

# **Casos de Uso Security Server Management**

# Índice

Índice .....	2
Propósito .....	4
Visión General .....	4
Modelo de Casos de Uso .....	5
Actores.....	5
UC SS_01: Iniciar sesión en la Interfaz Gráfica de Usuario .....	6
UC SS_02: Cerrar sesión en la Interfaz Gráfica de Usuario .....	7
UC SS_03: Cerrar sesión a un usuario en la Interfaz Gráfica de Usuario .....	7
UC SS_04: Cambiar el idioma de la Interfaz Gráfica de Usuario .....	8
UC SS_05: Ver la versión del software instalado.....	9
UC SS_06: Ver los Servicios de Sello de Tiempo.....	9
UC SS_07: Añadir un Servicio de Sello de Tiempo.....	10
UC SS_08: Eliminar un Servicio de Sello de Tiempo.....	11
UC SS_09: Ver los Detalles de un Certificado.....	12
UC SS_10: Ver el Certificado TLS del Servidor de Seguridad .....	12
UC SS_11: Generar una Nueva Clave TLS y Certificado para el Servidor de Seguridad.....	13
UC SS_12: Exportar el Certificado TLS del Servidor de Seguridad .....	14
UC SS_13: Ver la Lista de Archivos de Respaldo de Configuración.....	15
UC SS_14: Resguardar Configuración .....	16
UC SS_15: Restaurar Configuración desde un Archivo de Respaldo .....	17
UC SS_16: Descargar un archivo de respaldo .....	18
UC SS_17: Eliminar un archivo de respaldo.....	19
UC SS_18: Subir un archivo de respaldo .....	20
UC SS_19: Ver la lista de tokens, claves y certificados .....	21
UC SS_20: Ver los detalles de un token.....	23

UC SS_21: Ver los detalles de una clave .....	23
UC SS_22: Editar el Nombre Amigable de un Token .....	24
UC SS_23: Editar el Nombre Amigable de una Clave .....	25
UC SS_24: Iniciar Sesión en un Token de Software .....	26
UC SS_25: Iniciar Sesión en un Token de Hardware.....	26
UC SS_26: Cerrar Sesión en un Token de Software .....	28
UC SS_27: Cerrar sesión de un token de hardware .....	29
UC SS_28: Generar una clave .....	30
UC SS_29: Generar una solicitud de firma de certificado para una clave.....	31
UC SS_30: Importar un Certificado desde el Sistema de Archivos Local.....	32
UC SS_31: Importar un Certificado desde un Token de Seguridad .....	36
UC SS_32: Activar un Certificado.....	37
UC SS_33: Deshabilitar un Certificado.....	37
UC SS_34: Registrar un Certificado de Autenticación .....	38
UC SS_35: Eliminar una clave de la configuración del sistema y de un token.....	39
UC SS_36: Eliminar una clave de un token de software.....	40
UC SS_37: Eliminar una clave de un token de hardware .....	41
UC SS_38: Desregistrar un certificado de autenticación .....	42
UC SS_39: Eliminar un certificado o una notificación de solicitud de firma de certificado de la configuración del sistema .....	43
UC SS_40: Eliminar un certificado de un token de hardware .....	45
UC SS_41: Analizar la Entrada del Usuario.....	46
UC SS_42: Desregistrar un Certificado de Autenticación al Eliminar la Clave .....	47
UC SS_43: Crear una Nueva Clave API.....	48

# Propósito

El propósito de este documento es describir la gestión del servidor de seguridad, incluyendo:

- La gestión de la interfaz gráfica de usuario;
- La gestión de los servicios de sellado de tiempo;
- La gestión del certificado TLS interno del servidor de seguridad;
- La gestión de claves y certificados; y
- La realización de copias de seguridad y la restauración de la configuración del servidor de seguridad.

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 aparecer en la mayoría de los casos de uso (por ejemplo, errores de conexión a la base de datos o errores por falta de memoria) no se describen en este documento.

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

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

# Visión General

Los servicios de sellado de tiempo se utilizan para preservar el valor probatorio de los mensajes intercambiados a través de X-Road. Los servicios de sellado de tiempo utilizados en un servidor de seguridad deben estar aprobados por la agencia de gobierno de X-Road.

Los certificados TLS se utilizan para establecer conexiones TLS con los sistemas de información del cliente del servidor de seguridad si se elige el método de conexión “HTTPS” para los servidores del cliente.

Los certificados de firma se utilizan para firmar mensajes de X-Road. Los certificados de autenticación se emplean para establecer canales seguros de intercambio de datos entre los servidores de seguridad.

Realizar copias de seguridad de la configuración del sistema garantiza que, en caso de fallo del sistema, se pueda restaurar la configuración del sistema a un estado previamente respaldado.

# Modelo de Casos de Uso

## Actores

El modelo de casos de uso para la gestión del servidor de seguridad de X-Road incluye los siguientes actores:

- **Administrador del servidor de seguridad (SS administrator):** una persona responsable de gestionar el servidor de seguridad.
- **Servidor central:** el servidor central de la instancia de X-Road. El servidor central proporciona servicios de gestión para los servidores de seguridad de esta instancia de X-Road. Las solicitudes de eliminación de certificados de autenticación son reenviadas al servidor central por el servidor de seguridad de los servicios de gestión. La solicitud de registro de un certificado de autenticación se envía directamente al servidor central desde el servidor de seguridad para el que se debe registrar el certificado.
- **Servidor de seguridad de los servicios de gestión:** un servidor de seguridad que tiene al proveedor de servicios de gestión para esta instancia de X-Road registrado como cliente del servidor de seguridad.

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

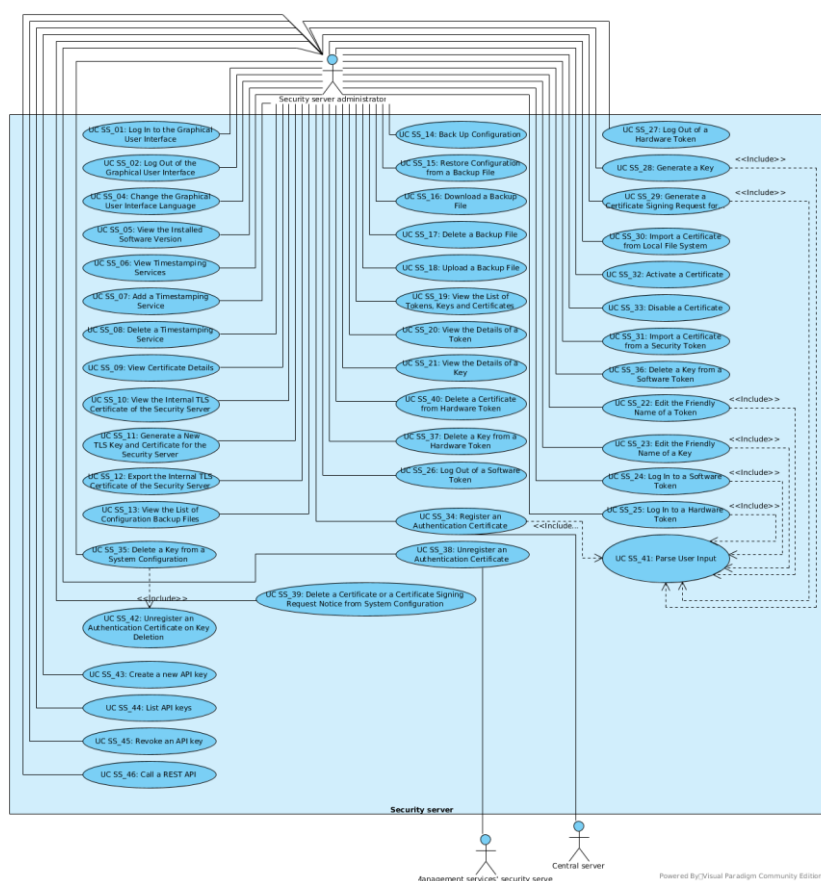


Figura 1. Diagrama de casos de uso para la gestión del servidor de seguridad.

