Direccionamientos IP y los nombres de dominio en uso deben ingresarse como nombres alternativos en el formato:

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

Para la configuración se recomienda por ejemplo la ip interna y la ip pública del servidor junto con el nombre del hostname y el dominio para el servidor.

Figura 13: Configuración inicial paso 3



Fuente: Corporación Agencia Nacional de Gobierno Digital

- El nombre distinguido del propietario del certificado TLS que se utiliza para asegurar el punto de acceso HTTPS de los sistemas de información. El nombre y las direcciones IP detectadas del sistema se sugieren como valores predeterminados.
- *El DN de Asunto* debe ser ingresado en el formato:

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

- Todas las direcciones IP y los nombres de dominio en uso deben ingresarse como nombres alternativos en el formato:

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

El meta-paquete xroad-securityserver también instala:

- El módulo metaservicios xroad-addon-metaservices
- El módulo de registro de mensajes xroad-addon-messagelog
- El módulo de validación WSDL xroad-addon-wsdlvalidator
- El meta-paquete xroad-securityserver-ee
- El módulo de monitoreo de datos operacionales xroad-addon-opmonitoring.

1.1.4 Comprobaciones posteriores a la instalación

Si la instalación se realiza correctamente se inician los servicios del sistema y la interfaz de usuario deberá estar respondiendo.

Desde la línea de comandos, los servicios de X-Road deberán estar en el estado: start/running (a continuación, se muestra el resultado):

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

Figura 14: Estado de X-Road tras la instalación

```
root@SRVIOSEGPR01:/home/administrator# systemctl list-units "xroad*"
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
xroad-confclient.service           loaded active running X-Road confclient
xroad-jetty.service                loaded active running X-Road Jetty server
xroad-monitor.service              loaded active running X-Road Monitor
xroad-proxy.service                loaded active running X-Road Proxy
xroad-signer.service               loaded active running X-Road signer

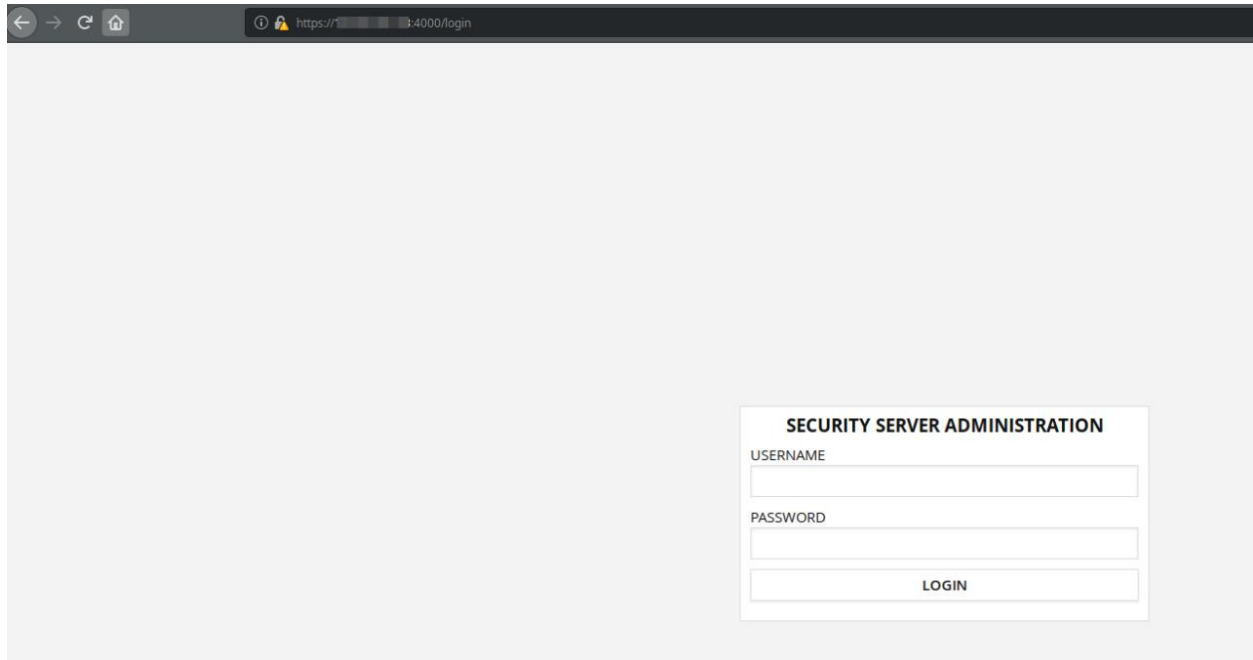
LOAD    = Reflects whether the unit definition was properly loaded.
ACTIVE  = The high-level unit activation state, i.e. generalization of SUB.
SUB     = The low-level unit activation state, values depend on unit type.

5 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
root@SRVIOSEGPR01:/home/administrator#
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

- Asegure que la interfaz de usuario del servidor de seguridad en [https:// SECURITYSERVER: 4000/](https://SECURITYSERVER:4000/) se pueda abrir en un navegador web. Para iniciar sesión, use el nombre de cuenta elegido durante la instalación. Mientras la interfaz de usuario se está iniciando, el navegador web puede mostrar el error "502 Bad Gateway".

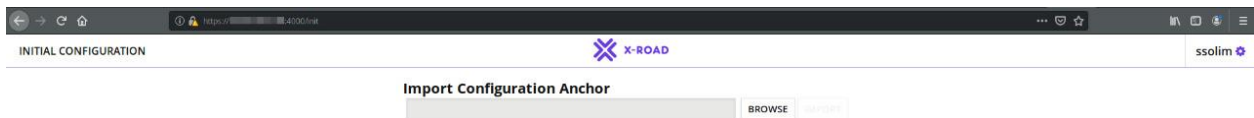
Figura 15: Interfaz de usuario a través de navegador web



Fuente: Corporación Agencia Nacional de Gobierno Digital

- Una vez ingrese el usuario y la contraseña se evidenciará de la siguiente manera:

Figura 16: Configuración inicial



Fuente: Corporación Agencia Nacional de Gobierno Digital

1.1.5 Instalar el soporte para tokens de hardware (Opcional)

Para configurar el soporte para tokens de seguridad de hardware (tarjeta inteligente, token USB, módulo de seguridad de hardware), haga lo siguiente:

1. Instale el módulo de soporte de token de hardware usando el siguiente comando:

```
sudo apt-get install xroad-addon-hwtokens
```

2. Instale y configure un controlador PKCS # 11 para el token de hardware de acuerdo con las instrucciones del fabricante.
3. Agregue la ruta al controlador PKCS # 11 al archivo `/etc/xroad/devices.ini`
4. Después de instalar y configurar el controlador, se debe reiniciar el servicio `xroad-signer`:

```
sudo service xroad-signer restart
```

Si está ejecutando una configuración de token de hardware de alta disponibilidad (HA) (como un clúster con tokens replicados), es posible que deba restringir el formato del identificador del token para que las réplicas del token puedan verse como el mismo token. El formato del identificador de token se puede cambiar en `/etc/xroad/devices.ini`, a través de la propiedad:

`token_id_format` (valorpredeterminado: `{moduleType}{slotIndex}{serialNumber}{label}`).

La eliminación de ciertas partes del identificador permitirá que la configuración de HA funcione correctamente cuando uno de los tokens se desactiva y se reemplaza por una réplica. Por ejemplo, si se informa que las réplicas de token están en diferentes ranuras, la parte `{slotIndex}` debe eliminarse del formato del identificador.

Dependiendo del token de hardware, puede ser necesaria una configuración adicional.

Todos los parámetros configurables posibles en el `/etc/xroad/devices.ini` se describen en la siguiente tabla.

Tabla 3: Parámetros configurables del token

Parámetro	Tipo	Valor por defecto	Explicación
habilitado	Bolo	<i>cierto</i>	Indica si este dispositivo está habilitado.
biblioteca	CUERDA		La ruta a la biblioteca pkcs # 11 del controlador del dispositivo.
library_cant_create_os_threads	Bolo	<i>falso</i>	Indica si los subprocesos de la aplicación, que están ejecutando llamadas a la biblioteca pkcs # 11, no pueden usar llamadas del sistema operativo nativo para generar nuevos subprocesos (en otras palabras, el código de la biblioteca puede no crear sus propios subprocesos).

Parámetro	Tipo	Valor por defecto	Explicación
<i>os_locking_ok</i>	Bolo	<i>falso</i>	Indica si la biblioteca pkcs # 11 puede usar el modelo de subprocesamiento del sistema operativo nativo para el bloqueo.
<i>sign_verify_pin</i>	Bolo	<i>falso</i>	Indica si se debe ingresar el PIN por operación de firma.
<i>token_id_format</i>	CUERDA	<i>{moduleType}</i> <i>{slotIndex}</i> <i>{serialNumber}</i> <i>{label}</i>	Especifica el formato de identificador utilizado para identificar de forma única un token. En ciertas configuraciones de alta disponibilidad, es posible que deba restringirse la compatibilidad con tokens replicados (por ejemplo, eliminando la parte del índice de la ranura que puede ser diferente para las réplicas de token).
<i>Sign_mechanism</i>	CUERDA	<i>CKM_RSA_PKCS</i>	Especifica el mecanismo de firma. Valores admitidos: <i>CKM_RSA_PKCS</i> , <i>CKM_RSA_PKCS_PSS</i> .
<i>pub_key_attribute_encrypt</i>	Bolo	<i>cierto</i>	Indica si la clave pública se puede utilizar para el cifrado.
<i>pub_key_attribute_verify</i>	Bolo	<i>cierto</i>	Indica si la clave pública se puede utilizar para la verificación.
<i>pub_key_attribute_wrap</i>	Bolo		Indica si la clave pública se puede utilizar para envolver otras claves.
<i>pub_key_attribute_allowed_mechanisms</i>	Lista de cuerdas		Especifica mecanismos de clave pública permitidos. Valores respaldados: <i>CKM_RSA_PKCS</i> , <i>CKM_SHA256_RSA_PKCS</i> , <i>CKM_SHA384_RSA_PKCS</i> , <i>CKM_SHA512_RSA_PKCS</i> y <i>CKM_RSA_PKCS_PSS</i> , <i>CKM_SHA256_RSA_PKCS_PSS</i> , <i>CKM_SHA384_RSA_PKCS_PSS</i> , <i>CKM_SHA512_RSA_PKCS_PSS</i> .
<i>priv_key_attribute_sensitive</i>	Bolo	<i>cierto</i>	Indica si la clave privada es sensible.
<i>priv_key_attribute_decrypt</i>	Bolo	<i>cierto</i>	Indica si la clave privada se puede utilizar para el cifrado.
<i>priv_key_attribute_sign</i>	Bolo	<i>cierto</i>	Indica si la clave privada se puede utilizar para firmar.
<i>priv_key_attribute_unwrap</i>	Bolo		Indica si la clave privada se puede utilizar para desenvolver claves envueltas.

Parámetro	Tipo	Valor por defecto	Explicación
<i>priv_key_attribute_allowed_mechanisms</i>	Lista de cuerdas		Especifica mecanismos de clave privada permitidos. Valores respaldados: CKM_RSA_PKCS, CKM_SHA256_RSA_PKCS, CKM_SHA384_RSA_PKCS, CKM_SHA512_RSA_PKCS y CKM_RSA_PKCS_PSS, CKM_SHA256_RSA_PKCS_PSS, CKM_SHA384_RSA_PKCS_PSS, CKM_SHA512_RSA_PKCS_PSS.

Fuente: Corporación Agencia Nacional de Gobierno Digital

Nota 1: Sólo la *biblioteca de parámetros* es obligatoria, todas las demás son opcionales.

Nota 2: El separador de elementos del tipo LISTA DE CADENA es coma ", ".

1.1.6 Instalación del soporte para monitoreo.

El paquete X-Road-monitor, que se instala de forma predeterminada, proporciona la compatibilidad con la funcionalidad de supervisión del entorno en un servidor de seguridad. El paquete se instala e inicia el xroad-monitor que reunirá y pondrá a disposición la información de monitoreo.

1.1.7 Manejo de errores de instalación

No se puede establecer LC_ALL a la configuración regional predeterminada. Si la ejecución del comando de configuración regional produce el mensaje de error:

```
locale: Cannot set LC_ALL to default locale: No such file or directory
```

Entonces el soporte para este idioma en particular no se ha instalado. Para instalarlo, ejecute el comando (el ejemplo usa el idioma inglés):

```
sudo apt-get install language-pack-en
```

Luego, para actualizar los archivos de configuración regional del sistema, ejecute los siguientes comandos (el ejemplo utiliza la configuración regional de EE. UU.):

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

```
sudo update-locale en_US.UTF-8
```

Establecer la configuración regional del sistema operativo. Agregue la siguiente línea al `/etc/environment`:

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

Después de actualizar la configuración regional del sistema, se recomienda reiniciar el sistema operativo.

1.1.7.1 PostgreSQL no es compatible con UTF8

Si la instalación del servidor de seguridad se cancela con el mensaje de error

```
postgreSQL is not UTF8 compatible,
```

Entonces el paquete PostgreSQL se instala con una configuración regional incorrecta. Una forma de resolverlo es eliminar el almacén de datos creado en la instalación de PostgreSQL y recrearlo con la codificación correcta.

ADVERTENCIA: ¡Todos los datos en la base de datos serán borrados!

```
sudo pg_dropcluster --stop 9.3 main LC_ALL="en_US.UTF-8" sudo pg_create cluster --start 9.3 main
```

Para completar la instalación interrumpida, ejecute el comando:

```
sudo apt-get -f install
```

1.1.7.2 No se pudo crear el clúster predeterminado

Si se muestra el siguiente mensaje de error durante la instalación de PostgreSQL:

```
Error: The locale requested by the environment is invalid.
```

```
Error: could not create default cluster. Please create it manually with pg_createcluster 9.3 main -start,
```

use el siguiente comando para crear el grupo de datos PostgreSQL:

```
LC_ALL="en_US.UTF-8" sudo pg_createcluster --start 9.3 main
```

La instalación interrumpida puede ser terminada usando

```
sudo apt-get -f install
```


1.1.7.3 ¿Se está ejecutando Postgres en el puerto 5432?

Si aparece el siguiente mensaje de error durante la instalación:

```
Is postgres running on port 5432?
```

```
Aborting installation! please fix issues and rerun with apt-get -f install,
```

Verifique si alguno de los siguientes errores ocurrió durante la instalación de PostgreSQL.

- Error al instalar el clúster de datos. Consulte la sección "No se pudo crear el clúster predeterminado".
- El grupo de datos de PostgreSQL instalado durante la instalación del servidor de seguridad no está configurado para escuchar en el puerto 5432. Para verificar y configurar el puerto de escucha, edite el archivo de configuración de PostgreSQL en /etc/postgresql/9.3/main/postgresql.conf. Si cambia el puerto de escucha, el servicio postgresql debe reiniciarse.

La instalación interrumpida puede ser terminada usando

```
sudo apt-get -f install
```

1.1.7.4 Versiones diferentes de paquetes xroad- * después de una actualización exitosa

A veces, después de usar el comando `sudo apt-get upgrade`, algunos de los paquetes no se actualizan. En el siguiente ejemplo, la versión del paquete `xroad-securityserver` aún es 6.8.3, aunque otros paquetes se actualizan a 6.8.5:

```
# sudo dpkg -l | grep xroad-  
ii xroad-addon-messagelog 6.8.5.20160929134539gitfe60f90  
ii xroad-addon-metaservices 6.8.5.20160929134539gitfe60f90  
ii xroad-addon-wsdvalidator 6.8.5.20160929134539gitfe60f90  
ii xroad-common 6.8.5.20160929134539gitfe60f90  
ii xroad-jetty9 6.8.5.20160929134539gitfe60f90  
ii xroad-proxy 6.8.5.20160929134539gitfe60f90  
ii xroad-securityserver 6.8.3-3-201605131138
```

El comando apt-get upgrade no instala nuevos paquetes; en este caso particular, se necesitan nuevos paquetes xroad-monitor y xroad-addon-proxymonitor, para actualizar el paquete xroad-securityserver.

Para asegurarse que los paquetes estén instalados correctamente, use los comandos sudo apt upgrade o sudo apt full-upgrade.

1.2 Instalación del Servidor de Seguridad en Sistema Operativo REDHAT

Tabla 4: Requerimientos para instalación REDHAT

Ítem	Requisito	Explicación
1.0	https://artifactory.niis.org/xroad-release-rpm	Repositorio de paquetes X-Road
1.1	https://artifactory.niis.org/api/gpg/key/public	La clave del repositorio
1.2	ENTRANTE	
	TCP 5500	Intercambio de mensajes entre servidores de seguridad. Se recomienda utilizar el filtrado de IP (en la lista blanca solo de AND IP y Nodos).
	TCP 5577	Consulta de respuestas OCSP entre servidores de seguridad. Se recomienda utilizar el filtrado de IP (en la lista blanca solo de AND IP y Nodos)
	TCP 9011	Puerto de escucha JMX del demonio de monitoreo de datos operativos
	TCP 9999	Puerto de escucha JMX del demonio de monitoreo ambiental
1.5	SALIDA	Puertos para conexiones salientes (desde el servidor de seguridad a la red externa)
	TCP 5500	Intercambio de mensajes entre servidores de seguridad.
	TCP 5577	Consulta de respuestas OCSP entre servidores de seguridad.
	TCP 4001	Comunicación con el servidor central.
	TCP 2080	Puertos para conexiones salientes (desde el servidor de seguridad a la red interna) Intercambio de mensajes entre el servidor de seguridad y el demonio de monitoreo de datos operativos (de forma predeterminada en localhost)

Ítem	Requisito	Explicación
	TCP 80	Descarga de la configuración global desde el servidor central.
	TCP 80,443	Los servicios de OCSP y de sellado de tiempo más comunes.
1.6	TCP 4000	Interfaz de usuario (red local). ¡No debe ser accesible desde internet!
1.7	TCP 80, 443	Puntos de acceso al sistema de información (en la red local). ¡No debe ser accesible desde internet!
	TCP 2080	Intercambio de mensajes entre el servidor de seguridad y el Proceso de monitoreo de datos operativos (de forma predeterminada en localhost)
	TCP 9011	Puerto de escucha JMX del demonio de monitoreo de datos operacionales
1.8	Direcciones IP	Direcciones IP internas de servidor de seguridad y nombre (s) de host
1.9	Dirección Ip Servidor de Seguridad	Servidor de seguridad, dirección IP pública, dirección NAT.
1.10	<de forma predeterminada, las direcciones IP y los nombres del servidor se agregan al campo del Nombre Distinguido (DN) del Certificado Digital>	Información sobre el certificado TLS de la interfaz de usuario.
1.11	<de forma predeterminada, las direcciones IP y los nombres del servidor se agregan al campo del Nombre Distinguido (DN) del Certificado Digital>	Información sobre los servicios del certificado TLS.
1.12	TCP 2552	Puerto para comunicaciones entre los xroad-proxy y xroad-monitoring
1.13	IP PÚBLICA	Monitoreo de seguridad del servidor IP en instancia de Gobierno

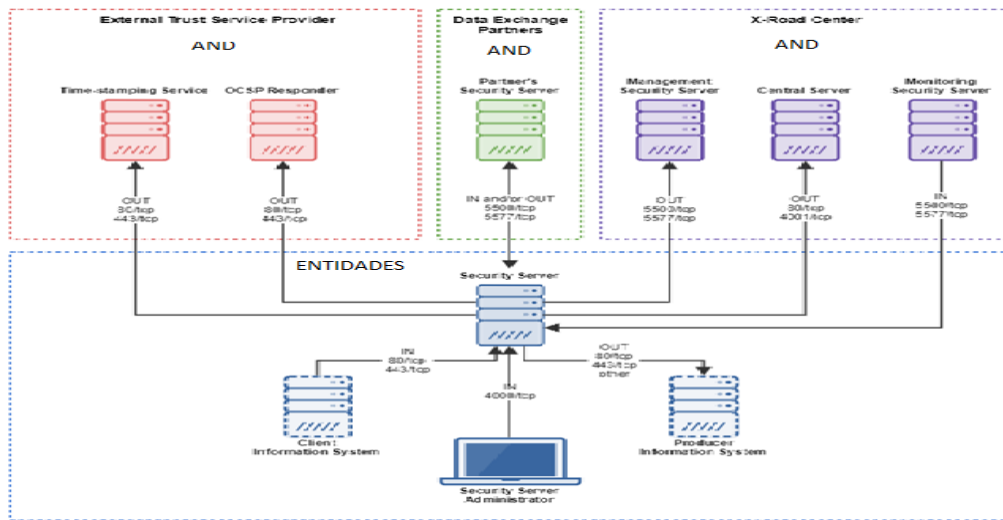
Fuente: Corporación Agencia Nacional de Gobierno Digital

1.2.1 Diagrama de red

El siguiente diagrama de red es un ejemplo de una configuración simple e independiente del Servidor de seguridad. La entidad deberá garantizar que no existan configuraciones erróneas (por ejemplo, la exposición del puerto 80/TCP a la Internet pública) esto puede ocasionar que el servidor sea vulnerable.

Permitir las conexiones entrantes desde el servidor de monitoreo del servidor de seguridad en los puertos 5500/TCP y 5577/TCP (datos de referencia: 1.13) es necesario para que X-Road Center pueda monitorear el ecosistema y brindar estadísticas y apoyo a los Nodos.

Figura 17: Diagrama de red REDHAT



Fuente: Corporación Agencia Nacional de Gobierno Digital

1.2.2 Preparación del Sistema Operativo

Establecer la configuración regional del sistema operativo. Agregue la siguiente línea al /etc/environment archivo.

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

Figura 18: Configuración regional REDHAT

```
[root@srvsecserv etc]# echo "LC_ALL=en_US.UTF-8" >> /etc/environment
[root@srvsecserv etc]# cat /etc/environment
LC_ALL=en_US.UTF-8
[root@srvsecserv etc]#
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

Install yum-utils, una colección de utilidades que se integran con yum para ampliar sus funciones nativas.

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

Figura 19: Instalación de utilidades que se integran con yum

```
=====
Instalando:
yum-utils          noarch          1.1.31-52.el7          base          121 k
Instalando para las dependencias:
libxml2-python    x86_64          2.9.1-6.el7_2.3        base          247 k
python-chardet    noarch          2.2.1-3.el7            base          227 k
python-kitchen    noarch          1.1.1-5.el7            base          267 k
=====
Resumen de la transacción
=====
Instalar 1 Paquete (+3 Paquetes dependientes)

Tamaño total de la descarga: 862 k
Tamaño instalado: 4.3 M
Is this ok [y/d/N]: y
Downloading packages:
(1/4): libxml2-python-2.9.1-6.el7_2.3.x86_64.rpm | 247 kB 00:00
(2/4): yum-utils-1.1.31-52.el7.noarch.rpm        | 121 kB 00:00
(3/4): python-kitchen-1.1.1-5.el7.noarch.rpm     | 267 kB 00:00
(4/4): python-chardet-2.2.1-3.el7.noarch.rpm     | 227 kB 00:00
=====
Total                                          995 kB/s | 862 kB 00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Instalando : python-chardet-2.2.1-3.el7.noarch          1/4
  Instalando : python-kitchen-1.1.1-5.el7.noarch         2/4
  Instalando : libxml2-python-2.9.1-6.el7_2.3.x86_64     3/4
  Instalando : yum-utils-1.1.31-52.el7.noarch            4/4
  Comprobando: python-kitchen-1.1.1-5.el7.noarch        1/4
  Comprobando: yum-utils-1.1.31-52.el7.noarch           2/4
  Comprobando: libxml2-python-2.9.1-6.el7_2.3.x86_64   3/4
  Comprobando: python-chardet-2.2.1-3.el7.noarch       4/4

Instalado:
yum-utils.noarch 0:1.1.31-52.el7

Dependencia(s) instalada(s):
libxml2-python.x86_64 0:2.9.1-6.el7_2.3 python-chardet.noarch 0:2.2.1-3.el7
python-kitchen.noarch 0:1.1.1-5.el7

¡Listo!
[root@srvsecserv etc]#
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

Si el directorio /tmp está montado utilizando el conmutador noexec, la IU de administración no se inicia porque utiliza el directorio /tmp. Debe validar si el directorio /tmp está montado utilizando el conmutador noexec:

```
mount | grep /tmp
```

¿La salida contiene /tmp y noexec?

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

Si es así, entonces el conmutador noexec debe ser eliminado modificando en el archivo /etc/fstab. Adicionalmente el directorio debe volver a montarse para que los cambios queden inmediatamente:

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

Es necesario verificar y/o establecer la zona horaria para este caso America/Bogota (-5)

Figura 20: Zona horaria REDHAT

```
[root@srvsecserv ~]# date
vie ene 24 10:40:31 -05 2020
[root@srvsecserv ~]#
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

1.2.3 Instalación

Para instalar el software del servidor de seguridad X-Road en el sistema operativo RHEL7, siga estos pasos:

- Agregue el repositorio de paquetes X-Road y los repositorios de Paquetes adicionales para Enterprise Linux (EPEL):

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

Figura 21: Agregar el repositorio de paquetes X-Road paso 1 REDHAT

```
[root@srvsecserv etc]# yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
Complementos cargados:fastestmirror
epel-release-latest-7.noarch.rpm
Examinando /var/tmp/yum-root-x1OV5t/epel-release-latest-7.noarch.rpm: epel-release-7-12.noarch
Marcando /var/tmp/yum-root-x1OV5t/epel-release-latest-7.noarch.rpm para ser instalado
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete epel-release.noarch 0:7-12 debe ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

=====
Package                               Arquitectura  Versión
=====
Instalando:
epel-release                           noarch       7-12

Resumen de la transacción
=====
Instalar 1 Paquete

Tamaño total: 24 k
Tamaño instalado: 24 k
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Instalando   : epel-release-7-12.noarch
  Comprobando  : epel-release-7-12.noarch

Instalado:
  epel-release.noarch 0:7-12

¡Listo!
[root@srvsecserv etc]#
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

```
sudo yum-config-manager --add-repo https://artifactory.niis.org/xroad-release-rpm/rhel/7/current
```

Figura 22: Agregar el repositorio de paquetes X-Road paso 2 REDHAT

```
[root@srvsecserv etc]# yum-config-manager --add-repo https://artifactory.niis.org/xroad-release-rpm/rhel/7/current
Complementos cargados:fastestmirror
adding repo from: https://artifactory.niis.org/xroad-release-rpm/rhel/7/current

[artifactory.niis.org xroad-release-rpm_rhel_7_current]
name=added from: https://artifactory.niis.org/xroad-release-rpm/rhel/7/current
baseurl=https://artifactory.niis.org/xroad-release-rpm/rhel/7/current
enabled=1

[root@srvsecserv etc]# █
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

Los siguientes paquetes se obtienen de EPEL: crudini, rlwrapja nginx.

