

# **Casos de Uso Federation**

# Índice

Índice .....	2
Introducción .....	3
Propósito .....	3
Descripción general .....	3
Modelo de casos de uso .....	4
Actores .....	4
UC FED_01: Ver Anclas Confiables .....	5
UC FED_02: Cargar un Ancla Confiable .....	5
UC FED_03: Descargar y Validar la Configuración .....	8
UC FED_04: Verificar la Firma del Directorio de Configuración .....	9
UC FED_05: Descargar un Archivo de Parte de Configuración .....	10
<b>Sistema:</b> Servidor central .....	10
UC FED_06: Descargar un Ancla de Confianza .....	11
UC FED_07: Eliminar un Ancla de Confianza .....	12

# Introducción

## Propósito

El propósito de este documento es describir los casos de uso relacionados con la federación de instancias X-Road.

Los casos de uso incluyen las verificaciones que se realizan y las principales condiciones de error que pueden encontrarse 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 memoria insuficiente) no se describen en este documento.

Los casos de uso suponen que los componentes del software X-Road involucrados están instalados e inicializados.

Los casos de uso que incluyen un actor humano (el nivel del caso de uso es tarea de usuario) suponen que el actor ha iniciado sesión en el sistema y tiene los derechos de acceso necesarios para llevar a cabo el caso de uso.

## Descripción general

La federación de confianza de las instancias X-Road permite que los miembros de una instancia X-Road utilicen los servicios proporcionados por los miembros de otra instancia, lo que hace que los sistemas X-Road sean interoperables.

Para que los sistemas federados se reconozcan entre sí, el ancla de configuración externa del socio de la federación debe cargarse como un ancla confiable en los servidores centrales de las instancias X-Road federadas.

Las anclas confiables se distribuyen a los servidores de seguridad como parte de la configuración interna. Los servidores de seguridad utilizan las anclas confiables para descargar la configuración externa de los socios de la federación. La configuración externa contiene la información que los servidores de seguridad de los socios de la federación necesitan para comunicarse entre sí.

Para finalizar una relación de federación con una instancia X-Road, se debe eliminar el ancla confiable de esa instancia del servidor central.

Para más información sobre la distribución de configuraciones, consulte los documentos "X-Road: Protocolo para Descargar Configuración" y "X-Road: Modelo de Casos de Uso para la Distribución de Configuración Global".

# Modelo de casos de uso

## Actores

El modelo de casos de uso para la federación de sistemas X-Road incluye los siguientes actores:

- **Administrador de CS** (Administrador del servidor central) – una 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 externa.

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

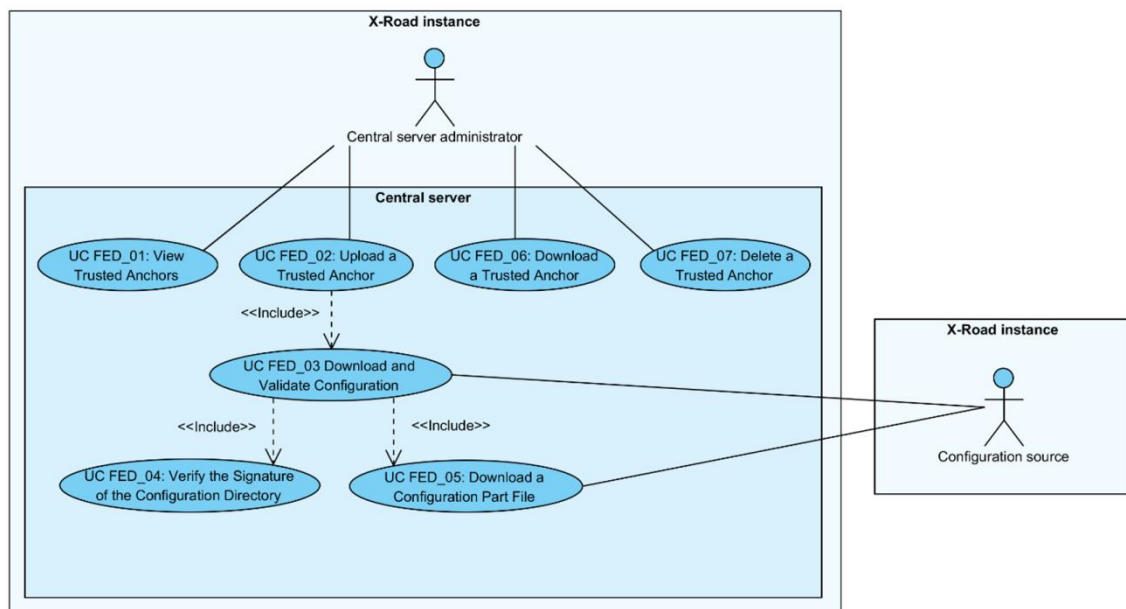


Figura 1. Diagrama de casos de uso para la federación de sistemas X-Road.