## UC SS\_01: Iniciar sesión en la Interfaz Gráfica de Usuario

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actor:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad inicia sesión en la interfaz gráfica de usuario (GUI) del servidor de seguridad.

**Condiciones previas:** -

**Condiciones posteriores:** Se crea un registro en el log de auditoría para el evento.

**Desencadenante:** El administrador del servidor de seguridad desea iniciar sesión en la GUI para ver o gestionar la configuración del servidor de seguridad.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona iniciar sesión en la GUI.
2. El administrador del servidor de seguridad introduce el nombre de usuario y la contraseña.
3. El sistema verifica que no se esté llevando a cabo actualmente el proceso de restauración del sistema.
4. El sistema verifica que exista un usuario con el nombre de usuario y la contraseña introducidos en la configuración del sistema y permite el acceso del administrador del servidor de seguridad a la GUI.
5. El sistema registra el evento "Iniciar sesión usuario" en el log de auditoría.

**Extensiones:**

- 3a. El sistema está actualmente en proceso de restauración del sistema.
  - 3a.1. El sistema muestra el mensaje de error "Restauración en progreso, intente más tarde".
  - 3a.2. El sistema registra el evento "Cerrar sesión usuario" en el log de auditoría.
  - 3a.3. El administrador del servidor de seguridad selecciona reintroducir el nombre de usuario y/o la contraseña. El caso de uso continúa desde el paso 3.
  - 3a.3a. El administrador del servidor de seguridad selecciona terminar el caso de uso.
- 4a. El usuario con el nombre de usuario introducido no existe o la contraseña es incorrecta.
  - 4a.1. El sistema muestra el mensaje de error "Autenticación fallida. Por favor intente de nuevo". Los campos de texto se vacían.
  - 4a.2. El sistema registra el evento "Fallo en inicio de sesión usuario" en el log de auditoría.

- 4a.3. El administrador del servidor de seguridad selecciona reintroducir el nombre de usuario y/o la contraseña. El caso de uso continúa desde el paso 3.
- 4a.3a. El administrador del servidor de seguridad selecciona terminar el caso de uso.

---

## UC SS\_02: Cerrar sesión en la Interfaz Gráfica de Usuario

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actor:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad cierra sesión en la GUI.

**Condiciones previas:** -

**Condiciones posteriores:**

- El administrador del servidor de seguridad ha cerrado sesión de la GUI.
- Se crea un registro en el log de auditoría para el evento.

**Desencadenante:** El administrador del servidor de seguridad desea cerrar sesión en la GUI.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona cerrar sesión en la GUI (Menú de Perfil > Cerrar sesión).
2. El sistema cierra sesión del administrador del servidor de seguridad en la GUI y lo redirige a la vista de inicio de sesión.
3. El sistema registra el evento "Cerrar sesión usuario" en el log de auditoría.

---

## UC SS\_03: Cerrar sesión a un usuario en la Interfaz Gráfica de Usuario

**Sistema:** Servidor de seguridad

**Nivel:** Tarea del sistema

**Componente:** Servidor de seguridad

---

**Actor:** -

**Descripción breve:** El sistema cierra sesión a un usuario en la GUI cuando el usuario ha estado inactivo durante 30 minutos.

**Condiciones previas:** -

**Condiciones posteriores:** El usuario ha cerrado sesión en la GUI.

**Desencadenante:** El usuario ha estado inactivo durante 30 minutos.

**Escenario de éxito principal:**

1. El usuario ha estado inactivo durante 30 minutos.
2. El sistema muestra el diálogo "Sesión expiró - Has estado inactivo durante 30 minutos y tu sesión ha expirado. Por razones de seguridad, serás desconectado".
3. El sistema cierra sesión al administrador del servidor de seguridad en la GUI y lo redirige a la vista de inicio de sesión.

---

## UC SS\_04: Cambiar el idioma de la Interfaz Gráfica de Usuario

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actor:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad cambia el idioma de la GUI.

**Condiciones previas:** -

**Condiciones posteriores:**

- El idioma de la GUI ha sido cambiado.
- Se crea un registro en el log de auditoría para el evento.

**Desencadenante:** El administrador del servidor de seguridad desea cambiar el idioma de la GUI.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona cambiar el idioma de la GUI.



2. El sistema muestra la lista de idiomas soportados.
3. El administrador del servidor de seguridad selecciona un idioma.
4. El sistema guarda la elección del administrador y muestra la GUI en el idioma seleccionado.
5. El sistema registra el evento "Establecer idioma de la UI" en el log de auditoría.

---

## UC SS\_05: Ver la versión del software instalado

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actor:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad ve la versión del software instalado.

**Condiciones previas:** -

**Condiciones posteriores:** La versión del software ha sido mostrada al administrador del servidor de seguridad.

**Desencadenante:** El administrador del servidor de seguridad desea ver la versión del software instalado.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona ver la versión del software instalado.
2. El sistema muestra la información de la versión.

---

## UC SS\_06: Ver los Servicios de Sello de Tiempo

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad ve la lista de servicios de sello de tiempo configurados para el servidor de seguridad.

**Condiciones previas:** -

**Condiciones posteriores:** La lista de servicios de sello de tiempo utilizados por el servidor de seguridad se ha mostrado al administrador del servidor de seguridad.

**Desencadenante:** El administrador del servidor de seguridad desea ver la lista de servicios de sello de tiempo.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona ver la lista de servicios de sello de tiempo.
2. El sistema muestra la lista de servicios de sello de tiempo. Para cada servicio, se muestra la siguiente información:
  - El nombre del servicio de sello de tiempo.
  - La URL del servicio de sello de tiempo.
3. El administrador del servidor de seguridad tiene la posibilidad de elegir entre las siguientes acciones:
  - Añadir un servicio de sello de tiempo: 3.8.
  - Eliminar un servicio de sello de tiempo: 3.9.

---

## UC SS\_07: Añadir un Servicio de Sello de Tiempo

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad añade un servicio de sello de tiempo para ser utilizado por el servidor de seguridad.

**Condiciones previas:** Uno o más servicios de sello de tiempo han sido aprobados por la agencia gubernamental de X-Road.