- Agregue la clave de firma del repositorio de X-Road a la lista de claves confiables

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

Nota: Si es sistema operativo es una distribución Centos es necesario descargar la llave publica de manera manual utilizando el comando

wget <https://artifactory.niis.org/api/gpg/key/public> ubicando la descarga en la ruta /etc/pki/rpm-gpg/

Figura 23: Agregar la clave de firma del repositorio de X-Road a la lista de claves confiables REDHAT

```
[root@srvsecserv etc]# cd /etc/pki/rpm-gpg/
[root@srvsecserv rpm-gpg]# wget https://artifactory.niis.org/api/gpg/key/public
--2020-01-24 11:09:00-- https://artifactory.niis.org/api/gpg/key/public
Resolviendo artifactory.niis.org (artifactory.niis.org)... 185.78.44.254
Conectando con artifactory.niis.org (artifactory.niis.org)[185.78.44.254]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: no especificado [text/plain]
Grabando a: "public"

[ <=> ] 988 --.-K/s en 0s

2020-01-24 11:09:01 (65,9 MB/s) - "public" guardado [988]
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

Se escribe las características en el repositorio de <https://artifactory.niis.org/xroad-release-rpm/rhel/7/current> de la siguiente manera

Figura 24: características en el repositorio REDHAT

```
[artifactory.niis.org xroad-release-rpm rhel_7 current]
name=added from: https://artifactory.niis.org/xroad-release-rpm/rhel/7/current
baseurl=https://artifactory.niis.org/xroad-release-rpm/rhel/7/current
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/artifactory.gpg.public
gpgcheck=0
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

- Ejecute el siguiente comando para instalar los paquetes del servidor de seguridad:

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

Figura 25: instalar los paquetes del servidor de seguridad REDHAT

```
Comprobando : libcom_err-1.4.4-4.el7.x86_64 54/63
Comprobando : python-lxml-3.2.1-4.el7.x86_64 55/63
Comprobando : uuid-1.6.2-26.el7.x86_64 56/63
Comprobando : xroad-nginx-6.22.1-1.el7.x86_64 57/63
Comprobando : xroad-addon-metaservices-6.22.1-1.el7.x86_64 58/63
Comprobando : xroad-addon-messagelog-6.22.1-1.el7.x86_64 59/63
Comprobando : postgresql-server-9.2.24-1.el7_5.x86_64 60/63
Comprobando : postgresql-libs-9.2.24-1.el7_5.x86_64 61/63
Comprobando : copy-jdk-configs-3.3-10.el7_5.noarch 62/63
Comprobando : postgresql-9.2.24-1.el7_5.x86_64 63/63
Comprobando : libgroup-0.41-21.el7.x86_64

Instalado:
xroad-securityserver.noarch 0:6.22.1-1.el7

Dependencias instaladas:
audit-libs-python.x86_64 0:2.8.5-4.el7          awahi-libs.x86_64 0:0.6.31-19.el7          centos-indexhtml.noarch 0:7-9.el7.centos
checkpolicy.x86_64 0:2.5-9.el7                 copy-jdk-configs.noarch 0:3.3-10.el7_5          crudini.noarch 0:0.9-1.el7
 cups-libs.x86_64 1:1.6.3-40.el7                dejavu-fonts-common.noarch 0:2.33-6.el7          dejavu-sans-fonts.noarch 0:2.33-6.el7
 fontconfig.x86_64 0:2.13.0-4.3.el7            fontpackages-filesystem.noarch 0:1.44-8.el7          gd.x86_64 0:2.0.35-26.el7
 gperftools-libs.x86_64 0:2.6.1-1.el7          java-1.8.0-openjdk-headless.x86_64 1:1.8.0.232.b09-0.el7_7  javapackages-tools.noarch 0:3.4.1-11.el7
 libX11.x86_64 0:1.6.7-2.el7                  libX11-common.noarch 0:1.6.7-2.el7          libXau.x86_64 0:1.0.8-2.1.el7
 libXpm.x86_64 0:3.5.12-1.el7                 libgroup.x86_64 0:0.41-21.el7          libjpeg-turbo.x86_64 0:1.2.90-8.el7
 libsemaphore-python.x86_64 0:2.5-14.el7       libtirpc.x86_64 0:0.2.4-0.16.el7        libxcb.x86_64 0:1.13-1.el7
 libxslt.x86_64 0:1.1.28-5.el7                lkctp-tools.x86_64 0:1.0.17-2.el7         nginx.x86_64 1:1.16.1-1.el7
 nginx-all-modules.noarch 1:1.16.1-1.el7       nginx-filesystem.noarch 1:1.16.1-1.el7          nginx-mod-http-image-filter.x86_64 1:1.16.1-1.el7
 nginx-mod-http-perl.x86_64 1:1.16.1-1.el7    nginx-mod-http-xslt-filter.x86_64 1:1.16.1-1.el7  nginx-mod-mail.x86_64 1:1.16.1-1.el7
 nginx-mod-stream.x86_64 1:1.16.1-1.el7      pcre-lite-libs.x86_64 0:1.8.8-9.el7          policycoreutils-python.x86_64 0:2.5-33.el7
 postgresql.x86_64 0:9.2.24-1.el7_5          postgresql-contrib.x86_64 0:9.2.24-1.el7_5        postgresql-libs.x86_64 0:9.2.24-1.el7_5
 postgresql-server.x86_64 0:9.2.24-1.el7_5   python-IPy.noarch 0:0.6.8-10.el7          python-javapackages.noarch 0:3.4.1-11.el7
 python-lxml.x86_64 0:3.2.1-4.el7            python3.x86_64 0:3.6.8-10.el7          python3-libs.x86_64 0:3.6.8-10.el7
 python3-pip.noarch 0:9.0.3-5.el7            python3-setuptools.noarch 0:39.2.0-10.el7        r1wrap.x86_64 0:0.43-2.el7
 setuptools-libs.x86_64 0:3.3.8-4.el7        tzdata-java.noarch 0:2019c-1.el7          uuid.x86_64 0:1.6.2-26.el7
 xroad-addon-messagelog.x86_64 0:6.22.1-1.el7  xroad-addon-metaservices.x86_64 0:6.22.1-1.el7  xroad-addon-proxymonitor.x86_64 0:6.22.1-1.el7
 xroad-addon-wsdlvalidator.x86_64 0:6.22.1-1.el7  xroad-base.x86_64 0:6.22.1-1.el7        xroad-confclient.x86_64 0:6.22.1-1.el7
 xroad-jetty9.x86_64 0:6.22.1-1.el7         xroad-monitor.x86_64 0:6.22.1-1.el7      xroad-nginx.x86_64 0:6.22.1-1.el7
 xroad-proxy.x86_64 0:6.22.1-1.el7          xroad-signer.x86_64 0:6.22.1-1.el7
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

- Agregar usuario del sistema a los que se otorgan todos los roles en la interfaz de usuario. Añadir un nuevo usuario con el comando.

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


Figura 26: Añadir un nuevo usuario REDHAT

```
[root@srvsecserv yum.repos.d]# xroad-add-admin-user ssand
Note. Making /etc/shadow readable by the group 'shadow'
Adding user ssand
Cambiando la contraseña del usuario ssand.
Nueva contraseña:
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 8 caracteres
Vuelva a escribir la nueva contraseña:
passwd: todos los símbolos de autenticación se actualizaron con éxito.
[root@srvsecserv yum.repos.d]#
```

Fuente: Corporación Agencia Nacional de Gobierno Digital

- Una vez completa la instalación, inicie el servidor de seguridad.

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

1.2.4 Comprobaciones posteriores a la instalación

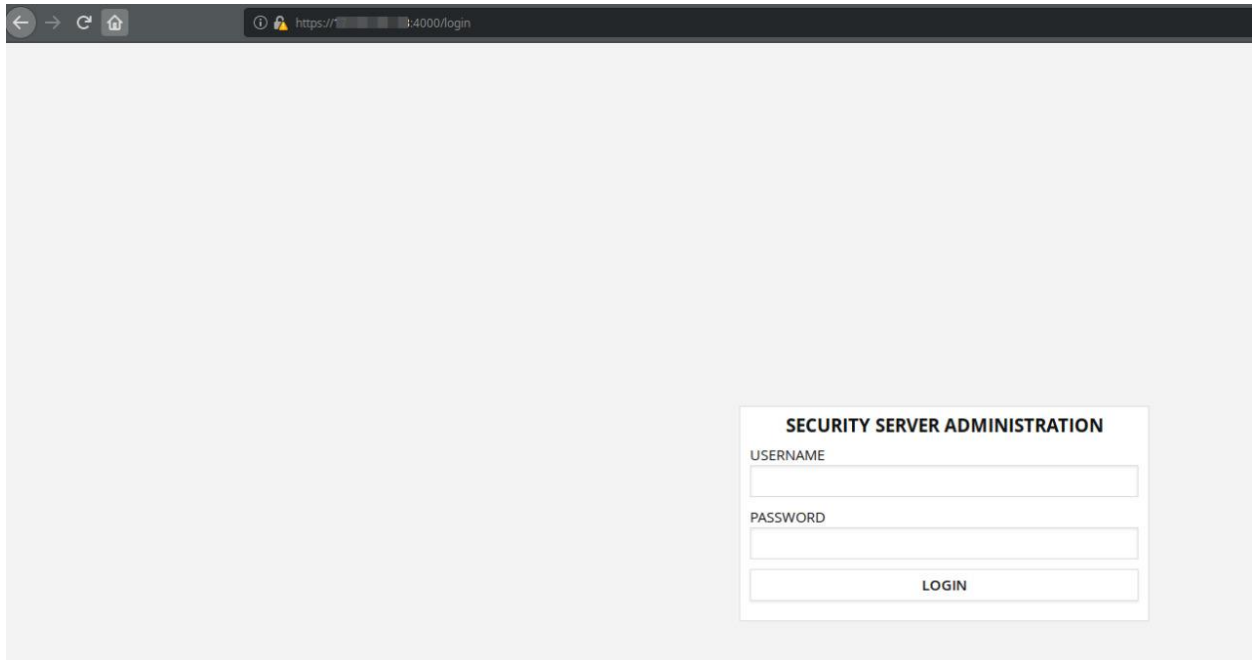
La instalación se realiza correctamente si se inician los servicios del sistema y la interfaz de usuario está respondiendo.

- Asegúrese de que, desde la línea de comandos, los servicios de X-Road estén en el running como estado (a continuación, se muestra un ejemplo de salida):

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

Asegúrese de que la interfaz de usuario del servidor de seguridad en <https://SECURITYSERVER:4000/> se pueda abrir en un navegador web. Para iniciar sesión, use el nombre de cuenta elegido durante la instalación. Mientras la interfaz de usuario todavía se está iniciando, el navegador web puede mostrar el error "502 Bad Gateway".

Figura 27: Interfaz de usuario a través de navegador web



Fuente: Corporación Agencia Nacional de Gobierno Digital

1.2.5 Instalación del soporte para tokens de hardware

Los tokens de seguridad de hardware (tarjeta inteligente, token USB, módulo de seguridad de hardware) no se han probado en RHEL7. Por lo tanto, no se proporciona soporte.

1.2.6 Instalación del soporte para monitoreo.

El paquete X-Road-monitor, que se instala de forma predeterminada, proporciona la compatibilidad con la funcionalidad de supervisión del entorno en un servidor de seguridad. El paquete se instala e inicia el xroad-monitor que reunirá y pondrá a disposición la información de monitoreo.

1.2.7 Manejo de errores de instalación

La interfaz de usuario no responde o devuelve un mensaje de error.

- Abra el `/etc/xroad/nginx/default-xroad.conf` archivo con su editor de texto favorito.
Cambia la siguiente línea:

```
proxy pass http://localhost:8083
```

a

```
proxy pass http://127.0.0.1:8083
```

Guarde los cambios y reinicie Nginx:

```
systemctl restart nginx
```

2. Configuración de los servidores de seguridad en red hat y ubuntu para la integración con la plataforma de interoperabilidad-pdi

Durante la configuración inicial del servidor de seguridad, se configuran, la información de miembro del nodo X-Road del servidor y el PIN del token de software.

2.1 Prerrequisitos

La configuración del servidor de seguridad supone que el propietario del servidor de seguridad es miembro de X-Road.

2.2 Datos de referencia

ATENCIÓN: Los elementos de referencia 2.1 - 2.3 en los datos de referencia son proporcionados por el propietario del servidor de seguridad por el administrador de X-Road central (en este caso la Agencia Nacional Digital).

El código del servidor de seguridad y el PIN del token de software serán determinados durante la instalación, a más tardar, por la persona que realiza la instalación.

Tabla 5: Datos de referencia

Ítem	Descripción	Explicación
2.1	<archivo de anclaje global> o <URL> ee-dev - entorno de desarrollo ee-test - entorno de prueba EE - entorno de producción	Archivo de anclaje de configuración global
2.2	GOV - gobierno	Clase de miembro del propietario del servidor de seguridad

Ítem	Descripción	Explicación
2.3	<código de registro del propietario del servidor de seguridad central>	El código del servidor de seguridad central
2.4	<elija el nombre del identificador del servidor de seguridad de la entidad>	El código del miembro deberá ser la sigla de la entidad + el código SIGEP
2.5	<elegir PIN para el token de software>	PIN del token de software

Fuente: Corporación Agencia Nacional de Gobierno Digital

2.3 Configuración

Para realizar la configuración inicial, abra la dirección.

`https://SECURITYSERVER:4000/`

En un navegador web iniciar sesión, use el nombre de cuenta elegido durante la instalación. Al iniciar sesión por primera vez, el sistema solicita la siguiente información:

- El archivo de anclaje de configuración global (Solicitarlo a la Agencia Nacional Digital)

Verifique el valor de hash del ancla con el valor publicado.

Si la configuración se descarga correctamente, el sistema solicita la siguiente información:

- La clase miembro del propietario del servidor de seguridad
- El código de miembro del propietario del servidor de seguridad Si la clase de miembro y el código de miembro se ingresan correctamente, el sistema muestra el nombre del propietario del servidor de seguridad registrado en el centro de X-Road.

NOTA: El propietario del servidor de seguridad o el cliente debe tener la clase de miembro "GOV" y debe seleccionarse en el servidor de seguridad.

El Código de Miembro debe estar formado de la siguiente manera:

"sigla de la Entidad-código SIGEP" - sin espacios en blanco

Ejemplo:

- Ministerio de tecnologías de la información y las Comunicaciones (Entidad Estatal)

- **Nombre de miembro:** MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
- **Clase de miembro:** GOV
- **Código de miembro:** MinTIC-0012

Dichos requisitos del Código de miembro de GOV son necesarios para garantizar la singularidad del Código de miembro de organizaciones en X-Road. Además, los miembros del Código de miembro de X-Road deben corresponder con el campo Identificador de organización (2.5.4.97) en el perfil de certificado de sello electrónico.

2.4 Anclaje de configuración

El anclaje de configuración es un conjunto de información que se puede utilizar para descargar y verificar información. Se proporciona un enlace a una configuración descargada. Los anclajes de configuración se distribuyen como archivos XML.

Cada entorno de X-Road tiene una configuración diferente. Utilice la configuración del entorno X-Road que va a utilizar.

Los anclajes de configuración de los tres entornos son los siguientes:

Entorno de desarrollo: Solicitar a la Agencia Nacional Digital

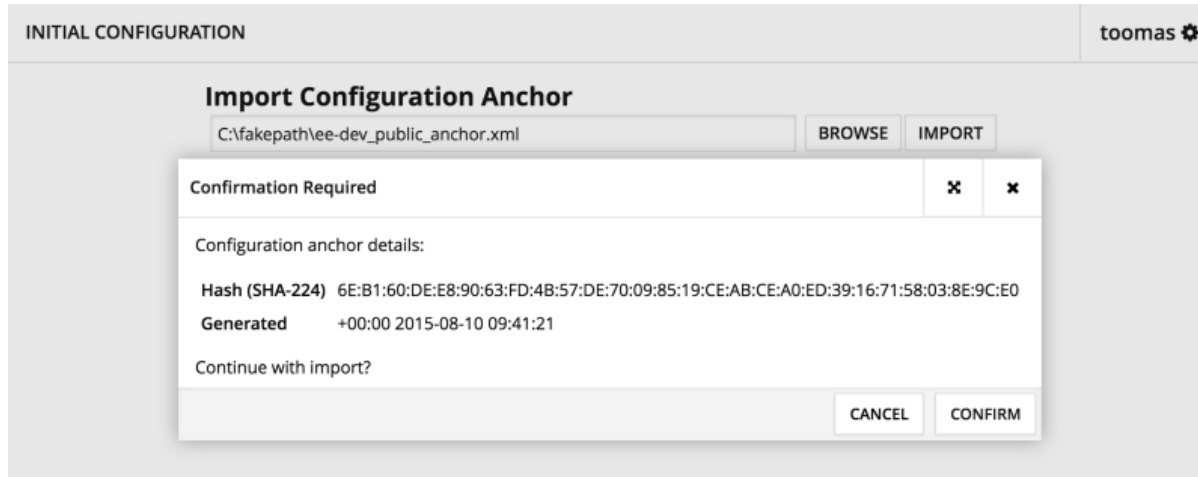
Entorno de prueba: Solicitar a la Agencia Nacional Digital

Entorno de producción: Solicitarla a la Agencia Nacional Digital

Cuando inicie sesión en su servidor web, [https:// <SECURITYSERVER IP ADDRESS>: 4000/](https://<SECURITYSERVER IP ADDRESS>:4000/) por primera vez adjuntar el archivo XML enviado por la Agencia Nacional Digital.

Nota: ¡Este paso es definitivo! Para definir un entorno diferente, se necesita hacer una instalación nueva.

Figura 28: Anclaje de configuración



Fuente: <https://x-road.global/xroad-playground>

2.5 Clase de miembro, código de miembro, código de servidor de seguridad y PIN de token de software

Después de cargar el anclaje de configuración, debe definir lo siguiente:

Clase de miembro: Clase de miembro agrupa a miembros de X-Road con propiedades similares en una unidad común. Por ejemplo, las entidades estatales se agrupan en la clase de miembros "GOV".

Código de miembro: Asociado con un determinado miembro de X-Road, es una combinación de caracteres única dentro de su clase de miembro en particular. El código de miembro permanece sin cambios durante toda la vida útil del miembro. Por ejemplo, el código de miembro para las entidades se proporcionará por la Agencia Nacional Digital al momento de ingresar la PDI.

Código del servidor de seguridad: Es un identificador de servidor de seguridad que debe ser único dentro de una organización.

PIN de token de software: Es un código de seguridad que se debe definir sin importar el entorno que esté configurando. Debe garantizar que este seguro y almacenado conforme a la política de seguridad de la entidad.

Una vez completado, el servidor de seguridad X-Road se inicializa y se puede configurar para usar servicios de confianza.

2.6 Gestión de servicios de estampa cronológica de tiempo

Para agregar un servicio de marca de tiempo, realizar lo siguiente:

1. En el menú "Configuración", seleccione "Parámetros del sistema". Abra la vista de parámetros del sistema.
2. En la sección "Servicios de marca de tiempo", haga clic en "Agregar".
3. En la ventana que se abre, seleccione el servicio apropiado y haga clic en "Aceptar".

2.7 Generando una clave de firma haciendo uso del certificado digital

Antes de generar una clave de firma, asegúrese que la hora del servidor de seguridad sea correcta. y realizar lo siguiente:

- En el menú "Administración", seleccione "Claves y certificados".
- Si está utilizando un dispositivo de llave de hardware, verifique que el dispositivo esté conectado a un servidor de seguridad. El dispositivo debe mostrarse en la tabla Claves y certificados.
- Para iniciar sesión en el teclado, haga clic en el botón "Ingresar PIN" en la línea del dispositivo en la tabla e ingrese el PIN. Si se ingresa el PIN correcto, se mostrará el botón "Cerrar sesión" en lugar del botón "Ingresar PIN".
- Para generar una clave de firma, seleccione el dispositivo en la tabla haciendo clic en su línea y haga clic en el botón "Generar clave". Introduzca una etiqueta para la clave y haga clic en "Aceptar". La clave generada se muestra en la tabla debajo de la línea del dispositivo. El nombre de la clave se muestra como el valor de la etiqueta.

2.8 Generando una solicitud de certificado digital para una clave de firma

Para generar una solicitud de certificado para una clave de firma, realizar lo siguiente:

- En el menú "Administración", seleccione "Claves y certificados".
- Seleccione la clave de la tabla y haga clic en el botón "Generar CSR". En el diálogo que se abre realizar lo siguiente:
- Seleccione el menú desplegable "Usar uso" ("SIGN" para la firma del certificado);
- Seleccione el miembro de X-Road en el menú desplegable "Cliente";
- Seleccione la Autoridad de certificación en el menú desplegable "Servicio de certificación";
- Seleccione el formato de solicitud de certificado en el menú desplegable (de acuerdo con los requisitos de servicio de certificación seleccionados PEM o DER);
- Haga clic en "Aceptar".

- Revise el formulario que abrió los datos del titular del certificado que se agregarán a la CSR y complete los campos en blanco si es necesario.
- Para completar la generación de CSR, haga clic en "Aceptar" y guarde el archivo provisto en el sistema de archivos local.
- Después de generar la CSR, la entrada "Solicitud" se agrega a la tabla debajo de la fila de la clave, lo que indica que se ha creado una solicitud de certificado para esa clave. La entrada también agregará si la solicitud no se guardó en el sistema de archivos local.

Para certificar una clave de firma, solicite un certificado a la entidad de certificación digital de servicios de certificación provisto por la Agencia Nacional Digital y acepte el certificado de firma creado sobre la base de la solicitud de certificado.

En el entorno de desarrollo, los certificados pueden aplicarse al servidor de seguridad por correo electrónico enviando una solicitud de certificado, el nombre de la organización, el número de registro de la organización y el código del servidor a la dirección de correo electrónico:

- serviciosciudadanosdigitales@and.gov.co

2.9 Generando clave de autenticación

Las claves de autenticación del servidor de seguridad solo se pueden generar con dispositivos de clave de software. Y deberá realizar lo siguiente.

- En el menú "Administración", seleccione "Claves y certificados".
- Para iniciar sesión en el llavero del software, haga clic en el botón "Ingresar PIN" en la línea del dispositivo en la tabla ingrese el PIN. Si se ingresa el PIN correcto, se mostrará el botón "Cerrar sesión" en lugar del botón "Ingresar PIN".
- Para generar una clave de autenticación, seleccione el dispositivo en la tabla haciendo clic en su línea y haga clic en el botón "Generar clave". Introduzca una etiqueta para la clave y haga clic en "Aceptar". La clave generada se muestra en la tabla debajo de la línea del dispositivo. El nombre de la clave se muestra como el valor de la etiqueta.

2.10 Generación de solicitud de certificado para clave de autenticación

Para generar una solicitud de certificado para una clave de autenticación, realice lo siguiente:

- En el menú "Administración", seleccione "Claves y certificados".

- Seleccione la clave de autenticación de la tabla y haga clic en el botón " Generar CSR ". En el diálogo que se abre:
- seleccione el menú desplegable " Uso " en el menú desplegable ("AUTH" para el certificado de autenticación);
- seleccione la Autoridad de certificación en el menú desplegable " Servicio de certificación ";
- seleccione el formato de solicitud de certificado en el menú desplegable (de acuerdo con los requisitos de servicio de certificación seleccionados PEM o DER);
- haga clic en " Aceptar ".
- Revise el formulario que se agrega a la CSR y complete los campos en blanco si es necesario.
- Para completar la generación de CSR, haga clic en "Aceptar" y guarde el archivo provisto en el sistema de archivos local.

Después de generar la CSR, la entrada "Solicitud" se agrega a la tabla bajo la fila de la clave, lo que indica que se ha creado una solicitud de certificado para esa clave. La entrada también se agregará si la solicitud no se guardó en el sistema de archivos local.

Para autenticar una clave de autenticación, solicite un certificado a un proveedor de servicios de certificación autorizado por la Agencia Nacional Digital y acepte el certificado de autenticación creado en base a la aplicación del certificado.

En el entorno de desarrollo, los certificados pueden aplicarse al servidor de seguridad por correo electrónico enviando una solicitud de certificado, el nombre de la organización, el número de registro de la organización y el código del servidor a la dirección de correo electrónico:

- serviciosciudadanosdigitales@and.gov.co

2.11 Importar un certificado de firma desde un sistema de archivos local

Para importar un certificado de firma a un servidor de seguridad, realice lo siguiente:

- En el menú " Administración ", seleccione " Claves y certificados".
- Haga clic en " Importar certificado ".
- Busque un archivo de certificado de su sistema de archivos local y haga clic en " Aceptar ".
- Después de importar el certificado, la entrada "Solicitud" debajo de la fila de la clave de la firma será reemplazada por los datos del certificado importado.

De forma predeterminada, el certificado de firma se importa como Registrado.

2.12 Importar un certificado de firma desde un dispositivo criptográfico

Para importar un certificado desde un dispositivo criptográfico:

- En el menú " Administración ", seleccione " Claves y certificados".
- Asegúrese de que el dispositivo criptográfico contiene la clave de firma y el certificado de firma estén conectados al servidor de seguridad. El dispositivo y las claves y certificados almacenados en el dispositivo deben mostrarse en la vista Claves y certificados.
- Para iniciar sesión en un dispositivo de teclado, haga clic en el botón " Ingresar PIN " en la línea del dispositivo en la tabla e ingrese el PIN. Si se ingresa el PIN correcto, se mostrará el botón "Cerrar sesión " en lugar del botón " Ingresar PIN ".
- Haga clic en el botón " Importar " en la línea de certificado.
- El certificado se importa por defecto como registrado.

2.13 Importar un certificado de autenticación de un sistema de archivos local

Para importar un certificado de autenticación a un servidor de seguridad, realice lo siguiente:

- En el menú " Administración ", seleccione " Claves y certificados".
- Haga clic en "Importar certificado".
- Busque un archivo de certificado de su sistema de archivos local y haga clic en "Aceptar".

Después de importar el certificado, la entrada "Solicitud" en la fila Clave de autenticación será reemplazada por los datos del certificado importado.

El certificado de autenticación se importa en los estados "Guardado" y "Deshabilitado".

2.14 Registro del servidor de seguridad en la administración de X-Road.

Para registrar un servidor de seguridad en una administración de X-Road, la aplicación para el registro del certificado de autenticación debe enviarse desde el servidor de seguridad.

La solicitud para registrar un servidor de seguridad debe enviarse a la Administración de X-Road de acuerdo con el procedimiento definido por la Agencia Nacional Digital. La Administración de X-Road debe aprobar la solicitud de registro.

La aplicación de registro del servidor de seguridad debe estar firmada en el servidor de seguridad con la clave de firma del propietario del servidor y la clave de autenticación del servidor. Por lo tanto, debe

asegurar que los certificados correspondientes se importen al servidor de seguridad y se encuentren en el estado de uso, es decir, los dispositivos clave se registren y el estado del protocolo OCSP sea "Bueno".

2.15 Registro de un servidor de seguridad en una autoridad de gestión de X-Road (continuación)

Para enviar una solicitud de certificado de autenticación, realice lo siguiente:

- En el menú " Administración ", seleccione " Claves y certificados".
- Seleccione el certificado de autenticación a registrar (debe estar en el estado "Guardado"), haga clic en " Activar " y luego en " Registrar ".
- En el cuadro de diálogo que se abre, ingrese el nombre DNS público del servidor de seguridad o la dirección IP visible en la red externa y haga clic en " Aceptar ".

Después de enviar la solicitud, se muestra el mensaje "Solicitud enviada" y el certificado de autenticación es "Registro en curso".

2.16 Registro de un servidor de seguridad en una autoridad de gestión de X-Road (continuación)

Después de enviar una solicitud de registro a través de la interfaz de usuario del servidor de seguridad, el servidor de seguridad debe registrarse por correo electrónico (serviciosciudadanosdigitales@and.gov.co) enviando la siguiente información:

- solicitud de registro del servidor de seguridad;
- certificado de autenticación;
- el nombre de la organización;
- número de registro de la organización;
- persona de contacto

Este requisito se aplica solo si el servidor de seguridad se utiliza en un entorno de prueba o producción.

Una vez que la Administración de X-Road ha aprobado el registro, el estado de registro del Certificado de autenticación es "Registrado" y se completa el proceso de registro.

2.17 Agregar un certificado de prueba a la lista de prueba de OCSP

Para ciertos certificados de prueba de Trust Service Provider, puede ser necesario agregar manualmente un certificado de prueba a la lista de prueba de OCSP.

2.18 Estados de disponibilidad de dispositivos clave, claves y certificados

Los siguientes colores de fondo se utilizan en Claves y Certificados para acceder a dispositivos, claves y certificados.

Fondo gris: El objeto no está disponible en el servidor de seguridad. Los certificados de fondo gris no se pueden utilizar para enviar mensajes.

Fondo amarillo: El objeto es accesible para el servidor de seguridad, pero los datos del objeto no se almacenan en la configuración del servidor de seguridad. Por ejemplo, la tarjeta inteligente puede estar conectada al servidor, pero los certificados de la tarjeta inteligente no se importan al servidor. Los certificados con un fondo amarillo no se pueden utilizar para la mensajería.

Fondo blanco: El servidor de seguridad puede acceder al objeto y los datos del objeto se almacenan en la configuración del servidor de seguridad. Los certificados de fondo blanco se pueden utilizar para enviar mensajes.

El dispositivo clave y los datos clave se almacenan automáticamente al importar un certificado relacionado con la configuración al servidor de seguridad o al generar una solicitud de certificado. De manera similar, el dispositivo clave y los datos clave se eliminan automáticamente de la configuración del servidor de seguridad al eliminar el último certificado asociado y / o la solicitud de certificado.

2.19 Condiciones de registro de certificados

Los estados de registro indican cómo se puede utilizar el certificado en el sistema X-Road.

La vista Claves y certificados muestra el estado de registro del certificado (excepto el estado "Eliminado" en la columna " Estado " en la tabla.

Los certificados deben validarse en el servidor central de X-Road. Esto se hace manualmente durante las horas de trabajo. Por lo tanto, cambiar el estado del certificado puede llevar algún tiempo.

2.20 Firma del certificado de registro de estados.

El certificado de firma del servidor de seguridad puede estar en uno de los siguientes estados de registro.

- Registrado (Registrado) El certificado es una configuración de servidor de seguridad importada y almacenada en el servidor de seguridad. El certificado de firma iniciada puede utilizarse para firmar mensajes de X-Road.
- Eliminado El certificado ha sido eliminado de la configuración del servidor. Si el certificado eliminado está ubicado en un dispositivo de llave de hardware conectado al servidor de seguridad, el certificado se muestra con un color de fondo amarillo.

2.21 Certificado de autenticación Condiciones de registro

El certificado de autenticación del servidor de seguridad puede estar en uno de los siguientes estados de registro.

- Guardado. El certificado es una configuración de servidor de seguridad importada y almacenada en el servidor de seguridad, pero el certificado no se envía para su registro.
- Registro en curso. La solicitud de registro de certificado de autenticación se ha creado y enviado al servidor central, pero la relación entre el certificado y el servidor de seguridad aún no se ha confirmado.
- Registrado (Registrado) La relación entre el certificado de autenticación y el servidor de seguridad se confirma en el servidor central. El Certificado de autenticación registrado se puede utilizar para crear un canal de intercambio de datos seguro para intercambiar mensajes de X-Road.
- Error global La relación entre el certificado de autenticación y el servidor de seguridad se ha cancelado en el servidor central.
- Eliminación en curso. Se ha enviado una aplicación para eliminar un certificado de autenticación al servidor central. Es posible cambiar este estado incluso si falla el envío de la solicitud de eliminación del certificado de autenticación.
- Eliminado. El certificado ha sido eliminado de la configuración del servidor de seguridad.

2.22 Validez de los certificados.

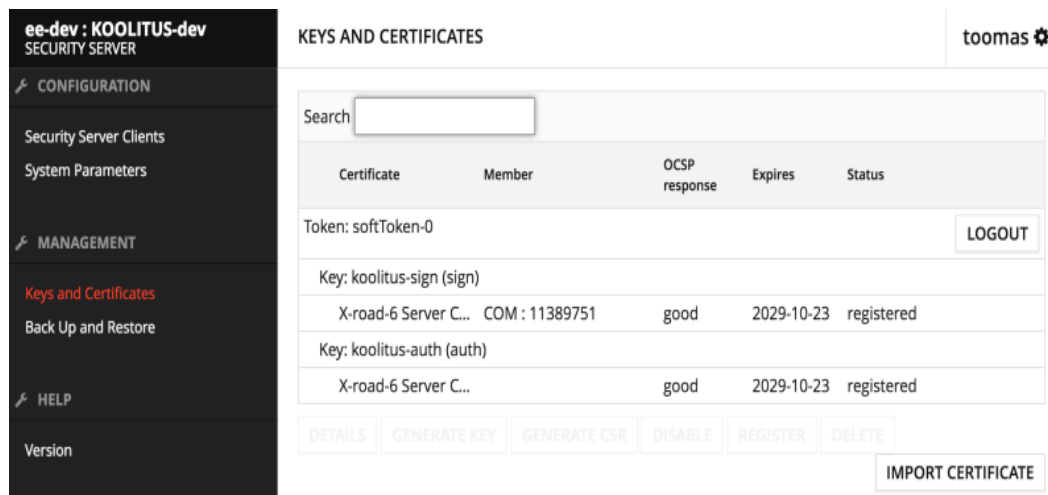
La validez indica si el certificado tiene una respuesta válida del Protocolo de estado de certificado en línea (OCSP).

En la vista "Claves y certificados", la validez del certificado se muestra en la columna "Respuesta de OCSP". La validez (excepto para el estado "Deshabilitado") se muestra para los certificados que están registrados como "Registrados".

El certificado del servidor de seguridad puede estar en uno de los siguientes estados válidos:

- Desconocido (faltante). El certificado no tiene una respuesta OCSP válida (el período de respuesta OCSP lo establece la Autoridad de gestión de X-Road) o la última respuesta OCSP es "Desconocida" (no hay información sobre el certificado solicitado) o un mensaje de error.
- Suspendido. La última respuesta de OCSP es "Suspendida".
- Bueno. La última respuesta de OCSP es "Buena". Solo los certificados de estado válidos se pueden usar para firmar consultas o conectarse a servidores de seguridad.
- Expirado. La fecha de caducidad del certificado ha expirado. El certificado no está activo y no se realizan solicitudes de OCSP.
- Revocado (cancelado). La última respuesta de OCSP es "Revocada". El certificado no está activo y no se realizan solicitudes de OCSP.
- Inactivo. El usuario ha marcado el certificado inactivado. El certificado no está activo y no se realizan solicitudes de OCSP.

Figura 29: Estado de certificados OCSP



Certificate	Member	OCSP response	Expires	Status
Token: softToken-0 LOGOUT				
Key: koolitus-sign (sign)				
X-road-6 Server C...	COM : 11389751	good	2029-10-23	registered
Key: koolitus-auth (auth)				
X-road-6 Server C...		good	2029-10-23	registered

Fuente: <https://x-road.global/xroad-playground>

2.23 Activar y desactivar certificados.

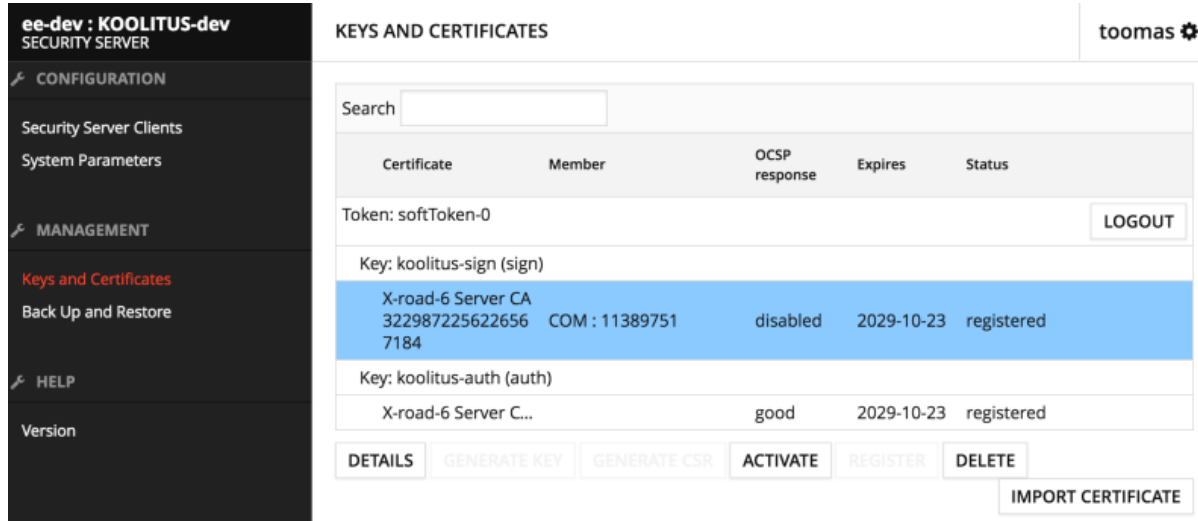
Los certificados inactivos no se utilizan para firmar mensajes o crear un canal seguro entre servidores de seguridad. Para los certificados inactivos, la columna "Respuesta OCSP" muestra "Deshabilitado" en la columna "Respuesta OCSP".

Para activar o desactivar un certificado, haga lo siguiente:

- En el menú "Administración", seleccione "Claves y certificados".

- Para activar el certificado, seleccione el certificado inactivo de la tabla y haga clic en " Activar ". Para desactivar el certificado, seleccione el certificado activo de la tabla y haga clic en Deshabilitar.

Figura 30: Activar y desactivar certificados OSCP



The screenshot shows the 'KEYS AND CERTIFICATES' management interface. On the left is a dark sidebar with navigation options: CONFIGURATION (Security Server Clients, System Parameters), MANAGEMENT (Keys and Certificates, Back Up and Restore), and HELP (Version). The main area has a search bar and a table with columns: Certificate, Member, OSCP response, Expires, and Status. Below the table are buttons for 'DETAILS', 'GENERATE KEY', 'GENERATE CSR', 'ACTIVATE', 'REGISTER', 'DELETE', and 'IMPORT CERTIFICATE'. A 'LOGOUT' button is also visible near the token information.

Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Key: koolitus-sign (sign)				
X-road-6 Server CA 322987225622656 7184	COM : 11389751	disabled	2029-10-23	registered
Key: koolitus-auth (auth)				
X-road-6 Server C...		good	2029-10-23	registered

Fuente: <https://x-road.global/xroad-playaround>

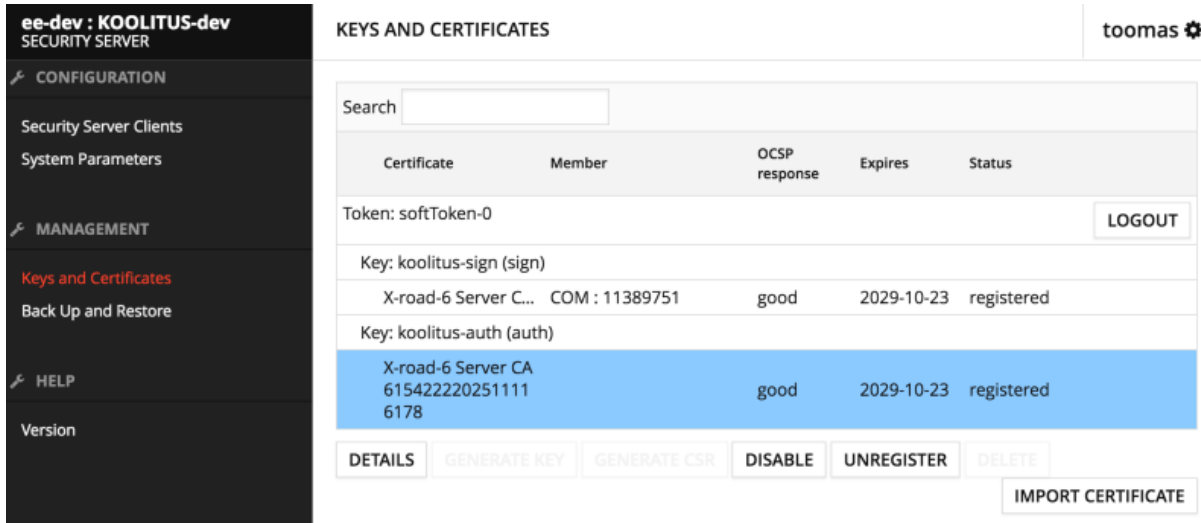
2.24 Cancelar el registro de autenticación

El registro de un certificado de autenticación registrado o archivado con la Administración de X-Road (estado "Registrado" o "Registro en curso") debe cancelarse antes de eliminar el certificado.

Para eliminar un registro de certificado de autenticación, siga estos pasos:

- En el menú " Administración ", seleccione " Claves y certificados".
- Seleccione un certificado de autenticación "Registrado" o "Registro en curso" y haga clic en " Cancelar registro".

Figura 31: Cancelar el registro de autenticación



Certificate	Member	OCSP response	Expires	Status
Token: softToken-0 LOGOUT				
Key: koolitus-sign (sign)				
X-road-6 Server C...	COM : 11389751	good	2029-10-23	registered
Key: koolitus-auth (auth)				
X-road-6 Server CA 615422220251111 6178		good	2029-10-23	registered

Fuente: <https://x-road.global/xroad-playground>

Una aplicación para eliminar un certificado de autenticación se envía automáticamente al servidor central de X-Road, al recibir el certificado de autenticación correspondiente que se elimina del servidor central. Después de enviar la solicitud, se mostrará el mensaje "Solicitud enviada" y el certificado de autenticación quedará en estado "Eliminación en curso".

El certificado de autenticación registrado en X-Road Center también se puede eliminar del servidor central sin enviar una solicitud de eliminación a través del servidor de seguridad. Para hacer esto, el administrador del servidor de seguridad debe enviar una solicitud al administrador del servidor central que contiene los datos del certificado de autenticación que se eliminará. Si el certificado de autenticación se elimina del servidor central sin que la solicitud de eliminación se envíe a través del servidor de seguridad, el certificado se encuentra en el servidor "Error global".

2.25 Eliminar certificado o solicitud de certificado

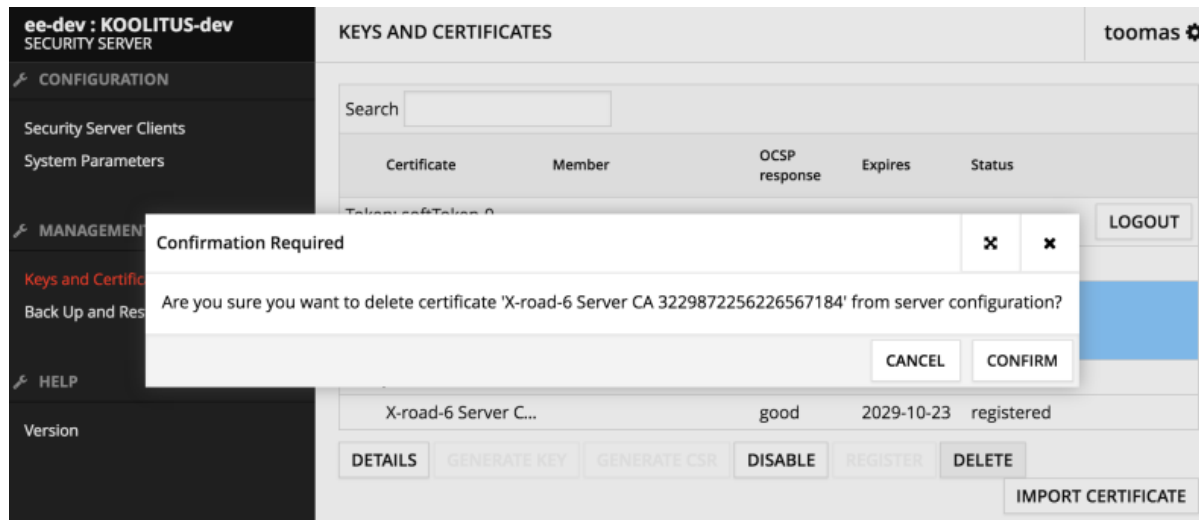
El certificado de autenticación almacenado en la configuración del sistema se puede eliminar si está "Guardado", "Error global" o "Eliminación en curso". Siempre puede eliminar el certificado de firma y la solicitud de certificado de la configuración del sistema. Si el certificado se encuentra en un dispositivo de llave de hardware, el certificado se elimina en dos niveles:

- Si el certificado se almacena en la configuración del servidor, el certificado se elimina de la configuración, pero no del dispositivo clave.
- Si el certificado no está almacenado en la configuración del servidor (el certificado se muestra en fondo amarillo), el certificado se elimina del dispositivo clave (suponiendo que el dispositivo sea compatible con esta operación).

Para eliminar un certificado o una aplicación de certificado, siga estos pasos:

- En el menú "Administración", seleccione "Claves y certificados".
- Seleccione un certificado o una aplicación de certificado de la tabla y haga clic en Eliminar. Confirme la eliminación haciendo clic en "Confirmar".

Figura 32: Eliminar certificado o solicitud de certificado



Fuente: <https://x-road.global/xroad-playaround>

2.26 Borrando de la llave privada

Eliminación de clave de la configuración del servidor también se elimina todas las claves relacionadas con los certificados digitales (y solicitud de certificado digital).

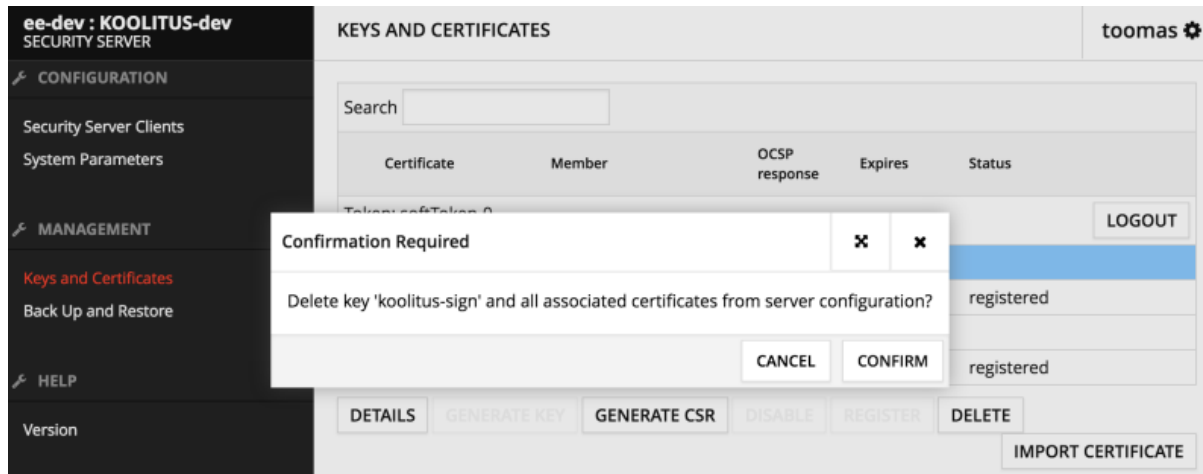
La clave se elimina en dos niveles:

- Si la clave se almacena en la configuración del servidor, la clave (y el certificado asociado) se eliminan de la configuración del servidor, pero no del dispositivo clave;
- Si la clave no está almacenada en la configuración del servidor (el certificado se muestra en fondo amarillo), la clave se elimina del teclado (suponiendo que el teclado admita esta operación).

Para eliminar una clave, haga lo siguiente:

- En el menú " Administración ", seleccione " Claves y certificados".
- Seleccione la clave y haga clic en Eliminar. Confirme la eliminación de la clave (y los certificados relacionados) haciendo clic en " Confirmar ".

Figura 33: Borrar llave privada



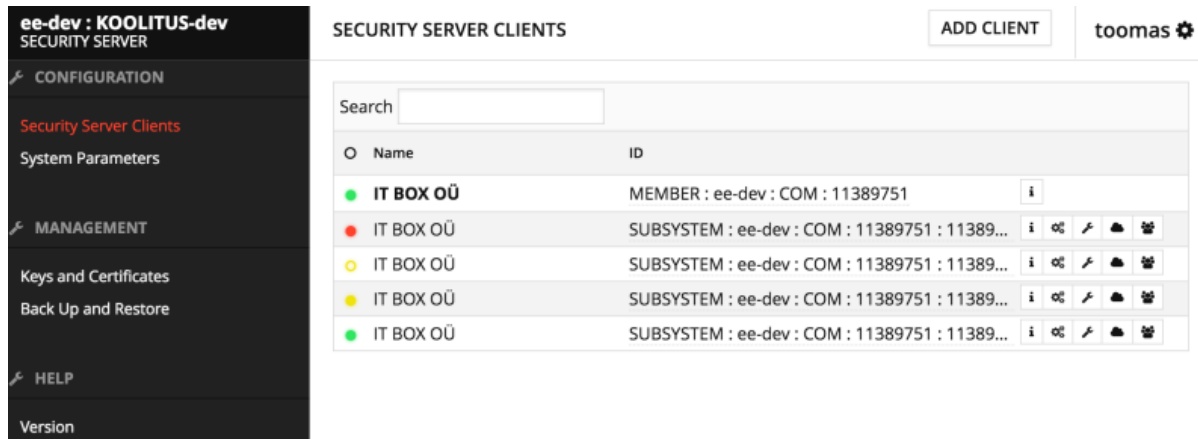
Fuente: <https://x-road.global/xroad-playground>

2.27 Propietario y cliente del servidor de seguridad

El propietario del servidor de seguridad es el miembro legalmente responsable de X-Road para el servidor de seguridad.

La información del propietario del servidor de seguridad se muestra en negrita en la lista Configuración -> Clientes del servidor de seguridad.

Figura 34: Clientes del servidor de seguridad



Name	ID
IT BOX OÜ	MEMBER : ee-dev : COM : 11389751
IT BOX OÜ	SUBSYSTEM : ee-dev : COM : 11389751 : 11389...
IT BOX OÜ	SUBSYSTEM : ee-dev : COM : 11389751 : 11389...
IT BOX OÜ	SUBSYSTEM : ee-dev : COM : 11389751 : 11389...
IT BOX OÜ	SUBSYSTEM : ee-dev : COM : 11389751 : 11389...

Fuente: <https://x-road.global/xroad-playground>

Antes de que se registre el servidor de seguridad, el propietario es "Guardado". Una vez que se completa el proceso de registro, el propietario está en el estado Registrado. El registro del propietario del servidor de seguridad no incluye subsistemas de propietario. Los subsistemas deben estar registrados como clientes individuales.

Un cliente de servidor de seguridad es un subsistema de un miembro de X-Road cuya relación con un servidor de seguridad está registrada con X-Road Management Authority y puede ser utilizada por el servidor de seguridad para usar y / o proporcionar servicios de X-Road. El subsistema es el punto de conexión entre el sistema de información y el servidor de seguridad.

2.28 Estados del cliente del servidor de seguridad

Los estados del cliente del servidor de seguridad son los siguientes:

Los datos guardados del cliente se ingresan y almacenan en la configuración del servidor de seguridad, pero la relación cliente-servidor de seguridad aún no está registrada con la Autoridad de Administración de X-Road. (Si el enlace se registra en el servidor central antes de que se ingresen los datos, el cliente se convierte en "Registrado" al ingresar los datos).

- Registro en curso: La solicitud de registro del cliente se ha enviado desde el servidor de seguridad al servidor central, pero la conexión entre el cliente y el servidor de seguridad aún no ha sido confirmada por la autoridad de X-Road.

- Registrado: La relación entre el cliente y el servidor de seguridad está confirmada por la Autoridad de Gestión de X-Road. En este estado, el cliente puede proporcionar y utilizar los servicios de X-Road (siempre que se cumplan todas las demás suposiciones).
- Error global: La relación entre el cliente y el servidor de seguridad se ha cancelado en el servidor central.
- Eliminación en curso: La solicitud para eliminar un cliente se ha enviado desde el servidor de seguridad.
- Los datos del cliente eliminados: se han eliminado de la configuración del servidor de seguridad.

2.29 Adicionar un cliente al servidor de seguridad

Para agregar un cliente al servidor de seguridad, haga lo siguiente:

- En el menú " Configuración ", seleccione "Clientes del servidor de seguridad".
- Haga clic en Agregar cliente. En la ventana que se abre, puede ingresar la información del cliente manualmente o buscar datos de clientes de todos los miembros de X-Road y sus subsistemas haciendo clic en el botón " Seleccionar cliente de la lista global ".
- Cuando se ingresa la información del cliente, haga clic en " Aceptar ".

El nuevo cliente se agregará a la lista "Guardado" de los clientes del servidor de seguridad.

2.30 Configure una clave de firma y un certificado para un cliente de servidor de seguridad

Para el cliente del servidor de seguridad, debe configurar la clave de firma y el certificado para que el cliente del servidor de seguridad pueda firmar los mensajes intercambiados a través de X-Road.

No se emiten certificados para subsistemas. Por lo tanto, en el caso de un subsistema, se utiliza el certificado del propietario (miembro de X-Road).

Todos los subsistemas miembros de X-Road registrados en el mismo servidor de seguridad utilizan el mismo certificado de firma para firmar los mensajes. Si el servidor de seguridad ya tiene un certificado de firma de miembro de X-Road, no es necesario obtener una nueva clave de firma y / o certificado al agregar el mismo subsistema.

La configuración del servidor de firmas y el certificado para el cliente del servidor de seguridad se realiza de manera similar a la certificación del propietario del servidor de seguridad.

2.31 Registro del cliente del servidor de seguridad en la administración de X-Road.

Para registrar un cliente de servidor de seguridad en una administración de X-Road, debe hacer lo siguiente:

- La aplicación de registro de cliente del servidor de seguridad debe enviarse desde el servidor de seguridad.
- La autoridad de gestión de X-Road debe ser notificada de la solicitud de registro del cliente de acuerdo con el procedimiento para X-Road.
- La Administración de X-Road debe aprobar la solicitud de registro.

2.32 Registro de cliente del servidor de seguridad

Para enviar una solicitud de registro de cliente, haga lo siguiente:

- En el menú "Configuración", seleccione "Clientes del servidor de seguridad".
- Seleccione un cliente con el estado "Guardado" en la lista de clientes del servidor de seguridad.
- Haga clic en el ícono "Detalles" y haga clic en "Registrarse" en la ventana que se abre.
- Haga clic en "Confirmar" para enviar su solicitud.

Después de enviar la solicitud, se mostrará el mensaje "Solicitud enviada" y el estado del cliente será "Registro en curso". Una vez que la Autoridad de Gestión de X-Road ha aprobado el registro, el estado del Cliente es "Registrado" y se completa el proceso de registro.

2.33 Cancelación del registro de clientes y eliminación de clientes

Eliminar un cliente de un servidor de seguridad también eliminará toda la información relacionada con el cliente (WSDL, servicios REST, derechos de acceso y, si corresponde, certificados) del servidor.

Si los clientes del servidor de seguridad son varios subsistemas del mismo miembro de X-Road, no se recomienda eliminar uno de ellos para eliminar los certificados de firma si otros clientes registrados con el servidor de seguridad utilizan el mismo certificado de firma.

El registro de un cliente registrado o archivado en la Administración de X-Road (cuyo estado es "Registrado" o "Registro en curso") debe cancelarse antes de la eliminación del Cliente. Al cancelar el registro, se envía una solicitud de eliminación del cliente del servidor de seguridad desde el servidor de seguridad al servidor central.

Una vez que se cancele el registro del cliente, el cliente ya no podrá utilizar el servidor de seguridad. Esta acción no se puede deshacer.

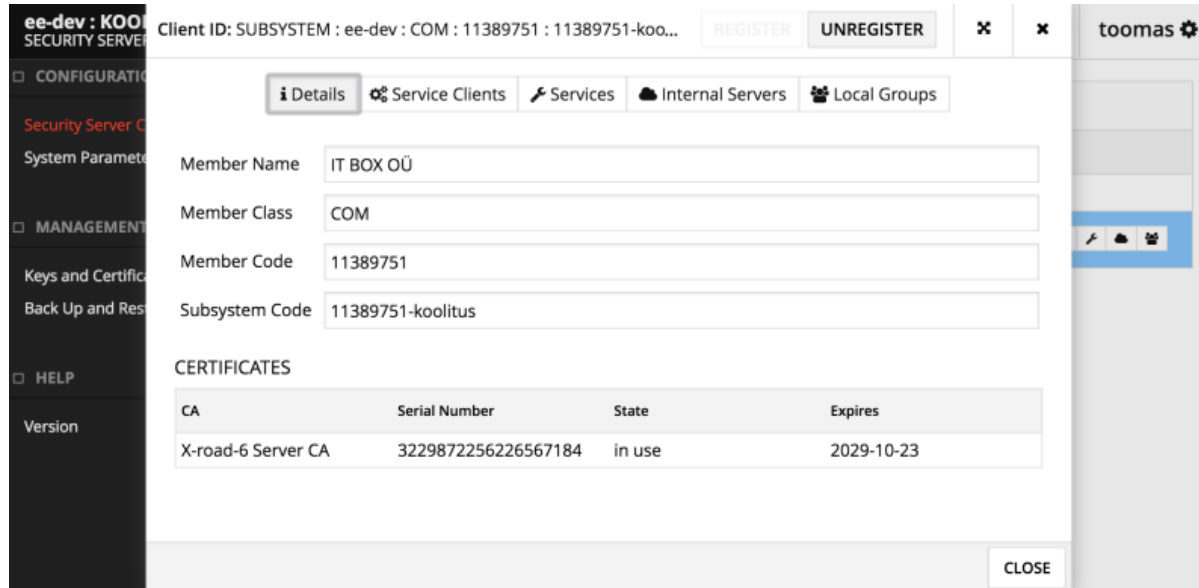
2.34 Cancelación de registro de cliente

Para cancelar un registro de cliente, siga estos pasos:

- En el menú "Configuración", seleccione "Clientes del servidor de seguridad".
- Seleccione el cliente que desea eliminar del servidor y haga clic en el icono Detalles en esta línea de cliente.

- En la ventana que se abre, haga clic en "Cancelar registro" y luego en "Confirmar".

Figura 35: Detalles cliente servidor de seguridad



Fuente: <https://x-road.global/xroad-playground>

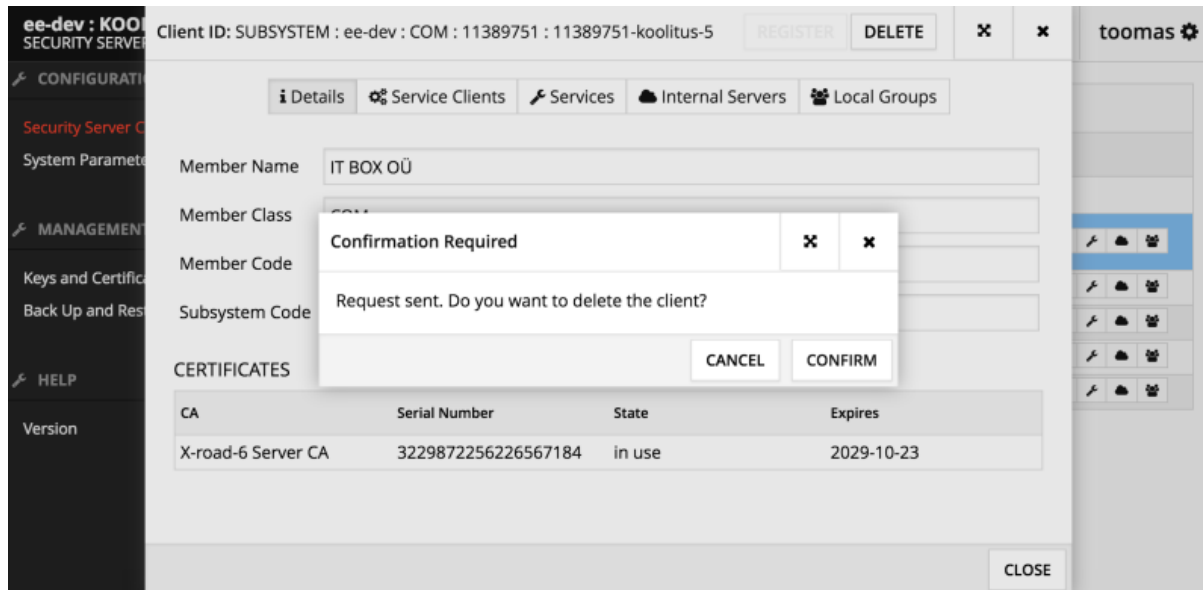
Una solicitud de eliminación de seguridad se envía automáticamente desde el servidor de seguridad al servidor central de X-Road, al recibir la confirmación de la relación entre el servidor de seguridad y el cliente.

2.35 Cancelación del registro de clientes (continuación)

A continuación, se mostrará una notificación sobre el envío de una solicitud de eliminación al servidor central y se proporcionará una confirmación sobre la eliminación de los datos del cliente (excepto los certificados).

- Si desea eliminar los datos del cliente inmediatamente, haga clic en " Confirmar ". La siguiente es la opción de eliminar certificados de cliente. Haga clic en " Confirmar " de nuevo para eliminar los certificados.
- Si desea almacenar datos de clientes, haga clic en Cancelar. En este caso, el cliente se convierte en "Eliminación en curso". En este estado, el cliente no puede intercambiar mensajes y no puede volver a registrarse con X-Road Management Authority.

Figura 36: Confirmación para eliminar cliente



Fuente: <https://x-road.global/xroad-playground>

Para eliminar los datos del cliente en el estado "Eliminación en curso", seleccione el cliente haciendo clic en el icono " Detalles " en la línea del cliente, en la ventana " Eliminar " que se abre, y luego haga clic en " Confirmar " .

El registro de un cliente registrado también se puede cancelar en el servidor central sin enviar una solicitud de eliminación a través del servidor de seguridad. Para este propósito, el administrador del servidor de seguridad responsable del cliente debe enviar una solicitud al administrador del servidor central que contiene los datos del cliente respectivo. Si el cliente se ha eliminado del servidor central sin que la solicitud de eliminación se envíe a través del servidor de seguridad, el cliente se encuentra en el servidor de seguridad "Error global".

2.36 Borrando un cliente

El cliente del servidor de seguridad se puede eliminar si su estado es "Guardado", "Error global" o "Eliminación en curso". Si el cliente está en "Registrado" o "Registro en curso", su registro debe cancelarse antes de la eliminación.

Para eliminar un cliente, haga lo siguiente:

- En el menú "Configuración", seleccione "Clientes del servidor de seguridad".
- Seleccione el cliente que desea eliminar del servidor de seguridad de la tabla y haga clic en el icono " Detalles " en la línea del cliente.
- Haga clic en la ventana " Eliminar ". Confirme la eliminación haciendo clic en " Confirmar " .

2.37 Administración de servicios de datos.

Los servicios de datos de X-Road se gestionan en dos niveles. La adición, eliminación y desactivación de servicios se realiza en el nivel WSDL o REST. WSDL (Lenguaje de definición de servicios web) es un lenguaje de formato XML que le permite describir los servicios de red con una serie de puntos finales a los que se puede acceder mediante mensajes que contienen información basada en documentos o procedimientos. Las operaciones y los mensajes se describen en el resumen y luego se asocian con un protocolo de red y un formato de mensaje específicos para definir el punto final.

Un archivo WSDL es un archivo que describe la configuración del servicio. Esta información, junto con la IP del servicio, debe solicitarse al desarrollador del sistema de información de una organización que debe hacer que el archivo WSDL esté disponible a través de la URL. La dirección del servicio, el método de conexión a la intranet y la duración máxima del servicio se establecen en el nivel de servicio.

Sin embargo, es fácil extender la configuración de un servicio a todos los servicios descritos en el mismo WSDL.

2.38 Añadiendo WSDL O REST

Cuando agrega un nuevo servicio, el servidor de seguridad lee los datos del servicio y los muestra en la tabla de servicios. El WSDL es el código, nombre y dirección del servicio.

Para agregar WSDL o REST, haga lo siguiente:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione el cliente de la tabla y haga clic en el icono " Servicios " en la línea del cliente.
- Haga clic en " Agregar WSDL o REST ", ingrese la dirección en la ventana que se abre y haga clic en " Aceptar ". Los datos de los servicios contenidos en ellos se incluyen en la tabla de servicios. De forma predeterminada, WSDL o REST se agrega en estado inactivo.

2.39 Actualizar WSDL o REST

Cuando actualice, el servidor de seguridad volverá a cargar el archivo del servicio al servidor de seguridad y verificará si todos los datos de servicio contenidos en el archivo recargado están incluidos en los servicios existentes.

Para actualizar el archivo WSDL o REST, siga estos pasos:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione el cliente de la tabla y haga clic en el icono " Servicios " en la línea del cliente.

- Seleccione el servicio que desea actualizar de la tabla y haga clic en el botón Actualizar.
- Si servicio web en comparación con los existentes en el servidor de seguridad, se mostrará una advertencia. Haga clic en Continuar para continuar actualizando.

2.40 Activar y desactivar Servicios Web

Los datos de los servicios web inactivos se muestran en rojo en la tabla de servicios con la palabra "Deshabilitado". Los servicios descritos como inactivo no pueden ser utilizados por los clientes.

Tras la activación, los servicios contenidos en él están disponibles para los usuarios. Por lo tanto, antes de activar servicio, debe asegurarse de que todas las funciones del servicio estén configuradas correctamente.

Para activar un Servicio Web, haga lo siguiente:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione el cliente de la tabla y haga clic en el icono " Servicios " en la línea del cliente.
- Seleccione el servicio inactivo de la tabla y haga clic en Habilitar.
- Para desactivar un servicio web, haga lo siguiente:
 - En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione el cliente de la tabla y haga clic en el icono " Servicios " en la línea del cliente.
 - Para desactivar el servicio, seleccione el servicio activo de la tabla y haga clic en Deshabilitar.
 - Notificará un mensaje de error que se mostrará a los clientes cuando intenten acceder a los servicios y haga clic en " Aceptar ".

2.41 Cambiar la dirección WSDL o REST

Para cambiar la dirección WSDL, haga lo siguiente:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione el cliente de la tabla y haga clic en el icono " Servicios " en la línea del cliente.
- Seleccione el servicio que desea cambiar de la tabla y haga clic en Editar.
- En la ventana que se abre, ingrese la dirección del servicio y haga clic en " Aceptar ". Cambiar la dirección actualizará WSDL.

2.42 Borrando WSDL o REST

Al eliminar un servicio web, se eliminan todos los datos relacionados con los servicios descritos en este, incluidos los derechos de acceso.

Para eliminar un servicio, haga lo siguiente:

- En el menú " Configuración, seleccione " Clientes del servidor de seguridad ", seleccione el cliente de la tabla y haga clic en el icono " Servicios " en la línea del cliente.
- Seleccione el Servicio Web que desea eliminar de la tabla y haga clic en el botón Eliminar.
- Confirme la eliminación haciendo clic en la ventana " Confirmar ".

2.43 Modificar parámetros de servicio.

Los parámetros de servicio son:

- "URL del servicio" significa la URL a la que se transmiten las consultas orientadas al servicio;
- 'Tiempo de espera (s)' significa la duración máxima de la consulta de la base de datos en segundos;
- Verificar certificado TLS: verifique un certificado al establecer una conexión TLS.

Para cambiar los parámetros de servicio:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione el cliente de la tabla y haga clic en el icono " Servicios " en la línea del cliente.
- Seleccione un servicio de la tabla y haga clic en Editar.
- Configure los parámetros de servicio en la ventana abierta. Para aplicar el parámetro especificado a todos los servicios descritos, marque la casilla junto al parámetro "Aplicar a todos los servicios ". Haga clic en " Aceptar " para aplicar los parámetros configurados.

2.44 Protocolos de comunicación con el sistema de información del cliente.

El servidor de seguridad puede comunicarse con los servidores del sistema de información que proporcionan o utilizan servicios a través de HTTP, HTTPS o HTTPSNOAUTH.

- El protocolo HTTP debe usarse cuando un segmento de red privada al que no se conecta ninguna otra computadora se usa para la comunicación entre el servidor y el servidor de seguridad. Además, el servidor del sistema de información no debe ofrecer una función de inicio de sesión interactiva.
- El protocolo HTTPS debe usarse cuando no es posible separar un segmento de red separado para la comunicación entre el servidor del sistema de información y el servidor de seguridad. En este caso, la comunicación entre ellos está protegida contra una posible vigilancia e intervención por métodos

criptográficos. Cuando se utiliza el protocolo HTTPS, los certificados TLS para la intranet se generarán para los servidores del sistema de información, que se cargan en el servidor de seguridad.

- HTTPS NOAUTH debe utilizarse si desea que el servidor de seguridad omita la verificación TLS del sistema de información.

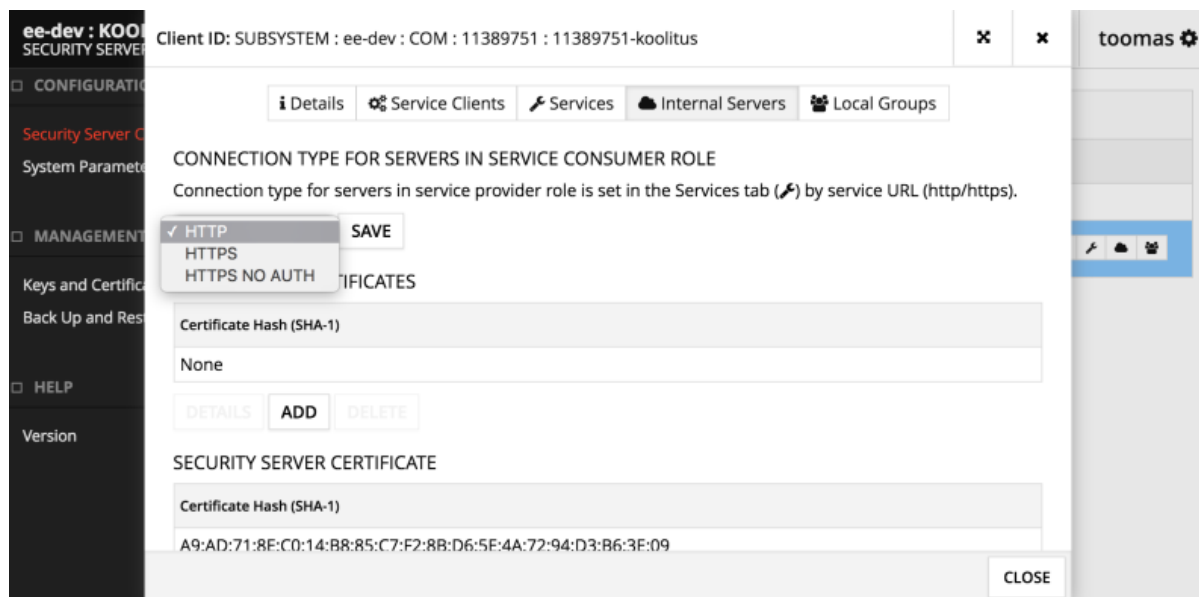
Si se selecciona HTTP como método de conexión, pero el sistema de información se conecta al servidor de seguridad a través de HTTPS o HTTPS NOAUTH, se acepta la conexión, pero no se verifica el certificado TLS de la intranet del cliente.

2.45 Conectar un servidor de intranet en el rol de un usuario de servicio

Para determinar cómo se conecta el servidor de intranet en la función del usuario del servicio, siga estos pasos:

- En el menú "Configuración", seleccione "Clientes del servidor de seguridad" y haga clic en el icono "Servidores internos" en la línea del cliente.
- Seleccione el tipo de conexión en el menú desplegable "Tipo de conexión" y haga clic en "Guardar"

Figura 37: Conectar un servidor de intranet en el rol de un usuario de servicio



Fuente: <https://x-road.global/xroad-playground>

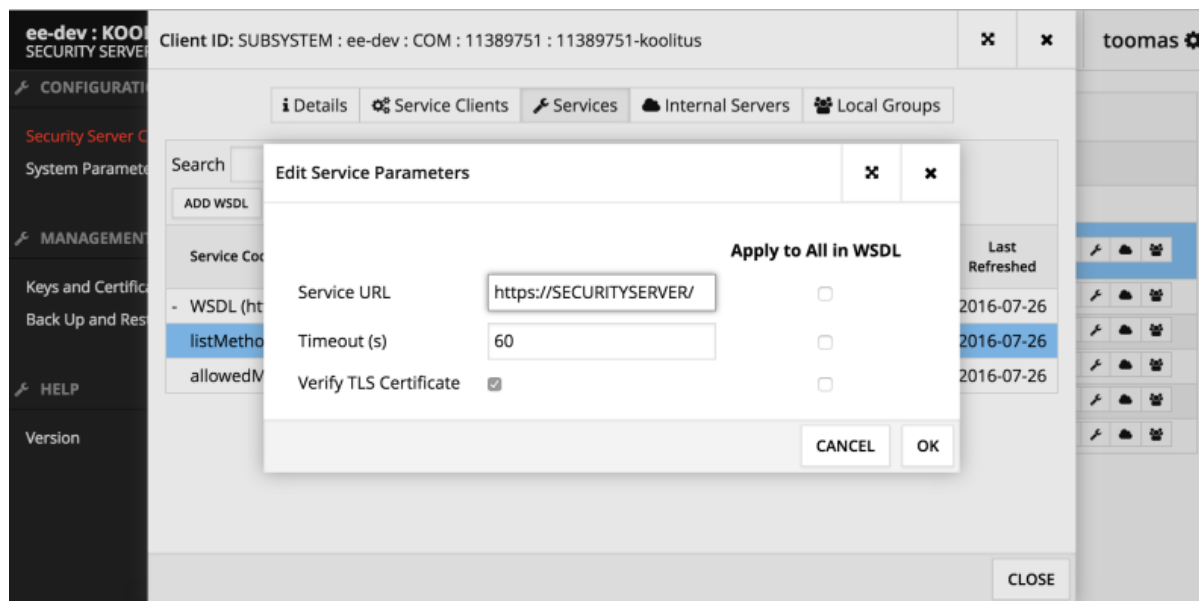
Dependiendo del tipo de conexión que seleccionó, la URL de consulta del sistema de información es `http://SECURITYSERVER/` o `https://SECURITYSERVER/`. Al realizar una consulta, la dirección SECURITYSERVER debe reemplazarse con la dirección real del servidor de seguridad.

2.46 Conexión de un servidor de intranet en la función de un proveedor de servicios

El modo de conexión del servidor de intranet en la función del proveedor de servicios está determinado por el protocolo contenido en la URL del servicio. Para cambiar el método de conexión, haga lo siguiente:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione el cliente de la tabla y haga clic en el icono " Servicios " en la línea del cliente.
- Seleccione un servicio de la tabla y haga clic en Editar.
- Establezca la URL del servicio en HTTP o HTTPS. Para HTTPS, marque la casilla Verificar certificado TLS si es necesario.

Figura 38: Conexión de un servidor de intranet en la función de un proveedor de servicios



Fuente: <https://x-road.global/xroad-playground>

2.47 Adición de un certificado TLS de red interna

Para agregar un certificado TLS para la intranet al cliente del servidor de seguridad (método de conexión para HTTPS), haga lo siguiente.

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad " y haga clic en el icono " Servidores internos " en la línea del cliente.
- Para agregar un certificado, haga clic en el botón " Agregar " en el menú " Certificados TLS internos ", seleccione el archivo de certificado del sistema de archivos local y haga clic en " Aceptar ". La huella digital del certificado se muestra en la tabla " Certificados TLS internos ".

2.48 Gestionando el Certificado Intranet TLS

Para ver el certificado TLS interno de seguridad TLS, siga estos pasos:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad " y haga clic en el icono " Servidores internos " en la línea del cliente.
- Seleccione la tabla "certificados TLS internas" certificado y haga clic en " Detalles".

Para eliminar el TLS en la intranet, siga estos pasos:

- En el menú " Configuración", seleccione " Clientes del servidor de seguridad " y haga clic en el icono " Servidores internos " en la línea del cliente.
- Seleccione el certificado de la tabla " Certificados TLS internos " y haga clic en " Eliminar ".
- Confirme la eliminación haciendo clic en la ventana " Confirmar ".

Para exportar un certificado de seguridad TLS interno, siga estos pasos:

- En el menú " Configuración", seleccione " Clientes del servidor de seguridad " y haga clic en el icono " Servidores internos " en la línea del cliente.
- Haga clic en " Exportar " y guarde el archivo proporcionado en el sistema de archivos local.

2.49 Cambiar la clave TLS y el certificado para la intranet.

Para cambiar la clave TLS interna y el certificado para el servidor de seguridad, haga lo siguiente:

- En el menú " Configuración ", seleccione "Parámetros del sistema". Abra la vista de parámetros del sistema.
- Haga clic en " Generar nueva clave TLS " en la sección " Certificado interno TLS " y haga clic en " Confirmar " en la ventana que se abre.

El servidor de seguridad crea la clave utilizada para comunicarse con los sistemas de información del cliente y el correspondiente certificado autofirmado. La huella dactilar del certificado del servidor de seguridad también cambia. El nombre de dominio del servidor de seguridad se almacena en el campo "Nombre común" del certificado y la dirección IP interna en el campo de asunto "subjectAltName".

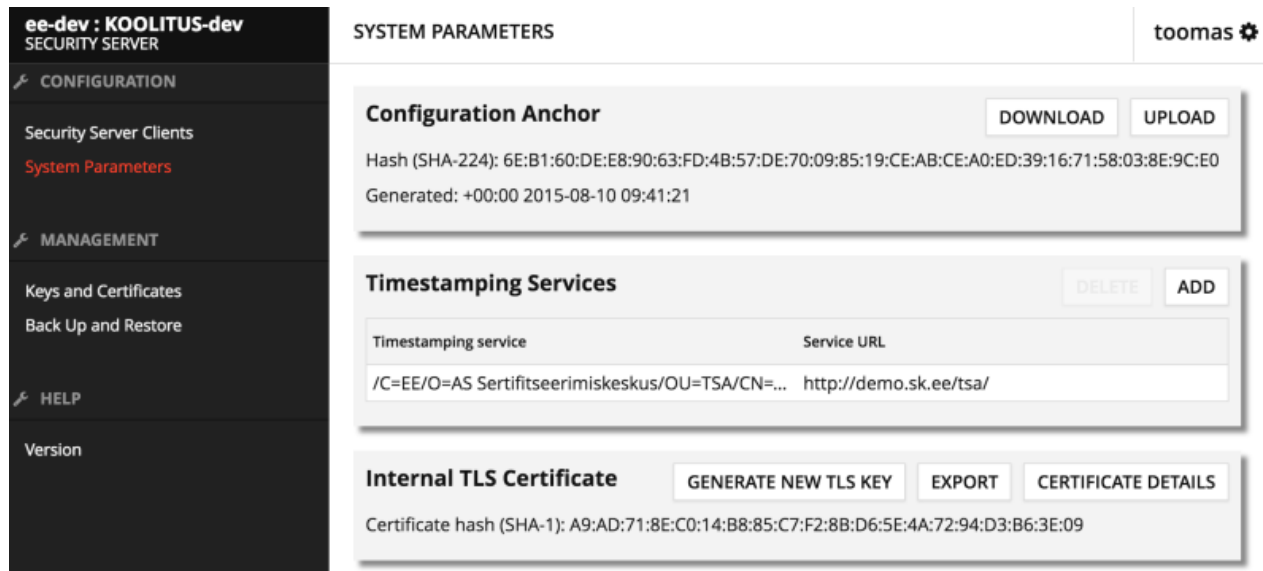
Para exportar un certificado de seguridad TLS interno, siga estos pasos:

- En el menú "Configuración", seleccione "Parámetros del sistema". Abre la vista de parámetros del sistema.
- En la sección " Certificado TLS interno ", haga clic en " Exportar " y guarde el archivo provisto en el sistema de archivos local.

Para ver el certificado TLS interno de seguridad TLS, siga estos pasos:

- En el menú " Configuración ", seleccione " Parámetros del sistema ". Abre la vista de parámetros del sistema.
- En la sección " Certificado TLS interno ", haga clic en " Detalles del certificado ".
-

Figura 39: Parámetros del sistema



Fuente: <https://x-road.global/xroad-playaround>

2.50 Validación de la instalación

Puede verificar si la instalación del servidor de seguridad de X-Road ha sido exitosa solicitando información sobre posibles proveedores de servicios (es decir, miembros y subsistemas) de la instancia de X-Road. Para hacer esto, la consulta HTTP GET debe hacerse al servidor de seguridad.

La URL de consulta es `http:// SECURITYSERVER / listClients` o `https:// SECURITYSERVER / listClients`, dependiendo de si el protocolo HTTPS está configurado para la comunicación entre el servidor de seguridad y el sistema de información. Al realizar una consulta, la dirección SECURITYSERVER debe reemplazarse con la dirección real del servidor de seguridad.

La respuesta del servidor de seguridad debe ser contenido / tipo text / xml y la respuesta DEBE incluir el elemento XML clientList definido a continuación:

Figura 40: Validación de la instalación

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<ns2:clientList xmlns:ns1="http://x-road.eu/xsd/identifiers" xmlns:ns2="http://x-road.eu/xsd/xroad.xsd">
  <ns2:member>
    <ns2:id ns1:objectType="MEMBER">
      <ns1:xRoadInstance>ee-dev</ns1:xRoadInstance>
      <ns1:memberClass>GOV</ns1:memberClass>
      <ns1:memberCode>70006317</ns1:memberCode>
    </ns2:id>
    <ns2:name>Riigi Infosüsteemi Amet</ns2:name>
  </ns2:member>
  <ns2:member>
    <ns2:id ns1:objectType="SUBSYSTEM">
      <ns1:xRoadInstance>ee-dev</ns1:xRoadInstance>
      <ns1:memberClass>GOV</ns1:memberClass>
      <ns1:memberCode>70006317</ns1:memberCode>
      <ns1:subsystemCode>testservice</ns1:subsystemCode>
    </ns2:id>
    <ns2:name>Riigi Infosüsteemi Amet</ns2:name>
  </ns2:member>
  <ns2:member>
    <ns2:id ns1:objectType="SUBSYSTEM">
      <ns1:xRoadInstance>ee-dev</ns1:xRoadInstance>
      <ns1:memberClass>GOV</ns1:memberClass>
      <ns1:memberCode>70006317</ns1:memberCode>
      <ns1:subsystemCode>aar</ns1:subsystemCode>
    </ns2:id>
    <ns2:name>Riigi Infosüsteemi Amet</ns2:name>
  </ns2:member>
  <ns2:member>
    <ns2:id ns1:objectType="SUBSYSTEM">
      <ns1:xRoadInstance>ee-dev</ns1:xRoadInstance>
      <ns1:memberClass>GOV</ns1:memberClass>
```

