

# **Casos de Uso**

## **Global**

### **Configuration**

### **Distribution**

# Índice

Índice .....	2
Introducción .....	4
Propósito .....	4
Visión General .....	4
2.1 Actores .....	5
2.2 Casos de Uso del Servidor Central.....	6
2.2.1 UC GCONF_01: Ver una Fuente de Configuración .....	6
2.2.2 UC GCONF_02: Descargar un Archivo Ancla de Fuente de Configuración .....	7
2.2.3 UC GCONF_03: Re-crear un Ancla de Fuente de Configuración .....	7
2.2.4 UC GCONF_04: Describir Datos de Parte Opcional de Configuración .....	8
2.2.5 UC GCONF_05: Subir un Archivo de Parte Opcional de Configuración .....	9
2.2.6 UC GCONF_06: Descargar un Archivo de Parte de Configuración .....	10
2.2.7 UC GCONF_07: Iniciar Sesión en un Token de Seguridad de Software .....	11
2.2.8 UC GCONF_08: Iniciar Sesión en un Token de Seguridad de Hardware .....	12
2.2.9 UC GCONF_09: Cerrar sesión en un token de seguridad de software .....	13
2.2.10 UC GCONF_10: Cerrar sesión en un token de seguridad de hardware.....	14
2.2.11 UC GCONF_11: Agregar una clave de firma de fuente de configuración.....	15
2.2.12 UC GCONF_12: Activar una Clave de Firma de Fuente de Configuración .....	16
2.2.13 UC GCONF_13: Eliminar una Clave de Firma de Fuente de Configuración .....	17
2.2.14 UC GCONF_14: Ver Parámetros del Sistema.....	18
2.2.15 UC GCONF_15: Editar la Dirección del Servidor Central .....	18
2.2.16 UC GCONF_16: Analizar la Entrada del Usuario .....	19
2.2.17 UC GCONF_17: Generar un Ancla de Configuración .....	20
2.2.18 UC GCONF_18: Generar Configuración .....	21
2.2.19 UC GCONF_19: Manejar una Solicitud de Descarga de Configuración .....	22
2.3 Casos de Uso del Servidor de Seguridad .....	23
2.3.1 UC GCONF_20: Ver la Información del Ancla de Configuración .....	23
2.3.2 UC GCONF_21: Descargar el Archivo del Ancla de Configuración .....	24
2.3.3 UC GCONF_22: Subir un Archivo de Ancla de Configuración.....	24
2.3.4 UC GCONF_23: Actualizar Configuración .....	26

2.3.5 UC GCONF\_24: Descargar Configuración desde una Fuente de Configuración..... 27

2.3.6 UC GCONF\_25: Verificar la Firma del Directorio de Configuración..... 30

2.3.7 UC GCONF\_26: Manejar una Parte de Configuración del Directorio de Configuración  
..... 31

# Introducción

## Propósito

El propósito de este documento es describir:

- **La gestión de las fuentes de configuración en el servidor central y servidor de seguridad,**
- **La generación y distribución de la configuración global en el servidor central, y**
- **La descarga y verificación de la configuración global en el servidor de seguridad.**

Este documento no incluye casos de uso para:

- **La federación de sistemas X-Road** – estos casos de uso están descritos en el documento “X-Road: Use Case Model for Federation”.
- **La funcionalidad del proxy de configuración** – estos casos de uso están descritos en el documento “X-Road: Use Case Model for the Configuration Proxy”.

Los casos de uso incluyen verificaciones que tienen lugar y las principales condiciones de error que se pueden encontrar durante el proceso descrito. Los errores generales del sistema que pueden ocurrir en la mayoría de los casos de uso (por ejemplo, errores de conexión a la base de datos o errores de falta de memoria) no están descritos en este documento.

Los casos de uso suponen que los componentes de software de X-Road involucrados en los casos de uso están instalados e inicializados (ver [IG-CS] y [IG-SS]).

Los casos de uso que incluyen un actor humano (el nivel del caso de uso es tarea de usuario) suponen que el actor está conectado al sistema y tiene los derechos de acceso necesarios para realizar el caso de uso.

## Visión General

Los servidores de seguridad de X-Road descargan periódicamente la configuración global distribuida por los proveedores de configuración. La configuración global se utiliza para verificar las partes que se comunican a través de X-Road y para comprobar la validez de varios elementos de datos, como certificados de autenticación, respuestas OCSP y marcas de tiempo.

La información necesaria para que los servidores de seguridad descarguen y verifiquen la configuración global está contenida en los **anclajes de configuración**. Los **anclajes de configuración** son distribuidos por los proveedores de configuración internos a los propietarios de los servidores de seguridad a través de medios fuera de banda.

Los proveedores de configuración aseguran la integridad de la configuración distribuida mediante la firma del directorio de configuración.

## 2.1 Actores

El modelo de casos de uso para la descarga de configuración incluye los siguientes actores:

- **Administrador de SS** (administrador del servidor de seguridad) – persona responsable de gestionar el servidor de seguridad.
- **Administrador de CS** (administrador del servidor central) – persona responsable de gestionar el servidor central.
- **Fuente de configuración** – un componente (servidor HTTP) gestionado por el servidor central o el proxy de configuración que distribuye la configuración global.
- **Cliente de configuración** – servidor de seguridad que descarga la configuración desde las fuentes de configuración.

Las relaciones entre los actores, los sistemas y los casos de uso se describen en la **Figura 1**.

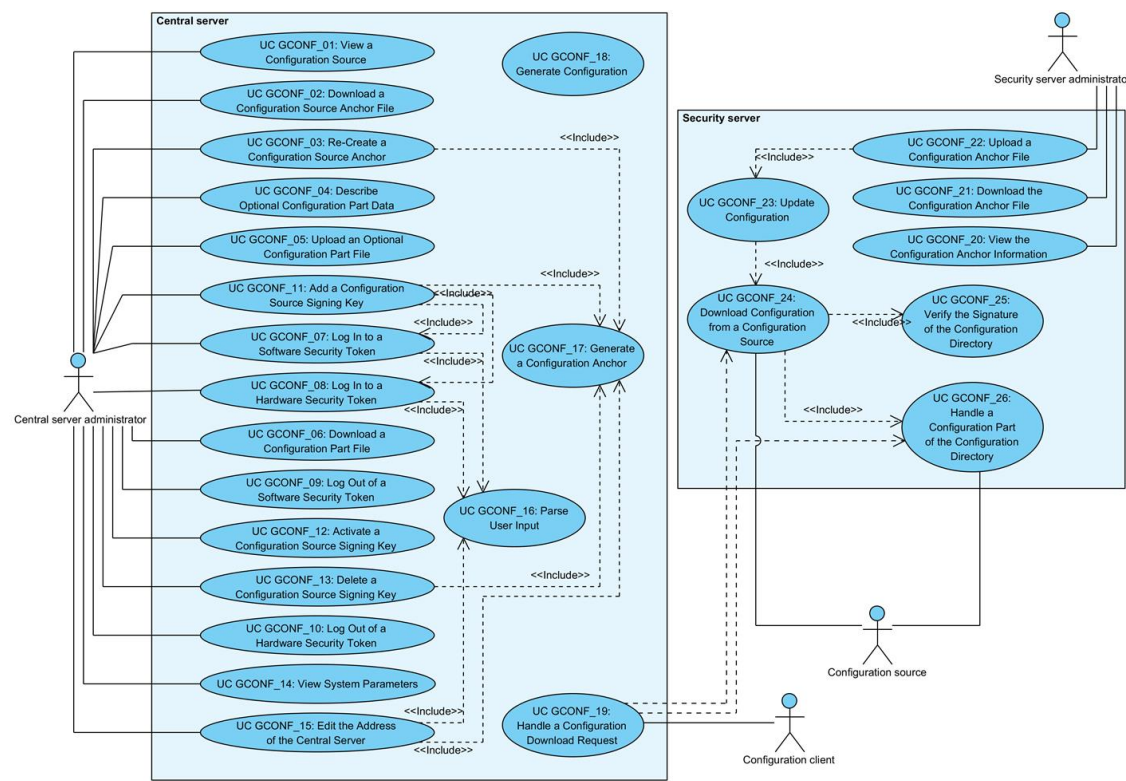


Figura 1. Diagrama de casos de uso para distribuir la configuración global

## 2.2 Casos de Uso del Servidor Central

### 2.2.1 UC GCONF\_01: Ver una Fuente de Configuración

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS (servidor central)

**Descripción breve:** El administrador de CS ve la información sobre una fuente de configuración proporcionada por el servidor central.