**Condiciones posteriores:** Se crea un registro en el log de auditoría para el evento.

**Desencadenante:** El administrador del servidor de seguridad desea añadir un servicio de sello de tiempo para ser utilizado por el servidor de seguridad en los registros de mensajes de log.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona añadir un servicio de sello de tiempo.

2. El administrador del servidor de seguridad selecciona el servicio de sello de tiempo que desea añadir al servidor de seguridad desde la lista de servicios aprobados.
3. El sistema verifica que el servicio de sello de tiempo seleccionado no esté ya configurado para ser utilizado por el sistema.
4. El sistema guarda el servicio de sello de tiempo en la lista de servicios de sello de tiempo que pueden ser utilizados para sellar los registros de mensajes de log.
5. El sistema registra el evento "Añadir servicio de sello de tiempo" en el log de auditoría.

**Extensiones:**

- 3a. El administrador del servidor de seguridad seleccionó un servicio de sello de tiempo que ya existe en el servidor de seguridad.
  - 3a.1. El sistema muestra un mensaje de error "Fallo al añadir el servicio de sello de tiempo: el servicio de sello de tiempo ya existe".
  - 3a.2. El sistema registra el evento "Fallo al añadir servicio de sello de tiempo" en el log de auditoría.
  - 3a.3. El caso de uso termina.

---

## UC SS\_08: Eliminar un Servicio de Sello de Tiempo

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad elimina un servicio de sello de tiempo del servidor de seguridad.

**Condiciones previas:** -

**Condiciones posteriores:**

- El servidor de seguridad ya no podrá utilizar el servicio de sello de tiempo eliminado para sellar los registros de mensajes de log.
- Se crea un registro en el log de auditoría para el evento.

**Desencadenante:** El administrador del servidor de seguridad desea eliminar un servicio de sello de tiempo.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona eliminar un servicio de sello de tiempo.

2. El sistema elimina el servicio de sello de tiempo seleccionado de la lista de servicios de sello de tiempo utilizables.
3. El sistema registra el evento "Eliminar servicio de sello de tiempo" en el log de auditoría.

---

## UC SS\_09: Ver los Detalles de un Certificado

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad ve el contenido de un certificado.

**Condiciones previas:** -

**Condiciones posteriores:** Los detalles del certificado han sido mostrados al administrador del servidor de seguridad.

**Desencadenante:** El administrador del servidor de seguridad desea ver los detalles de un certificado.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona ver los detalles de un certificado.
2. El sistema muestra el contenido y el valor del hash SHA-1 del certificado.

---

## UC SS\_10: Ver el Certificado TLS del Servidor de Seguridad

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad ve la información sobre el certificado TLS del servidor de seguridad.

**Condiciones previas:** -

**Condiciones posteriores:** La información sobre el certificado TLS del servidor de seguridad ha sido mostrada al administrador del servidor de seguridad.

**Desencadenante:** El administrador del servidor de seguridad desea ver la información sobre el certificado TLS del servidor de seguridad.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona ver el certificado TLS del servidor de seguridad.
2. El sistema muestra el valor del hash SHA-1 del certificado TLS del servidor de seguridad. El administrador del servidor de seguridad tiene la posibilidad de elegir entre las siguientes acciones:
  - Generar una nueva clave TLS y certificado para el servidor de seguridad: 3.12.
  - Generar una nueva solicitud de certificado TLS: 3.12.
  - Importar una solicitud de certificado TLS: 3.12.
  - Ver los detalles del certificado TLS del servidor de seguridad: 3.10.
  - Exportar el certificado TLS del servidor de seguridad: 3.13.

---

## UC SS\_11: Generar una Nueva Clave TLS y Certificado para el Servidor de Seguridad

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad genera una nueva clave TLS y el respectivo certificado autofirmado para el servidor de seguridad.

**Condiciones previas:** -

**Condiciones posteriores:** -

**Desencadenante:** El administrador del servidor de seguridad desea cambiar la clave y el certificado utilizados para las conexiones TLS con los sistemas de información cliente.

**Escenario de éxito principal:**

---

1. El administrador del servidor de seguridad selecciona generar una nueva clave TLS.
2. El sistema solicita confirmación.
3. El administrador del servidor de seguridad confirma.
4. El sistema genera y guarda la nueva clave TLS y el respectivo certificado autofirmado, reemplazando la clave y el certificado existentes (si existen) con los nuevos.
5. El sistema calcula el valor del hash SHA-1 del certificado (para mostrarlo en la GUI).
6. El sistema registra el evento “Generar nueva clave y certificado TLS internos” en el log de auditoría.
7. El administrador del servidor de seguridad selecciona generar una nueva solicitud de certificado TLS.
8. El sistema solicita definir un nombre distinguido (Distinguished Name).
9. El administrador del servidor de seguridad inserta un nombre distinguido.
10. El sistema solicita descargar la solicitud de certificado generada.
11. El servidor de seguridad genera una solicitud de certificado utilizando la clave actual y el Nombre Distinguido proporcionado.
12. El administrador del servidor de seguridad descarga y guarda el archivo de solicitud de certificado en el sistema

de archivos local.

13. Después de que una autoridad certificadora haya emitido un certificado TLS, el administrador del servidor de seguridad importa y guarda el archivo de certificado en el sistema de archivos local.

**Extensiones:**

- 3a. El administrador del servidor de seguridad cancela la generación de la nueva clave TLS.
  - 3a.1. El caso de uso termina.
- 4a. El sistema no pudo generar la clave o el certificado autofirmado respectivo.
  - 4a.1. El sistema muestra un mensaje de error “Fallo al generar nueva clave: 'X'” (donde “X” es la razón del fallo). El caso de uso termina.

---

## UC SS\_12: Exportar el Certificado TLS del Servidor de Seguridad

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad exporta el certificado TLS interno del servidor de seguridad al sistema de archivos local.

**Condiciones previas:** Se ha creado un certificado TLS interno.

**Condiciones posteriores:** El certificado TLS interno ha sido exportado.

**Desencadenante:** El administrador del servidor de seguridad desea exportar un certificado TLS interno.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona exportar el certificado TLS interno del servidor de seguridad.
2. El sistema solicita un archivo tar.qz para descargar, que contiene el certificado TLS en formato PEM y CER.
3. El administrador del servidor de seguridad guarda el archivo en el sistema de archivos local.

---

## UC SS\_13: Ver la Lista de Archivos de Respaldo de Configuración

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad ve la lista de archivos de respaldo de configuración guardados en la configuración del sistema.

**Condiciones previas:** -

**Condiciones posteriores:** Se muestra la lista de archivos de respaldo de configuración al administrador del servidor de seguridad.

**Desencadenante:** El administrador del servidor de seguridad desea ver la lista de archivos de respaldo de configuración.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona ver la lista de archivos de respaldo de configuración.
  2. El sistema muestra la lista de archivos de respaldo. Para cada archivo, se muestra la siguiente información:
    - El nombre del archivo de respaldo.
  3. El administrador del servidor de seguridad tiene la posibilidad de elegir entre las siguientes acciones:
    - Resguardar configuración: 3.15;
-

- Subir un archivo de respaldo: 3.19;
- Descargar un archivo de respaldo: 3.17;
- Restaurar la configuración del sistema desde un archivo de respaldo: 3.16;
- Eliminar un archivo de respaldo: 3.18.