Fuente: <https://x-road.global/xroad-playaround>

2.51 Sujetos de derechos de acceso.

Los derechos de acceso del servidor de seguridad se pueden otorgar a:

- Subsistema de miembros de X-Road

Los grupos globales de Global Access Group se crean en una X-Road Management Authority. Si se otorga acceso al grupo, este grupo se extiende a todos los miembros. Grupo de acceso local para facilitar la administración de los derechos de acceso, cada cliente del servidor de seguridad puede crear grupos con derechos de acceso locales. Si se otorga acceso al grupo, este grupo se extiende a todos los miembros.

La diferencia entre un grupo con derechos de acceso global y local es su origen. Los grupos de acceso global están definidos por X-Road Management Authority, pero los grupos locales se pueden crear en el

servidor de seguridad. Los grupos globales son más generales, pero los grupos locales con sus miembros son más específicos.

2.52 Gestión de derechos de acceso.

Hay dos formas de administrar los derechos de acceso en un servidor de seguridad.

- La gestión de derechos de acceso basada en servicios permite abrir o cerrar un servicio para múltiples clientes de servicios.
- Administración de derechos de acceso basada en el cliente: si necesita abrir o cerrar varios servicios para un cliente de servicio.

2.53 Cambiar los derechos de acceso al servicio.

Para cambiar los derechos de acceso a un servicio, haga lo siguiente:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione el cliente de la tabla y haga clic en el icono " Servicios " en la línea del cliente.
- Seleccione un servicio de la tabla y haga clic en Derechos de acceso. En la ventana que se abre, la información sobre todos los subsistemas y grupos de X-Road que tienen acceso al servicio seleccionado se muestra en la tabla de derechos de acceso.
- Para agregar uno o más derechos de acceso al servicio, haga clic en el botón "Agregar asuntos". Aparece la ventana de búsqueda de asunto. Puede buscar desde todos los subsistemas y grupos globales en X-Road Management Authority y desde los grupos locales de clientes en el servidor de seguridad. Seleccione uno o más temas de la tabla y haga clic en el botón " Agregar seleccionados a ACL". Haga clic en " Agregar todo a ACL" para otorgar derechos de acceso a todos los sujetos en el resultado de búsqueda.
- Para eliminar asuntos para acceder al servicio, seleccione las líneas correspondientes en la tabla de derechos de acceso y haga clic en el botón Eliminar selección. Para borrar la lista de derechos de acceso (es decir, eliminar todos los temas), haga clic en el botón "Eliminar todos".

2.54 Añadir un cliente de servicio

En la Vista del cliente del servicio (Configuración -> Clientes del servidor de seguridad -> Clientes del servicio) se muestran todos los temas con derechos de acceso a los servicios intermedios del cliente del servidor de seguridad. En otras palabras, si a un subsistema o grupo de X-Road se le da acceso al servicio de ese cliente, el tema se muestra en esa vista.

Para agregar un cliente de servicio, haga lo siguiente:

- En el menú " Configuración ", seleccione "Clientes del servidor de seguridad".
- Seleccione un cliente de la tabla y haga clic en el icono "Clientes de servicio", luego seleccione "Agregar".
- En la ventana que se abre, busque y seleccione el asunto (subsistema o grupo local o global) al que desea otorgar acceso y haga clic en el botón "Siguiente".
- Busque los servicios a los que desea otorgar acceso al tema seleccionado. Para otorgar acceso a los servicios seleccionados para este tema, haga clic en el botón " Agregar seleccionados a ACL". Para otorgar derechos de acceso a este servicio para todos los servicios en el filtro, haga clic en el botón " Agregar todos a ACL".
- El asunto se agrega a la lista de clientes del servicio y, a continuación, se muestra la vista de derechos de acceso del cliente del servicio, donde se pueden modificar los derechos de acceso.

2.55 Cambio de los derechos de acceso del cliente de servicio.

Para cambiar los derechos de acceso de un cliente de servicio, haga lo siguiente:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione un cliente de la tabla y haga clic en el icono " Clientes del servicio " en la línea del cliente.
- En la ventana que se abre, busque y seleccione el asunto (subsistema o grupo local o global) cuyos derechos de acceso desea cambiar y seleccione Derechos de acceso.
- En la ventana que se abre, se muestra una lista de servicios abiertos al servidor de seguridad para el tema seleccionado.
- Para eliminar los derechos de acceso a un servicio de un cliente de servicio, seleccione uno o más servicios de la tabla y haga clic en el botón "Eliminar todo", y luego haga clic en "Confirmar".
- Para eliminar todos los derechos de acceso del cliente del servicio, haga clic en el botón "Eliminar todos" y luego en el botón "Confirmar".
- Para agregar derechos de acceso a un cliente del servicio, haga clic en el botón Agregar servicio. En la ventana que se abre, seleccione el (los) servicio (s) que desea brindar al sujeto (los servicios ya proporcionados aparecen en gris) y haga clic en el botón "Agregar selección a ACL". Haga clic en "Agregar todo a ACL" para agregar todos los servicios encontrados en la búsqueda.

Tenga en cuenta que, si actualiza la página, todos los clientes del servicio que no tengan derechos de acceso a ningún servicio serán eliminados de la vista de los clientes del servicio.

2.56 Grupos con derechos de acceso locales y globales.

Se puede crear un grupo de acceso local para el cliente del servidor de seguridad para facilitar la administración del acceso al servicio para el grupo del subsistema X-Road que utiliza los mismos servicios. Los derechos de acceso otorgados al grupo se aplican a todos los miembros del grupo.

Los grupos locales se basan en el cliente o subsistema. Los grupos locales se utilizan para administrar los derechos de acceso a un solo cliente de servidor de seguridad en un servidor de seguridad.

Los grupos globales tienen derechos de acceso similares a los grupos locales. Por ejemplo, puede otorgar acceso a todos los miembros de X-Road dando acceso al grupo Todos los consumidores.

2.57 Añadiendo un grupo local

Para crear un grupo local para el cliente del servidor de seguridad, haga lo siguiente:

- En el menú "Configuración", seleccione "Clientes del servidor de seguridad", seleccione el cliente y haga clic en el icono "Grupos locales" en esta línea. La ventana de apertura muestra los grupos locales del cliente.
- Haga clic en el botón "Agregar grupo" para crear un nuevo grupo. En la ventana que se abre, ingrese el código y la descripción del nuevo grupo y haga clic en Aceptar

2.58 Ver y editar miembros del grupo local

Para ver los miembros del grupo local, siga estos pasos:

- En el menú "Configuración", seleccione "Clientes del servidor de seguridad", seleccione el cliente y haga clic en el icono "Grupos locales" en esta línea.
- En la ventana que se abre, seleccione el grupo cuyos miembros desea ver o editar y haga clic en Detalles para abrir la vista de detalles.

Para agregar uno o más miembros a un grupo local, siga las instrucciones en la vista de detalles del grupo.

- Haga clic en el botón Agregar miembros.
- En la ventana que se abre, busque y seleccione el subsistema que desea agregar al grupo y haga clic en el botón "Agregar seleccionado al grupo". Para agregar todos los subsistemas encontrados en la función de búsqueda al grupo, haga clic en el botón "Agregar todos al grupo".

Para eliminar miembros de su grupo local, seleccione los miembros que desea eliminar en la vista de detalles del grupo y haga clic en el botón Eliminar miembros seleccionados. Para eliminar a todos los miembros del grupo, haga clic en "Eliminar todos los miembros".

2.59 Cambiar la descripción del grupo local

Para cambiar la descripción del grupo local, haga lo siguiente:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione un cliente de la tabla y haga clic en el icono "Grupos locales" en esta línea.
- Seleccione un grupo de la tabla de grupos locales y haga clic en "Detalles".
- En la vista de detalles del grupo, haga clic en Editar para cambiar la descripción.
- Ingrese una descripción para el grupo y seleccione OK

2.60 Eliminar un grupo local

Tenga en cuenta que cuando se elimina un grupo local, se cancelan todos los derechos de acceso para los miembros del grupo que se les asignaron.

Para eliminar un grupo local, siga estos pasos:

- En el menú " Configuración ", seleccione " Clientes del servidor de seguridad ", seleccione un cliente de la tabla y haga clic en el icono "Grupos locales" en esta línea.
- Seleccione un grupo de la tabla de grupos locales y haga clic en "Detalles".
- Haga clic en el comando "Eliminar grupo" en la vista de detalles del grupo y confirme la eliminación en la ventana que se abre. Para ello, haga clic en el botón "Confirmar".

2.61 Necesidad de monitoreo del servidor de seguridad

La calidad del servicio está determinada, entre otras cosas, por su disponibilidad. Para garantizar que los servicios estén siempre disponibles, los servidores de seguridad que proporcionan el servicio deben tener suficientes recursos.

Por ejemplo, se pueden seguir los siguientes, que determina, entre otras cosas, los requisitos de disponibilidad. Los cuatro niveles de disponibilidad son:

- K0: disponibilidad inferior al 80% anual, tiempo de interrupción máximo permisible durante las horas de servicio superior a 24 horas,
- K1: disponibilidad 80% -99% anual, tiempo de interrupción único permitido máximo durante las horas de servicio 4-24 horas,

- K2: disponibilidad 99% -99.9% anual, tiempo de interrupción único permitido máximo durante las horas de servicio 1-4 horas,
- K3: disponibilidad de al menos el 99,9% anual, tiempo máximo de interrupción permitido durante las horas de servicio hasta 1 hora.
- Los requisitos de disponibilidad y los tiempos de respuesta generalmente se definen en el Acuerdo de Nivel de Servicio (SLA). Estos requisitos generalmente los define la entidad a la que se le debe solicitar dicha información.

2.62 Comandos de monitoreo del servidor de seguridad

A continuación, en este tutorial, se explican los comandos utilizados para monitorear el servidor de seguridad:

- " Top"
- " El tiempo de actividad"
- " Sal"
- " Libre"
- " Df"
- " Iostat"
- " Mpstat"
- " Netstat"
- " Iptraf" y
- " Iftop."

2.63 Comando superior

El comando "top" es un comando de actividad de proceso. El programa "top" proporciona una vista dinámica en tiempo real del sistema en ejecución. Esto puede mostrar información agregada del sistema, así como una lista de procesos o subprocesos actualmente administrados por el kernel de Linux. El usuario puede configurar los tipos de información agregada del sistema mostrado y los tipos, colas y volúmenes de información mostrada para los procesos, y su configuración puede hacerse permanente para todos los reinicios.