**Precondiciones:** -

**Postcondiciones:** La información de la fuente de configuración ha sido mostrada al administrador de CS.

**Desencadenante:** El administrador de CS desea ver la información de la fuente de configuración.

#### Escenario principal de éxito:

1. El administrador de CS selecciona ver una fuente de configuración.
2. El sistema muestra una fuente de configuración proporcionada por el servidor central. Se muestra la siguiente información:
  - Tipo de la fuente de configuración (interno/externo).
  - El valor hash SHA-224 del ancla de configuración.
  - La fecha y hora de generación (UTC) del ancla de configuración.
  - La URL de descarga de la configuración: dirección desde donde se puede descargar el directorio de configuración proporcionado por esta fuente. El sistema compone la URL de descarga agregando /internalconf o /externalconf (dependiendo del tipo de la fuente de configuración) a la dirección del servidor central.
  - Lista de claves de firma de configuración. Para cada clave se muestra la siguiente información:
    - El identificador del dispositivo que posee la clave.
    - El identificador de la clave.
    - La fecha y hora de generación de la clave.
  - Se resalta la clave actualmente utilizada para firmar la configuración. Sólo se muestran las claves que tienen un certificado asociado.
  - Lista de archivos de partes de configuración distribuidos por la fuente. Para cada parte de configuración se muestra la siguiente información:
    - Nombre del archivo de la parte de configuración.
    - Identificador de contenido de la parte de configuración.
    - Fecha y hora en que el archivo de la parte de configuración fue actualizado por última vez.
  - Se muestran las siguientes opciones de acción de usuario:
    - Descargar el archivo ancla de la fuente de configuración: **2.2.2**;
    - Re-crear el archivo ancla de la fuente de configuración: **2.2.3**;
    - Agregar una clave de firma de configuración: **2.2.11**;
    - Eliminar una clave de firma de configuración: **2.2.13**;
    - Activar una clave de firma de configuración: **2.2.12**;
    - Iniciar sesión en un token de seguridad que posea una clave de firma de configuración: **2.2.7** o **2.2.8**;
    - Cerrar sesión en un token de seguridad que posea una clave de firma de configuración: **2.2.9** o **2.2.10**;
    - Descargar un archivo de parte de configuración: **2.2.6**;

- Subir un archivo de parte de configuración opcional: **2.2.5**, en caso de que la parte opcional esté descrita en el sistema: **2.2.4**.

### 2.2.2 UC GCONF\_02: Descargar un Archivo Ancla de Fuente de Configuración

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS (servidor central)

**Descripción breve:** El administrador de CS descarga el ancla de configuración de una fuente de configuración.

**Precondiciones:** El archivo ancla ha sido generado.

**Postcondiciones:** El administrador de CS ha descargado el archivo ancla.

**Desencadenante:** El administrador de CS desea descargar el ancla de configuración, ya sea para ver su contenido o distribuir el ancla a los clientes de configuración.

#### Escenario principal de éxito:

1. El administrador de CS selecciona descargar el ancla de configuración de una fuente de configuración (interna o externa).
2. El sistema presenta el archivo ancla de configuración para su descarga.
3. El administrador de CS guarda el archivo ancla en el sistema de archivos de la computadora local.

### 2.2.3 UC GCONF\_03: Re-crear un Ancla de Fuente de Configuración

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS (servidor central)

**Descripción breve:** El administrador de CS re-crea el ancla de configuración de una fuente de configuración. Bajo el comportamiento normal del sistema, la generación del archivo ancla por el administrador de CS no es necesaria, ya que el sistema genera el archivo ancla automáticamente cuando se necesita. La re-creación permite recuperar de fallos del sistema.

**Precondiciones:** -

**Postcondiciones:** Se ha creado un registro de auditoría para el evento.

**Desencadenante:** El administrador de CS desea re-crear el ancla de configuración para una fuente de configuración.

#### Escenario principal de éxito:

1. El administrador de CS selecciona re-crear el ancla de configuración.
2. El sistema genera el ancla de configuración: **2.2.17**.
3. El sistema muestra el mensaje: "Ancla de configuración interna generada con éxito" o "Ancla de configuración externa generada con éxito", dependiendo de la fuente de configuración para la que se haya re-creado el ancla.



4. El sistema registra el evento “Re-crear ancla de configuración interna” o “Re-crear ancla de configuración externa” en el registro de auditoría, dependiendo de la fuente de configuración.

**Extensiones:**

- 2a. El proceso de generación del ancla terminó con un mensaje de error.
  - 2a.1. El sistema muestra el mensaje de error: “La generación del ancla de configuración X falló: Y”, donde “X” es el tipo de fuente de configuración (interna o externa) y “Y” es el motivo de la falla.
  - 2a.2. El sistema registra el evento “Re-crear ancla de configuración interna fallida” o “Re-crear ancla de configuración externa fallida” en el registro de auditoría. El caso de uso termina.

**Información relacionada:**

El registro de auditoría se encuentra en /var/log/xroad/audit.log. El conjunto de registros de auditoría se describe en el documento “X-Road: Audit Log Events” [SPEC-AL].

#### 2.2.4 UC GCONF\_04: Describir Datos de Parte Opcional de Configuración

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS (servidor central)

**Descripción breve:** El administrador de CS crea un archivo en la configuración del sistema que contiene la información necesaria para que el sistema reconozca, valide y distribuya una parte opcional de la configuración.

**Precondiciones:** -

**Postcondiciones:** Se ha guardado un archivo que describe una parte opcional de la configuración en la configuración del sistema. La opción de subir el archivo de parte opcional está habilitada en la interfaz gráfica.

**Desencadenante:** Se necesita agregar información no contenida en las partes de parámetros compartidos o privados a la configuración global.

**Escenario principal de éxito:**

1. El administrador de CS crea un archivo INI (ver [INI]) en el directorio /etc/xroad/configuration-parts que contiene las siguientes parejas clave-valor:
  - content-identifier = (ej., FOO)
  - file-name = (ej., foo.xml)
2. El administrador de CS guarda el archivo creado.

**Extensiones:** -

**Información relacionada:**

El archivo de descripción debe ser un archivo INI válido y debe otorgarse el permiso de lectura al grupo “xroad” para el archivo de descripción creado. El sistema utiliza los valores de las claves content-identifier y file-name respectivamente como valores de los encabezados MIME Content-identifier y Content-file-name en el directorio de configuración (para más información, véase el documento “X-Road: Protocol for Downloading Configuration” [PR-GCONF]) y también para mostrar información sobre las partes de configuración en la interfaz gráfica.



Editar o eliminar el archivo INI manualmente no es compatible actualmente y puede resultar en un comportamiento inconsistente del sistema. La solución actual asume que los archivos INI que describen parámetros opcionales de configuración son agregados, editados y eliminados por paquetes de instalación o actualización de software.

---

### 2.2.5 UC GCONF\_05: Subir un Archivo de Parte Opcional de Configuración

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS (servidor central)

**Descripción breve:** El administrador de CS sube un archivo de parte opcional de configuración.

**Precondiciones:** Los datos de parte opcional de configuración están descritos en el sistema (ver 2.2.4).

**Postcondiciones:** Se ha creado un registro de auditoría para el evento.

**Desencadenante:** El contenido del archivo de parte opcional de configuración ha cambiado y el administrador de CS desea subir el archivo actualizado al sistema.

#### Escenario principal de éxito:

1. El administrador de CS selecciona subir un archivo de parte opcional de configuración.
2. El administrador de CS inserta la ruta al archivo de parte de configuración en el sistema de archivos de la computadora.
3. El sistema verifica que el archivo subido cumple con el esquema XSD para el identificador de contenido dado.
4. El sistema muestra el mensaje “Archivo de configuración para el identificador de contenido 'X' subido con éxito.”, donde “X” es el identificador de contenido descrito para la parte de configuración.
5. El sistema verifica que ya existe un archivo para esta parte de configuración opcional en la configuración del sistema y reemplaza el archivo existente con el subido.
6. El sistema registra el evento “Subir parte de configuración” en el registro de auditoría.