## UC FED\_01: Ver Anclas Confiables

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS

**Descripción breve:** El administrador de CS visualiza la lista de anclas confiables.

**Precondiciones:** -

**Postcondiciones:** Se ha mostrado la lista de anclas confiables al administrador de CS.

**Desencadenante:** -

**Escenario de éxito principal:**

1. El administrador de CS selecciona ver las anclas confiables.
2. El sistema muestra la lista de anclas confiables cargadas en el servidor central.  
Para cada ancla, se muestra la siguiente información:
  - El identificador de instancia de la instancia X-Road de la que proviene el ancla confiable.
  - El valor hash SHA-224 del archivo del ancla confiable.
  - La fecha y hora de generación (UTC) del archivo del ancla confiable.
3. Se muestran las siguientes opciones de acción del usuario:
  - Cargar un ancla confiable: 3.3;
  - Descargar un ancla confiable: 3.7;
  - Eliminar un ancla confiable: 3.8.

---

## UC FED\_02: Cargar un Ancla Confiable

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS

**Descripción breve:** El administrador de CS carga un ancla confiable al sistema. El sistema valida el archivo del ancla y descarga la configuración desde la fuente indicada por el ancla para verificar que la fuente funcione. El sistema incluye el ancla cargada en la lista de fuentes de configuración distribuidas a los servidores de seguridad de esta instancia X-Road a través de la configuración global.

**Precondiciones:** El administrador de CS ha recibido un archivo de ancla de configuración externa de un socio de federación y ha validado la integridad del ancla.

**Postcondiciones:** -

**Desencadenante:** El administrador de CS recibe un archivo de ancla de configuración externa de un socio de federación. El archivo de ancla externa debe distribuirse (por medios ajenos al canal normal) a los socios de federación cuando se configura la federación por primera vez o cuando se actualizan los contenidos del ancla de configuración externa (por ejemplo, debido a cambios en las claves de firma de configuración externa, cambios en la dirección del servidor central, cambios en la configuración de alta disponibilidad del servidor central).

**Escenario de éxito principal:**

1. El administrador de CS selecciona cargar un ancla confiable.
2. El administrador de CS selecciona el archivo del ancla desde el sistema de archivos local.
3. El sistema verifica que el archivo seleccionado es un archivo válido de ancla de configuración validando el archivo cargado contra el esquema de ancla de configuración.
4. El sistema verifica que el ancla de configuración no apunte a una fuente de configuración de esta instancia X-Road.
5. El sistema calcula y muestra el valor hash SHA-224 y la hora de generación del archivo del ancla seleccionado y solicita confirmación.
6. El administrador de CS confirma.
7. El sistema descarga la configuración firmada desde la fuente definida por el ancla cargada y valida la configuración: 3.4.
8. El sistema verifica que no exista un ancla con el mismo identificador de instancia que el cargado en la configuración del sistema y reemplaza el ancla existente con el cargado.
9. El sistema registra el evento "Agregar ancla confiable" en el registro de auditoría.

**Extensiones:**

- 3a.** El archivo seleccionado no es un archivo válido de ancla de configuración.
- 3a.1.** El sistema muestra el mensaje de error: "No se pudo cargar el ancla confiable: Estructura de archivo incorrecta."
- 3a.2.** El administrador de CS selecciona volver a seleccionar el archivo del ancla de configuración. El caso de uso continúa desde el paso 3.
- 3a.2a.** El administrador de CS selecciona terminar el caso de uso.
- 4a.** El ancla apunta a una fuente de configuración de la instancia local X-Road.
- 4a.1.** El sistema muestra el mensaje de error: "No se pudo cargar el ancla confiable: No se admiten anclas originarias de esta instancia como anclas confiables."
- 4a.2.** El administrador de CS selecciona volver a seleccionar el archivo del ancla de configuración. El caso de uso continúa desde el paso 3.
- 4a.2a.** El administrador de CS selecciona terminar el caso de uso.
- 6a.** El administrador de CS selecciona terminar el caso de uso.