Figura 41: Comando "Top"

```
top - 10:17:27 up 2:39, 1 user, load average: 0.00, 0.01, 0.05
Tasks: 166 total, 2 running, 164 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.7 us, 0.3 sy, 0.0 ni, 99.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 2049104 total, 1595732 used, 453372 free, 69340 buffers
KiB Swap: 2095100 total, 0 used, 2095100 free. 375264 cached Mem

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
 1093 xroad    20   0 2091008 186356 30956 S   0.7   9.1   1:35.16 java
 1095 xroad    20   0 2242312 235192 31712 S   0.7  11.5   0:46.01 java
 1086 xroad    20   0 2266496 406224 32604 S   0.3  19.8   3:52.63 java
 1090 xroad    20   0 2102500 192612 31548 S   0.3   9.4   1:21.33 java
   1 root      20   0  33504   3924  2600 S   0.0   0.2   0:01.35 init
   2 root      20   0     0     0     0 S   0.0   0.0   0:00.00 kthreadd
   3 root      20   0     0     0     0 S   0.0   0.0   0:00.02 ksoftirqd/0
   5 root      0 -20     0     0     0 S   0.0   0.0   0:00.00 kworker/0:0H
   7 root      20   0     0     0     0 S   0.0   0.0   0:00.34 rcu_sched
   8 root      20   0     0     0     0 S   0.0   0.0   0:00.00 rcu_bh
   9 root      20   0     0     0     0 R   0.0   0.0   0:00.31 rcuos/0
  10 root      20   0     0     0     0 S   0.0   0.0   0:00.00 rcuob/0
  11 root      rt   0     0     0     0 S   0.0   0.0   0:00.00 migration/0
```

Fuente: <https://x-road.global/xroad-playground>

El comando "superior" proporciona una buena descripción general del tiempo de inactividad del servidor, el promedio de carga del sistema de 1, 5 y 15 minutos y el uso de memoria y CPU en general, así como para cada proceso individual.

El comando "top" proporciona varios atajos útiles:

Tabla 6: Opciones comando "Top"

t	Activa y desactiva la información agregada.
m	Activa y desactiva la información de la memoria.
Un	Ordena la pantalla por usuarios principales del sistema de diferentes recursos del sistema (útil para identificar tareas que requieren rendimiento del sistema).
f	Inserta una imagen de configuración interactiva para la parte superior. (útil para establecer la parte superior para una tarea específica).
o	Le permite seleccionar interactivamente el orden interno de la parte superior.
1	Muestra la carga de la CPU.
k	Emite el comando "matar".

Fuente: Corporación Agencia Nacional de Gobierno Digital

La regla general es que el servidor no debe atraer la memoria y la carga no debe exceder 1 (1 = 100%) de acuerdo con el volumen de CPU disponible. Por lo tanto, si tiene cuatro núcleos, la carga no debe exceder de 4.

2.64 Comando de tiempo de actividad

El comando de tiempo de actividad se puede usar para ver cuánto tiempo se ha estado ejecutando el servidor.

- El comando también ayuda a comprobar:
- tiempo
- el número de usuarios actualmente conectados y
- carga promedio del sistema en los últimos 1, 5 y 15 minutos.

Figura 42: Comando "uptime"

```
toomas@xt:~$ uptime
10:18:15 up 2:40, 1 user, load average: 0.16, 0.05, 0.06
toomas@xt:~$ █
```

Fuente: <https://x-road.global/xroad-playground>

2.65 Comando "ps"

El comando "ps" muestra información sobre la selección de procesos activos.

- Use ps -A para mostrar todos los procesos.

Figura 43: Comando "ps"

```
toomas@xt:~$ ps -A
  PID TTY          TIME CMD
    1 ?            00:00:01 init
    2 ?            00:00:00 kthreadd
    3 ?            00:00:00 ksoftirqd/0
    5 ?            00:00:00 kworker/0:0H
    7 ?            00:00:00 rcu_sched
    8 ?            00:00:00 rcu_bh
    9 ?            00:00:00 rcuos/0
   10 ?            00:00:00 rcuob/0
   11 ?            00:00:00 migration/0
   12 ?            00:00:00 watchdog/0
   13 ?            00:00:00 khelper
   14 ?            00:00:00 kdevtmpfs
   15 ?            00:00:00 netns
   16 ?            00:00:00 perf
   17 ?            00:00:00 khungtaskd
   18 ?            00:00:00 writeback
```

Fuente: <https://x-road.global/xroad-playground>

Utilice ps auxf para mostrar el árbol de procesos.

Figura 44: Comando "ps auxf"

```
  1 1086 1086 1086 ?          -1 Ssl 107 3:55 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx128m -XX:MaxMetaspaceSize=100m -Djruby.co
  1 1088 1088 1088 ?          -1 Ss  0 0:00 /usr/sbin/sshd -D
1088 2749 2749 2749 ?          -1 Ss  0 0:00 \_ sshd: toomas [priv]
2749 2819 2749 2749 ?          -1 S   1000 0:00 \_ sshd: toomas@pts/0
2819 2820 2820 2820 pts/0 2871 Ss 1000 0:00 \_ -bash
2820 2871 2871 2820 pts/0 2871 R+ 1000 0:00 \_ ps auxf
  1 1090 1090 1090 ?          -1 Ssl 107 1:22 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlogback.co
  1 1091 1091 1091 ?          -1 Ssl 107 0:19 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlogback.co
  1 1093 1093 1093 ?          -1 Ssl 107 1:36 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=50m -Dlogback.co
  1 1094 1094 1094 ?          -1 Ss  0 0:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
  1 1095 1095 1095 ?          -1 Ssl 107 0:46 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xms100m -Xmx150m -XX:MaxMetaspaceSize=70m -D
  1 1096 1096 1096 ?          -1 Ss  1 0:00 atd
  1 1097 1097 1097 ?          -1 Ss  0 0:00 cron
  1 1220 1217 1217 ?          -1 S   105 0:00 /usr/lib/postgresql/9.3/bin/postgres -D /var/lib/postgresql/9.3/main -c config_file=/etc/pos
1220 1222 1222 1222 ?          -1 Ss  105 0:00 \_ postgres: checkpointer process
1220 1223 1223 1223 ?          -1 Ss  105 0:00 \_ postgres: writer process
1220 1224 1224 1224 ?          -1 Ss  105 0:00 \_ postgres: wal writer process
1220 1225 1225 1225 ?          -1 Ss  105 0:00 \_ postgres: autovacuum launcher process
1220 1226 1226 1226 ?          -1 Ss  105 0:00 \_ postgres: stats collector process
1220 2537 2537 2537 ?          -1 Ss  105 0:00 \_ postgres: serverconf serverconf 127.0.0.1(39750) idle
1220 2539 2539 2539 ?          -1 Ss  105 0:00 \_ postgres: serverconf serverconf 127.0.0.1(39762) idle
1220 2585 2585 2585 ?          -1 Ss  105 0:00 \_ postgres: serverconf serverconf 127.0.0.1(40112) idle
```

Fuente: <https://x-road.global/xroad-playground>

Use ps auxw para mostrar todas las opciones de proceso.

Figura 45: Comando "ps auxw"

```

root      1088  0.0  0.2  61380  5588 ?        Ss   07:38   0:00 /usr/sbin/sshd -D
xroad    1090  0.8  9.3 2102500 192092 ?    Ssl  07:38   1:22 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlo
xroad    1091  0.1  6.0 2058060 124952 ?    Ssl  07:38   0:19 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlo
xroad    1093  0.9  9.1 2091008 186640 ?    Ssl  07:38   1:37 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=50m -Dlo
root     1094  0.0  0.0   4372  1560 ?        Ss   07:38   0:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
xroad    1095  0.4 11.4 2242312 235232 ?    Ssl  07:38   0:47 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xms100m -Xmx150m -XX:MaxMetaspaceSiz
daemon   1096  0.0  0.0   1914    160 ?        Ss   07:38   0:00 atd
root     1097  0.0  0.1  23656  2144 ?        Ss   07:38   0:00 cron
postgres 1220  0.0  1.0 247784  21076 ?    S   07:38   0:00 /usr/lib/postgresql/9.3/bin/postgres -D /var/lib/postgresql/9.3/main -c config_file=
postgres 1222  0.0  0.2 247920  5516 ?    Ss   07:38   0:00 postgres: checkpointer process
postgres 1223  0.0  0.2 247784  4700 ?    Ss   07:38   0:00 postgres: writer process
postgres 1224  0.0  0.1 247784  3268 ?    Ss   07:38   0:00 postgres: wal writer process
postgres 1225  0.0  0.3 248644  6156 ?    Ss   07:38   0:00 postgres: autovacuum launcher process
postgres 1226  0.0  0.1 103596  3600 ?    Ss   07:38   0:00 postgres: stats collector process
ntp      1554  0.0  0.2  31452  4416 ?        Ss   07:38   0:00 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 106:114
root     1614  0.0  0.0  15820  2008 tty1    Ss+  07:39   0:00 /sbin/getty -8 38400 tty1
root     1940  0.0  0.0     0     0 ?        S   08:17   0:00 [kauditd]
postgres 2537  0.0  0.6 250344 12296 ?    Ss   09:46   0:00 postgres: serverconf serverconf 127.0.0.1(39750) idle
postgres 2539  0.0  0.5 249324 11972 ?    Ss   09:47   0:00 postgres: serverconf serverconf 127.0.0.1(39762) idle
postgres 2585  0.0  0.5 250328 12264 ?    Ss   09:54   0:00 postgres: serverconf serverconf 127.0.0.1(40112) idle
postgres 2588  0.0  0.5 249324 11972 ?    Ss   09:54   0:00 postgres: serverconf serverconf 127.0.0.1(40138) idle
postgres 2633  0.0  0.6 250344 12376 ?    Ss   10:01   0:00 postgres: serverconf serverconf 127.0.0.1(40490) idle
    
```

Fuente: <https://x-road.global/xroad-playground>

Utilice el siguiente comando para mostrar los primeros 10 procesos basados en el consumo de memoria.

```
ps -auxf | ordenar -nr -k 4 | cabeza -10
```

Figura 46: Comando "ps -auxf | sort -nr -k 4 | head -10"

```

toomas@xti:~$ ps -auxf | sort -nr -k 4 | head -10
xroad    1086  2.4 19.8 2266496 406144 ?        Ssl  07:38   3:56 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx128m -XX:MaxMetaspaceSize=100m -D
jruby.compile.mode=OFF -Djetty.admin.port=8083 -Djetty.public.port=8084 -Daddon.extraClasspath= -Dlogback.configurationFile=/etc/xroad/conf.d/jetty-l
ogback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/ -cp /usr/share/xroad/jetty9/start.jar org.eclipse.
jetty.start.Main jetty.home=/usr/share/xroad/jetty9
xroad    1095  0.4 11.4 2242312 235388 ?        Ssl  07:38   0:47 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xms100m -Xmx150m -XX:MaxMetaspaceSiz
e=70m -Dlogback.configurationFile=/etc/xroad/conf.d/proxy-logback.xml -Dxroad.proxy.clientHandlers=ee.ria.xroad.proxy.clientproxy.AsicContainerHandle
r,ee.ria.xroad.proxy.clientproxy.MetadataHandler -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/ -cp /usr/sha
re/xroad/jlib/proxy.jar:/usr/share/xroad/jlib/addon/proxy/messageLog-1.0.jar:/usr/share/xroad/jlib/addon/proxy/metaservice-1.0.jar -Dxroad.proxy.mess
ageLogManagerImpl=ee.ria.xroad.proxy.messageLog.LogManager -Dxroad.proxy.serverServiceHandlers=ee.ria.xroad.proxy.serverproxy.MetadataServiceHandlerI
mpl -Dxroad.monitoringagent.uri=akka.tcp://XRoadProxyMonitorAgent@127.0.0.1:2554/user/ProxyMonitorAgent ee.ria.xroad.proxy.ProxyMain
xroad    1090  0.8  9.3 2102500 192092 ?    Ssl  07:38   1:22 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlc
gback.configurationFile=/etc/xroad/conf.d/addons/proxy-monitor-agent-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/u
sr/share/xroad/lib/ -cp /usr/share/xroad/jlib/monitoring-proxy-agent.jar ee.ria.xroad.proxy.monitoragent.Main
xroad    1093  0.9  9.1 2091008 186644 ?    Ssl  07:38   1:37 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=50m -Dlc
gback.configurationFile=/etc/xroad/conf.d/signer-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/
-cp /usr/share/xroad/jlib/signer.jar ee.ria.xroad.signer.SignerMain
xroad    1091  0.1  6.0 2058060 124952 ?    Ssl  07:38   0:19 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlc
gback.configurationFile=/etc/xroad/conf.d/confclient-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/l
ib/ -cp /usr/share/xroad/jlib/configuration-client.jar ee.ria.xroad.common.conf.globalconf.ConfigurationClientMain
postgres 1220  0.0  1.0 247784  21076 ?    S   07:38   0:00 /usr/lib/postgresql/9.3/bin/postgres -D /var/lib/postgresql/9.3/main -c config_file=
/etc/postgresql/9.3/main/postgresql.conf
postgres 2689  0.0  0.8 255452 16744 ?        Ss   10:09   0:00 \_ postgres: serverconf serverconf 127.0.0.1(40914) idle

postgres 2839  0.0  0.6 250192 12436 ?    Ss   10:16   0:00 \_ postgres: serverconf serverconf 127.0.0.1(41362) idle

postgres 2633  0.0  0.6 250344 12376 ?    Ss   10:01   0:00 \_ postgres: serverconf serverconf 127.0.0.1(40490) idle

postgres 2537  0.0  0.6 250344 12296 ?    Ss   09:46   0:00 \_ postgres: serverconf serverconf 127.0.0.1(39750) idle

toomas@xti:~$
    
```

Fuente: <https://x-road.global/xroad-playground>

Utilice el siguiente comando para mostrar los primeros 10 procesos basados en el consumo de CPU.

```
ps -auxf | ordenar -nr -k 3 | cabeza -10
```


Figura 47: Comando "ps -auxf | sort -nr -k 3 | head -10"

```
toomas@xt:~$ ps -auxf | sort -nr -k 3 | head -10
xroad      1086  2.4 19.8 2266496 406240 ?        Ssl  07:38   3:57 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx128m -XX:MaxMetaspaceSize=100m -D
jruby.compile.mode=OFF -Djetty.admin.port=8083 -Djetty.public.port=8084 -Daddon.extraClasspath=-Dlogback.configurationFile=/etc/xroad/conf.d/jetty-l
ogback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/ -cp /usr/share/xroad/jetty9/start.jar org.eclipse
jetty.start.Main jetty.home=/usr/share/xroad/jetty9
xroad      1093  0.9  9.1 2091008 186636 ?        Ssl  07:38   1:37 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=50m -Dlo
gback.configurationFile=/etc/xroad/conf.d/signer-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/
-cp /usr/share/xroad/jlib/signer.jar ee.ria.xroad.signer.SignerMain
xroad      1090  0.8  9.3 2102580 192220 ?        Ssl  07:38   1:23 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlo
gback.configurationFile=/etc/xroad/conf.d/addons/proxy-monitor-agent-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/u
sr/share/xroad/lib/ -cp /usr/share/xroad/jlib/monitoring-proxy-agent.jar ee.ria.xroad.proxy.monitoragent.Main
xroad      1095  0.4 11.6 2242312 238388 ?        Ssl  07:38   0:48 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xms100m -Xmx150m -XX:MaxMetaspaceSiz
e=70m -Dlogback.configurationFile=/etc/xroad/conf.d/proxy-logback.xml -Dxroad.proxy.clientHandlers=ee.ria.xroad.proxy.clientproxy.AsicContainerHandle
r,ee.ria.xroad.proxy.clientproxy.MetadataHandler -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/lib/ -cp /usr/sha
re/xroad/jlib/proxy.jar:/usr/share/xroad/jlib/addon/proxy/message-log-1.0.jar:/usr/share/xroad/jlib/addon/proxy/metaservice-1.0.jar -Dxroad.proxy.mess
ageLogManagerImpl=ee.ria.xroad.proxy.messageLog.LogManager -Dxroad.proxy.serverServiceHandlers=ee.ria.xroad.proxy.serverproxy.MetadataServiceHandlerI
mpl -Dxroad.monitoringagent.uri=akka.tcp://XRoadProxyMonitorAgent@127.0.0.1:2554/user/ProxyMonitorAgent ee.ria.xroad.proxy.ProxyMain
xroad      1091  0.1  6.0 2058060 124952 ?        Ssl  07:38   0:19 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xmx50m -XX:MaxMetaspaceSize=70m -Dlo
gback.configurationFile=/etc/xroad/conf.d/confclient-logback.xml -XX:+UseG1GC -Dfile.encoding=UTF-8 -Xshare:on -Djava.library.path=/usr/share/xroad/l
ib/ -cp /usr/share/xroad/jlib/configuration-client.jar ee.ria.xroad.common.conf.globalconf.ConfigurationClientMain
www-data   934  0.0  0.2 42372 5496 ?          S    07:38   0:00 \_ nginx: worker process
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
toomas    2899  0.0  0.0   7216 1756 pts/0    S+   10:22   0:00          \_ head -10
toomas    2898  0.0  0.0  15720 1972 pts/0    S+   10:22   0:00          \_ sort -nr -k 3
toomas    2897  0.0  0.1 18608 2724 pts/0    R+   10:22   0:00          \_ ps -auxf
toomas@xt:~$
```

Fuente: <https://x-road.global/xroad-playground>

2.66 Comando free

El comando "free" muestra la cantidad total de memoria física y de intercambio libre y usada en el sistema, así como las cachés utilizadas por el núcleo.

Figura 48: Comando "free"

```
toomas@xt:~$ free
              total        used        free      shared    buffers     cached
Mem:          2049104      1601928      447176       15144       70268      375444
-/+ buffers/cache:      1156216       892888
Swap:          2095100           0       2095100
toomas@xt:~$
```

Fuente: <https://x-road.global/xroad-playground>

2.67 Comando df

El comando "df" proporciona información sobre el uso del espacio en disco del sistema de archivos.

Utilice `df -h` para mostrar información legible por humanos.

Figura 49: Comando "df-h"

```
toomas@xt:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            990M  4.0K  990M   1% /dev
tmpfs           201M  712K  200M   1% /run
/dev/sda1       7.8G  2.2G  5.2G  30% /
none            4.0K   0  4.0K   0% /sys/fs/cgroup
none            5.0M   0  5.0M   0% /run/lock
none           1001M   0 1001M   0% /run/shm
none            100M   0  100M   0% /run/user
toomas@xt:~$ █
```

Fuente: <https://x-road.global/xroad-playground>

2.68 Comando "iostat"

El comando "iostat" proporciona información sobre las estadísticas de la CPU y la entrada / salida del dispositivo y la sección.

El comando "iostat" se usa para monitorear el dispositivo de entrada / salida del sistema. Para este propósito, se monitoriza el tiempo durante el cual los dispositivos están activos en comparación con su velocidad de transmisión normal. El comando "iostat" genera informes que se pueden usar para modificar la configuración del sistema para equilibrar mejor la carga de entrada / salida entre los discos físicos.

Figura 50: Comando "iostat"

```
toomas@xt:~$ iostat
Linux 4.2.0-27-generic (xt)      07/22/2016      _x86_64_      (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           4.02    0.00    0.46    0.10    0.00   95.42

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda                 3.88         49.09         38.62     488091     384016
scd0                0.00          0.00          0.00         44          0
toomas@xt:~$ █
```

Fuente: <https://x-road.global/xroad-playground>

Este comando también ayuda a identificar si el espacio de almacenamiento es un cuello de botella en algún servidor específico. Muestra tres informes de estadísticas extendidas para el disco con intervalos de cinco segundos.

Figura 51: Comando "iostat -d -x 5 3"

```
toomas@xt:~$ iostat -d -x 5 3
Linux 4.2.0-27-generic (xt)      07/22/2016      _x86_64_      (1 CPU)

Device:            rrqm/s   wrqm/s     r/s     w/s    rkB/s    wkB/s  avgrq-sz  avgqu-sz   await  r_await  w_await  svctm  %util
sda                 0.42     3.47     1.38    2.50   48.83    38.55    45.08     0.02     5.25   14.41    0.20    0.43   0.17
scd0                0.00     0.00     0.00    0.00    0.00     0.00     8.00     0.00     5.09    5.09    0.00    5.09   0.00

Device:            rrqm/s   wrqm/s     r/s     w/s    rkB/s    wkB/s  avgrq-sz  avgqu-sz   await  r_await  w_await  svctm  %util
sda                 0.00     0.20     0.00    0.40    0.00     2.42    12.00     0.00     0.00    0.00    0.00    0.00   0.00
scd0                0.00     0.00     0.00    0.00    0.00     0.00     0.00     0.00     0.00    0.00    0.00    0.00   0.00

Device:            rrqm/s   wrqm/s     r/s     w/s    rkB/s    wkB/s  avgrq-sz  avgqu-sz   await  r_await  w_await  svctm  %util
sda                 0.00    13.16     0.00    3.85    0.00    68.02    35.37     0.00     0.00    0.00    0.00    0.00   0.00
scd0                0.00     0.00     0.00    0.00    0.00     0.00     0.00     0.00     0.00    0.00    0.00    0.00   0.00

toomas@xt:~$
```

Fuente: <https://x-road.global/xroad-playground>

Lo más importante es que sigas lo siguiente.

- svctm: tiempo de servicio mediano (en milisegundos) para las solicitudes de entrada / salida del dispositivo,
- % util: Porcentaje de tiempo de CPU durante el cual las solicitudes de entrada / salida se enviaron al dispositivo (uso de ancho de banda para el dispositivo). La saturación del dispositivo se produce cuando el valor se acerca al 100 por ciento.
- Si estos números son altos, tienes que lidiar con eso.

2.69 Comando mpstat

El comando mpstat proporciona información sobre estadísticas relacionadas con el proceso. El comando mpstat escribe las acciones de salida habituales para cada procesador disponible. El primer procesador es 0. También se informa sobre la actividad global promedio por procesador.

Figura 52: Comando "mpstat"

```
toomas@xt:~$ mpstat -P ALL
Linux 4.2.0-27-generic (xt)      07/22/2016      _x86_64_      (1 CPU)

10:26:55 AM CPU   %usr  %nice   %sys %iowait  %irq   %soft  %steal  %guest  %gnice  %idle
10:26:55 AM all   4.01   0.00   0.42  0.10   0.00  0.04   0.00   0.00   0.00   0.00  95.44
10:26:55 AM  0     4.01   0.00   0.42  0.10   0.00  0.04   0.00   0.00   0.00   0.00  95.44

toomas@xt:~$
```

Fuente: <https://x-road.global/xroad-playground>

2.70 Comando "netstat"

El comando "netstat" imprime conexiones de red, tablas de enrutamiento, estadísticas de interfaz, conexiones de enmascaramiento y membresía de multidifusión. Puede usar netstat -a para mostrar todas las conexiones de red. Para mostrar direcciones numéricas en lugar de tratar de definir un host y un puerto simbólicos, use netstat -an. También puede usar netstat -anp para vincular los puertos de escucha a los programas.

Figura 53: Comando "netstat"

```
toomas@xt:~$ netstat -anp
(No info could be read for "-p": geteuid()=1000 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:4000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432         127.0.0.1:41108        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:40490        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:41750        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:40138        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:41728        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:40112        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:41362        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:40542        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:40546        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:40502        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:40548        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:40936        ESTABLISHED -
tcp        0      0 195.222.5.8:22        195.222.5.1:36574      ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:40544        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:41112        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:41114        ESTABLISHED -
tcp        0      0 127.0.0.1:5432         127.0.0.1:40540        ESTABLISHED -
```

Fuente: <https://x-road.global/xroad-playaround>

2.71 Comando iptraf

"Iptraf" es un monitor de LAN IP basado en ncurses que genera varias estadísticas de red (incluida información TCP, números UDP, información ICMP, información de carga Ethernet, estadísticas de nodos, errores de suma de comprobación de IP, etc.).

"Ipftaf" puede dar la siguiente información en un formato fácil de leer:

- Estadísticas de tráfico de red por conexión TCP,
- Estadísticas de tráfico IP por interfaz de red.
- Estadísticas de tráfico de red por protocolo.
- Estadísticas de tráfico de red por puerto TCP / UDP y tamaño de paquete
- Estadísticas de tráfico de red por dirección Layer2.

Figura 54: Comando "IPTraf"

```

IPTraf
-----
Statistics for eth0

          Total      Total      Incoming   Incoming   Outgoing   Outgoing
          Packets    Bytes     Packets    Bytes     Packets    Bytes
Total:    289      64568      143      15620      146      48948
IP:       289      60522      143      13618      146      46904
TCP:     287      60354      142      13534      145      46820
UDP:      0         0         0         0         0         0
ICMP:     2        168         1         84         1         84
Other IP: 0         0         0         0         0         0
Non-IP:   0         0         0         0         0         0

Total rates:    63.6 kbits/sec      Broadcast packets: 0
                35.2 packets/sec      Broadcast bytes: 0

Incoming rates:  9.4 kbits/sec
                17.6 packets/sec

Outgoing rates: 54.2 kbits/sec      IP checksum errors: 0
                17.6 packets/sec
  
```

Fuente: <https://x-road.global/xroad-playground>

2.72 Comando iftop

El comando "iftop" muestra el ancho de banda en la interfaz en tiempo real por el host.

El comando "iftop" escucha el tráfico de red en esa interfaz o la primera interfaz que encuentra y se parece a una interfaz externa si no se especifica nada y muestra la tabla actual de uso de ancho de banda por pares de hosts.

El comando "iftop" debe ejecutarse con permisos suficientes para monitorear todo el tráfico de red en la interfaz.

Figura 55: Comando "iftop"

```

          12.5kb      25.0kb      37.5kb      50.0kb      62.5kb
-----
xt.box.ee => ns.box.ee 4.52kb 2.02kb 2.28kb
           <= 2.84kb 914b 901b
xt.box.ee => 195.80.109.140 0b 346b 247b
           <= 0b 2.34kb 1.67kb
xt.box.ee => cs01.dev.roksnet.com 0b 347b 248b
           <= 0b 1.47kb 1.05kb
xt.box.ee => wsrp.test.digilugu.ee 0b 346b 247b
           <= 0b 1.46kb 1.04kb
xt.box.ee => golem.canonical.com 0b 61b 43b
           <= 0b 61b 43b

TX: [redacted] cum: 5.33kB peak: 6.17kb rates: 4.52kb 3.10kb 3.05kb
RX: [redacted] 8.19kB 26.5kb 2.84kb 6.22kb 4.68kb
TOTAL: 13.5kB 32.7kb 7.36kb 9.31kb 7.73kb
  
```

Fuente: <https://x-road.global/xroad-playground>

2.73 Aplicaciones de monitoreo

Las herramientas enumeradas lo ayudarán a supervisar el servidor de seguridad cuando inicie sesión. A largo plazo, es aconsejable utilizar aplicaciones que recopilen información a lo largo del tiempo y la presenten, por ejemplo, gráficamente. Esto proporciona una mejor comprensión de cómo funciona el sistema con carga alta.

Para obtener resultados confiables, las aplicaciones de monitoreo deben instalarse en un servidor separado. Por ejemplo, los mensajes de error de la red no se pueden enviar por correo electrónico si la propia red no funciona.

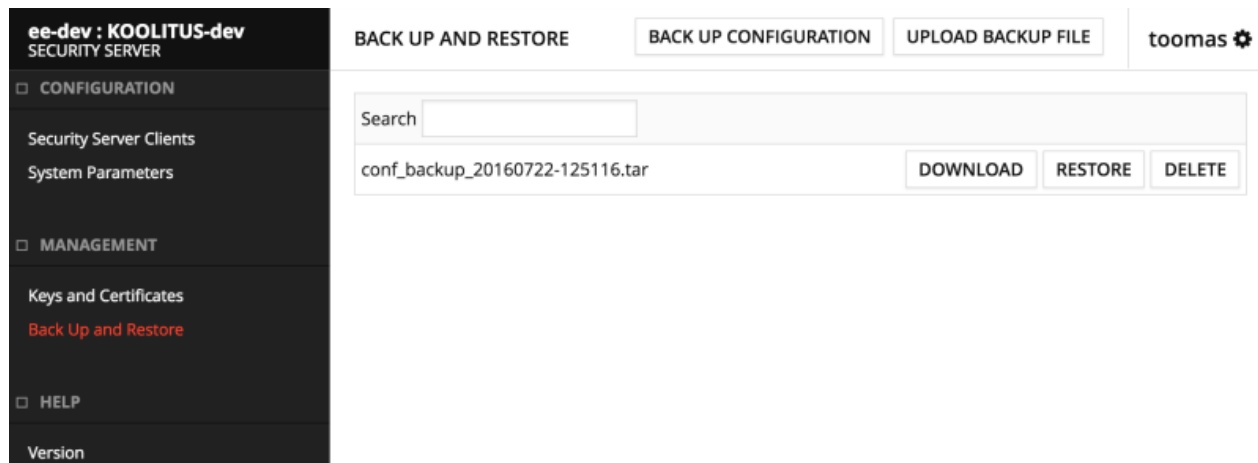
A continuación, las siguientes herramientas de monitoreo se presentarán

- Cactus
- Nagios

2.74 Vista de la interfaz de usuario del servidor de seguridad de respaldo

Se puede acceder a la copia de seguridad a través del menú "Administración" seleccionando "Copia de seguridad y restauración".

Figura 56: Interfaz copia de seguridad y restauración



Fuente: <https://x-road.global/xroad-playground>

2.75 Copia de seguridad de la configuración del servidor de seguridad

Para hacer una copia de seguridad de su configuración, siga estos pasos:

- Haga clic en el botón "Haga clic en Configuración de copia de seguridad".
- En la ventana que se abre, se muestra la salida del script de copia de seguridad. Haga clic en Aceptar para cerrarla. El archivo de copia de seguridad de configuración se muestra en la lista de archivos de copia de seguridad de configuración.
- Para guardar el archivo de copia de seguridad de la configuración en el sistema de archivos local, haga clic en el botón "Descargar" en la línea del archivo de configuración y guarde el archivo al que se hace referencia.

2.76 Cargar y eliminar un archivo de copia de seguridad de configuración

Para cargar el archivo de copia de seguridad de la configuración desde el sistema de archivos local al servidor de seguridad, haga clic en el botón Cargar archivo de carga, seleccione el archivo y haga clic en el botón Aceptar. El archivo de configuración cargado se muestra en la lista de archivos de configuración.

Para eliminar un archivo de respaldo de configuración, haga clic en el botón "Eliminar" en la línea correspondiente en la lista de respaldo de configuración, y luego haga clic en "Confirmar".

2.77 Restaurar la configuración de la interfaz de usuario

Se puede acceder a la vista de recuperación a través del menú "Administración" si selecciona "Copia de seguridad y restauración".