#### Extensiones:

- 3a. No se describe un validador para esta parte de configuración.
  - 3a.1. El caso de uso continúa desde el paso 5.
- 3b. El sistema no puede encontrar el programa de validación descrito para esta parte de configuración.
  - 3b.1. El sistema muestra el mensaje de error: “Falló al subir la parte de configuración: El programa de validación 'X' no existe en el sistema de archivos.”, donde “X” es la ruta del programa de validación descrito para esta parte de configuración.
  - 3b.2. El sistema registra el evento “Falló la subida de la parte de configuración” en el registro de auditoría.
  - 3b.3. El administrador de CS selecciona volver a insertar la ruta al archivo de parte de configuración. El caso de uso continúa desde el paso 3.

- 3b.3a. El administrador de CS selecciona terminar el caso de uso.
- 3c. La comunicación con el programa de validación se cerró inesperadamente.
  - 3c.1. El sistema muestra el mensaje de error: “El programa de validación 'X' terminó prematuramente, asegúrese de que haga lo correcto.”, donde “X” es la ruta del programa de validación descrito para esta parte de configuración.
  - 3c.2. El sistema registra el evento “Falló la subida de la parte de configuración” en el registro de auditoría.
  - 3c.3. El administrador de CS selecciona volver a insertar la ruta al archivo de parte de configuración. El caso de uso continúa desde el paso 3.
  - 3c.3a. El administrador de CS selecciona terminar el caso de uso.
- 3d. Ocurrió un error al ejecutar el programa de validación.
  - 3d.1. El sistema muestra el mensaje de error: “Ocurrió un error de IO al ejecutar el programa de validación 'X', mensaje: 'Y'”, donde “X” es la ruta del programa de validación descrito para esta parte de configuración y “Y” es la descripción del error.
  - 3d.2. El sistema registra el evento “Falló la subida de la parte de configuración” en el registro de auditoría.
  - 3d.3. El administrador de CS selecciona volver a insertar la ruta al archivo de parte de configuración. El caso de uso continúa desde el paso 3.
  - 3d.3a. El administrador de CS selecciona terminar el caso de uso.
- 4a. La validación tuvo éxito con errores de validación.
  - 4a.1. El sistema muestra el mensaje de error: “Falló al subir la parte de configuración: La validación del archivo de configuración con identificador de contenido 'X' no pasó correctamente con errores de validación.”

---

#### 2.2.6 UC GCONF\_06: Descargar un Archivo de Parte de Configuración

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS

**Descripción breve:** El administrador de CS descarga un archivo de parte de configuración.

**Precondiciones:** El archivo de parte de configuración ha sido generado por el sistema o cargado al sistema.

**Postcondiciones:** El administrador de CS ha descargado el archivo de parte de configuración.

**Desencadenante:** El administrador de CS desea descargar un archivo de parte de configuración, por ejemplo, para ver el contenido del archivo.

##### Escenario principal de éxito:

1. El administrador de CS selecciona descargar un archivo de parte de configuración.
2. El sistema presenta el archivo de parte de configuración para su descarga.

3. El administrador de CS guarda el archivo de parte de configuración en el sistema de archivos de la computadora.

### 2.2.7 UC GCONF\_07: Iniciar Sesión en un Token de Seguridad de Software

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS

**Descripción breve:** El administrador de CS inicia sesión en un token de seguridad de software introduciendo el código PIN del token.

**Precondiciones:** El token está en estado cerrado de sesión.

**Postcondiciones:** Se ha creado un registro de auditoría para el evento.

**Desencadenantes:**

- El administrador de CS desea hacer disponible la funcionalidad del token para el sistema.
- Paso 4a.1. de **2.2.11**.

**Escenario principal de éxito:**

1. El administrador de CS selecciona iniciar sesión en un token de seguridad de software.
2. El administrador de CS introduce el código PIN del token.
3. El sistema procesa la entrada del usuario: **2.2.16**.
4. El sistema verifica que el código PIN es correcto y se inicia sesión en el token.
5. El sistema registra el evento "Iniciar sesión en token" en el registro de auditoría.

**Extensiones:**

- 3a. El proceso de análisis de la entrada del usuario termina con un mensaje de error.
  - 3a.1. El sistema muestra el mensaje de terminación del proceso de análisis.
  - 3a.2. El sistema registra el evento "Falló iniciar sesión en token" en el registro de auditoría.
  - 3a.3. El administrador de CS selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
  - 3a.3a. El administrador de CS selecciona terminar el caso de uso.
- 4a. El código PIN ingresado es incorrecto:
  - 4a.1. El sistema muestra el mensaje de error: "PIN incorrecto".
  - 4a.2. El sistema registra el evento "Falló iniciar sesión en token" en el registro de auditoría.
  - 4a.3. El administrador de CS selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
  - 4a.3a. El administrador de CS selecciona terminar el caso de uso.

## 2.2.8 UC GCONF\_08: Iniciar Sesión en un Token de Seguridad de Hardware

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS

**Descripción breve:** El administrador de CS inicia sesión en un token de seguridad de hardware introduciendo el código PIN del token.

**Precondiciones:**

- El token de seguridad de hardware está inicializado y conectado al sistema.
- El token está en estado cerrado de sesión.

**Postcondiciones:** Se ha creado un registro de auditoría para el evento.

**Desencadenantes:**

- El administrador de CS desea hacer disponible la funcionalidad del token para el sistema.
- Paso 4a.1. de **2.2.11**.

**Escenario principal de éxito:**

1. El administrador de CS selecciona iniciar sesión en un token de seguridad de hardware que posee una clave de firma de configuración.
2. El administrador de CS introduce el código PIN del token.
3. El sistema procesa la entrada del usuario: **2.2.16**.
4. El sistema verifica que el token no está bloqueado.
5. El sistema verifica que el código PIN ingresado cumple con el formato configurado para el token.
6. El sistema verifica que el código PIN ingresado es correcto y se inicia sesión en el token.
7. El sistema registra el evento “Iniciar sesión en token” en el registro de auditoría.

**Extensiones:**

- 3a. El proceso de análisis de la entrada del usuario termina con un mensaje de error.
  - 3a.1. El sistema muestra el mensaje de terminación del proceso de análisis.
  - 3a.2. El sistema registra el evento “Falló iniciar sesión en token” en el registro de auditoría.
  - 3a.3. El administrador de CS selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
  - 3a.3a. El administrador de CS selecciona terminar el caso de uso.
- 4-6a. El intento de inicio de sesión falló (por ejemplo, el PIN ingresado fue incorrecto):
  - 4-6a.1. El sistema muestra el mensaje de error: “Inicio de sesión fallido: X”, donde “X” es el código de error de la interfaz criptográfica PKCS #11 (ver [PKCS11]).
  - 4-6a.2. El sistema registra el evento “Falló iniciar sesión en token” en el registro de auditoría.
  - 4-6a.3. El administrador de CS selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
  - 4-6a.3a. El administrador de CS selecciona terminar el caso de uso.
- 4b. El token es inaccesible:

- 4b.1. El sistema muestra el mensaje de error: “Token 'X' no disponible”, donde “X” es el identificador del token de seguridad.
  - 4b.2. El sistema registra el evento “Falló iniciar sesión en token” en el registro de auditoría.
  - 4-6a.3. El administrador de CS selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
  - 4-6a.3a. El administrador de CS selecciona terminar el caso de uso.
- 4b. El token de seguridad está bloqueado (demasiados intentos incorrectos del PIN):
  - 4b.1. El sistema muestra el mensaje de error: “PIN bloqueado”.
  - 4b.2. El sistema registra el evento “Falló iniciar sesión en token” en el registro de auditoría.
  - 4b.3. El administrador de CS selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
  - 4b.3a. El administrador de CS selecciona terminar el caso de uso.
- 5b. El formato del código PIN ingresado no es aceptable para el token:
  - 5b.1. El sistema muestra el mensaje de error: “Formato de PIN incorrecto”.
  - 5b.2. El sistema registra el evento “Falló iniciar sesión en token” en el registro de auditoría.
  - 5b.3. El administrador de CS selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
  - 5b.3a. El administrador de CS selecciona terminar el caso de uso.
- 6b. El código PIN ingresado es incorrecto y queda un intento de inicio de sesión:
  - 6b.1. El sistema muestra el mensaje de error: “Inicio de sesión fallido: CKR\_PIN\_INCORRECT, intentos restantes: 1”.
  - 6b.2. El sistema registra el evento “Falló iniciar sesión en token” en el registro de auditoría.
  - 6b.3. El administrador de CS selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
  - 6b.3a. El administrador de CS selecciona terminar el caso de uso.
- 6c. El código PIN ingresado es incorrecto y no quedan intentos de inicio de sesión (es decir, el token está bloqueado):
  - 6c.1. El sistema muestra el mensaje de error: “Inicio de sesión fallido: CKR\_PIN\_INCORRECT. PIN bloqueado”.
  - 6c.2. El sistema registra el evento “Falló iniciar

sesión en token” en el registro de auditoría.