---

## UC SS\_14: Resguardar Configuración

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad realiza un respaldo de la configuración del servidor de seguridad.

**Condiciones previas:** -

**Condiciones posteriores:** Se crea un registro en el log de auditoría para el evento.

**Desencadenante:** El administrador del servidor de seguridad desea realizar un respaldo de la configuración del servidor de seguridad.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona realizar un respaldo de la configuración del servidor de seguridad.
2. El sistema ejecuta el script de respaldo, que:
  - a. Crea un archivo de volcado de la base de datos (incluido el esquema) en la ubicación `/var/lib/xroad/dbdump.dat`, que contiene el contenido de la base de datos del servidor de seguridad;
  - b. Crea el archivo de respaldo que contiene el archivo de volcado de la base de datos y el siguiente directorio:
    - `/etc/xroad/`  
E incluye la siguiente información como etiqueta en el archivo `.tar` creado:
      - El tipo de servidor ("security" para los servidores de seguridad),
      - La versión del software del servidor de seguridad,
      - El identificador X-Road del servidor de seguridad;
    - c. Guarda el archivo de respaldo creado en `/var/lib/xroad/backup`.
  3. El sistema muestra el mensaje "Respaldo de configuración creado" y la salida del script de respaldo al administrador del servidor de seguridad.



4. El sistema registra el evento “Resguardar configuración” en el log de auditoría.

**Extensiones:**

- 3a. Falló el respaldo de la configuración del servidor de seguridad.
  - 3a.1 El script de respaldo produce un código de error que provoca que el manejo de errores elimine cualquier archivo de respaldo incompleto.
  - 3a.2 El sistema muestra el mensaje de error “Error al hacer el respaldo de configuración, el script salió con el código de estado 'X'” (donde “X” es el código de salida del script de respaldo) y la salida del script de respaldo.
  - 3a.3 El sistema registra el evento “Falló el respaldo de configuración” en el log de auditoría.
  - 3a.4 El caso de uso termina.

## UC SS\_15: Restaurar Configuración desde un Archivo de Respaldo

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad (SS administrator)

**Descripción breve:** El administrador del servidor de seguridad restaura la configuración del servidor de seguridad desde un archivo de respaldo almacenado en la configuración del sistema.

**Condiciones previas:** El archivo de respaldo existe en la configuración del sistema.

**Condiciones posteriores:** -

**Desencadenante:** El administrador del servidor de seguridad desea restaurar la configuración del servidor de seguridad a un estado previamente respaldado.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona restaurar la configuración del servidor de seguridad desde un archivo de respaldo guardado en la configuración del sistema.
2. El sistema solicita confirmación.
3. El administrador del servidor de seguridad confirma.
4. El sistema ejecuta el script, que:
  - a. Verifica que el archivo sea un archivo de respaldo válido;
  - b. Verifica la etiqueta del archivo de respaldo:

- Verifica que el tipo de servidor en la etiqueta corresponda al tipo de servidor que está siendo restaurado;
- Nota: El sistema solo verifica el tipo de servidor e ignora el resto de la información de la etiqueta en caso de que el script de restauración se llame desde la CLI con la opción -F.
- Verifica que la versión del software del servidor en la etiqueta sea compatible con la versión de software instalada del servidor que se está restaurando;
- Verifica que el identificador del servidor de seguridad en la etiqueta corresponda al identificador del servidor de seguridad que se está restaurando;
- c. Limpia la memoria compartida;
- d. Detiene todos los servicios del sistema, excepto el xroad-proxy-ui-api;
- e. Crea un respaldo pre-restauración de la configuración del sistema (paso 2 de 3.15) en /var/lib/xroad/conf\_prerestore\_backup.tar (el archivo de respaldo pre-restauración se sobrescribe en cada restauración);
- f. Elimina el contenido del siguiente directorio:
- /etc/xroad/
  - g. Escribe el volcado de la base de datos desde el archivo de respaldo en /var/lib/xroad/dbdump.dat;
  - h. Restaura el contenido del directorio /etc/xroad/ desde el archivo de respaldo;
  - i. Restaura los datos de la base de datos (incluido el esquema) desde el archivo de volcado /var/lib/xroad/dbdump.dat;
  - j. Reinicia todos los servicios que fueron detenidos previamente.
- 5. El sistema muestra el mensaje “Configuración restaurada con éxito desde el archivo 'X'.” (donde “X” es el nombre del archivo de respaldo) y la salida del script de restauración al administrador del servidor de seguridad.
- 6. El sistema notifica al administrador del servidor de seguridad: “Durante la restauración, los tokens de seguridad fueron desconectados de.”
- 7. El sistema registra el evento “Restaurar configuración” en el log de auditoría.

#### Extensiones:

- 3a. El administrador del servidor de seguridad cancela la restauración de la configuración desde el archivo de respaldo.
  - 3a.1. El caso de uso termina.
- 4a. La restauración de la configuración del servidor de seguridad falló.
  - 4a.1. El sistema muestra el mensaje de error “Restaurar configuración desde el archivo 'X' falló.” (donde X es el nombre del archivo de respaldo) y la salida del script de restauración.
  - 4a.2. El sistema registra el evento “Restaurar configuración falló” en el log de auditoría.
  - 4a.3. El caso de uso termina.

---

## UC SS\_16: Descargar un archivo de respaldo

Sistema: Servidor de seguridad

---

Nivel: Tarea de usuario

Componente: Servidor de seguridad

Actores: Administrador del servidor de seguridad

Descripción breve: El administrador del servidor de seguridad descarga un archivo de respaldo.

Precondiciones: Un archivo de respaldo está guardado en la configuración del sistema.

Postcondiciones: Un archivo de respaldo ha sido descargado.

Disparador: El administrador del servidor de seguridad desea descargar un archivo de respaldo.

#### Escenario de éxito principal:

1. El administrador del servidor de seguridad selecciona descargar un archivo de respaldo.
2. El sistema solicita el archivo para su descarga.
3. El administrador del servidor de seguridad guarda el archivo en el sistema de archivos local.

## UC SS\_17: Eliminar un archivo de respaldo

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad

**Descripción breve:** El administrador del servidor de seguridad elimina un archivo de respaldo.

**Precondiciones:** Un archivo de respaldo está guardado en la configuración del sistema.

**Postcondiciones:** -

**Disparador:** El administrador del servidor de seguridad desea eliminar un archivo de respaldo.

#### Escenario de éxito principal:

1. El administrador del servidor de seguridad selecciona eliminar un archivo de respaldo.
2. El sistema solicita confirmación.
3. El administrador del servidor de seguridad confirma.
4. El sistema elimina el archivo de respaldo y muestra el mensaje "El respaldo seleccionado ha sido eliminado exitosamente" al administrador del servidor de seguridad.
5. El sistema registra el evento "Eliminar archivo de respaldo" en el registro de auditoría.

Extensiones:

- 3a. El administrador del servidor de seguridad cancela la eliminación del

archivo de respaldo.  
3a.1. El caso de uso termina.