**7a.** La descarga de la configuración falla.

**7a.1.** El sistema muestra el mensaje de error: “No se pudo guardar el ancla confiable cargada: No se puede acceder a la fuente de configuración, verifique la URL de la fuente en el archivo del ancla cargado.”

**7a.2.** El sistema registra el evento “Agregar ancla confiable fallida” en el registro de auditoría.

**7a.3.** El caso de uso termina.

**7b.** La configuración descargada está caducada.

**7b.1.** El sistema muestra el mensaje de error: “No se pudo guardar el ancla confiable cargada: La configuración de la fuente está desactualizada.”

**7b.2.** El sistema registra el evento “Agregar ancla confiable fallida” en el registro de auditoría.

**7b.3.** El caso de uso termina.

**7c.** La verificación del valor de la firma de la configuración descargada falló.

**7c.1.** El sistema muestra el mensaje de error: “No se pudo guardar el ancla confiable cargada: No se puede verificar la firma de la configuración.”

**7c.2.** El sistema registra el evento “Agregar ancla confiable fallida” en el registro de auditoría.

**7c.3.** El caso de uso termina.

**7d.** El directorio de configuración descargado contiene parámetros privados (es decir, el ancla de configuración apunta a una fuente de configuración interna).

**7d.1.** El sistema muestra el mensaje de error: “No se pudo cargar el ancla confiable: El ancla apunta a una fuente de configuración interna. Solo se admiten anclas de fuentes de configuración externas.”

**7d.2.** El sistema registra el evento “Agregar ancla confiable fallida” en el registro de auditoría.

**7d.3.** El caso de uso termina.

**7e.** La verificación de la configuración descargada falla por razones distintas a las listadas en las extensiones 7b-7d.

**7e.1.** El sistema muestra el mensaje de error: “No se pudo guardar el ancla confiable cargada: La configuración de la fuente no pasó la verificación.”

**7e.2.** El sistema registra el evento “Agregar ancla confiable fallida” en el registro de auditoría.

**7e.3.** El caso de uso termina.

**8a.** No existe un ancla con el mismo identificador de instancia que el cargado en la configuración del sistema.

**8a.1.** El sistema guarda el ancla cargada en la configuración del sistema.

---

## UC FED\_03: Descargar y Validar la Configuración

**Sistema:** Servidor central

**Nivel:** Subfunción

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

**Actor:** Fuente de configuración

**Breve descripción:** 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 descarga los archivos de configuración descritos en el directorio de configuración.

**Precondiciones:** -

**Postcondiciones:** -

**Disparador:** Paso 7 de 3.3.

**Escenario principal de éxito:**

- El sistema encuentra las direcciones de las fuentes de configuración en el ancla de configuración.
- El sistema descarga el directorio de configuración firmado haciendo una solicitud HTTP GET a una dirección de fuente de configuración seleccionada aleatoriamente que se encuentra en el ancla de configuración.
- El sistema analiza el directorio de configuración descargado y verifica que el directorio esté firmado y no haya caducado (compara el valor del encabezado Expire-date del directorio de configuración con la fecha actual).
- El sistema verifica la firma del directorio de configuración: 3.5.
- El sistema descarga los archivos de las partes de configuración encontrados en el directorio de configuración: 3.6.

**Extensiones:**

2a. La descarga desde una dirección de fuente de configuración falla.

2a.1. El sistema descarga el directorio de configuración firmado haciendo una solicitud HTTP GET a la siguiente dirección de fuente de configuración seleccionada aleatoriamente encontrada en el ancla de configuración.

2a.1a. 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: "Error al descargar la configuración desde cualquier 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.



3a. El análisis del directorio de configuración resultó en un error (por ejemplo, el valor del encabezado MIME Content-transfer-encoding no es "base64").

3a.1. El sistema registra el mensaje de error. El caso de uso termina.

3b. El directorio de configuración no tiene el encabezado Expire-date.

3b.1. El sistema registra el mensaje de error: "La instancia de configuración X no tiene la fecha de expiración de los datos firmados" (donde "X" es el identificador de instancia de la configuración). El caso de uso termina.

3c. La configuración descargada no está firmada. El sistema registra el mensaje de error: "La instancia de configuración X no tiene datos firmados" (donde "X" es el identificador de instancia de la configuración). El caso de uso termina.

3d. La configuración descargada está caducada.

3d.1. El sistema registra el mensaje de error: "La instancia de configuración X expiró en Y" (donde "X" es el identificador de instancia de la configuración y "Y" es la fecha y hora de expiración del directorio de configuración descargado). El caso de uso termina.