- 6c.3. El administrador de CS selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
- 6b.3a. El administrador de CS selecciona terminar el caso de uso.

### 2.2.9 UC GCONF\_09: Cerrar sesión en un token de seguridad de software

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS

**Descripción breve:** El administrador de CS cierra sesión en un token de seguridad de

software.

**Precondiciones:**

- El token de seguridad de software contiene una o más claves de firma de configuración.
- El token de seguridad de software está en estado de sesión iniciada.

**Postcondiciones:**

- El token está en estado cerrado de sesión.
- El sistema no puede usar las claves del token para firmar configuraciones.
- Se ha creado un registro de auditoría para el evento.

**Desencadenante:** El administrador de CS desea cerrar sesión en un token de seguridad de software.

**Escenario principal de éxito:**

1. El administrador de CS selecciona cerrar sesión en un token.
2. El sistema cierra la sesión del token.
3. El sistema registra el evento "Cerrar sesión en token" en el registro de auditoría.

## 2.2.10 UC GCONF\_10: Cerrar sesión en un token de seguridad de hardware

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS

**Descripción breve:** El administrador de CS cierra sesión en un token de seguridad de hardware.

**Precondiciones:**

- El token de seguridad de hardware contiene una o más claves de firma de configuración.
- El token de seguridad de hardware está en estado de sesión iniciada.

**Postcondiciones:**

- El sistema no puede usar las claves del token para firmar configuraciones.
- Se ha creado un registro de auditoría para el evento.

**Desencadenante:** El administrador de CS desea cerrar sesión en un token de seguridad de hardware.

**Escenario principal de éxito:**

1. El administrador de CS selecciona cerrar sesión en un token de seguridad.
2. El sistema cierra la sesión del token.
3. El sistema registra el evento "Cerrar sesión en token" en el registro de auditoría.

**Extensiones:**

- 2a. El intento de cierre de sesión falla (por ejemplo, el token no es accesible):

- 2a.1. El sistema muestra el mensaje de error: "Error al cerrar sesión: X", donde "X" es el código de error de la interfaz criptográfica PKCS #11 [PKCS11].
- 2a.2. El sistema registra el evento "Falló cerrar sesión en token" en el registro de auditoría.
- 2a.3. El caso de uso termina.

---

### 2.2.11 UC GCONF\_11: Agregar una clave de firma de fuente de configuración

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS

**Descripción breve:** El administrador de CS genera una clave de firma de fuente de configuración en un token de seguridad. El sistema crea un certificado autofirmado que contiene la parte pública de la clave generada y genera el ancla de configuración que contiene el certificado creado.

**Precondiciones:** Un token de seguridad está inicializado y conectado al sistema.

**Postcondiciones:** -

**Desencadenante:** El administrador de CS desea agregar una clave de firma para una fuente de configuración (por ejemplo, como parte de un cambio regular de clave).

#### Escenario principal de éxito:

1. El administrador de CS selecciona agregar una clave de firma de fuente de configuración para una fuente de configuración (ya sea interna o externa).
2. El sistema muestra la lista de tokens de seguridad disponibles.
3. El administrador de CS selecciona un token de seguridad e ingresa la etiqueta de la clave.
4. El sistema genera una nueva clave de firma de configuración con la etiqueta insertada en el token seleccionado.
5. El sistema crea un certificado autofirmado que contiene la parte pública de la clave generada.
6. El sistema guarda la información de la clave generada y el certificado creado en la configuración del sistema.
7. El sistema verifica que la fuente de configuración seleccionada ya tenga una clave activa.
8. El sistema registra el evento "Generar clave de firma de configuración interna" o "Generar clave de firma de configuración externa", dependiendo de la fuente de configuración, en el registro de auditoría.
9. El sistema genera el ancla de configuración para la fuente de configuración:  
**2.2.17.**

#### Extensiones:

- 3a. El token deseado no está en la lista:
  - 3a.1. El administrador de CS termina el caso de uso.
- 4a. La generación de la clave falla porque el token no está iniciado sesión:
  - 4a.1. El sistema inicia el caso de uso **2.2.7** o **2.2.8**, dependiendo del tipo de token seleccionado.



- 4a.2. El sistema verifica que el proceso de inicio de sesión haya terminado correctamente. El caso de uso continúa desde el paso 4.
  - 4a.2a. El proceso de inicio de sesión termina con un error.
  - 4a.2a.1. El administrador de CS selecciona volver a seleccionar un token de seguridad. El caso de uso continúa desde el paso 4.
  - 4a.2a.1a. El administrador de CS selecciona terminar el caso de uso.
- 4b. La generación de la clave falla:
  - 4b.1. El sistema muestra el mensaje de error: “No se pudo generar la clave de firma: X”, donde “X” es la descripción del error. Si la generación de la clave falló en un token de seguridad de hardware, “X” es el código de error de la interfaz criptográfica PKCS #11 [PKCS11].
  - 4b.2. El sistema registra el evento “Generar clave de firma de configuración interna fallida” o “Generar clave de firma de configuración externa fallida”, dependiendo de la fuente de configuración, en el registro de auditoría.
  - 4b.3. El administrador de CS selecciona volver a seleccionar un token de seguridad. El caso de uso continúa desde el paso 4.
  - 4b.3a. El administrador de CS selecciona terminar el caso de uso.
- 5a. La generación del certificado autofirmado falla:
  - 5a.1. El sistema elimina la clave generada.
  - 5a.1a. La eliminación de la clave falla.
  - 5a.1a.1. El caso de uso continúa desde el paso 5a.2.
  - 5a.2. El sistema muestra el mensaje de error: “No se pudo generar la clave de firma: X”, donde “X” es la descripción del error.
  - 5a.3. El sistema registra el evento “Generar clave de firma de configuración interna fallida” o “Generar clave de firma de configuración externa fallida”, dependiendo de la fuente de configuración, en el registro de auditoría.
  - 5a.4. El administrador de CS selecciona volver a seleccionar un token de seguridad. El caso de uso continúa desde el paso 4.
  - 5a.4a. El administrador de CS selecciona terminar el caso de uso.
- 7a. La fuente seleccionada no tiene una clave activa:
  - 7a.1. El sistema marca la clave como activa y comienza a usarla para firmar la configuración proporcionada por la fuente.
  - 7a.2. El caso de uso continúa desde el paso 8.

---

#### 2.2.12 UC GCONF\_12: Activar una Clave de Firma de Fuente de Configuración

**Sistema:** Servidor central

**Nivel:** Tarea del usuario

**Componente:** Servidor central

**Actor:** Administrador del CS

**Breve descripción:** El administrador del CS activa una clave de firma de fuente de configuración. El sistema utiliza la clave activa para firmar la configuración proporcionada por la fuente de configuración.

**Precondiciones:** Un token de seguridad que contiene una clave de firma inactiva asociada con la fuente de configuración está conectado al sistema.

**Postcondiciones:** -

**Desencadenante:** El administrador del CS desea cambiar la clave que el sistema utiliza para firmar la configuración proporcionada por la fuente.