---

## UC SS\_18: Subir un archivo de respaldo

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad

**Descripción breve:** El administrador del servidor de seguridad sube un archivo de respaldo al servidor de seguridad.

**Precondiciones:** -

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

**Disparador:** El administrador del servidor de seguridad desea subir un archivo de respaldo.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona subir un archivo de respaldo.
2. El administrador del servidor de seguridad inserta la ruta al archivo.
3. El sistema verifica que el nombre del archivo contenga caracteres válidos.
4. El sistema verifica que el archivo subido tenga una extensión válida.
5. El sistema verifica que el contenido del archivo subido esté en formato tar.
6. El sistema verifica que no exista un archivo de respaldo con el mismo nombre en la configuración del sistema.
7. El sistema guarda el archivo de respaldo en la configuración del sistema y muestra el mensaje "Nuevo archivo de respaldo subido exitosamente" al administrador del servidor de seguridad.
8. El sistema registra el evento "Subir archivo de respaldo" en el registro de auditoría.

**Extensiones:**

- 3a. El nombre del archivo contiene caracteres inválidos.
- 3a.1. El sistema muestra el mensaje de error "No se pudo subir el nuevo archivo de respaldo: El nombre del archivo 'X' contiene caracteres inválidos. Los caracteres válidos son: (A-Z), (a-z), (0-9), ( \_ ), ( . ), ( - )." (donde "X" es el nombre del archivo subido).
- 3a.2. El sistema registra el evento "Fallo al subir archivo de respaldo" en el registro de auditoría.
- 3a.3. El administrador del servidor de seguridad selecciona reinserir la ruta al archivo de respaldo. El caso de uso continúa desde el paso 3.
- 3a.3a. El administrador del servidor de seguridad selecciona terminar el caso de uso.
- 4a. El archivo tiene una extensión inválida.

4a.1. El sistema muestra el mensaje de error “No se pudo subir el nuevo archivo de respaldo: El archivo subido 'X' tiene una extensión inválida, la válida es 'tar'” (donde “X” es el nombre del archivo subido).

4a.2. El sistema registra el evento “Fallo al subir archivo de respaldo” en el registro de auditoría.

4a.3. El administrador del servidor de seguridad selecciona reinserir la ruta al archivo de respaldo. El caso de uso continúa desde el paso 3.

4a.3a. El administrador del servidor de seguridad selecciona terminar el caso de uso.

5a. El contenido del archivo no está en formato tar.

5a.1. El sistema muestra el mensaje de error “No se pudo subir el nuevo archivo de respaldo: El contenido del archivo subido debe estar en formato tar”.

5a.2. El sistema registra el evento “Fallo al subir archivo de respaldo” en el registro de auditoría.

5a.3. El administrador del servidor de seguridad selecciona reinserir la ruta al archivo de respaldo. El caso de uso continúa desde el paso 3.

5a.3a. El administrador del servidor de seguridad selecciona terminar el caso de uso.

6a. Existe un archivo de respaldo con el mismo nombre en la configuración del sistema.

6a.1. El sistema muestra el mensaje “Ya existe un archivo de respaldo con el nombre 'X', ¿desea sobrescribirlo?” (donde “X” es el nombre del archivo subido) y solicita confirmación.

6a.2. El administrador del servidor de seguridad confirma. El caso de uso continúa desde el paso 7.

6a.2a. El administrador del servidor de seguridad cancela la carga.

6a.2a.1. El administrador del servidor de seguridad selecciona reinserir la ruta al archivo de respaldo. El caso de uso continúa desde el paso 3.

6a.2a.1a. El administrador del servidor de seguridad selecciona terminar el caso de uso.

---

## UC SS\_19: Ver la lista de tokens, claves y certificados

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad

**Descripción breve:** El administrador del servidor de seguridad ve la lista de tokens, claves, certificados y solicitudes de registro de certificados.

**Precondiciones:** -

**Postcondiciones:** La lista de tokens, claves y certificados ha sido mostrada al administrador del servidor de seguridad.

**Disparador:** El administrador del servidor de seguridad desea ver la lista de tokens, claves y certificados.

**Escenario de éxito principal:**

---

1. El administrador del servidor de seguridad selecciona ver la lista de tokens, claves y certificados que están guardados en la configuración del sistema y/o son visibles para el sistema.
2. El sistema muestra la lista de tokens, claves y certificados.

Para cada token, se muestra la siguiente información:

- El nombre amigable del token. Para los tokens que no están guardados en la configuración del sistema, y para los tokens que están guardados en la configuración pero cuyo nombre amigable no ha sido cambiado, el nombre amigable se muestra en el formato <ID del módulo>-<número de serie>--<índice de ranura>;
- El estado del token marcado como 'BLOQUEADO' cuando el token está bloqueado.  
Para cada clave, se muestra la siguiente información:
- El nombre amigable de la clave. Para las claves que no están guardadas en la configuración del sistema, y para las claves que están guardadas en la configuración pero cuyo nombre amigable no se ha establecido, se muestra la etiqueta o el identificador (si la etiqueta no está establecida) de la clave como el nombre amigable;
- El tipo de la clave ('firma' para claves utilizadas para firmar; 'autenticación' para claves utilizadas para autenticación; '?' para claves cuyo uso no está definido).  
Para cada certificado, se muestra la siguiente información:
- El nombre común (CN) del emisor del certificado;
- El número de serie del certificado;
- El identificador del miembro de X-Road para el cual se emitió el certificado en el formato clase de miembro : código de miembro para certificados de firma (si un certificado no ha sido importado a un token de hardware, no se muestra el identificador del miembro de X-Road);
- La última respuesta OCSP para certificados en estado registrado, o el aviso de estado deshabilitado si el certificado está deshabilitado;
- La fecha de caducidad del certificado;
- El estado de registro del certificado (si un certificado no ha sido importado a un token de hardware, no se muestra el estado de registro).

Para cada solicitud de registro de certificado, se muestra la siguiente información:

- El identificador del miembro de X-Road para el cual se generó la solicitud de registro de certificado en el formato clase de miembro : código de miembro (solo se muestra para solicitudes de firma de certificados).

El administrador del servidor de seguridad tiene la posibilidad de elegir entre las siguientes acciones:

- Ver los detalles de un token: 3.21;
- Ver los detalles de una clave: 3.22;
- Ver los detalles de un certificado: 3.10;
- Iniciar sesión en un token: 3.25 y 3.26;
- Cerrar sesión de un token: 3.27 y 3.28;
- Generar una clave en un token de seguridad: 3.29;
- Generar una solicitud de registro de certificado: 3.30;
- Importar un certificado: 3.31 y 3.32;

- Activar un certificado: 3.33;
- Deshabilitar un certificado: 3.34;
- Enviar una solicitud de registro de certificado de autenticación: 3.35;
- Eliminar una clave: 3.36, 3.37 y 3.38;
- Desregistrar un certificado de autenticación: 3.39;
- Eliminar una solicitud de registro de certificado: 3.40;
- Eliminar un certificado: 3.40 y 3.41.