Para restaurar la configuración, haga lo siguiente:

- Haga clic en "Restaurar" en la línea correspondiente en la Lista de respaldo de configuración y luego en "Confirmar".
- La salida de la ventana de salida se muestra en la ventana que se abre. Haga clic en Aceptar para cerrarla.

2.78 Restaura la configuración desde la línea de comandos

Para restaurar la configuración desde la línea de comandos, debe estar disponible una ID de servidor de seguridad. Se supone que el comando de recuperación es ejecutado por el usuario de X-Road.

Para restaurar la configuración, use el siguiente comando (todo en una línea):

```
/usr/share/xroad/scripts/restore_xroad_proxy_configuration.sh s <ID del servidor de seguridad> -f <ruta + nombre de archivo>
```

Por ejemplo (todo en una línea):

```
/usr/share/xroad/scripts/restore_xroad_proxy_configuration.sh/A / GOV / TS1OWNER / TS1 -f /var/lib/xroad/backup/conf_backup_20140703-110438.tar
```

Es muy necesario restaurar el sistema desde un archivo de copia de seguridad realizado en un servidor de seguridad diferente y usar el comando forzado para usar la opción -F.

Por ejemplo (todo en una línea):

```
/usr/share/xroad/scripts/restore_xroad_proxy_configuration.sh \ -F -F /var/lib/xroad/backup/conf_backup_20140703-110438.tar
```

2.79 Importancia de archivar los registros de mensajes

La función de registro de mensajes es para demostrar la recepción de los mensajes de solicitud o respuesta ordinarios intercambiados a través de X- Road.

Para cada mensaje, el servidor produce un contenedor de mensajes completo y con sello de tiempo (Associated Signature Container, ASiC) y lo archiva en el sistema de archivos local. Los archivos archivados son contenedores zip con un archivo especial para la información del revestimiento para una verificación de integridad adicional.

2.80 Cambiar la configuración de archivo de la configuración del registro de mensajes

Los parámetros de configuración se definen en el archivo INI, donde cada sección contiene los parámetros de un componente específico del servidor de seguridad.

La configuración predeterminada del registro de mensajes está en el archivo.

```
/etc/xroad/conf.d/addons/message-log.ini
```

Crea o edita un archivo para anular los valores predeterminados

```
/etc/xroad/conf.d/local.ini
```

Cree [message-log] en el archivo (si aún no lo ha hecho). Al comienzo de la sección, haga una lista de los valores de los parámetros, uno por línea. Por ejemplo, para configurar los parámetros archive-path y archive-max-filesize, se debe agregar un archivo de configuración


```
[registro de mensajes]
```

```
archive-ruta = / mi / archive / ruta /
```

```
archive-max-filesize = 67108864
```

Es posible configurar el parámetro hash SHA-id. Este es un algoritmo utilizado para el hash de registro de mensajes. Las opciones posibles son SHA-256, SHA-384 y SHA-512. (Predeterminado SHA-512)

2.90 Parámetros de sellado de tiempo

Se pueden utilizar los siguientes parámetros de sellado de tiempo.

```
timestamp-immediate
```

Cuando se establece en Verdadero, se crea una marca de tiempo de forma síncrona para cada mensaje de solicitud o respuesta. Esta es una política de seguridad que garantiza la marca de tiempo en el momento de registrar el mensaje. Para una mejor disponibilidad, el valor predeterminado se establece en Falso.

```
timestamp-records-limit
```

Número máximo de artículos con sello de tiempo por paquete

Al configurar este valor, debe considerar el rendimiento de la mensajería (mensaje por minuto) y el rango de sellado de tiempo del servidor de seguridad.

Este parámetro no se puede cambiar sin una razón específica.

Predeterminado 10000

2.91 Transferencia de archivos de un servidor de seguridad

El paquete de registro de mensajes proporciona un script de ayuda para transferir archivos de archivado:

```
/usr/share/xroad/scripts/archive-http-transporter.sh
```

La secuencia de comandos utiliza el protocolo HTTP / HTTPS (método POST, archivo de nombre de formulario) para transferir archivos de archivado al servidor de archivado.

Utilizando el script:

Tabla 7: Secuencia de comandos para transferencia de archivos de un servidor de seguridad

<code>-d, --dir, DIR</code>	Directorio de archivos Por defecto / var / lib / xroad
-----------------------------	--

-r, --eliminar	Elimina los archivos transportados del directorio de archivos.
-k, --key, KEY	Nombre de archivo de clave privada en formato PEM (TLS) Predeterminado /etc/xroad/ssl/internal.key
-c, --cert, CERT	le cliente en formato PEM (TLS) /ssl/internal.crt
--cacert, ARCHIVO CA	Archivo de certificado para la verificación de afiliados (TLS) El archivo puede contener múltiples certificados de CA. Los certificados deben estar en formato PEM.
-h, --ayudar	Texto de ayuda

Fuente: Corporación Agencia Nacional de Gobierno Digital

El archivo de almacenamiento se ha transferido correctamente cuando el servidor de archivo devuelve el código de estado HTTP 200.

Para configurar el script de transferencia, anule el parámetro de configuración archive-transfer-command (cree o edite el archivo, etc. / xroad / conf.d / local.ini). Por ejemplo:

[registro de mensajes]

```
Archivo de transferencia de mando = / usr / share / XROAD / scripts / Archivo-http  
transporter.sh -r http: // mi-archivo del servidor / cgi-bin / carga
```

El paquete de registro de mensajes contiene un script CGI para el servidor de archivos de demostración para pruebas o desarrollo

```
/usr/share/doc/xroad-addon-messagelog/archive-server/demo-upload.pl
```

3. Intervención a los servicios web soap y rest (framework desarrollo pdi 1.0)

SERVICIOS SOAP: De acuerdo con las reglas de X-Road, los encabezados específicos obligatorios de X-Road siempre deben ser descritos y transmitidos en mensajes. Los encabezados deben tener una estructura y un espacio de nombres correctos, que es <http://x-road.eu/xsd/identifiers> . Los campos de encabezado obligatorios y adicionales se describen en la especificación del protocolo de mensajes X-Road (http://x-road.eu/docs/x-road_message_protocol_v4.0.pdf).

3.1 Los campos de encabezado obligatorios de X-Road son los siguientes:

Client: campo obligatorio de tipo complejo que identifica al cliente que inició la solicitud, que se describe con los siguientes elementos:

xRoadInstance: El valor del campo para los miembros de X-Road es EE en la instancia de producción, ee-test en la instancia de prueba y ee-dev en la instancia de desarrollo;

memberClass - el campo diferencia las clases de miembros (GOV);

memberCode: el valor del campo es el código de registro de la autoridad;

subsystemCode: el valor del campo corresponde al nombre del subsistema.

< service >< centralService > - campos de tipo complejo, uno de los cuales es obligatorio. El campo especifica el servicio de datos que se utilizará. Los elementos descriptivos del campo son idénticos al campo **< client >** (xRoadInstance, memberClass, memberCode y subsystemCode), a los que se agregan los siguientes campos:

serviceCode: nombre de la envoltura correspondiente al mensaje SOAP del servicio de datos;

serviceVersion - versión del servicio de datos.

< id > - campo obligatorio, cuyo valor es un identificador único del mensaje. El ID de mensaje debe ser único para cada miembro. El formato recomendado del campo **<id>** es UUID. Véase también https://en.wikipedia.org/wiki/Universally_unique_identifier

< protocolVersion > - un campo obligatorio que muestra la versión del protocolo de mensajes X-Road. El valor del campo debe ser 4.0

< requestHash >: el servidor de seguridad llena automáticamente el contenido de este encabezado. El campo tiene contenido solo en el caso de mensajes de respuesta e incluye hash de solicitud.

< requestHash / @ algorithmId >: el contenido de este atributo muestra qué algoritmo se utilizó para calcular el hash de solicitud.

3.2 Los campos de encabezado adicionales no obligatorios de X-Road son los siguientes:

<userId> - un campo no obligatorio, cuyo valor es el código de identificación personal del usuario que inició la solicitud junto con un prefijo de dos letras del código de país ISO (por ejemplo, EE12345678901). Si el usuario final está autenticado, debe incluirse el campo ID de usuario;

<issue> - un campo no obligatorio, cuyo valor es la base de la solicitud (código interno del remitente de la solicitud para indicar un archivo o una referencia en la gestión de documentos, etc.). Habilita la referencia a solicitudes, por ejemplo, si se usan datos personales y es necesario responder a las solicitudes de un ciudadano o Inspector de Protección de Datos.

3.3 Creación de un servicio de datos X-Road y un cliente basado en WSDL (en la plataforma Java)

Para crear un servicio de datos de X-Road, usamos Maven de Eclipse, que genera un código necesario a través de CXF. Para esto, cambiamos el archivo pom.xml. Agregando los componentes necesarios **<properties>**, **<dependency>** y **<plugin>**.

En primer lugar, agregue <properties> y <dependency> para que Maven descargue todos los archivos jar necesarios. Si es necesario, todos los archivos se pueden descargar manualmente.¹

```
<!-- properties -->
<properties>
<cxf.version> 3.2.0 </cxf.version>
<spring.version> 4.3.11.RELEASE </spring.version>
<cxf.scope> build </cxf.scope>
<compileSource> 1.8 </compileSource>
<maven.compiler.target> 1.8 </maven.compiler.target>
<maven.compiler.source> 1.8 </maven.compiler.source>
<project.build.sourceEncoding> UTF-8 </project.build.sourceEncoding>
</properties>
<dependency>
<!-- apache cxf jax-ws 3.2.0 -->
<dependencia>
<groupId> org.apache.cxf </groupId>
<artifactId> cxf-core </artifactId>
<version> $ {cxf.version} </version>
</dependency>
<dependency>
<groupId> org.apache.cxf </groupId>
<artifactId> cxf-rt-frontend-jaxws </artifactId>
<version> $ {cxf.version} </version>
<scope> $ {cxf.scope} </scope>
</dependency>
<dependency>
```

¹ <https://moodle.ria.ee/mod/page/view.php?id=571>

```
<groupId> org.apache.cxf </groupId>
<artifactId> cxf-rt-transport-http </artifactId>
<version> $ {cxf.version} </version>
<scope> $ {cxf.scope} </scope>
</dependency>
<! - Marco de resorte 4.3.11 ->
<dependency>
<groupId> org.springframework </groupId>
<artifactId> spring-web </artifactId>
<version> $ {spring.version} </version>
<scope> build </scope>
</dependency>
</dependency>
```

Después de esto, seleccione Ejecutar como> Instalación de Maven en el proyecto para que Maven descargue todos los archivos Jar necesarios.

Agregue <plugin>, que permite generar los archivos. Para esto, tiene que cambiar:

- **<sourceRoot>**: catálogo donde se generan los archivos Java. Por defecto, es "target / generate-sources / cxf". Establézcalo como, por ejemplo: "\$ {basedir} / src / main / java"
- **<wsdl>**: WSDL desde el cual se generan los archivos
- **<wsdlLocation>**: ubicación a la que se referirá @WebService

```
<build>
<finalName> persons_register </finalName>
<plugins>
<! - plugin 4- apache cxf codegen wsdl2java goal ->
<plugin>
<groupId> org.apache.cxf </groupId>
<artifactId> cxf-codegen-plugin </artifactId>
<version> $ {cxf.version} </version>
<executions> <execution>
<configuration>
<sourceRoot> $ {basedir} / src / main / java </sourceRoot>
<wsdlOptions> <wsdlOption>
<wsdl> $ {basedir} / src / main / resources / persons_register.wsdl </wsdl>
```

```
<wsdlLocation> classpath: persons_register.wsdl </wsdlLocation>
<extraargs>
<extraarg> -impl </extraarg>
<extraarg> -exsh </extraarg>
<extraarg> true </extraarg>
</extraargs>
</wsdlOption>
</wsdlOptions>
</configuration>
<goals><goal>wsdl2java</goal></goals>
</execution></executions></plugin></plugins> </build>
```

Para generar, seleccione en el proyecto **Ejecutar como> fuentes generadas de Maven** .

Información adicional sobre pom.xml: <https://maven.apache.org/guides/introduction/introduction-to-the-pom.html>

También puede leer: <http://cxf.apache.org/docs/maven-cxf-codegen-plugin-wsdl-to-java.html>

<extraargs> afecta cómo se genera el código. Puede leer sobre esto: <http://cxf.apache.org/docs/wsdl-to-java.html>

3.4 Configuración del servicio de datos X-Road

Para que el servicio de datos esté disponible, debe cambiar **src> main> webapp> WEB-INF> web.xml**.

<param-value> nombre de archivo de beans, donde puede determinar el punto final del servicio.

```
<? xml version = "1.0" encoding = "UTF-8"?>
```

```
<web-app xmlns: xsi = "http://www.w3.org/2001/XMLSchema-instance"
```

```
xmlns = "http://java.sun.com/xml/ns/javaee"
```

```
xsi: schemaLocation = "http://java.sun.com/xml/ns/javaee
```

```
http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd "id =" WebApp_ID "version =" 3.0 ">
```

```
<display-name> persons_register </display-name>
```

```
<welcome-file-list>
```

```
<welcome-file> index.html </welcome-file>
```

```
<welcome-file> index.htm </welcome-file>
```

```
<welcome-file> index.jsp </welcome-file>
```

```
</welcome-file-list>

<servlet>

<description> Endpoint Apache CXF </description>
<display-name> cxf </display-name>
<servlet-name> cxf </servlet-name>
<servlet-class> org.apache.cxf.transport.servlet.CXFServlet </servlet-class>
<load-on-startup> 1 </load-on-startup>
</servlet>

<servlet-mapping>
<servlet-name> cxf </servlet-name> <url-pattern> / services / * </url-pattern>
</servlet-mapping>

<session-config><session-timeout>60</session-timeout> </session-config>

<context-param>
<param-name> contextConfigLocation </param-name>
<param-value> WEB-INF / cxf-beans.xml </param-value>
</context-param>

<listener>
<listener-class> org.springframework.web.context.ContextLoaderListener </listener-class>
</listener>

</web-app>
```

Configure <jaxws: endpoint> de acuerdo con su servicio de datos.

- **id**: el nombre de los beans. No es obligatorio y puede ser omitido.
- **Implementor: Implementación** Java del servicio.
- **wSDLLocation** : archivo WSDL
- **address**: dirección de servicio

```
<?xml version = "1.0" encoding = "UTF-8"?>
<beans xmlns = "http://www.springframework.org/schema/beans"
  xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
  xmlns:jaxws = "http://cxf.apache.org/jaxws"
  xsi:schemaLocation = "
    http://www.springframework.org/schema/beans
    http://www.springframework.org/schema/beans/spring-beans.xsd
    http://cxf.apache.org/jaxws
    http://cxf.apache.org/schemas/jaxws.xsd">
  <jaxws:
    endpoint          id          = "personregisterSOAP" implementor
= "ee.x_road.persons_register.Person_RegisterSOAPImpl"
    wsdlLocation = "classpath: persons_register.wsdl"
    address = "/PersonRegisterSOAP">
  </jaxws: punto final>
</beans>
```

- **Compruebe el servicio de datos generado.**
- Se ha generado un nuevo servicio de datos. verifique:
- el código fuente del servicio se ha generado en la carpeta *src*;
- se ha creado un nuevo paquete java, por ejemplo: *ee.x_road.persons_register* (el nombre depende de WSDL);
- compruebe el punto final del servicio de datos y el WSDL:
- El servicio generado se ha activado y responde en la dirección:

http://localhost:8080/persons_register/services

(¡NOTA! Aquí, en lugar de *persons_register*, todos tienen su propio nombre de proyecto de Eclipse)

Para verificar el servicio de datos, ingrese dicha dirección en el navegador, después de lo cual se mostrará información sobre el servicio de datos creado:

- la dirección del *final point del* servicio de datos
- Dirección WSDL del servicio de datos (enlace a WSDL)

Figura 57: Comprobación del servicio SOAP

Available SOAP services:	
person_register <ul style="list-style-type: none">• personList	Endpoint address: http://localhost:8080/person_register/services/person_registerSOAP WSDL : http://persons_register.x-road.ee/person_register Target namespace: http://persons_register.x-road.ee

Fuente: <https://x-road.global/xroad-playground>

Compruebe si se muestra la dirección WSDL del servicio de datos haciendo clic en el enlace WSDL, por ejemplo: http://localhost:8080/persons_register/services/person_registerSOAP?WSDL

(La dirección exacta del enlace depende del WSDL utilizado)

Usaremos esta dirección WSDL más adelante cuando configuremos el servicio en el servidor de seguridad X-Road y cuando lo probemos a través de SoapUI.

Solicitar datos de respuesta

El servicio de datos X-Road generado, garantiza la generación constante de datos en la respuesta de la solicitud. En la vida real, los datos generados deben eliminarse del código y, para obtener los datos, se debe utilizar la solicitud de la base de datos.

Al realizar la prueba, puede utilizar los datos generados en la respuesta o cambiarlos manualmente.

3.5 Creación de la aplicación de cliente Java X-Road

La creación del proyecto de la aplicación cliente de Java es la misma que la creación del servicio. WSDL debe copiarse del servicio a la aplicación cliente porque con ambos, se debe usar el mismo archivo WSDL.

Las <propiedades> y <dependencia> en el archivo pom.xml también son idénticas a las que se agregaron durante la creación del servicio. En la etiqueta <plugin>, se debe usar el parámetro <extraarg> -client </extraarg> en lugar de <extraarg> -impl </extraarg>.

Web.xml no necesita ser cambiado, ni beans.xml necesita ser creado.

Debe agregar un **punto final** en el archivo generado del cliente:

```
((javax.xml.ws.BindingProvider) puerto) .getRequestContext (). put (
javax.xml.ws.BindingProvider. ENDPOINT_ADDRESS_PROPERTY,
"http:// localhost: 8080 / persons_register / services / PersonRegisterSOAP");
```

Se ha generado el código Java del cliente del servicio de datos, verifique :

- El código generado está dentro de la carpeta src
- la llamada ejemplar del servicio se implementa en el método *main ()* del archivo *SOAP_Client.java* `<PersonRegister_PersonRegister>`, donde , en lugar de *PersonRegister*, hay un nombre que depende del WSDL de un servicio de datos específico.
- Se han creado objetos de datos inicializados con datos generados para llamar al servicio.
- **Activación del programa cliente del servicio:**
- Seleccionar archivo * *SOAP_Client.java*
- Seleccione en el menú: Ejecutar como / Aplicación Java
- Compruebe la salida del programa en la consola.

Pruebas de cliente Java a través del servidor de seguridad X-Road:

- cambie el punto final del servicio en el archivo * *SOAP_Client.java*, para que se refiera al servidor de seguridad:

// X-road: cambia la dirección del punto final del servicio por la dirección del servidor de seguridad

```
((javax.xml.ws.BindingProvider) puerto) .getRequestContext ();
```

```
put (javax.xml.ws.BindingProvider. ENDPOINT_ADDRESS_PROPERTY, "http://10.239.255.100");
```

- Compruebe si es correcto en el código generado:

```
eu.x_road.xsd.identifiers.XRoadObjectType _personList_serviceObjectType = ;
```

```
eu.x_road.xsd.identifiers.XRoadObjectType. SERVICE;
```

```
eu.x_road.xsd.identifiers.XRoadObjectType _personList_clientObjectType =
```

```
eu.x_road.xsd.identifiers.XRoadObjectType. SUBSystem;
```

Ajuste el código generado por * *SOAP_Client.java* corrigiendo los campos del encabezado de X-Road que contienen datos generados (con pruebas como programa SoapUI)

3.6 SERVICIOS REST

Normalmente se usan cuatro verbos HTTP diferentes para interactuar con los recursos en el sistema REST

- GET - recuperar un recurso
- POST - crear nuevo recurso
- PUT - actualizar un recurso
- DELETE - eliminar un recurso

Los encabezados más comunes utilizados en la comunicación REST son Accept Content-Type. Al incluir el Accept header en la solicitud, el cliente especifica los tipos de contenido que puede leer. Al leer la solicitud, el servidor debe respetar el Accept header y proporcionar la respuesta en el formato especificado. El servidor establece el Content-Type header en el mensaje de respuesta para revelar el tipo real de contenido.

Las solicitudes deben especificar la ruta al recurso en el que está operando. No hay reglas estrictas sobre cómo se deben definir las rutas, pero hay recomendaciones comúnmente utilizadas. En las API de REST, las rutas deben diseñarse de forma lógica y coherente para que las operaciones sean fáciles de usar para el cliente. Por ejemplo, una solicitud GET <https://petstore.niis.org/v2/pets/1124> leerá la información de cierta información y POST <https://petstore.niis.org/v2/pets> creará un nuevo registro.

La respuesta indica el resultado de la operación con el código de estado HTTP. El código de estado de éxito esperado varía según la operación solicitada.

- GET - 200 OK
- POST - 201 CREADO
- PUT - 200 OK
- DELETE - 204 SIN CONTENIDO

También cuando la operación falla, la razón se indica con el estado HTTP. Algunos de los códigos de error más comunes se enumeran a continuación.

- 400 PETICIÓN INCORRECTA
- 404 NO ENCONTRADO
- ERROR INTERNO DE SERVIDOR 500

3.7 Interfaz REST

El protocolo utiliza la versión 1.1 de HTTP, como se describe en [RFC2616]. El miembro / subsistema consumidor se especifica mediante encabezados HTTP. El servicio a llamar se codifica como parte de la URL de solicitud HTTP / HTTPS. Aquí está la forma genérica de la llamada de servicio REST.

Formato de solicitud

```
{http-request-method} /{protocol-version}/{serviceld}/[path][?query-parameters]
```

Encabezados de solicitud HTTP

```
X-Road-Client: {client}
```

{http-request-method} puede ser uno de los métodos de solicitud definidos en [RFC7231]. Por ejemplo, GET, POST, PUT y DELETE.

{protocol-version} : especifica la versión principal del protocolo de mensajes X-Road para REST. Para la versión inicial DEBE ser utilizada.

{client} : Especifica el miembro / subsistema que se usa como cliente de servicio, una entidad que inicia la llamada de servicio. El identificador consta de las siguientes partes: [X-Road instance]/[member class]/[member code]/[subsystem code]. Incluir el código del subsistema es OPCIONAL.

{serviceld} identifica el servicio que está registrado en **{provider-subsystem}** e invocado por la solicitud. {serviceld} contiene las siguientes partes:

[X-Road instance]/[member class]/[member code]/[subsystem code]/[service code]. Incluir el código del subsistema es OPCIONAL.

El **{serviceld}** está asignado a una URL de servicio real por el Servidor de seguridad (consulte el ejemplo a continuación).

[route] contiene la ruta relativa al servicio a llamar

[query parameters] contiene los parámetros de consulta que se enviarán al servicio

Aquí hay un ejemplo práctico de una llamada REST de X-Road.

Ejemplo de solicitud:

GET /r1/INSTANCE/CLASS2/MEMBER2/SUBSYSTEM2/BARSERVICE/v1/bar/zyggy?quu=1

Encabezados de solicitud HTTP

X-Road-Client: INSTANCE/CLASS1/MEMBER1/SUBSYSTEM1

Desglose de la solicitud URI:

{http-request-method} :GET

{protocol version} :/r1

{client} :INSTANCE/CLASS1/MEMBER1/SUBSYSTEM1

{serviceld} :/INSTANCE/CLASS2/MEMBER2/SUBSYSTEM2/BARSERVICE

[path] :/v1/bar/zyggy

[query parameters] :?quu=1

Suponiendo que el ID de servicio se asigne a la URL <https://barservice.example.org/>, el proveedor verá la solicitud GET <https://barservice.example.org/v1/bar/zyggy?quu=1>. La razón para nombrar el servicio independientemente de la ruta es que el mismo proveedor, también podría tener un servicio de emergencia (<https://fooservice.example.org/>), en cuyo caso sería difícil diferenciar los servicios si la ruta fuera el Id. de servicio (ambos servicios podrían tener rutas como "/v1 / ...") a menos que el servicio de servidor se conectara a un subsistema separado.

- **Cabeceras específicas de X-Road devueltas en la respuesta.**

La respuesta contiene algunos encabezados específicos de X-Road establecidos por el servidor de seguridad del proveedor. El servicio del proveedor NO DEBE establecer estos encabezados, ya que en ese caso se sobrescribirán.

- **X-Road-Client:** especifica el miembro / subsistema que se utiliza como un cliente de servicio
- **X-Road-Service:** especifica el ID de servicio que invoca el cliente de servicio
- **X-Road-Id:** identificador único para este mensaje
- **X-Road-Request-Hash:** para las respuestas, este campo contiene el hash codificado sha-512 del mensaje de solicitud
- **X-Road-Error:** este encabezado se proporciona en caso de que haya un error al procesar la solicitud y se haya producido en algún lugar de X-Road (en el servidor de seguridad del consumidor o proveedor)
- **X-Road-Request-Id:** identificador único para la solicitud
- **X-Road-Client:** **INSTANCE/CLASS/MEMBER/SUBSYSTEM**
- **X-Road-Service:** **INSTANCE/CLASS/MEMBER/SUBSYSTEM/PETSTORE**
- **X-Road-Id:** **fa2e18a5-c2cb-4d09-b994-f57727f7c3fb**
- **X-Road-Request-Hash:** **4c519cf0-0e5e-4ccf-b72b-8ed6fe289e6e**
- **X-Road-Request-Id:** **f92591a3-6bf0-49b1-987b-0dd78c034cc3**

Solicitud de encabezado de hash

- **X-Road-Request-Hash:** para las respuestas, este campo DEBE contener el SHA512 codificado en base 64 (SHA512 (encabezados) + SHA512 (cuerpo)). Si no hay un cuerpo, entonces solo se incluyen los encabezados en el cálculo, es decir, el campo contiene el SHA512 codificado en base 64 (encabezados). Este campo se completa automáticamente con el servidor de seguridad del proveedor de servicios. El campo se utiliza para crear una conexión segura entre una solicitud y una respuesta. Por lo tanto, es posible probar, por ejemplo, que un determinado registro de registro se devuelve en respuesta a una consulta determinada.
- El encabezado hash de la solicitud DEBE ser creado automáticamente por el servidor de seguridad del proveedor del servicio y DEBE ser verificado por el servidor de seguridad del cliente del servicio
- El mensaje de solicitud NO DEBE contener el encabezado de hash de solicitud.
- El mensaje de respuesta devuelto por un proveedor de servicios NO DEBE contener el encabezado de hash de solicitud. Si el mensaje de respuesta contiene el encabezado hash de solicitud, el Servidor de seguridad del proveedor del servicio DEBE ignorar el campo y reemplazarlo con el campo creado.
- **X-Road-Request-Hash:**
14sEri8SmLNy/DJyTob0ZddAskmdRy5ZUyhbr33iLkAA+gLpWcivUH16fzbulS7hhs2AnA4IJDloylihXMIVQ
A==

Encabezado de tipo de contenido

- Con los mensajes REST que incluyen el cuerpo de la solicitud, se RECOMIENDA que el tipo de contenido multimedia se indique con este encabezado. Además, se RECOMIENDA utilizar el parámetro charset para indicar la codificación de caracteres utilizada en el mensaje REST.
- Los mensajes REST que se originan en el Servidor de seguridad (por ejemplo, mensajes de error) DEBEN incluir el encabezado e indicar el tipo de contenido y la codificación de caracteres con él.

- Si el sistema de información del consumidor incluye el encabezado Content-Type en el mensaje de solicitud, DEBE ser transportado sin modificaciones a través de X-Road al sistema de información del proveedor
- Si el sistema de información del proveedor incluye el encabezado Content-Type en el mensaje de respuesta, y DEBE ser transportado sin modificaciones a través de X-Road al sistema de información del consumidor

```
Content-Type: application/json; charset=utf-8
```

```
Content-Type: multipart/form-data; boundary=something
```

En caso de que el consumidor del servicio no proporcione el Content-Typeheader (o algunos de sus componentes), el mensaje de solicitud se pasa al servicio del proveedor, que puede decidir qué hacer con él.

Aceptar encabezado

- Se RECOMIENDA que el consumidor de servicios anuncie los tipos de contenido que puede comprender al incluir el Acceptheader en el mensaje de solicitud.
- Si el Acceptheader está incluido en el mensaje de solicitud, DEBE ser transportado sin modificación a través de X-Road al proveedor de servicios.

```
Accept: application/xml
```

En caso de que el consumidor del servicio no proporcione el encabezado Accept, el Servidor de seguridad DEBE usar el tipo de contenido predeterminado application/json.

Servidores de seguridad y encabezados de extensión X-Road

- **X-Road-Security-Server:** para enviar la solicitud a un Security Server específico, este encabezado debe incluirse. las siguientes partes
- [X-Road instance]/[member class]/[member code]/[server code]
- Otras cabeceras de extensión X-Road no están definidas en este documento. Más bien, solo son contratos entre sistemas de información y X-Road los maneja como cualquier encabezado definido por el usuario.

```
X-Road-Security-Server: INSTANCE/MEMBERCLASS/MEMBERCODE/SERVERCODE
```

Cabeceras opcionales de X-Road

- **X-Road-Id:** identificador único para este mensaje. Se RECOMIENDA usar identificadores universalmente únicos [[UUID](#)]. Si X-Road-Idno se proporciona, DEBE ser generado por el servidor de seguridad del consumidor. El proveedor Security Server DEBE incluir el X-Road-Idencabezado en el mensaje de respuesta.
- **X-Road-UserId:** usuario cuya acción inició la solicitud. La ID de usuario debe tener un prefijo con el código de país ISO de dos letras (por ejemplo, EE12345678901).
- **X-Road-Issue :** identifica la solicitud, problema o documento recibido que fue la causa de la solicitud de servicio. Este campo puede ser utilizado por el sistema de información del cliente para conectar las solicitudes de servicio (y las respuestas) a los procedimientos de trabajo.
- **X-Road-Id:** fa2e18a5-c2cb-4d09-b994-f57727f7c3fb
- **X-Road-UserId:** EE12345678901
- **X-Road-Issue:** MT324223MSD

Encabezado de error X-Road

X-Road-Error: este encabezado se proporciona en caso de que haya un error al procesar la solicitud y se haya producido en algún lugar de X-Road (en el servidor de seguridad del consumidor o proveedor). Con ello, el cliente puede distinguir fácilmente entre los errores que se producen en los servicios del proveedor y los errores en los servidores de seguridad X-Road. Tenga en cuenta que el encabezado no contiene información de error detallada, sino que se parece más a un indicador de bandera para las partes interesadas. El encabezado solo contiene el tipo de error y la información más detallada, como el código de respuesta HTTP, el cuerpo del mensaje de error, etc., debe leerse desde el cuerpo de la respuesta.

```
Server.ServerProxy.DatabaseError
```

Encabezados definidos por el usuario

- Los encabezados HTTP definidos por el usuario (es decir, los encabezados que no se mencionan en [[LIST-OF-HTTP-HEADERS](#)] o este documento) DEBEN pasarse al destinatario no modificado por X-Road Security Server.
- X-Powered-By: PHP/5.2.17
- X-Pingback: <https://example.com/xmlrpc.php>

Encabezados de caché

- X-Road no almacena mensajes en caché. Los encabezados de la memoria caché DEBEN pasarse tal como están y el consumidor / proveedor PUEDE aprovechar esta información.
- Cache-Control: no-cache, no-store, must-revalidate
- Pragma: no-cache

Intercambio de recursos de origen cruzado

- Security Server no está diseñado para ser un proxy directo para un front-end web. No hace nada específico para habilitar el intercambio de recursos de origen cruzado (CORS).