**Escenario de éxito principal:**

- El administrador del CS selecciona activar una clave de firma de fuente de configuración inactiva.
- El sistema solicita confirmación.
- El administrador del CS confirma.
- El sistema verifica que la clave a activar esté accesible, marca la clave como activa y comienza a usarla para firmar la configuración proporcionada por la fuente.
- El sistema registra el evento "Activar clave interna de firma de configuración" o "Activar clave externa de firma de configuración", dependiendo de la fuente de configuración, en el registro de auditoría.

**Extensiones:**

- 3a. El administrador del CS cancela la activación de la clave.
    - 3a.1. El sistema termina el caso de uso.
  - 4a. La clave a activar no está accesible.
    - 4a.1. El sistema muestra el mensaje de error: "No se pudo activar la clave de firma: token o clave no disponible".
    - 4a.2. El sistema registra el evento "Activar clave interna de firma de configuración fallida" o "Activar clave externa de firma de configuración fallida", dependiendo de la fuente de configuración, en el registro de auditoría.
    - 4a.3. El caso de uso termina.
- 

**2.2.13 UC GCONF\_13: Eliminar una Clave de Firma de Fuente de Configuración**

**Sistema:** Servidor central

**Nivel:** Tarea del usuario

**Componente:** Servidor central

**Actor:** Administrador del CS

**Breve descripción:** El administrador del CS elimina una clave de firma de fuente de configuración y el certificado asociado. El sistema genera el ancla de configuración que contiene los certificados actualizados para la fuente de configuración.

**Precondiciones:** La clave de firma no está en estado activo (es decir, el sistema está utilizando otra clave para firmar la configuración).

**Postcondiciones:** -

**Desencadenante:** El administrador del CS desea eliminar una clave de firma de configuración.

**Escenario de éxito principal:**

- El administrador del CS selecciona eliminar una clave de firma de fuente de configuración.
  - El sistema solicita confirmación.
  - El administrador del CS confirma.
  - El sistema elimina la información de la clave de firma seleccionada y el certificado asociado de la configuración del sistema y muestra el mensaje: "Clave eliminada exitosamente de la configuración del servidor central".
-

- El sistema genera el ancla de configuración para la fuente de configuración: 2.2.17.
- El sistema registra el evento “Eliminar clave interna de firma de configuración” en el registro de auditoría.
- El sistema elimina la clave de firma del token de seguridad y muestra el mensaje: “Clave eliminada exitosamente del token 'X'”, donde “X” es el identificador del token.

**Extensiones:**

- 3a. El administrador del CS cancela la eliminación de la clave.
  - 3a.1. El sistema termina el caso de uso.
- 7a. El sistema no puede eliminar la clave de firma del token de seguridad.
  - 7a.1. El sistema muestra el mensaje de error: “No se pudo eliminar la clave del token 'X': Y”, donde “X” es el identificador del token y “Y” son los detalles del error.

---

**2.2.14 UC GCONF\_14: Ver Parámetros del Sistema****Sistema:** Servidor central**Nivel:** Tarea del usuario**Componente:** Servidor central**Actor:** Administrador del CS**Breve descripción:** El administrador del CS visualiza los parámetros del sistema del servidor central.**Precondiciones:** -**Postcondiciones:** Los parámetros del sistema han sido mostrados al administrador del CS.**Desencadenante:** El administrador del CS desea ver los parámetros del sistema.**Escenario de éxito principal:**

- El administrador del CS selecciona ver los parámetros del sistema.
- El sistema muestra la siguiente información:
  - El identificador de la instancia de esta instancia de X-Road;
  - La dirección del servidor central.
- Las siguientes opciones de acción del usuario son mostradas:
  - Editar la dirección del servidor central: 2.2.15.

---

**2.2.15 UC GCONF\_15: Editar la Dirección del Servidor Central****Sistema:** Servidor central**Nivel:** Tarea del usuario**Componente:** Servidor central**Actor:** Administrador del CS**Breve descripción:** El administrador del CS cambia la dirección del servidor central.**Precondiciones:** -

**Postcondiciones:** Se ha creado un registro en el registro de auditoría para el evento.

**Desencadenante:** El administrador del CS desea cambiar la dirección en la que el servidor central está disponible para solicitudes entrantes (por ejemplo, solicitudes del servicio de gestión, solicitudes de descarga de configuración).

**Escenario de éxito principal:**

- El administrador del CS selecciona cambiar la dirección pública del servidor central.
- El administrador del CS inserta la dirección.
- El sistema analiza la entrada del usuario: 2.2.16.
- El sistema verifica que la dirección insertada sea un nombre DNS o una dirección IP válida.
- El sistema guarda la dirección.
- El sistema registra el evento “Editar dirección del servidor central” en el registro de auditoría.
- El sistema genera anclas de configuración para la configuración interna y externa: 2.2.17.

**Extensiones:**

- 3a. El análisis de la entrada del usuario termina con un mensaje de error.
  - 3a.1. El sistema muestra el mensaje de terminación del proceso de análisis.
  - 3a.2. El sistema registra el evento “Editar dirección del servidor central fallido” en el registro de auditoría.
  - 3a.3. El usuario selecciona reinsertar la dirección. El caso de uso continúa desde el paso 3.
  - 3a.3a. El usuario selecciona terminar el caso de uso.
- 4a. La dirección insertada no es válida.
  - 4a.1. El sistema muestra el mensaje de error: “La dirección del servidor central debe ser un nombre DNS o una dirección IP”.
  - 4a.2. El sistema registra el evento “Editar dirección del servidor central fallido” en el registro de auditoría.
  - 4a.3. El usuario selecciona reinsertar la dirección. El caso de uso continúa desde el paso 3.
  - 4a.3a. El usuario selecciona terminar el caso de uso.

---

## 2.2.16 UC GCONF\_16: Analizar la Entrada del Usuario

**Sistema:** Servidor central

**Nivel:** Subfunción

**Componente:** Servidor central

**Actores:** -

**Breve descripción:** El sistema elimina los espacios en blanco al inicio y al final de la entrada del usuario y verifica que los campos requeridos no estén vacíos.

**Precondiciones:** -

**Postcondiciones:** -

**Desencadenantes:**

- Paso 3 de 2.2.7.
- Paso 3 de 2.2.8.
- Paso 3 de 2.2.15.

**Escenario de éxito principal:**

- El sistema elimina los espacios en blanco al inicio y al final.
- El sistema verifica que los campos obligatorios estén completos.
- El sistema verifica que la entrada del usuario no exceda los 255 caracteres.

**Extensiones:**

- 2a. Uno o más campos obligatorios no están completos.
  - 2a.1. El caso de uso termina con el mensaje de error "Falta parámetro: 'X'", donde "X" es el nombre del parámetro faltante.
- 3a. La entrada del usuario excede los 255 símbolos.
  - 3a.1. El caso de uso termina con el mensaje de error "La entrada del parámetro X excede los 255 caracteres", donde "X" es el nombre del parámetro que tenía más de 255 caracteres.

---

**2.2.17 UC GCONF\_17: Generar un Ancla de Configuración****Sistema:** Servidor central**Nivel:** Subfunción**Componente:** Servidor central**Actor:** -**Breve descripción:** El sistema genera para una fuente de configuración un ancla de configuración que contiene la información necesaria para que los clientes de configuración descarguen y verifiquen la configuración de la fuente de configuración.**Precondiciones:** El identificador de la instancia y la dirección del servidor central están guardados en la configuración del sistema.**Postcondiciones:** -**Desencadenantes:**

- Paso 2 de 2.2.3.
- Paso 9 de 2.2.11.
- Paso 5 de 2.2.13.
- Paso 7 de 2.2.15.

**Escenario de éxito principal:**

- El sistema verifica que al menos una clave de firma con el certificado correspondiente esté guardada en la configuración del sistema para la fuente de configuración.
- El sistema genera el archivo de ancla y calcula el hash del archivo.
- El sistema guarda el archivo de ancla, el hash del archivo y la hora de generación del archivo en la configuración del sistema.
- El sistema muestra el mensaje: "Ancla de configuración interna generada exitosamente" o "Ancla de configuración externa generada exitosamente", dependiendo de la fuente de configuración.