---

## UC SS\_20: Ver los detalles de un token

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad

**Descripción breve:** El administrador del servidor de seguridad ve los detalles de un token de seguridad.

**Precondiciones:** -

**Postcondiciones:** Se muestran los detalles del token de seguridad al administrador del servidor de seguridad.

**Disparador:** El administrador del servidor de seguridad desea ver los detalles de un token de seguridad.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona ver los detalles de un token.
2. El sistema muestra los detalles del token:
  - El nombre amigable del token;
  - El identificador del token;
  - La información técnica del estado del token.El administrador del servidor de seguridad tiene la posibilidad de elegir entre las siguientes acciones:
  - Editar el nombre amigable del token: 3.23.

---

## UC SS\_21: Ver los detalles de una clave

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad

**Descripción breve:** El administrador del servidor de seguridad ve los detalles de una clave.

**Precondiciones:** -

**Postcondiciones:** Se muestran los detalles de la clave al administrador del servidor de seguridad.

**Disparador:** El administrador del servidor de seguridad desea ver los detalles de una clave.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona ver los detalles de una clave.
2. El sistema muestra la siguiente información:
  - El nombre amigable de la clave;
  - El identificador de la clave;
  - La etiqueta de la clave;
  - La información, si la clave es de solo lectura o no.El administrador del servidor de seguridad tiene la posibilidad de elegir entre las siguientes acciones:
  - Editar el nombre amigable de la clave: 3.24.

---

## UC SS\_22: Editar el Nombre Amigable de un Token

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad

**Descripción breve:** El administrador del servidor de seguridad cambia el nombre amigable de un token de seguridad.

**Precondiciones:** La información del token está guardada en la configuración del sistema.

**Postcondiciones:** Se crea un registro en el log de auditoría para el evento.

**Disparador:** El administrador del servidor de seguridad desea cambiar el nombre amigable de un token de seguridad.

**Escenario de éxito principal:**

1. El administrador del servidor de seguridad selecciona cambiar el nombre amigable de un token.
  2. El administrador cambia el nombre.
  3. El sistema analiza la entrada del usuario: 3.42.
  4. El sistema guarda los cambios en la configuración del sistema.
  5. El sistema registra el evento “Se configuró el nombre amigable para el token” en el log de auditoría.
- Extensiones:
- 2a. El proceso de análisis de la entrada del usuario termina con un mensaje de



error.

2a.1. El sistema muestra el mensaje de terminación del proceso de análisis.

2a.2. El sistema registra el evento “Falló al configurar el nombre amigable para el token” en el log de auditoría.

2a.3. El administrador selecciona reinsertar el nombre amigable. El caso de uso continúa desde el paso 2.

2a.3a. El administrador selecciona terminar el caso de uso.

---

## UC SS\_23: Editar el Nombre Amigable de una Clave

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad

**Descripción breve:** El administrador del servidor de seguridad cambia el nombre amigable de una clave.

**Precondiciones:** La información de la clave está guardada en la configuración del sistema.

**Postcondiciones:** Se crea un registro en el log de auditoría para el evento.

**Disparador:** El administrador del servidor de seguridad desea cambiar el nombre amigable de una clave.

### Escenario de éxito principal:

1. El administrador del servidor de seguridad selecciona cambiar el nombre amigable de una clave.
2. El administrador cambia el nombre.
3. El sistema analiza la entrada del usuario: 3.42.
4. El sistema guarda los cambios en la configuración del sistema.
5. El sistema registra el evento “Se configuró el nombre amigable para la clave” en el log de auditoría.

Extensiones:

2a. El proceso de análisis de la entrada del usuario termina con un mensaje de error.

2a.1. El sistema muestra el mensaje de terminación del proceso de análisis.

2a.2. El sistema registra el evento “Falló al configurar el nombre amigable para la clave” en el log de auditoría.

2a.3. El administrador selecciona reinsertar el nombre amigable. El caso de uso continúa desde el paso 2.

2a.3a. El administrador selecciona terminar el caso de uso.

---

## UC SS\_24: Iniciar Sesión en un Token de Software

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad

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

**Precondiciones:** El token está en estado de desconexión.

**Postcondiciones:** Se crea un registro en el log de auditoría para el evento.

**Disparador:** El administrador del servidor de seguridad desea activar la funcionalidad del token en el sistema.

### Escenario de éxito principal:

1. El administrador selecciona iniciar sesión en un token de software.
2. El administrador ingresa el código PIN del token.
3. El sistema analiza la entrada del usuario: 3.42.
4. El sistema verifica que el código PIN es correcto y da acceso al token.
5. El sistema registra el evento "Inicio de sesión en el token" en el log 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 el inicio de sesión en el token" en el log de auditoría.
  - 3a.3. El administrador selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
    - 3a.3a. El administrador 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 el inicio de sesión en el token" en el log de auditoría.
  - 4a.3. El administrador selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
    - 4a.3a. El administrador selecciona terminar el caso de uso.

---

## UC SS\_25: Iniciar Sesión en un Token de Hardware

---

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad

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

**Precondiciones:**

- El token de hardware está inicializado y conectado al sistema.
  - El token está en estado de desconexión.
- Postcondiciones: Se crea un registro en el log de auditoría para el evento.  
 Disparador: El administrador del servidor de seguridad desea activar la funcionalidad del token en el sistema.

**Escenario de éxito principal:**

1. El administrador selecciona iniciar sesión en un token de hardware.
  2. El administrador ingresa el código PIN del token.
  3. El sistema analiza la entrada del usuario: 3.42.
  4. El sistema verifica que el token no esté bloqueado.
  5. El sistema verifica que el formato del código PIN ingresado es correcto.
  6. El sistema verifica que el código PIN es correcto y da acceso al token.
  7. El sistema registra el evento "Inicio de sesión en el token" en el log 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 el inicio de sesión en el token" en el log de auditoría.
    - 3a.3. El administrador selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
      - 3a.3a. El administrador selecciona terminar el caso de uso.
  - 4-6a. El intento de inicio de sesión falló (por ejemplo, el token no está accesible).
    - 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 el inicio de sesión en el token" en el log de auditoría.
    - 4-6a.3. El administrador selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
      - 4-6a.3a. El administrador selecciona terminar el caso de uso.
  - 4b. El token de seguridad está bloqueado.
    - 4b.1. El sistema muestra el mensaje de error: "PIN bloqueado".
    - 4b.2. El sistema registra el evento "Falló el inicio de sesión en el token" en el log de auditoría.
    - 4b.3. El administrador selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
      - 4b.3a. El administrador selecciona terminar el caso de uso.
  - 5b. El formato del código PIN ingresado es incorrecto.