Encabezados filtrados

Algunos encabezados HTTP DEBEN ser reescritos por el Security Server. El valor original, si lo hubiera, no se transferirá. El Servidor de seguridad proporcionará un nuevo valor o no enviará el encabezado.

- Cabeceras salto por salto
 - Connection, Keep-Alive, Autentication Proxy, Autoritation Proxy, TEA, trailer, transfer coding, update
- Encabezados que pueden filtrar el nombre o la dirección del host de origen
 - Host
 - User agent
 - Server

Cabeceras de manejo especial

Algunos encabezados HTTP son manejados por el Servidor de seguridad y el usuario no debe esperar que se pasen a través de X-Road sin modificar.

- Wait
 - La expectativa 100 PUEDE ser manejada localmente en el servidor de seguridad del consumidor. El apoyo a otras expectativas es OPCIONAL.
 - (100 esperas la única expectativa definida por [[RFC7231](#)])
- Content length
 - El Servidor de seguridad PUEDE cambiar la codificación de transferencia, eliminando o agregando un encabezado de longitud de contenido según sea necesario.

3.8 Redirecciones HTTP

El proveedor del servicio puede responder con redireccionamiento HTTP. Las redirecciones HTTP son respuestas con un código de estado de 3xx. Existen varios tipos de redirecciones y se dividen en tres categorías: redirecciones permanentes, temporales y especiales. X-Road no sigue las redirecciones y pasa

la redirección sin modificar al consumidor de servicios. El consumidor de servicios puede decidir qué hacer con esta respuesta. En general, los redireccionamientos representan una amenaza para la seguridad y no deben seguirse a ciegas. Se recomienda desactivar la configuración predeterminada para los siguientes redireccionamientos.

3.9 Uso de los parámetros de consulta

Se admite el uso de parámetros de consulta en las llamadas de servicio REST de X-Road. Los parámetros de consulta deben estar codificados [PERCENT-ENCODING] por el sistema de información del consumidor como se describe en [RFC3986]. Los parámetros de consulta DEBEN pasarse sin modificaciones a través de los Servidores de Seguridad X-Road al servicio del proveedor.

3.10 Manejo de errores

En una situación normal, la solicitud llega al servicio del proveedor y devuelve la respuesta al sistema de información del consumidor. Sin embargo, Security Server puede encontrar errores técnicos y, en estos casos, debe responder de manera predecible. Cuando se produce un error técnico, el Servidor de seguridad DEBE usar los códigos de estado HTTP definidos en [[RFC7231](#)] para comunicárselo al sistema de información del consumidor.

[[RFC7231](#)] define más de 70 códigos de estado HTTP. La mayoría de los desarrolladores no los tienen memorizados, por lo que tienen que ir a Internet y buscarlos. Para hacerlo más simple para los desarrolladores, el protocolo de mensajes X-Road para REST utiliza solo un pequeño subconjunto de códigos de estado HTTP.

Cuando se reduce, existen realmente 4 categorías de errores entre el cliente y el Servidor de seguridad.

1. Todo funcionó en la integración del Servidor de seguridad, pero el sistema de información del proveedor devuelve una respuesta de error.
2. El sistema de información del proveedor encuentra un error técnico y no puede devolver una respuesta.
3. El sistema de información del consumidor envía una solicitud que no cumple con el Protocolo de mensajes de X-Road para REST.
4. El servidor de seguridad encuentra un error técnico.

Asignamos estas categorías a los códigos de estado HTTP y cuerpos de respuesta.

1. El código de estado, el cuerpo de la respuesta y los encabezados HTTP son generados por el sistema de información del proveedor y se devuelven tal como están.
2. 500 - El servidor de seguridad devuelve el código de estado, el cuerpo de la respuesta y los encabezados HTTP.

3. 400 Petición Incorrecta. El código de estado, el cuerpo de la respuesta y los encabezados HTTP son devueltos por el Servidor de seguridad.
4. Error interno de servidor 500. El código de estado, el cuerpo de la respuesta y los encabezados HTTP son devueltos por el Servidor de seguridad.

Usando solo los códigos de estado HTTP es imposible saber si el error ocurrió en los Servidores de Seguridad X-Road o en el servicio del proveedor. El typefield en el cuerpo de la respuesta proporciona algunas herramientas, ya que los errores de X-Road comienzan con Client(servicio al consumidor), Server.ClientProxy(servidor de seguridad del consumidor) o Server.ServerProxy(servidor de seguridad del proveedor). Para facilitar la distinción entre los errores provenientes del Servidor de seguridad X-Road y el servicio del proveedor, el Servidor de seguridad DEBE agregar un encabezado HTTP adicional a la respuesta cuando ocurra el error en el Servidor de seguridad. El X-Road-Errorheader.

Cuando se produce el error en el Servidor de seguridad, la implementación del Servidor de seguridad DEBERÍA respetar el Acceptheader especificado por el sistema de información del consumidor y devolver la respuesta de error de X-Road utilizando el tipo de contenido sugerido, de forma predeterminada application/json. Además, el Servidor de seguridad DEBE incluir el Content-Typeheader en la respuesta para indicar el tipo de medio de la respuesta.

Ejemplo 1 (Categoría 1)

Todo funcionó en la perspectiva del Servidor de seguridad, pero el servicio devolvió un error. El código de estado, el cuerpo de la respuesta y los encabezados HTTP son generados por el sistema de información del proveedor y se devuelven tal como están a continuación.

Código de estado HTTP:

```
405
```

Cuerpo de respuesta:

```
{
  "timestamp" : " 2019-03-21T09: 45: 19.904Z ",
  "state" : 405 ,
  "error" : " Método no permitido ",
  "message" : " Método de solicitud 'PUT' no admitido ",
  "path" : " /v3 / pet / findByStatus "
}
```

Encabezados HTTP:

```
Content-Type: application/json;charset=utf-8
Date: Thu, 21 Mar 2019 09:45:19 GMT
x-road-id: 5ea48ae9-15c1-465a-be15-9b6ef2c7ef4a
x-road-client: DEV/COM/222/TESTCLIENT
x-road-service: DEV/COM/222/TESTSERVICE/petstore
x-road-request-id: f92591a3-6bf0-49b1-987b-0dd78c034cc3
x-road-request-hash:
yFOLGuJ0zmLhZSgwp3ooSBQbR9ejSvTc6p6FvBmcSEB2tDD6bxpjiv8sHORxqz4MMgEADH7IcARNprLfEwud
Nw==
Content-Length: 159
```

Ejemplo 2 (Categoría 2)

Todo funcionó en la perspectiva del Servidor de seguridad, pero el servicio expiró. El código de estado, el cuerpo de la respuesta y los encabezados HTTP son devueltos por el Servidor de seguridad.

Código de estado HTTP:

```
500
```

Cuerpo de respuesta:

```
{
  " type " : " Server.ServerProxy.NetworkError " ,
  " message " : " Connect to 10.139.178.1:8080 [/10.139.178.1] error: Connection timed out (Connection
timed out) " ,
  " detail " : " 9bc95b6e- 2f1d-4a41-a7e6-11eda7d734d5 "
}
```

Encabezados HTTP:

```
Date: Thu, 21 Mar 2019 11:42:03 GMT
Content-Type: application/json;charset=utf-8
X-Road-Error: Server.ServerProxy.NetworkError
Content-Length: 199
```

Ejemplo 3 (Categoría 3)

El sistema de información del consumidor envía una solicitud que no cumple con el Protocolo de mensajes de X-Road para REST. El código de estado, el cuerpo de la respuesta y los encabezados HTTP son devueltos por el Servidor de seguridad.

Código de estado HTTP:

```
400
```

Cuerpo de respuesta:

```
{  
  " type " : " Client.BadRequest " ,  
  " message " : " Error al analizar la solicitud REST del cliente. Por favor, que el formato de la solicitud  
corresponda al Protocolo de mensajes X-Road para REST (r1). " ,  
  " detail " : " 018cbcae-537e-421b-b6f6-2608dc97bd90 "  
}
```

Encabezados HTTP:

```
Date: Thu, 21 Mar 2019 11:45:12 GMT  
Content-Type: application/json;charset=utf-8  
X-Road-Error: Client.BadRequest  
Content-Length: 167
```

Ejemplo 4 (Categoría 4)

Se produjo un error en el servidor de seguridad del proveedor. El código de estado, el cuerpo de la respuesta y los encabezados HTTP son devueltos por el Servidor de seguridad.

Código de estado HTTP:

```
500
```

Cuerpo de respuesta:

```
{
```

```
" type " : " Server.ServerProxy.DatabaseError " ,  
" message " : " Error al acceder a la base de datos (serverconf) " ,  
" detail " : " 3c4d0f08-440f-417f-b935-bc801e103d51 " }  
}
```

Encabezados HTTP:

```
Date: Thu, 21 Mar 2019 11:57:11 GMT  
Content-Type: application/json;charset=utf-8  
X-Road-Error: Server.ServerProxy.DatabaseError  
Content-Length: 141
```

Ejemplo 5 (Seguimiento de la fuente de error)

Cuando se produce un error, es importante poder rastrear el componente que está causando el error. Una de las respuestas de error más confusas puede ser el error interno HTTP 500.

HTTP 500 puede provenir del proveedor de servicios o de los servidores de seguridad.

A) Si la respuesta no contiene el X-Road-Error, la fuente del error es el sistema de información del proveedor.

B) Si la respuesta contiene el X-Road-Error, la fuente del error es X-Road y el componente más específico se puede deducir de type field en el cuerpo de la respuesta.

Por ejemplo, Server.ServerProxy.ServiceFailed significa que el proveedor Security Server no obtuvo respuesta del servicio del proveedor. Server.ServerProxy.DatabaseError significa que el servidor de seguridad del proveedor encontró un error interno. Server.ClientProxy.OutdatedGlobalConf apunta al problema del servidor de seguridad del consumidor.

3.11 Seguridad

Los servicios REST seguros solo deberían proporcionar endpoints HTTPS. Esto requiere tanto al consumidor del Security Server como al servicio del proveedor. HTTPS protege las credenciales de autenticación en tránsito, por ejemplo, contraseñas, claves API o JSON Web Tokens. También permite a los clientes autenticar el servicio y garantiza la integridad de los datos transmitidos.

Se recomienda el uso de certificados del lado del cliente autenticados mutuamente en las conexiones entre el Servidor de Seguridad y los sistemas de información, tanto los consumidores de servicios como los proveedores de servicios, para brindar protección adicional a los servicios web altamente seguros. El servidor de seguridad DEBE admitir certificados del lado del cliente autenticados mutuamente tanto en el

lado del consumidor como del proveedor. No se admite el uso de tokens JWT como un método de autenticación entre Security Server y el sistema de información. En su lugar, se admite el envío de tokens JWT en encabezados HTTP desde el consumidor del servicio al proveedor del servicio. X-Road pasa los encabezados sin modificar.

3.12 Servicios

3.12.1 Describiendo servicios

Los servicios REST que se van a conectar al Security Server DEBEN describirse con [[OPENAPI3](#)]. Es una especificación para archivos de interfaz legibles por máquina para describir, producir, consumir y visualizar servicios web RESTful. La especificación OpenAPI es una especificación abierta impulsada por la comunidad dentro de [[OPENAPI-INITIATIVE](#)], un proyecto colaborativo de la Fundación Linux.

En el [Apéndice 1](#) de la documentación técnica detalla de x-road se incluye un ejemplo de archivo de definición de servicio [[OPENAPI3](#)]. Este servicio se utiliza en los siguientes ejemplos:

3.12.2 Ejemplos

3.12.2.1 General

A continuación, se describe como ejemplo el servicio de mascotas como método de talles empleado en el NIIS:

El servicio de tienda de mascotas utilizado en los siguientes ejemplos tiene un archivo de descripción del servicio [[OPENAPI3](#)] disponible en el [Apéndice 1](#) . Los aspectos más importantes del servicio se describen en el texto, pero para obtener más detalles, consulte el archivo de descripción del servicio mencionado anteriormente.

Los ejemplos asumen que serviceld se asigna a <https://petstore.niis.org/> .

3.12.2.2 Solicitud y respuesta GET

SOLICITUD

Tabla 8: Método GET

Servicio	Método	Descripción	Parámetros
----------	--------	-------------	------------

<code>/pets/{petId}</code>	GET	Encuentra mascota por identificación	petId - ID de mascota retorno
----------------------------	-----	--------------------------------------	-------------------------------

Fuente: Corporación Agencia Nacional de Gobierno Digital

Servicio llamado directamente

```
curl -X GET "https://petstore.niis.org/v2/pets/1124" -H "accept: application/json"
```

Servicio llamado a través de X-Road

```
curl -X GET "https:// {securityserver} / r1 / {serviceId} / v2 / pets / 1124" -H "accept: application/json" -H "X-Road-Client: {client}"
```

Respuesta de servicio

```
{  
  "id": 1124,  
  "name": "Siddu",  
  "photoUrls": [],  
  "tags": [],  
  "status": "Offline"  
}
```

Código de respuesta de servicio

```
200
```

Cabeceras de respuesta de servicio

```
Content-Type: application/json;charset=utf-8  
Date: Thu, 21 Mar 2019 12:36:39 GMT  
x-road-id: 29f4d011-ef17-4f2f-9bb1-0452ce17d3f5  
x-road-client: DEV/COM/222/TESTCLIENT  
x-road-service: DEV/COM/222/TESTSERVICE/petstore  
x-road-request-id: f92591a3-6bf0-49b1-987b-0dd78c034cc3  
x-road-request-hash:  
Xvx9V2U5c5RhDUiXpVLtW7L8vTd5cM2IOBU2n9efEk7/m3ECKyGAp7yTpJpTWpo6HcmwSaGO+cinxMVKjx  
JTOQ==
```

Content-Length: 1148

3.12.2.3 PUT solicitud y respuesta

SOLICITUD

Tabla 9: Método PUT

Servicio	Método	Descripción	Parámetros
/ pets / {petId}	PUT	Actualizar una mascota existente	body - Objeto de mascota que se actualizará en la tienda.

Fuente: Corporación Agencia Nacional de Gobierno Digital

Servicio llamado directamente

```
curl -X PUT " https://petstore.niis.org/v2/pets/5657082955040009 " -H " accept: application / json " -H "
Tipo de contenido: application / json " -d ' {"id": 0 , "category": {"id": 0, "name": "string"}, "name":
"doggie", "photoUrls": ["string"], "tags": [{"id": 0, "nombre": "cadena"}, "estado": "disponible"} '
```

Servicio llamado a través de X-Road

```
" -H PUT " https: // {securityserver} / r1 / {servicId} / v2 / pets / 5657082955040009 " -H " accept:
application / json " -H " Tipo de contenido: application / json " -H " X-Road-Client: {client} " -d ' {" id ": 0,
category ": {" id ": 0, " name ": " string ", " name ": " doggie ", " photoUrls ": ["string"], "tags": [{"id": 0,
"name": "string"}], "status": "available"} '
```

Respuesta de servicio

```
{
  "id": 5657082955040009,
  "category": {
```



```
"id": 0,  
  "name": "string"  
},  
"name": "doggie",  
"photoUrls": [  
  "string"  
],  
"tags": [  
  {  
    "id": 0,  
    "name": "string"  
  }  
],  
"status": "available"  
}
```

Código de respuesta de servicio

200

Cabeceras de respuesta de servicio

```
Date: Thu, 21 Mar 2019 12:43:33 GMT  
x-road-id: acdb2c7a-c705-41c2-b595-4cd62e78316e  
x-road-client: DEV/COM/222/TESTCLIENT  
x-road-service: DEV/COM/222/TESTSERVICE/petstore  
x-road-request-id: f92591a3-6bf0-49b1-987b-0dd78c034cc3  
x-road-request-hash:  
MOEfTqBjdqYiX3db9hxJ6JvHvCpYqfA6t0Uhdv6gZl29fMY8ld4CbN8tslj6mUQPXoRaUdPm7NdZeAYTg6zi+A  
==  
Content-Length: 0
```

3.12.2.4 Solicitud y respuesta POST

SOLICITUD

Tabla 10: Método POST

Servicio	Método	Descripción	Parámetros
/mascotas	POST	Agrega una nueva mascota a la tienda	Body : objeto de mascota que debe agregarse a la tienda.

Fuente: Corporación Agencia Nacional de Gobierno Digital

Servicio llamado directamente

```
curl -X POST "https://petstore.niis.org/v2/pets" -H "accept: application / json" -H "Tipo de contenido: application / json" -d '{"id": 0, "category": {"id": 0, "name": "string"}, "name": "doggie", "photoUrls": ["string"], "tags": [{"id": 0, "name": "cadena"}], "estado": "disponible"}'
```

Servicio llamado a través de X-Road

```
curl -X POST "https:// {securityserver} / r1 / {serviceld} / v2 / pets" -H "accept: application / json" -H "Tipo de contenido: application / json" -H "X-Road- Cliente: {client}" -d '{"id": 0, "category": {"id": 0, "name": "string"}, "name": "doggie", "photoUrls": ["string"], "tags": [{"id": 0, "name": "string"}], "status": "available"}'
```

Respuesta de servicio

```
{
  "id": 5657082955040122,
  "category": {
    "id": 0,
    "name": "string"
  },
  "name": "doggie",
  "photoUrls": [
    "string"
  ]
}
```

```

],
"tags": [
  {
    "id": 0,
    "name": "string"
  }
],
"status": "available"
}

```

Código de respuesta de servicio

200

Cabeceras de respuesta de servicio

```

Date: Thu, 21 Mar 2019 12:49:38 GMT
x-road-id: dcaaa3a2-a158-41e1-8775-309848052358
x-road-client: DEV/COM/222/TESTCLIENT
x-road-service: DEV/COM/222/TESTSERVICE/petstore
x-road-request-id: f92591a3-6bf0-49b1-987b-0dd78c034cc3
x-road-request-hash:
VCNZdwTxI7m3XC6Mpfw1H6qJUtBcm3Y6tfCvg5b3W/fb2RRXsLF9wftR3u6ElclE+RFaiAN/OkSz02fAYbNKa
w==
Content-Length: 0

```

3.12.2.5 BORRAR Solicitud y Respuesta

SOLICITUD

Tabla 11: Método DELETE

Servicio	Método	Descripción	Parámetros
/ pets / {petId}	DELETE	Borra una mascota	petId - ID de mascota para borrar

Fuente: Corporación Agencia Nacional de Gobierno Digital

Servicio llamado directamente

```
curl -X DELETE " https://petstore.niis.org/v2/pets/1124 " -H " accept: application / json "
```

Servicio llamado a través de X-Road

```
curl -X DELETE " https:// {securityserver} / r1 / {serviceld} / v2 / pets / 1124 " -H " accept: application / json "
```

Código de respuesta de servicio

200

Cabeceras de respuesta de servicio

Cabeceras de respuesta de servicio

Date: Thu, 21 Mar 2019 12:49:38 GMT

x-road-id: 6209d61b-6ab5-4443-a09a-b8d2a7c491b2

x-road-client: DEV/COM/222/TESTCLIENT

x-road-service: DEV/COM/222/TESTSERVICE/petstore

x-road-request-id: f92591a3-6bf0-49b1-987b-0dd78c034cc3

x-road-request-hash:

IQBoldcyul3BerjHfkleRQ45AyYoFIF7zXSN6yH/RwvTNWEcsTQM18EfqMxYfdkyGGB26oxAjAWv/AcfmZF7og==

Content-Length: 0

3.12.2.6 Definición del Servicio de Ejemplo

openapi: 3.0.0

info:

description: >-

This is a sample server Petstore server.

version: 1.0.0

title: Petstore

```
contact:
  email: info@niis.org
license:
  name: Apache 2.0
  url: 'http://www.apache.org/licenses/LICENSE-2.0.html'
tags:
  - name: pet
    description: Everything about your Pets
  externalDocs:
    description: Find out more
    url: 'https://niis.org'
  - name: store
    description: Access to Petstore orders
  - name: user
    description: Operations about user
  externalDocs:
    description: Find out more about our store
    url: 'https://niis.org'
paths:
  /pets:
    get:
      tags:
        - pet
      summary: Get pets from store
      description: Search pets
      operationId: getPets
      parameters:
```

```
- name: term
  in: query
  description: search term
  required: false
  schema:
    type: string
responses:
  '200':
    description: successful operation
    content:
      application/xml:
        schema:
          type: array
          items:
            $ref: '#/components/schemas/Pet'
      application/json:
        schema:
          type: array
          items:
            $ref: '#/components/schemas/Pet'
  '400':
    description: Invalid ID supplied
  '404':
    description: Pet not found
security:
  - api_key: []
post:
```

```
tags:
  - pet
summary: Add a new pet to the store
description: ''
operationId: addPet
responses:
  '201':
    description: pet created
  '405':
    description: Invalid input
security:
  - petstore_auth:
    - 'write:pets'
    - 'read:pets'
requestBody:
  $ref: '#/components/requestBodies/Pet'
'/pets/{petId}':
  get:
    tags:
      - pet
    summary: Find pet by ID
    description: Returns a single pet
    operationId: getPetById
    parameters:
      - name: petId
        in: path
        description: ID of pet to return
```

```
required: true

schema:

  type: integer

  format: int64

responses:

  '200':

    description: successful operation

    content:

      application/xml:

        schema:

          $ref: '#/components/schemas/Pet'

      application/json:

        schema:

          $ref: '#/components/schemas/Pet'

  '400':

    description: Invalid ID supplied

  '404':

    description: Pet not found

security:

  - api_key: []

put:

  tags:

    - pet

  summary: Update an existing pet

  description: ''

  operationId: updatePet

  parameters:
```



```
- name: petId
  in: path
  description: ID of pet to return
  required: true
  schema:
    type: integer
    format: int64
responses:
  '200':
    description: Pet updated
  '400':
    description: Invalid ID supplied
  '404':
    description: Pet not found
  '405':
    description: Validation exception
security:
  - petstore_auth:
    - 'write:pets'
    - 'read:pets'
requestBody:
  $ref: '#/components/requestBodies/Pet'
delete:
  tags:
    - pet
  summary: Deletes a pet
  description: "
```

```
operationId: deletePet

parameters:
  - name: api_key
    in: header
    required: false
    schema:
      type: string
  - name: petId
    in: path
    description: Pet id to delete
    required: true
    schema:
      type: integer
      format: int64

responses:
  '200':
    description: Pet deleted
  '400':
    description: Invalid ID supplied
  '404':
    description: Pet not found

security:
  - petstore_auth:
    - 'write:pets'
    - 'read:pets'

'/pets/{petId}/images':
  post:
```

```
tags:
  - pet
summary: Uploads an image
description: ''
operationId: uploadFile
parameters:
  - name: petId
    in: path
    description: ID of pet to update
    required: true
    schema:
      type: integer
      format: int64
responses:
  '200':
    description: successful operation
    content:
      application/json:
        schema:
          $ref: '#/components/schemas/ApiResponse'
security:
  - petstore_auth:
    - 'write:pets'
    - 'read:pets'
requestBody:
  content:
    multipart/form-data:
```

```
schema:
  type: object
  properties:
    additionalMetadata:
      description: Additional data to pass to server
      type: string
    file:
      description: file to upload
      type: string
      format: binary
/store/inventories:
  get:
    tags:
      - store
    summary: Returns pet inventories by status
    description: Returns a map of status codes to quantities
    operationId: getInventory
  responses:
    '200':
      description: successful operation
      content:
        application/json:
          schema:
            type: object
            additionalProperties:
              type: integer
              format: int32
```

```
security:
  - api_key: []
/store/orders:
  post:
    tags:
      - store
    summary: Place an order for a pet
    description: ""
    operationId: placeOrder
    responses:
      '200':
        description: successful operation
        content:
          application/xml:
            schema:
              $ref: '#/components/schemas/Order'
          application/json:
            schema:
              $ref: '#/components/schemas/Order'
      '400':
        description: Invalid Order
    requestBody:
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/Order'
        description: order placed for purchasing the pet
```

required: true

'/store/orders/{orderId}':

get:

tags:

- store

summary: Find purchase order by ID

description: >-

For valid response try integer IDs with value ≥ 1 and ≤ 10 .

Other values will generated exceptions

operationId: getOrderById

parameters:

- name: orderId

in: path

description: ID of pet that needs to be fetched

required: true

schema:

type: integer

format: int64

minimum: 1

maximum: 10

responses:

'200':

description: successful operation

content:

application/xml:

schema:

\$ref: '#/components/schemas/Order'

```
application/json:
  schema:
    $ref: '#/components/schemas/Order'
  '400':
    description: Invalid ID supplied
  '404':
    description: Order not found
delete:
  tags:
    - store
  summary: Delete purchase order by ID
  description: >-
  For valid response try integer IDs with positive integer value.
  Negative or non-integer values will generate API errors
  operationId: deleteOrder
  parameters:
    - name: orderId
      in: path
      description: ID of the order that needs to be deleted
      required: true
      schema:
        type: integer
        format: int64
        minimum: 1
  responses:
    '200':
      description: Purchase order deleted
```

'400':

description: Invalid ID supplied

'404':

description: Order not found

/users:

post:

tags:

- user

summary: Create user

description: This can only be done by the logged in user.

operationId: createUser

responses:

default:

description: successful operation

requestBody:

content:

application/json:

schema:

\$ref: '#/components/schemas/User'

description: Created user object

required: true

/users/login:

get:

tags:

- user

summary: Logs user into the system

description: "


```
operationId: loginUser

parameters:
  - name: username
    in: query
    description: The user name for login
    required: true
    schema:
      type: string
  - name: password
    in: query
    description: The password for login in clear text
    required: true
    schema:
      type: string

responses:
  '200':
    description: successful operation
    headers:
      X-Rate-Limit:
        description: calls per hour allowed by the user
        schema:
          type: integer
          format: int32
      X-Expires-After:
        description: date in UTC when token expires
        schema:
          type: string
```

```
    format: date-time

  content:
    application/xml:
      schema:
        type: string
    application/json:
      schema:
        type: string

  '400':
    description: Invalid username/password supplied

/users/logout:
  get:
    tags:
      - user
    summary: Logs out current logged in user session
    description: ""
    operationId: logoutUser
  responses:
    default:
      description: successful operation

/users/{username}:
  get:
    tags:
      - user
    summary: Get user by user name
    description: ""
    operationId: getUserByName
```

```
parameters:
  - name: username
    in: path
    description: 'The name that needs to be fetched. Use user1 for testing.'
    required: true
    schema:
      type: string
responses:
  '200':
    description: successful operation
    content:
      application/xml:
        schema:
          $ref: '#/components/schemas/User'
      application/json:
        schema:
          $ref: '#/components/schemas/User'
  '400':
    description: Invalid username supplied
  '404':
    description: User not found
put:
  tags:
    - user
  summary: Updated user
  description: This can only be done by the logged in user.
  operationId: updateUser
```

```
parameters:
  - name: username
    in: path
    description: name that need to be updated
    required: true
    schema:
      type: string
responses:
  '200':
    description: User updated
  '400':
    description: Invalid user supplied
  '404':
    description: User not found
requestBody:
  content:
    application/json:
      schema:
        $ref: '#/components/schemas/User'
      description: Updated user object
      required: true
delete:
  tags:
    - user
  summary: Delete user
  description: This can only be done by the logged in user.
  operationId: deleteUser
```

```
parameters:
  - name: username
    in: path
    description: The name that needs to be deleted
    required: true
    schema:
      type: string
responses:
  '200':
    description: User deleted
  '400':
    description: Invalid username supplied
  '404':
    description: User not found
externalDocs:
  description: Find out more
  url: 'https://niis.org'
servers:
  - url: 'https://petstore.niis.org/v2'
  - url: 'http://petstore.niis.org/v2'
components:
  requestBodies:
    UserArray:
      content:
        application/json:
          schema:
            type: array
```

```
  items:
    $ref: '#/components/schemas/User'
  description: List of user object
  required: true
Pet:
  content:
    application/json:
      schema:
        $ref: '#/components/schemas/Pet'
    application/xml:
      schema:
        $ref: '#/components/schemas/Pet'
  description: Pet object that needs to be added to the store
  required: true
securitySchemes:
  petstore_auth:
    type: oauth2
    flows:
      implicit:
        authorizationUrl: 'http://petstore.niis.org/oauth/dialog'
        scopes:
          'write:pets': modify pets in your account
          'read:pets': read your pets
  api_key:
    type: apiKey
    name: api_key
    in: header
```

```
schemas:  
  
Order:  
  type: object  
  properties:  
    id:  
      type: integer  
      format: int64  
    petId:  
      type: integer  
      format: int64  
    quantity:  
      type: integer  
      format: int32  
    shipDate:  
      type: string  
      format: date-time  
    status:  
      type: string  
      description: Order Status  
      enum:  
        - placed  
        - approved  
        - delivered  
    complete:  
      type: boolean  
      default: false  
  xml:
```

name: Order

Category:

type: object

properties:

id:

type: integer

format: int64

name:

type: string

xml:

name: Category

User:

type: object

properties:

id:

type: integer

format: int64

username:

type: string

firstName:

type: string

lastName:

type: string

email:

type: string

password:

type: string


```
phone:  
  type: string  
userStatus:  
  type: integer  
  format: int32  
  description: User Status
```

```
xml:  
  name: User
```

```
Tag:  
  type: object  
  properties:  
    id:  
      type: integer  
      format: int64  
    name:  
      type: string
```

```
xml:  
  name: Tag
```

```
Pet:  
  type: object  
  required:  
    - name  
    - photoUrls  
  properties:  
    id:  
      type: integer  
      format: int64
```

```
category:
  $ref: '#/components/schemas/Category'
name:
  type: string
  example: doggie
photoUrls:
  type: array
xml:
  name: photoUrl
  wrapped: true
items:
  type: string
tags:
  type: array
xml:
  name: tag
  wrapped: true
items:
  $ref: '#/components/schemas/Tag'
status:
  type: string
  description: pet status in the store
  enum:
    - available
    - pending
    - sold
xml:
```

```
name: Pet
```

```
ApiResponse:
```

```
type: object
```

```
properties:
```

```
code:
```

```
type: integer
```

```
format: int32
```

```
type:
```

```
type: string
```

```
message:
```

```
type: string
```

4. Despliegue de Servidor de Seguridad para Ambiente de Desarrollo sin entorno de servicios de confianza y servidor central

Ambiente ideal para desarrolladores que no cuenten con un entorno para realizar integraciones en los servicios web:

La Imagen del servidor de seguridad autónomo se presenta en Docker

Las imágenes independientes del servidor de seguridad están estrictamente diseñadas para fines de prueba y desarrollo. ¡No lo use en entorno de producción!