**Extensiones:**

- 1a. El sistema no encontró claves de firma de configuración para la fuente de configuración.
    - 1a.1. El sistema muestra el mensaje de error: “Generación del ancla de configuración X fallida: No se configuraron claves de firma de configuración”, donde “X” representa “Interna” o “Externa”, dependiendo de la fuente de configuración. El caso de uso termina.
- 

**2.2.18 UC GCONF\_18: Generar Configuración**

**Sistema:** Servidor central

**Nivel:** Tarea del sistema

**Componente:** Servidor central

**Actor:** -

**Breve descripción:** El sistema genera los archivos de las partes de configuración privada y compartida, construye y firma los directorios de configuración para las fuentes de configuración, y pone la configuración global disponible para los clientes de configuración.

**Precondiciones:** -

**Postcondiciones:** -

**Desencadenante:** El temporizador de generación de configuración definido en el archivo de configuración del servidor central `/etc/cron.d/xroad-center*`.

**Escenario de éxito principal:**

- El sistema verifica que la configuración del sistema contenga los datos necesarios para generar la configuración y genera los archivos de las partes de configuración de parámetros privados y compartidos.
- El sistema verifica la validez de los archivos generados frente a los esquemas respectivos y guarda los archivos generados en la configuración del sistema.
- El sistema:
  - Calcula la hora de expiración de la configuración (sumando el valor del parámetro del sistema del servidor central `confExpireIntervalSeconds` al tiempo actual);
  - Calcula los valores hash de los archivos de configuración generados usando el algoritmo definido por el valor del parámetro del sistema del servidor central `confHashAlgoUri`; y
  - Construye los directorios de configuración internos y externos.
- El sistema firma los directorios de configuración internos y externos usando las claves de firma de configuración activas de las respectivas fuentes de configuración.
- El sistema pone los directorios de configuración firmados y los archivos de partes de configuración disponibles para los clientes de configuración.

**Extensiones:**

- 1a. La generación de los archivos de las partes de configuración falló porque no se configuró la dirección del servidor central.
-

- 1a.1. El sistema registra el mensaje de error “No se pudo generar una configuración global válida: No se encuentra la URL del servicio de autenticación. El servidor central puede no haberse inicializado”.
  - 1a.2. El sistema muestra el mensaje de error “Generación de configuración global fallando desde 'X'”, donde “X” es la fecha y hora desde la cual el sistema no ha podido generar una configuración global distribuible.
  - 1a.3. El caso de uso termina.
- 1b. La generación de los archivos de las partes de configuración falló porque no se configuró el proveedor de servicios de gestión.
  - 1b.1. El sistema registra el mensaje de error “No se pudo generar una configuración global válida: El proveedor de servicios de gestión no está configurado”.
  - 1b.2. El sistema muestra el mensaje de error “Generación de configuración global fallando desde 'X'”, donde “X” es la fecha y hora desde la cual el sistema no ha podido generar una configuración global distribuible.
  - 1b.3. El caso de uso termina.
- 1c. La generación de los archivos de las partes de configuración falló por cualquier otro motivo que no sea el indicado en las extensiones 1a y 1b.
  - 1c.1. El sistema registra el mensaje de error “No se pudo generar una configuración global válida: X”, donde “X” es el mensaje de error técnico del sistema.
  - 1c.2. El sistema muestra el mensaje de error “Generación de configuración global fallando desde 'X'”, donde “X” es la fecha y hora desde la cual el sistema no ha podido generar una configuración global distribuible.
  - 1c.3. El caso de uso termina.
- 2a. La validación de los archivos de las partes de configuración falló.
  - 2a.1. El sistema registra el mensaje de error “No se pudo generar una configuración global válida: X”, donde “X” es el mensaje de error específico del validador de XML Schema.
  - 2a.2. El sistema muestra el mensaje de error “Generación de configuración global fallando desde 'X'”, donde “X” es la fecha y hora desde la cual el sistema no ha podido generar una configuración global distribuible.
  - 2a.3. El caso de uso termina.
- 3-5a. La construcción o firma de los directorios de configuración falló.
  - 3-5a.1. El sistema registra el mensaje de error “No se pudo generar la configuración global: X”, donde “X” es la descripción del error que ocurrió.
  - 3-5a.3. El caso de uso termina.

---

### 2.2.19 UC GCONF\_19: Manejar una Solicitud de Descarga de Configuración

**Sistema:** Servidor central

**Nivel:** Tarea del sistema

**Componente:** Servidor central, servidor de seguridad, proxy de configuración

**Actor:** Cliente de configuración

**Breve descripción:** El sistema recibe una solicitud de descarga de configuración de un cliente de configuración y responde.

---



**Precondiciones:** El directorio de configuración firmado y los archivos de las partes de configuración han sido puestos a disposición para su descarga.

**Postcondiciones:** El cliente de configuración ha recibido el ítem de configuración solicitado (directorio de configuración firmado o un archivo de parte de configuración) o un mensaje de error.

**Desencadenante:** Solicitud de descarga de un cliente de configuración.

**Escenario de éxito principal:**

- El cliente de configuración solicita descargar el directorio de configuración firmado o un archivo de parte de configuración.
- El sistema responde con los archivos solicitados.

**Extensiones:**

- 2a. No se puede atender la solicitud.
  - 2a1. El sistema responde con un mensaje de error.

---

## 2.3 Casos de Uso del Servidor de Seguridad

### 2.3.1 UC GCONF\_20: Ver la Información del Ancla de Configuración

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actor:** Administrador del SS (Servidor de Seguridad)

**Breve descripción:** El administrador del SS ve la información relacionada con el ancla de configuración utilizada por el sistema para descargar la configuración global.

**Precondiciones:** Un ancla de configuración está guardada en la configuración del sistema (ver 2.3.3).

**Postcondiciones:** La información del ancla de configuración es mostrada al administrador del SS.

**Desencadenante:** El administrador del SS desea ver la información del ancla de configuración, por ejemplo, para verificar que el sistema esté utilizando el ancla más reciente proporcionada por la agencia gubernamental.

**Escenario de éxito principal:**

- El administrador del SS selecciona ver el ancla de configuración.
- El sistema muestra la siguiente información:
  - El valor de hash SHA-224 del ancla de configuración.
  - La fecha y hora de generación (UTC) del ancla de configuración.
  - Las siguientes opciones de acción del usuario son mostradas:
    - Descargar el archivo del ancla de configuración: 2.3.2
    - Subir un archivo de ancla de configuración: 2.3.3

### 2.3.2 UC GCONF\_21: Descargar el Archivo del Ancla de Configuración

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actor:** Administrador del SS

**Breve descripción:** El administrador del SS descarga el archivo del ancla de configuración utilizado por el sistema para descargar la configuración.

**Precondiciones:** Un ancla de configuración está guardada en la configuración del sistema.

**Postcondiciones:** El archivo del ancla de configuración utilizado por el sistema ha sido descargado por el administrador del SS.

**Desencadenante:** El administrador del SS desea ver el contenido del archivo del ancla de configuración o almacenar el archivo en una ubicación externa.

**Escenario de éxito principal:**

- El administrador del SS selecciona descargar el archivo del ancla de configuración.
  - El sistema presenta el archivo del ancla de configuración para su descarga.
  - El administrador del SS guarda el archivo del ancla en el sistema de archivos local.
- 

### 2.3.3 UC GCONF\_22: Subir un Archivo de Ancla de Configuración

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actor:** Administrador del SS

**Breve descripción:** El administrador del SS sube el archivo del ancla de configuración al sistema. El sistema muestra los detalles del ancla y solicita que el administrador del SS confirme la subida. Tras la confirmación, el sistema verifica que la configuración descargada de la fuente indicada por este ancla sea utilizable y comienza a usar el ancla subida.

**Precondiciones:** El administrador del SS ha recibido un archivo de ancla de configuración del proveedor interno de configuración y ha validado la integridad del ancla.

**Postcondiciones:** -

**Desencadenante:** El ancla de configuración necesita ser subida,

- en la inicialización del sistema o
- cuando la agencia gobernante de X-Road haya notificado al administrador del SS que el ancla de configuración necesita ser actualizada.