- 5b.1. El sistema muestra el mensaje de error: “Formato del PIN incorrecto”.
- 5b.2. El sistema registra el evento “Falló el inicio de sesión en el token” en el log de auditoría.
- 5b.3. El administrador selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
- 5b.3a. El administrador selecciona terminar el caso de uso.
- 6b. El código PIN ingresado es incorrecto.
- 6b.1. El sistema muestra el mensaje de error: “Inicio de sesión fallido: CKR\_PIN\_INCORRECTO”.
- 6b.2. El sistema registra el evento “Falló el inicio de sesión en el token” en el log de auditoría.
- 6b.3. El administrador selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
- 6b.3a. El administrador selecciona terminar el caso de uso.
- 6c. El código PIN ingresado es incorrecto y solo queda un intento de inicio de sesión.
- 6c.1. El sistema muestra el mensaje de error: “Inicio de sesión fallido: CKR\_PIN\_INCORRECTO, intentos restantes: 1”.
- 6c.2. El sistema registra el evento “Falló el inicio de sesión en el token” en el log de auditoría.
- 6c.3. El administrador selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
- 6c.3a. El administrador selecciona terminar el caso de uso.
- 6d. El código PIN ingresado es incorrecto y no quedan intentos de inicio de sesión.
- 6d.1. El sistema muestra el mensaje de error: “Inicio de sesión fallido: CKR\_PIN\_INCORRECTO. PIN bloqueado.”
- 6d.2. El sistema registra el evento “Falló el inicio de sesión en el token” en el log de auditoría.
- 6d.3. El administrador selecciona reingresar el código PIN. El caso de uso continúa desde el paso 3.
- 6d.3a. El administrador selecciona terminar el caso de uso.

---

## UC SS\_26: Cerrar Sesión en un Token de Software

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del servidor de seguridad

**Descripción breve:** El administrador del servidor de seguridad cierra sesión en un token de software.

**Precondiciones:** El token está en estado de conexión.

**Postcondiciones:** El token está en estado de desconexión. El sistema no puede usar las claves y certificados en el token.

**Disparador:** El administrador del servidor de seguridad desea cerrar sesión en un token de software.

---

### Escenario de éxito principal:

1. El administrador selecciona cerrar sesión en un token de software.
2. El sistema cierra sesión en el token.
3. El sistema registra el evento "Cierre de sesión del token" en el log de auditoría.

Extensiones: -

Información relacionada:

El log de auditoría se encuentra en /var/log/xroad/audit.log. El conjunto de registros del log de auditoría está descrito en el documento "X-Road: Eventos de Log de Auditoría" [SPEC-AL].

La información sobre los tokens, claves y certificados configurados para el sistema se guarda en el archivo /etc/xroad/signer/keyconf.xml.

## UC SS\_27: Cerrar sesión de un token de hardware

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

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

**Descripción breve:** El administrador del SS cierra sesión de un token de hardware.

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

**Postcondiciones:** El token está en estado de sesión cerrada. El sistema no puede usar las claves ni los certificados del token.

**Desencadenante:** El administrador del SS quiere cerrar sesión en un token de hardware.

### Escenario principal de éxito:

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

### Extensiones:

2a. El intento de cierre de sesión falló (por ejemplo, el token es inaccesible).

2a.1. El sistema muestra el mensaje de error: "Cierre de sesión fallido: X", donde "X" es el código de error de la interfaz criptográfica PKCS #11 [PKCS11].

2a.2. El sistema registra el evento "Cierre de sesión de token fallido" en el registro de auditoría.

2a.3. El caso de uso termina.

## UC SS\_28: Generar una clave

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del SS

**Descripción breve:** El administrador del SS genera una clave en un token de seguridad.

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

**Postcondiciones:** -

**Desencadenante:** El administrador del SS quiere generar una clave en un token de seguridad.

### Escenario principal de éxito:

1. El administrador del SS selecciona generar una clave en un token de seguridad.
2. El sistema solicita la etiqueta de la clave.
3. El administrador del SS inserta el valor de la etiqueta (no obligatorio, puede dejarse en blanco).
4. El sistema procesa la entrada del usuario: 3.42.
5. El administrador del SS selecciona el uso previsto del certificado (firma o autenticación) si el uso de la clave para el cual se genera la CSR no se ha asignado previamente,
6. El administrador selecciona el cliente del servidor de seguridad al cual se emitirá el certificado (solo para certificados de firma) de la lista de clientes de este servidor de seguridad.
7. El administrador selecciona el servicio de certificación de la lista de servicios de certificación aprobados que emitirá el certificado.
8. El administrador selecciona el formato de la solicitud de firma de certificado (PEM o DER).
9. El sistema usa la clase de información del perfil de certificado descrita para el CA seleccionado para mostrar los campos del nombre distinguido del sujeto de la CSR, rellenando los valores disponibles para el sistema.
10. El usuario inserta los valores del nombre distinguido del sujeto que no fueron pre-rellenados por el sistema.
11. El sistema procesa la entrada del usuario: 3.42.
12. El administrador del SS selecciona continuar o cancelar la creación de la clave.
13. El sistema genera la clave con la etiqueta insertada en el token.
14. El sistema verifica que la información del token que contiene la clave para la cual se generó la CSR no se ha guardado previamente en la configuración del sistema y guarda la información del token.
15. El sistema verifica que la clave para la cual se generó la CSR no se ha guardado previamente en la configuración del sistema y guarda la información de la clave, asignando el uso de la clave según el uso del certificado seleccionado para la CSR generada.
16. El sistema guarda una notificación sobre la CSR generada en la configuración del sistema.
17. El sistema registra el evento "Generar CSR" en el registro de auditoría.

18. El sistema genera la solicitud de firma de certificado y solicita la descarga del archivo.
19. El administrador del SS guarda el archivo CSR en el sistema de archivos local.

**Extensiones:**

- 4a. El proceso de procesamiento de la entrada del usuario terminó con un mensaje de error.
  - 4a.1. El sistema muestra el mensaje de terminación del proceso de análisis.
  - 4a.2. El sistema registra el evento "Generación de clave fallida" en el registro de auditoría.
  - 4a.3. El administrador selecciona reinsertar la etiqueta. El caso de uso continúa desde el paso 2.
- 10a. La generación de la clave falló (por ejemplo, el token es inaccesible).
  - 10a.1. El sistema muestra el mensaje de error describiendo el error encontrado. Si la generación de la clave falló en un token de hardware, el mensaje de error será un código de error de la interfaz criptográfica PKCS #11 (ver [PKCS11]).
  - 10a.2. El sistema registra el evento "Generar clave fallida" en el registro de auditoría.
  - 10a.3. El caso de uso termina.

---

## UC SS\_29: Generar una solicitud de firma de certificado para una clave

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del SS

**Descripción breve:** El administrador del SS genera una solicitud de firma de certificado para una clave y guarda el archivo de solicitud en el sistema de archivos local. El token, la clave (si no se ha guardado previamente en la configuración del sistema) y la notificación sobre la solicitud de firma de certificado se guardan en la configuración del sistema.

**Precondiciones:** La clave es accesible para el sistema. El token que contiene la clave está en estado de sesión iniciada.

**Postcondiciones:** -

**Desencadenante:** El administrador del SS quiere generar una solicitud de firma de certificado.

**Escenario principal de éxito:**

1. El administrador del SS selecciona generar una solicitud de firma de certificado para una clave.
2. El administrador del SS selecciona el uso previsto del certificado (firma o autenticación) si el uso de la clave para la cual se genera la CSR no se ha asignado previamente.
3. El administrador selecciona el cliente del servidor de seguridad al cual se emitirá el certificado (solo para certificados de firma) de la lista de clientes de este servidor de seguridad.