4a. El proceso de verificación de la firma terminó con un error.

4a.1. El caso de uso termina.

5a. La descarga de una parte de configuración terminó con un error.

5a.1. El caso de uso termina.

---

## UC FED\_04: Verificar la Firma del Directorio de Configuración

**Sistema:** Servidor central

**Nivel:** Subfunción

**Componente:** Servidor central

**Actor:** -

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

**Precondiciones:** -

**Postcondiciones:** -

**Disparador:** Paso 4 de 3.4.

**Escenario principal de éxito:**

- El sistema encuentra el algoritmo de firma de la configuración (valor del encabezado MIME Signature-algorithm-id) y el valor hash del certificado de verificación (valor del encabezado MIME Verification-certificate-hash) de la parte de firma del directorio de configuración descargado.
- El sistema utiliza el valor hash encontrado para localizar el certificado de verificación correspondiente desde el ancla de la fuente de configuración.
- El sistema verifica el valor de la firma de la 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 de certificado Y” (donde “X” es el identificador de la instancia de configuración y “Y” es el valor hash del certificado de verificación utilizado 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: “Error al verificar la firma de la instancia de configuración X” (donde “X” es el identificador del directorio de configuración). El caso de uso termina.

---

## UC FED\_05: Descargar un Archivo de Parte de Configuración

**Sistema:** Servidor central

**Nivel:** Subfunción

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

**Actor:** Fuente de configuración

**Breve descripción:** El sistema descarga un archivo de parte de configuración de la fuente de configuración y verifica la integridad del archivo descargado.

**Precondiciones:** -

**Postcondiciones:** -

**Disparador:** Paso 5 de 3.4.

**Escenario principal de éxito:**

- El sistema descarga el archivo de configuración desde la URL proporcionada por el encabezado MIME Content-location en la parte de configuración del directorio de configuración.
- El sistema calcula el valor hash del archivo descargado utilizando el algoritmo definido por el encabezado MIME Hash-algorithm-id y verifica que el valor hash del archivo descargado coincida con el valor hash en la parte de configuración.
- El sistema verifica que el identificador de la instancia declarado en el archivo de configuración descargado coincida con el valor del parámetro de instancia del encabezado MIME Content-identifier del directorio de configuración.

**Extensiones:**

1a. La descarga del archivo falló.

1a.1. El sistema registra el mensaje de error describiendo el motivo del fallo. El caso de uso termina.

2a. Los valores hash difieren.

2a.1. El sistema registra el mensaje de error: "Error al 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.

3a. El valor del identificador de la instancia en el archivo de configuración descargado difiere del valor del parámetro de instancia del encabezado MIME Content-identifier.

3a.1. El sistema registra el mensaje de error: "La parte de contenido X tiene un identificador de instancia no válido (se esperaba Y, pero se encontró 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.

---

## UC FED\_06: Descargar un Ancla de Confianza

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS

**Breve descripción:** El administrador de CS descarga un ancla de confianza.

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

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

**Disparador:** El administrador de CS desea ver el contenido del archivo de ancla de configuración o almacenarlo en una ubicación externa.

**Escenario principal de éxito:**

- El administrador de CS selecciona descargar el archivo de ancla de confianza.
- El sistema presenta el archivo de ancla para su descarga.
- El administrador de CS guarda el archivo de ancla en el sistema de archivos local.

---

## UC FED\_07: Eliminar un Ancla de Confianza

**Sistema:** Servidor central

**Nivel:** Tarea de usuario

**Componente:** Servidor central

**Actor:** Administrador de CS

**Breve descripción:** El administrador de CS elimina un ancla de confianza. El ancla es eliminada de la lista de fuentes de configuración distribuidas a los servidores de seguridad de esta instancia de X-Road a través de la configuración global.

**Precondiciones:** Un ancla de confianza ha sido cargada en el sistema.

**Postcondiciones**

: -

**Disparador:** Se termina una relación de federación.

**Escenario principal de éxito:**

- El administrador de CS selecciona eliminar un ancla de confianza.
- El sistema solicita confirmación.
- El administrador de CS confirma la eliminación.
- El sistema elimina el ancla de configuración seleccionada y muestra el mensaje “Ancla de configuración de la instancia 'X' eliminada con éxito”, donde “X” es el identificador de instancia de X-Road de donde provino el ancla eliminada.
- El sistema registra el evento “Eliminar ancla de confianza” en el registro de auditoría.

**Extensiones:**

3a. El administrador de CS selecciona terminar el caso de uso.