**Escenario de éxito principal:**

- El administrador del SS selecciona subir un archivo de ancla de configuración.
  - El administrador del SS inserta la ruta al archivo del ancla en el sistema de archivos local.
-

- El sistema verifica que el archivo es un archivo de ancla de configuración válido validando el archivo subido contra el esquema de ancla de configuración.
- El sistema verifica que el identificador de instancia en el archivo del ancla corresponde al identificador de instancia del servidor de seguridad.
- El sistema calcula y muestra el valor de hash SHA-224 y la hora de generación del archivo del ancla seleccionado y solicita la confirmación.
- El administrador del SS confirma.
- El sistema verifica que el archivo del ancla es funcional descargando la configuración de la fuente indicada por el ancla: 2.3.4.
- El sistema guarda el ancla de configuración (sobrescribiendo el ancla existente si existe).
- El sistema registra el evento "Subir ancla de configuración" en el registro de auditoría.

**Extensiones:**

- 3a. El archivo seleccionado no es un archivo de ancla de configuración válido.
  - 3a.1. El sistema muestra el mensaje de error: "Fallo en la importación del ancla de configuración: archivo de ancla inválido".
  - 3a.2. El administrador del SS selecciona volver a insertar la ruta del archivo del ancla de configuración. El caso de uso continúa desde el paso 3.
  - 3a.2a. El administrador del SS selecciona terminar el caso de uso.
- 4a. El identificador de instancia en el archivo del ancla no corresponde al identificador de instancia del servidor de seguridad.
  - 4a.1. El sistema muestra el mensaje de error: "Fallo en la subida del ancla de configuración: identificador de instancia inesperado encontrado en el ancla".
  - 4a.2. El sistema registra el evento "Fallo en la subida del ancla de configuración" en el registro de auditoría.
  - 4a.3. El administrador del SS selecciona volver a insertar la ruta del archivo del ancla de configuración. El caso de uso continúa desde el paso 3.
  - 4a.3a. El administrador del SS selecciona terminar el caso de uso.
- 6a. El administrador del SS cancela la importación.
  - 6a.2. El caso de uso termina.
- 7a. La descarga de la configuración interna falla.
  - 7a.1. El sistema muestra el mensaje de error: "No se puede alcanzar la fuente de configuración, revise la URL de la fuente en el archivo del ancla subido".
  - 7a.2. El sistema registra el evento "Fallo en la subida del ancla de configuración" en el registro de auditoría.
  - 7a.3. El administrador del SS selecciona volver a insertar la ruta del archivo del ancla de configuración. El caso de uso continúa desde el paso 3.
  - 7a.3a. El administrador del SS selecciona terminar el caso de uso.
- 7b. La configuración interna descargada está caducada.
  - 7b.1. El sistema muestra el mensaje de error: "La configuración de la fuente está desactualizada".
  - 7b.2. El sistema registra el evento "Fallo en la subida del ancla de configuración" en el registro de auditoría.

- 7b.3. El administrador del SS selecciona volver a insertar la ruta del archivo del ancla de configuración. El caso de uso continúa desde el paso 3.
  - 7b.3a. El administrador del SS selecciona terminar el caso de uso.
- 7c. La verificación del valor de la firma de la configuración interna descargada falló.
  - 7c.1. El sistema muestra el mensaje de error: “No se puede verificar la firma de la configuración”.
  - 7c.2. El sistema registra el evento "Fallo en la subida del ancla de configuración" en el registro de auditoría.
  - 7c.3. El administrador del SS selecciona volver a insertar la ruta del archivo del ancla de configuración. El caso de uso continúa desde el paso 3.
  - 7c.3a. El administrador del SS selecciona terminar el caso de uso.
- 7d. El directorio de configuración interna descargado no contiene parámetros privados.
  - 7d.1. El sistema muestra el mensaje de error: “Fallo en la importación del ancla de configuración: archivo de ancla inválido”.
  - 7d.2. El sistema registra el evento "Fallo en la subida del ancla de configuración" en el registro de auditoría.
  - 7d.3. El administrador del SS selecciona volver a insertar la ruta del archivo del ancla de configuración. El caso de uso continúa desde el paso 3.
  - 7d.3a. El administrador del SS selecciona terminar el caso de uso.
- 7e. La verificación de la configuración interna descargada falla por razones distintas a las enumeradas en las extensiones 7b-d.
  - 7e.1. El sistema muestra el mensaje de error: “La configuración de la fuente falló la verificación”.
  - 7e.2. El sistema registra el evento "Fallo en la subida del ancla de configuración" en el registro de auditoría.
  - 7e.3. El administrador del SS selecciona volver a insertar la ruta del archivo del ancla de configuración. El caso de uso continúa desde el paso 3.
  - 7e.3a. El administrador del SS selecciona terminar el caso de uso.

---

### 2.3.4 UC GCONF\_23: Actualizar Configuración

**Sistema:** Servidor de seguridad

**Nivel:** Tarea del sistema

**Componente:** Servidor de seguridad

**Actor:** -

**Descripción breve:** El sistema actualiza la configuración descargando la configuración global de cada fuente de configuración conocida y actualiza los estados de los objetos de configuración del sistema según la información encontrada en los archivos de configuración descargados.

**Precondiciones:** El ancla de configuración está guardada en la configuración del sistema.

**Postcondiciones:** -

**Disparadores:**

Paso 7 de 2.3.3.

Temporizador definido por el parámetro del sistema del servidor de seguridad configuration-client.update-interval.

**Escenario principal de éxito:**

1. El sistema descarga la configuración interna: 2.3.5.
2. El sistema encuentra anclas de configuración que apuntan a fuentes externas de configuración desde la parte de parámetros privados de la configuración interna y descarga la configuración de cada fuente señalada por las anclas: 2.3.5.
3. El sistema verifica que los valores de estado de uno o más objetos de configuración del sistema (es decir, certificados de autenticación, clientes del servidor de seguridad) necesitan ser actualizados y actualiza los valores.

**Extensiones:**

1a. La descarga de configuración interna termina con un error.

1a.1. El caso de uso termina.

2a. El sistema no encontró anclas de configuración que apunten a fuentes externas de configuración desde la parte de parámetros privados (es decir, la instancia de X-Road no está actualmente federada con ninguna otra instancia de X-Road).

2a.1. El caso de uso continúa desde el paso 3.

2b. La descarga de configuración desde una o más fuentes externas de configuración terminó con un error.

2b.1. El caso de uso continúa desde el paso 3.

---

### 2.3.5 UC GCONF\_24: Descargar Configuración desde una Fuente de Configuración

**Sistema:** Servidor de seguridad, servidor central, proxy de configuración

**Nivel:** Subfunción

**Componente:** Servidor de seguridad, servidor central, proxy de configuración

**Actor:** Fuente de configuración

**Descripción breve:** El sistema descarga el directorio de configuración que describe la configuración proporcionada por la fuente de configuración y verifica la integridad del directorio. El sistema actualiza los archivos de configuración almacenados en el sistema para que coincidan con la lista de partes de configuración descrita en el directorio de configuración, descargando la última versión de los archivos (o eliminando los archivos obsoletos o faltantes).

**Precondiciones:** -

**Postcondiciones:** -

**Disparadores:** Pasos 1 y 2 de 2.3.4.

**Escenario principal de éxito:**

1. El sistema encuentra las direcciones de las fuentes de configuración desde el ancla de configuración.
2. El sistema descarga el directorio de configuración firmado haciendo una solicitud HTTP GET a la dirección de la fuente de configuración encontrada en el ancla de configuración que atendió con éxito la última solicitud de descarga de configuración.
3. El sistema guarda la información sobre la fuente de configuración que atendió con éxito la solicitud de descarga de configuración.
4. El sistema analiza el directorio de configuración descargado y verifica que el directorio de configuración esté firmado y no haya expirado (compara el valor del encabezado Expire-date del directorio de configuración con la fecha actual).
5. El sistema verifica la firma del directorio de configuración: 2.3.6.
6. El sistema maneja cada parte de configuración encontrada en el directorio de configuración: 2.3.7.
7. El sistema verifica que se haya descargado uno o más archivos de configuración y guarda los archivos, reemplazando los archivos existentes (si los hubiera).
8. El sistema guarda la fecha de vencimiento de los archivos de configuración descargados.
9. El sistema verifica que cada archivo de configuración guardado en la configuración del sistema, que proviene de la fuente de configuración utilizada, esté descrito en el directorio de configuración.