La imagen del servidor de seguridad contiene un conjunto personalizado de módulos en lugar de xroad-securityserver:

- xroad-proxy
- xroad-addon-metaservices
- xroad-addon-wsdlvalidator
- XROAD-autologin

La imagen está construida a partir de fuentes de la versión bionic-6.21.0 o posterior. El servidor de seguridad instalado tiene una organización miembro registrada 'TestOrganization' y dos subsistemas 'TestClient' y 'TestService'.

El servidor de seguridad independiente permanece operativo durante un año.

Credenciales de usuario : xrd / secret

Desplegar en Docker

```
# Publish the container ports (4000 and 80) to localhost (loopback address).
docker run -p 4000:4000 -p 80:80 --name ss niis/xroad-security-server-standalone:bionic-6.21.0
```

Docker Pull Comand²

docker pull niis/xroad-security-server-standalone

5 Notas de la versión de X-Road v6.21.0 integrada a la PDI de Colombia.

Tabla 12: Notas de la versión de X-Road v6.21.0

Número de versión	6.21.0
Fecha de lanzamiento	30.04.2019
Versiones soportadas	6.21.0 6.20.1 6.19.1
Plataformas soportadas	<p>Servidor central Ubuntu 14.04 LTS Ubuntu 18.04 LTS</p> <p>Proxy de configuración Ubuntu 14.04 LTS Ubuntu 18.04 LTS</p> <p>Servidor de seguridad Ubuntu 14.04 LTS Ubuntu 18.04 LTS RHEL 7</p> <p>¡NOTA! v6.21.0 es la última versión nueva lanzada para Ubuntu 14.04 LTS. A partir de v6.22.0, las plataformas compatibles son Ubuntu 18.04 LTS y RHEL7. Las</p>

² <https://hub.docker.com/r/niis/xroad-security-server-standalone>

	versiones de Ubuntu 14.04 de versiones anteriores (v6.20.1, v6.21.0) son compatibles hasta el final del período de soporte oficial de la versión.
Documentación oficial	https://github.com/nordic-institute/X-Road/tree/master/doc
Código fuente	https://github.com/nordic-institute/X-Road/tree/master
Licencia de software	<u>MIT</u>

Fuente: Corporación Agencia Nacional de Gobierno Digital

- Security Server proporciona soporte para consumir y producir servicios SOAP y REST.
- Los sistemas basados en REST se pueden integrar a X-Road sin cambios técnicos y un componente de servicio de adaptador adicional.
- El soporte de REST no se limita solo a los mensajes JSON y XML, ya que Security Server no establece restricciones al tipo de contenido de la carga útil que se transfiere entre un consumidor de servicios y un productor de servicios.
- El consumo y la producción de servicios SOAP siguen siendo compatibles y no se requieren cambios para los consumidores y productores de servicios basados en SOAP existentes.
- El proceso de incorporación de X-Road se ha simplificado y permite la aprobación automática de las solicitudes de registro de las nuevas organizaciones miembros y sistemas de información de X-Road.
- El operador de X-Road puede elegir entre la aprobación automática y manual de las solicitudes de registro dentro de un ecosistema de X-Road.
- La aprobación automática acelera el proceso de registro y reduce las tareas de administración diarias del operador de X-Road.
- Standalone Security Server es una versión especial de Security Server que está lista para usar en minutos sin el proceso normal de instalación, configuración y registro de Security Server.
- Standalone Security Server está diseñado para fines de prueba en el desarrollo del servicio X-Road y no puede comunicarse con otros servidores de seguridad.
- Standalone Security Server está dirigido especialmente a desarrolladores y organizaciones que están desarrollando servicios que se publicarán a través de X-Road.
- Resumen más detallado de las características relacionadas con REST
- Funcionalidad básica de REST
- Intercambio de mensajes con firma y sellado de tiempo.
- Registro de mensajes con archivo
- Descarga y verificación de registros.
- Agregando un servicio REST usando una URL
- No hay soporte para definiciones de OpenAPI
- Seguimiento operacional de los servicios REST.
- Autorización de nivel de servicio
- Autenticación basada en certificados (clientes + servicios)

- Protocolo de mensajes de X-Road para REST 1.0

Tabla 13: Tipos de problemas: corrección (corrección de errores), mejora (mejora de una característica existente), nueva (una nueva característica)

ID de problema	Tipo	Resumen
<u>XRDDEV-120</u>	Nuevo	Crea la implementación a nivel de prueba de concepto (PoC) del soporte REST. Intercambio de mensajes REST básico entre servidores de seguridad sin validaciones, verificaciones, registros, etc.
<u>XRDDEV-149</u>	Nuevo	Crea una herramienta de actualización de número de versión para desarrolladores que se puede utilizar para actualizar el número de versión de X-Road en todos los archivos y ubicaciones relacionados.
<u>XRDDEV-155</u>	Nuevo	Defina aún más los problemas descubiertos en la implementación de REST PoC Planificación más detallada de la implementación del soporte REST.
<u>XRDDEV-225</u>	Nuevo	<p>Agrega la opción de configuración que le permita aceptar automáticamente las solicitudes de registro de certificados de autenticación en el Servidor Central. Cuando está habilitada, la función se aplica solo si el miembro que posee el Servidor de seguridad ya está registrado en el Servidor central.</p> <p>De forma predeterminada, la aceptación automática está deshabilitada y se puede habilitar agregando la siguiente configuración en "/etc/xroad/conf.d/local.ini" en el Servidor Central:</p> <pre>[center] auto-approve-auth-cert-reg-requests=true</pre>
<u>XRDDEV-226</u>	Nuevo	<p>Agrega la opción de configuración que le permita aceptar automáticamente las solicitudes de registro del cliente de Security Server en el Servidor Central. La solicitud de registro del cliente de Security Server se acepta automáticamente en el servidor central cuando se cumplen las siguientes condiciones:</p> <p>La aprobación automática de las solicitudes de registro de clientes de Security Server está habilitada en el servidor central.</p> <p>La solicitud de registro del cliente ha sido firmada por el miembro propietario del subsistema para registrarse como cliente de Security Server.</p> <p>La firma y el certificado han pasado la verificación.</p> <p>El miembro propietario del subsistema está registrado en el Servidor Central.</p>

ID de problema	Tipo	Resumen
		<p>Si alguna de las condiciones anteriores es falsa, se requiere la aprobación manual.</p> <p>Las versiones anteriores de Security Server no incluyen la firma del propietario del cliente en la solicitud de registro y, por lo tanto, siempre se requiere la aprobación manual.</p> <p>De forma predeterminada, la aceptación automática está deshabilitada y se puede habilitar agregando la siguiente configuración en "/etc/xroad/conf.d/local.ini" en el Servidor Central:</p> <p style="text-align: center;">[center]</p> <p style="text-align: center;">auto-approve-client-reg-requests=true</p>
<u>XRDDEV-230</u>	Mejora	<p>Agrega una identificación de mensaje única generada por el consumidor Security Server a cada par de mensajes de solicitud-respuesta, de modo que sea posible distinguir los mensajes en el registro de mensajes y la base de datos de monitoreo operacional.</p> <p>Las versiones de Security Server anteriores a la versión 6.21.0 ignoran el ID de mensaje adicional.</p>
<u>XRDDEV-245</u>	Nuevo	<p>Implementa el soporte de Docker para Security Server. Crear Security Server Dockerfile y la imagen de Docker. La imagen de Docker está disponible en Docker Hub .</p> <p>¡NOTA! La imagen de Security Server Docker es solo para fines de prueba y desarrollo. No se recomienda su uso en entornos de producción.</p>
<u>XRDDEV-258</u>	Fijar	<p>Actualizar la dependencia de JRuby de la versión 9.1.13 a 9.1.17.</p>
<u>XRDDEV-263</u>	Nuevo	<p>Agrega servicios REST al modelo de datos de Security Server. Actualice la base de datos y el esquema de la base de datos de configuración de Security Server para admitir los servicios REST además de los servicios SOAP.</p>
<u>XRDDEV-264</u>	Nuevo	<p>Agrega soporte para transferir mensajes REST de tamaño arbitrario. Los mensajes REST grandes pueden transferirse a través de X-Road con igual o mejor escalabilidad y rendimiento en comparación con SOAP con archivos adjuntos.</p>
<u>XRDDEV-284</u>	Nuevo	<p>Agrega soporte para configurar servicios REST en la IU de administración de Security Server. Los servicios REST pueden agregarse, modificarse, eliminarse y configurarse mediante la interfaz de usuario de administración, al igual que los servicios SOAP.</p>
<u>XRDDEV-285</u>	Nuevo	<p>Implementar el registro de mensajes REST a la base de datos de registro de mensajes.</p>

ID de problema	Tipo	Resumen
		<p>El registro de la carga útil del mensaje se habilita / inhabilita usando el nuevo parámetro "message-body-logging": se usa para habilitar / deshabilitar el registro de las cargas útiles de mensajes SOAP y REST. La eliminación del cuerpo del mensaje generalmente se realiza por razones de confidencialidad (el cuerpo contiene datos que no deben almacenarse en los registros, por ejemplo, datos personales). Un nuevo parámetro del sistema "max-loggable-body-size" define el tamaño máximo del cuerpo del mensaje REST (valor predeterminado: 10 MB). Si el cuerpo del mensaje REST excede el tamaño máximo del cuerpo registrable, el cuerpo se trunca en el registro si el parámetro del sistema "truncated-body-allowed" es verdadero, y el mensaje se rechaza si el parámetro del sistema "truncated-body-allowed" es falso (valor por defecto: falso). El cuerpo del mensaje se almacena en la base de datos como un objeto binario grande cuyo tamaño máximo es de 1 GB.</p> <p>¡NOTA! El uso del parámetro del sistema "soap-body-logging" está en desuso, use el parámetro "message-body-logging" de ahora en adelante. El parámetro "soap-body-logging" aún funciona en v6.21.0 y su valor se usa para habilitar / deshabilitar el registro de las cargas útiles de mensajes SOAP y REST. Sin embargo, el parámetro del sistema "soap-body-logging" se eliminará en futuras versiones.</p>
<u>XRDDEV-314</u>	Nuevo	Extiende la estructura de la base de datos de registro de mensajes para admitir el registro de mensajes REST.
<u>XRDDEV-328</u>	Nuevo	<p>Implementa el archivado de mensajes REST desde la base de datos de registro de mensajes a los contenedores ASiC.</p> <p>Los registros de mensajes REST se archivan desde la base de datos de registro de mensajes al disco de acuerdo con la programación de archivo del registro de mensajes. Los registros de registro de mensajes archivados se eliminan de la base de datos de registro de mensajes de acuerdo con el programa de eliminación.</p>
<u>XRDDEV-337</u>	Fijar	Soluciona los problemas de escala del logotipo de X-Road en las IU de Security Server y Central Server.
<u>XRDDEV-341</u>	Fijar	Actualiza la dependencia de Hibernate de la versión 4.3.11 a 5.1.17.
<u>XRDDEV-352</u>	Nuevo	Agrega soporte para descargar registros de mensajes REST a través de la interfaz del servicio web de descarga de documentos firmados por Security Server.
<u>XRDDEV-353</u>	Nuevo	Agrega soporte para verificar los contenedores ASiC que contienen mensajes REST.

ID de problema	Tipo	Resumen
		Es posible verificar la firma de los contenedores ASiC que contienen registros de mensajes REST utilizando la herramienta asicverifier. Es posible exportar mensajes REST desde el contenedor ASiC usando la herramienta asicverifier. Exportar mensajes es posible sin importar el resultado de la verificación.
<u>XRDDEV-358</u>	Nuevo	Agrega mensajes REST de grabación al monitoreo operativo. Los mensajes REST se registran mediante monitoreo operacional y los datos se almacenan en la base de datos de monitoreo operacional. La supervisión operativa recopila la misma información de los mensajes REST que se recopila de los mensajes SOAP.
<u>XRDDEV-361</u>	Fijar	Soluciona un problema en el uso de recursos de Security Server.
<u>XRDDEV-375</u>	Nuevo	Agrega soporte para la extensión del protocolo de Security Server en los mensajes REST. La implementación de Security Server REST admite el encabezado HTTP "X-Road-Security-Server" que se puede usar para enviar una solicitud a un Security Server específico.
<u>XRDDEV-380</u>	Fijar	Soluciona el mensaje de solicitud "getSecurityServerMetrics" que falta en el registro de mensajes. Antes de la corrección, el mensaje de solicitud "getSecurityServerMetrics" no se registraba en la base de datos del registro de mensajes.
<u>XRDDEV-398</u>	Nuevo	Agrega <u>X-Road Message Protocol para REST</u> en GitHub como un documento de Markdown. El protocolo de mensajes X-Road para REST se usa entre los sistemas de información y los servidores de seguridad X-Road para consumir y producir servicios REST.
<u>XRDDEV-400</u>	Mejora	Devuelve un mensaje de error descriptivo cuando se invoca el metaservicio getWsdI para un servicio REST.
<u>XRDDEV-412</u>	Mejora	Evita llamadas de servicio SOAP desde la interfaz REST y llamadas de servicio REST desde la interfaz SOAP. X-Road no proporciona conversiones automáticas de mensajes / protocolos entre los servicios SOAP y REST. Por lo tanto, los servicios deben consumirse utilizando sus implementaciones nativas: SOAP o REST.
<u>XRDDEV-418</u>	Fijar	Valida la implementación de REST contra X-Road Message Protocol para REST y alinee la implementación de REST con la especificación.
<u>XRDDEV-419</u>	Nuevo	Incluye el ID de mensaje único implementado en la tarea <u>XRDDEV-230</u> en la firma del mensaje REST y los encabezados de solicitud HTTP. El ID de mensaje único se incluye en los mensajes de solicitud y respuesta REST en el encabezado HTTP "X-Road-Request-Id".

ID de problema	Tipo	Resumen
<u>XRDDEV-423</u>	Fijar	Soluciona el error al ejecutar migraciones de la base de datos del monitor operativo en la actualización/ reinstalación en RHEL7.
<u>XRDDEV-426</u>	Fijar	Corrija la regresión de rendimiento y la pérdida de memoria nativa en el archivo de la base de datos de registro de mensajes.
<u>XRDDEV-432</u>	Fijar	Evitar agregar nuevos servicios REST utilizando un código de servicio que ya exista en el mismo subsistema. Los códigos de servicio REST deben ser únicos dentro de un subsistema. El mismo código de servicio se puede utilizar en diferentes subsistemas.
<u>XRDDEV-439</u>	Fijar	Corrige el error en la limpieza del registro de mensajes cuando hay más de ~ 50k mensajes para limpiar. En lugar de eliminar registros del registro de mensajes en una sola consulta, los registros se eliminan en lotes (por defecto: 10 000 registros por lote). Además, la limpieza del registro de mensajes se realiza 4 veces al día (2 veces al día en versiones <6.21.0) y la limpieza no se solapa con el archivo.
<u>XRDDEV-443</u>	Fijar	Soluciona error al actualizar el código de servicio REST. Antes de la corrección, la actualización del campo de código de servicio de un servicio REST eliminaba todos los derechos de acceso del servicio.

Fuente: Corporación Agencia Nacional de Gobierno Digital

Tabla 14: Dependencias nuevas / actualizadas

Dependencia	Versión antigua	Nueva versión	Notas
Apache HttpComponents HttpAsyncClient	4.1.1	4.1.4	
Apache HttpComponents HttpClient	4.5.2	4.5.6	
Hibernate	4.3.11	5.1.17	<u>Notas de lanzamiento</u> Correcciones de seguridad: CVE-2018-1000632
Embarcadero	9.4.6.v20170531	9.4.14.v20181114	<u>Notas de lanzamiento</u>
JRuby	9.1.13	9.1.17	<u>Notas de lanzamiento</u>
Controlador JDBC PostgreSQL	42.2.1	42.2.5	<u>Notas de lanzamiento</u> Correcciones de seguridad: CVE-2018-10936

Fuente: Corporación Agencia Nacional de Gobierno Digital

Otras notas

- Repositorios de paquetes

Tabla 15: Repositorio de paquetes

Repositorio	URL
Biónico	deb <a href="https://artifactory.niis.org/xroad-release-deb-bionic- <version> main">https://artifactory.niis.org/xroad-release-deb-bionic- <version> main
Fiel	deb <a href="https://artifactory.niis.org/xroad-release-deb-trusty- <version> main">https://artifactory.niis.org/xroad-release-deb-trusty- <version> main
RPM	<a href="https://artifactory.niis.org/xroad-release-rpm/rhel/7/ <version>">https://artifactory.niis.org/xroad-release-rpm/rhel/7/ <version>

Fuente: Corporación Agencia Nacional de Gobierno Digital

La clave de firma del repositorio se puede descargar desde: <https://artifactory.niis.org/api/gpg/key/public>
Paquetes

Ubuntu Bionic

Tabla 16: Ubuntu Bionic

Paquete	Suma de comprobación SHA256
xroad-addon-hwtokens_6.21.0-1.ubuntu18.04_all.deb	93070dfcaadeb024a1f85cb10d82a5399bd605427b8ba2ccda48b18ecdcc1fc7
xroad-addon-messagelog_6.21.0-1.ubuntu18.04_all.deb	6464ae22628dbafca933a93dfefdce44ece9e80485e52221cac69633ca422889
xroad-addon-metaservices_6.21.0-1.ubuntu18.04_all.deb	8ddb43702e6c92c53e268a3187cbcf6c25edd37f1c94e592cc072b541Zealandb18
xroad-addon-opmonitoring_6.21.0-1.ubuntu18.04_all.deb	b208e104f64f688ab4295891debe64f754e09821fea150ea8851576e11092811
xroad-addon-proxymonitor_6.21.0-1.ubuntu18.04_all.deb	66fb1d0a5be320f094d6a724007bfc0ba69bf5b625e9d3f6a123825689e6c7da
xroad-autologin_6.21.0-1.ubuntu18.04_all.deb	93a4197000e37771b70b292f19765e1a88f8f7e00ac58a4d41f4a496d08f500c
xroad-addon-wsdvalidator_6.21.0-1.ubuntu18.04_all.deb	503c91159ec8cf812d95b118c89535b0fe74e14f042ebdd016a206fc94954cb3

xroad-base_6.21.0-1.ubuntu18.04_amd64.deb	f7d33a8cfd700460ae5a271df223cd040b8943b9593973b078b24311b079c58e
xroad-center-clusterhelper_6.21.0-1.ubuntu18.04_all.deb	26386990663e017168154b6ba250ad38c8e576121af6e601cdf2bf79c3f9f3e5
xroad-center_6.21.0-1.ubuntu18.04_all.deb	6d04aa466f9f78849fa01b26f5f001e893d5c2330f5c9c19e1913b2e36cc12ac
xroad-centralserver-monitoring_6.21.0-1.ubuntu18.04_all.deb	c0f026afa1fbc2cefdccf57fbaf481bcd26e8dac39945dba2f11c12e0030787c
xroad-centralserver_6.21.0-1.ubuntu18.04_all.deb	88fcabae451ecb2bbeeb9f2e9e31665485600586ec15b8b8e71e9947298bd0c4
xroad-confclient_6.21.0-1.ubuntu18.04_amd64.deb	a26b39f94a8821eeb9cf98315060a3d072874e1d4f340eec0cbc8ffab4e31a91
xroad-confproxy_6.21.0-1.ubuntu18.04_all.deb	a8d854c41d9ecbbf1a12ba896b235e95de88dd630d2f60d10565023dc471cead
xroad-jetty9_6.21.0-1.ubuntu18.04_all.deb	9e8ea6d11e5c4e8988776fe55a87d61a781a92634cd4e560ac9e477399c88ebd
xroad-monitor_6.21.0-1.ubuntu18.04_all.deb	f1bce08b1fc2387bd78b2f91472f136dbd462e47f7719596ae6412abf1653153
xroad-nginx_6.21.0-1.ubuntu18.04_amd64.deb	7e13e039fc06c0c96bb8347ead9934e51c52d155c42e060590d4d12c7b87f856
xroad-opmonitor_6.21.0-1.ubuntu18.04_all.deb	76a7809a1e20e59ab60a80ca619650057ae5faacfc1baced509119a62c13a95a
xroad-proxy_6.21.0-1.ubuntu18.04_all.deb	2cd36de14991b813a0ae1bd210f5d49dc090f49be938a2e28389350a47f929a9
xroad-securityserver-ee_6.21.0-1.ubuntu18.04_all.deb	df8c58444021ba47c69d86e0ebd0a5d038a93d100e050f1371bbc3254f689057
xroad-securityserver-fi_6.21.0-1.ubuntu18.04_all.deb	2c1d89ebabe2dff9e038586187e20bda6df5061dc9b7d1e6e5cb04eb5fd9c6ec
xroad-securityserver_6.21.0-1.ubuntu18.04_all.deb	713a07de89150842ed32671f157b11b37b40c36fb7737783b68317308d109e1d

xroad-signer_6.21.0-1.ubuntu18.04_amd64.deb	23b95fd7f604723f4a6105db92fb011c865e6cd45376663ed079963583af7628
---	--

Fuente: Corporación Agencia Nacional de Gobierno Digital

Ubuntu Trusty

Tabla 17: Ubuntu Trusty

Paquete	Suma de comprobación SHA256
xroad-addon-hwtokens_6.21.0-1.ubuntu14.04_all.deb	d5f791c59e5d5b00b4bf581861c50799713f309e743bb82978c69d9deae9f0d1
xroad-addon-messagelog_6.21.0-1.ubuntu14.04_all.deb	707877c068a37ccf97a37a42b144e26438f7f10ba3f2eab755446e322f522151
xroad-addon-metaservices_6.21.0-1.ubuntu14.04_all.deb	359aec24a5d779af3ea1bda297006691055d6c230d07b3f5139c9b200e79daa6
xroad-addon-opmonitoring_6.21.0-1.ubuntu14.04_all.deb	bd99d410477d714f277fdaa6e043fbc6dbe3540b09f559fd31ca7f931f240e29
xroad-addon-proxymonitor_6.21.0-1.ubuntu14.04_all.deb	638d47282de6ae87d8f998cb6feba89275b17394fbc1343ff8672efc1ed8fd2e
xroad-addon-wsdlvalidator_6.21.0-1.ubuntu14.04_all.deb	5aeb0aca5d3615eaa9f2971c639b170df6ee3b7074a91a22cf599c4e390edaaf
xroad-autologin_6.21.0-1.ubuntu14.04_all.deb	59b0adac40abaef1e1b5b2fbe6a439e7812e8f608cf2c8a551cd914948087b54
xroad-base_6.21.0-1.ubuntu14.04_amd64.deb	5facd9f2c698a53c13f55402e6f9b41f0bcdfd2bbe5fumz408a354cccfa38df

Paquete	Suma de comprobación SHA256
xroad-center-clusterhelper_6.21.0-1.ubuntu14.04_all.deb	b06d866022607c70082245b4a24aa29c6aee565a1566383ace9d5ab3d82d4f04
xroad-center_6.21.0-1.ubuntu14.04_all.deb	5595563b1783916b4af913f4ce8287640bfc80e7cb722ab2241f0d2bf843d4fb
xroad-centralserver-Monitoring_6.21.0-1.ubuntu14.04_all.deb	d5f5433a4e4161fc54636f708b72d46c470cf14c0ca242823e8b524e45ea684d
xroad-centralserver_6.21.0-1.ubuntu14.04_all.deb	f807bf295b6421298f039b2ecaab7b7c94522cdba74bcd4c6671f2af6e3877fa
xroad-confclient_6.21.0-1.ubuntu14.04_amd64.deb	e905cb1337009beab09132d98faa751a9092614e8f88c8ba36e82c57abf4dd09
xroad-confproxy_6.21.0-1.ubuntu14.04_all.deb	181b3064f1658f8f693a0dfc3be4ec1ee33e8721fe57504c1029f0f28521d46d
xroad-jetty9_6.21.0-1.ubuntu14.04_all.deb	0679ebb28ad7ed83336ce76b17ee479fbd9b521ca5e0c94deb9832398d0f4cd
xroad-monitor_6.21.0-1.ubuntu14.04_all.deb	d1f717a951991f29eba64f1c4148dee7881da1618970fdd297f0674bb15f7c2a
xroad-nginx_6.21.0-1.ubuntu14.04_amd64.deb	db8cc5ff1e62d711afef24bea9c09d9053b0087e95460aa8892170edc577a755
xroad-opmonitor_6.21.0-1.ubuntu14.04_all.deb	ffe270d6794eba9c441c64b87a191b521ff475c024c20e079962caee29e9f933
xroad-proxy_6.21.0-1.ubuntu14.04_all.deb	f4002b9ee5e28cfeae43e715cd688141079c3417aae9b00d58b7f73c4da03371
xroad-securityserver-ee_6.21.0-1.ubuntu14.04_all.deb	4f0652513f23591880d2c06fae6cd9937dcac7a3785eda8da2b197410dfe6960

Paquete	Suma de comprobación SHA256
xroad-securityserver_6.21.0-1.ubuntu14.04_all.deb	eed44d5d0e159cdc1b64355874ec3068b9a749a114b7ab883de5f71fda6b6342
xroad-securityserver-fi_6.21.0-1.ubuntu14.04_all.deb	80cbca8130beeed11b5c13b423f402a6fefec2098a22289898ed641b200a4449
xroad-signer_6.21.0-1.ubuntu14.04_amd64.deb	f93866d8a44fd1ac9a5d756a6aea64824580bfa179d7a118c8ec904caecdaf4e

Fuente: Corporación Agencia Nacional de Gobierno Digital

RHEL 7

Tabla 18: RHEL 7

Paquete	Suma de comprobación SHA256
xroad-addon-messagelog-6.21.0-1.el7.x86_64.rpm	64909d8b1a1fb26101128ef5323a11550a80c9f49e650206de47733828f28ef0
xroad-addon-metaservices-6.21.0-1.el7.x86_64.rpm	ca5cabd82877afe1a0ad0c9e2db2120b18e15afef6b5048be5d964d8db8baf4e
xroad-addon-opmonitoring-6.21.0-1.el7.x86_64.rpm	37ae7eba02cb868bb978c07957e15d10d0d611619ae500f35ba377b78dd215d0
xroad-addon-proxymonitor-6.21.0-1.el7.x86_64.rpm	bf095245dbce5af6e49779f765560b9a84cb7a84bae8534a2c926a32817d76ae

Paquete	Suma de comprobación SHA256
xroad-addon-wsdlvalidator-6.21.0-1.el7.x86_64.rpm	016e7a8cf5248f679396ebfbcc93f83acf6d40810b0e8c8d68abc6d7af4c753d
xroad-autologin-6.21.0-1.el7.noarch.rpm	3b532c014adc671b138ba30d683b7806366a82d9ff32de5a8efcb0abf4bf7f99
xroad-base-6.21.0-1.el7.x86_64.rpm	bf90399c0a59516444cd5263e3159e8eac0ab1b14166b1515dfdb1908357cadb
xroad-common-6.21.0-1.el7.x86_64.rpm	36918875e4566042baa3c7c72e5ff4fa5c34cf8bf5a6db48970dc317495989e5
xroad-confclient-6.21.0-1.el7.x86_64.rpm	c478f9b757eb3f8ce91679fd21fb7dda4a3017652d25d90fbd9bf3e5764ca794
xroad-jetty9-6.21.0-1.el7.x86_64.rpm	0cc9fe25be9969ce14db5772748c68fcdab5d23efd19ccfaf01e59d414959813
xroad-monitor-6.21.0-1.el7.x86_64.rpm	f8b1278cc47fe4fb00939aac0484ac5e899f187aeacb921a685ff7f9636a5d6c
xroad-nginx-6.21.0-1.el7.x86_64.rpm	7f58ff98edcfc9067e8486eaaad2e77f66ee51220fe06b76459676a69cbe7e36
xroad-opmonitor-6.21.0-1.el7.x86_64.rpm	800c3ddca0473e51d75c79dc4b0a8ae5567260c2398ad7704f7177e3cccbbbe44
xroad-proxy-6.21.0-1.el7.x86_64.rpm	aba294d614931dfb643b2ff89892e7df986e40ae524a6cf24d70cb8fa27a76a4

Paquete	Suma de comprobación SHA256
xroad-securityserver-6.21.0-1.el7.noarch.rpm	9025ab8c125a45b8d579ea3ec8a10b960bcdd8e1fbda35778520e85e32006e86
xroad-securityserver-fi-6.21.0-1.el7.noarch.rpm	3129fa06b04133346f885e213922aedbc627adeb91e170b08f8bb49c6aa30919
xroad-signer-6.21.0-1.el7.x86_64.rpm	414af45b339d6a34e96541209704caca0f3347a541210d9eeda3b5c5b9c5987ae

Fuente: Corporación Agencia Nacional de Gobierno Digital