**Extensiones:**

1a. El sistema no puede encontrar el ancla de configuración.

1a.1. El sistema registra el mensaje de error: “No se puede descargar la configuración, el archivo de ancla X no existe”, donde “X” es el nombre del archivo de ancla.

2a. La descarga desde la última dirección de fuente de configuración exitosa falla.

2a.1. El sistema descarga el directorio de configuración firmado haciendo una solicitud HTTP GET a una dirección de descarga de configuración aleatoria encontrada en el ancla de configuración, excluyendo la(s) dirección(es) desde donde falló la descarga de configuración.

2a.1a. La descarga de la configuración falló. El caso de uso continúa desde el paso 2a.

2a.1b. La descarga falló desde todas las direcciones de fuentes de configuración listadas en el ancla de configuración.

2a.1a.1. El sistema registra el mensaje de error: “No se pudo descargar la configuración desde ninguna ubicación de configuración: X” (donde “X” es la lista de direcciones de fuentes de configuración que se intentaron). El caso de uso termina.

2a.2. El caso de uso continúa desde el paso 3.

4a. El análisis del directorio de configuración resultó en un error (por ejemplo, se encontró que el valor del encabezado MIME Content-transfer-encoding no era “base64”).

4a.1. El sistema registra el mensaje de error. El caso de uso termina.

4b. El directorio de configuración no tiene el encabezado Expire-date.

4b.1. El sistema registra el mensaje de error: “La instancia de configuración X carece de la fecha de expiración de los datos firmados” (donde “X” es el identificador de la instancia de configuración). El caso de uso termina.

4c. La configuración descargada no está firmada.

4c.1. El sistema registra el mensaje de error: “La instancia de configuración X carece de datos firmados” (donde “X” es el identificador de la instancia de configuración). El caso de uso termina.

4d. La configuración descargada ha expirado.

4d.1. El sistema registra el mensaje de error: “La instancia de configuración X expiró en Y” (donde “X” es el identificador de la instancia de configuración y “Y” es la fecha y hora de expiración del directorio de configuración descargado). El caso de uso termina.

5a. El proceso de verificación de la firma terminó con un error.

5a.1. El caso de uso termina.

6a. La descarga de un archivo de parte de configuración terminó con un error.

6a.1. El caso de uso termina.

7a. El sistema encuentra un error al guardar los archivos descargados.

7a.1. El sistema registra el mensaje de error: “No se pudo sincronizar la lista de archivos descargados” y restaura el estado anterior del conjunto de archivos de configuración. El caso de uso termina.

8b. No se descargaron archivos de configuración.

8b.1. El caso de uso continúa desde el paso 9.



9a. El sistema encuentra uno o más archivos de configuración que provienen de la fuente de configuración utilizada pero que no están descritos en la fuente de configuración.

9a.1. El sistema elimina los archivos de configuración.

---

### 2.3.6 UC GCONF\_25: Verificar la Firma del Directorio de Configuración

**Sistema:** Servidor de seguridad

**Nivel:** Subfunción

**Componente:** Servidor de seguridad

**Actor:** -

**Descripción breve:** El sistema verifica la firma del directorio de configuración utilizando el ancla de la fuente de configuración.

**Precondiciones:** -

**Postcondiciones:** -

**Disparador:** Paso 4 de 2.3.5.

**Escenario principal de éxito:**

1. El sistema encuentra el algoritmo de firma del directorio de configuración (valor del encabezado MIME Signature-algorithm-id) y el valor de hash del certificado de verificación (valor del encabezado MIME Verification-certificate-hash) de la parte de firma del directorio de configuración descargado.
2. El sistema utiliza el valor de hash encontrado para encontrar el certificado de verificación correspondiente en el ancla de la fuente de configuración.
3. El sistema verifica el valor de la firma del directorio de configuración utilizando el algoritmo de firma y el certificado de verificación de la firma.

**Extensiones:**

2a. El sistema no puede encontrar el certificado de verificación necesario para verificar la firma.

2a.1. El sistema registra el mensaje de error: “No se puede verificar la firma de la instancia de configuración X: no se pudo encontrar el certificado de verificación para el hash del certificado Y” (donde “X” es el identificador de la instancia de configuración y “Y” es el valor de hash del certificado de verificación que se utilizó para firmar el directorio de configuración). El caso de uso termina.

3a. La verificación de la firma falla.

3a.1. El sistema registra el mensaje de error: “No se pudo verificar la firma de la instancia de configuración X” (donde “X” es el identificador de la instancia del directorio de configuración). El caso de uso termina.

### 2.3.7 UC GCONF\_26: Manejar una Parte de Configuración del Directorio de Configuración

**Sistema:** Servidor de seguridad, servidor central, proxy de configuración

**Nivel:** Subfunción

**Componente:** Servidor de seguridad, servidor central, proxy de configuración

**Actor:** Fuente de configuración

**Descripción breve:** El sistema verifica si el archivo de configuración descrito en la parte del directorio de configuración está ausente del sistema o difiere del archivo almacenado en el sistema. Si el archivo falta o necesita ser actualizado, el sistema descarga el archivo desde la fuente de configuración y verifica la integridad del archivo descargado.

**Precondiciones:** -

**Postcondiciones:** El sistema ha verificado que el archivo de configuración correspondiente a la parte del directorio de configuración está actualizado o ha descargado la última versión del archivo desde la fuente de configuración.

**Disparador:** Paso 5 de 2.3.5.

**Escenario principal de éxito:**

1. El sistema encuentra un archivo de configuración almacenado en el sistema que corresponde al nombre del archivo parte del valor del encabezado MIME Content-location de la parte de configuración. El sistema calcula el valor de hash del archivo encontrado utilizando el algoritmo de hash indicado en el encabezado MIME Hash-algorithm-id de la parte de configuración.
2. El sistema verifica que el valor de hash dado como contenido de la parte de configuración sea diferente del valor de hash calculado para el archivo de configuración almacenado en el sistema.
3. El sistema descarga el archivo de configuración desde la URL proporcionada por el encabezado MIME Content-location en la parte de configuración.
4. El sistema calcula el valor de hash del archivo descargado utilizando el algoritmo definido por el encabezado MIME Hash-algorithm-id y verifica que el valor de hash del archivo descargado coincida con el valor de hash en la parte de configuración.
5. En caso de que el valor del encabezado MIME Content-identifier de la parte de configuración descargada sea PRIVATE-PARAMETERS o SHARED-PARAMETERS, el sistema verifica que el identificador de la instancia indicado

en el archivo descargado coincida con el valor del parámetro de instancia del encabezado MIME Content-identifier.

**Extensiones:**

1a. El sistema no puede encontrar un archivo almacenado correspondiente a la parte de configuración.

1a.1. El caso de uso continúa desde el paso 3.

2a. Los valores de hash son iguales.

2a.1. El caso de uso termina.

3a. La descarga del archivo falló.

3a.1. El sistema registra el mensaje de error que describe la razón de la falla. El caso de uso termina.

4a. Los valores de hash difieren.

4a.1. El sistema registra el mensaje de error: “No se pudo verificar la integridad del contenido X” (donde “X” es el valor del encabezado MIME Content-identifier o Content-location de la parte de configuración). El caso de uso termina.

5a. El valor de Content-identifier no es ni PRIVATE-PARAMETERS ni SHARED-PARAMETERS.

5a.1. El caso de uso termina.

5b. El valor del identificador de instancia en el archivo de configuración descargado difiere del valor del parámetro de instancia del encabezado MIME Content-identifier.

5b.1. El sistema registra el mensaje de error: “La parte de contenido X tiene un identificador de instancia no válido (se esperaba Y, pero fue Z)” (donde “X” es el valor del encabezado MIME Content-identifier o Content-location de la parte de configuración; “Y” es el valor del parámetro de instancia; y “Z” es el valor del identificador de instancia en el archivo de configuración descargado). El caso de uso termina.