4. El administrador selecciona el servicio de certificación de la lista de servicios de certificación aprobados que emitirá el certificado.
5. El administrador selecciona el formato de la solicitud de firma de certificado (PEM o DER).
6. El sistema utiliza la clase de información del perfil de certificado descrita para el CA seleccionado para mostrar los campos del nombre distinguido del sujeto de la CSR, rellenando los valores disponibles para el sistema.
7. El usuario inserta los valores del nombre distinguido del sujeto que no fueron pre-rellenados por el sistema.
8. El sistema procesa la entrada del usuario: 3.42.
9. El sistema genera la solicitud de firma de certificado y solicita la descarga del archivo.
10. El sistema verifica que la información del token que contiene la clave para la cual se generó la CSR no se ha guardado previamente en la configuración del sistema y guarda la información del token.
11. El sistema verifica que la clave para la cual se generó la CSR no se ha guardado previamente en la configuración del sistema y guarda la información de la clave, asignando el uso de la clave según el uso del certificado seleccionado para la CSR generada.
12. El sistema guarda una notificación sobre la CSR generada en la configuración del sistema.
13. El sistema registra el evento "Generar CSR" en el registro de auditoría.
14. El administrador del SS guarda el archivo CSR en el sistema de archivos local.

**Extensiones:**

- 5a. El proceso de procesamiento de la entrada del usuario terminó con un mensaje de error.
- 5a.1. El sistema muestra el mensaje de terminación del proceso de análisis.
- 5a.2. El sistema registra el evento "Generar CSR fallida" en el registro de auditoría.
- 5a.3. El administrador selecciona reinsertar el nombre distinguido. El caso de uso continúa desde el paso 5.

---

## UC SS\_30: Importar un Certificado desde el Sistema de Archivos Local

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del SS

**Breve descripción:** El administrador del SS importa un certificado desde el sistema de archivos local.

**Precondiciones:** -

---



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

**Disparador:** El administrador del SS desea importar un certificado desde el sistema de archivos local.

**Escenario de éxito principal:**

1. El administrador del SS selecciona importar un archivo de certificado.
2. El administrador del SS selecciona el archivo desde el sistema de archivos local.
3. El sistema verifica que la configuración global no haya expirado.
4. El sistema verifica que el archivo esté en formato DER o PEM.
5. El sistema verifica que el certificado importado sea un certificado de firma y usa el decodificador de identificador descrito para el servicio de certificación que emitió el certificado para decodificar el identificador X-Road del cliente del servidor de seguridad al que se emitió el certificado.
6. El sistema verifica que el miembro al que se emitió el certificado sea el propietario del servidor de seguridad o tenga un subsistema registrado como cliente del servidor de seguridad.
7. El sistema verifica que la clave privada, asociada con la clave pública en el certificado, no haya sido eliminada del token.
8. El sistema verifica que este certificado no esté ya guardado en la configuración del sistema.
9. El sistema verifica que el uso del certificado esté en conformidad con el uso de la clave.
10. El sistema verifica que el certificado haya sido emitido por un servicio de certificación aprobado, confirmando que el emisor esté listado en la configuración global.
11. El sistema verifica que el certificado no haya expirado.
12. El sistema verifica que el uso de la clave esté definido y guarda el certificado en la configuración del sistema.
13. El sistema establece el estado de registro del certificado de firma como “registrado”.
14. El sistema obtiene la respuesta OCSP para el certificado importado (ver UC MESS\_15 [UC-MESS] para más detalles).
15. El sistema verifica que exista una notificación de solicitud de firma de certificado correspondiente al certificado importado en la configuración del sistema y elimina la información de la solicitud de firma de certificado.
16. El sistema registra el evento “Importar certificado desde archivo” en el registro de auditoría.

**Extensiones:**

**3a.** La configuración global ha expirado.

**3a.1.** El sistema muestra el mensaje de error “La configuración global ha expirado”.

**3a.2.** El sistema registra el evento “Importar certificado desde archivo fallido” en el registro de auditoría.

**3a.3.** El administrador del SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.

**3a.3a.** El administrador del SS selecciona terminar el caso de uso.

- 4a.** El archivo no está en un formato válido.
  - 4a.1.** El sistema muestra el mensaje de error “No se pudo importar el certificado: Formato de archivo incorrecto. Solo se permiten archivos PEM y DER”.
  - 4a.2.** El sistema registra el evento “Importar certificado desde archivo fallido” en el registro de auditoría.
  - 4a.3.** El administrador del SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.
  - 4a.3a.** El administrador del SS selecciona terminar el caso de uso.
  
- 5a.** El decodificador de identificadores ha encontrado un error.
  - 5a.1.** El sistema muestra el mensaje de error describiendo el error encontrado.
  - 5a.2.** El sistema registra el evento “Importar certificado desde archivo fallido” en el registro de auditoría.
  - 5a.3.** El administrador del SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.
  - 5a.3a.** El administrador del SS selecciona terminar el caso de uso.
- 5b.** El certificado importado es un certificado de autenticación. El caso de uso continúa desde el paso 7.
  
- 6a.** El miembro al que se emitió el certificado no es un cliente del servidor de seguridad.
  - 6a.1.** El sistema muestra el mensaje de error “No se pudo importar el certificado: El certificado fue emitido a un miembro desconocido 'X'” (donde “X” es el identificador del miembro).
  - 6a.2.** El sistema registra el evento “Importar certificado desde archivo fallido” en el registro de auditoría.
  - 6a.3.** El administrador del SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.
  - 6a.3a.** El administrador del SS selecciona terminar el caso de uso.
  
- 7a.** El sistema no pudo encontrar la clave correspondiente al certificado.
  - 7a.1.** El sistema muestra el mensaje de error “No se pudo importar el certificado: No se pudo encontrar la clave correspondiente al certificado”.
  - 7a.2.** El sistema registra el evento “Importar certificado desde archivo fallido” en el registro de auditoría.
  - 7a.3.** El administrador del SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.
  - 7a.3a.** El administrador del SS selecciona terminar el caso de uso.
  
- 8a.** El certificado ya existe bajo la clave.
  - 8a.1.** El sistema muestra el mensaje de error “No se pudo importar el certificado: El certificado ya existe bajo la clave 'X'” (donde “X” es el nombre amigable de la clave).
  - 8a.2.** El sistema registra el evento “Importar certificado desde archivo fallido” en el registro de auditoría.
  - 8a.3.** El administrador del SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.
  - 8a.3a.** El administrador del SS selecciona terminar el caso de uso.
  
- 9a.** El administrador del SS intentó importar un certificado de autenticación para una clave de firma.
  - 9a.1.** El sistema muestra el mensaje de error “No se pudo importar el certificado: No se puede importar un certificado de autenticación en claves de firma”.

**9a.2.** El sistema registra el evento “Importar certificado desde archivo fallido” en el registro de auditoría.

**9a.3.** El administrador del SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.

**9a.3a.** El administrador del SS selecciona terminar el caso de uso.

**9b.** El administrador del SS intentó importar un certificado de firma para una clave de autenticación.

**9b.1.** El sistema muestra el mensaje de error “No se pudo importar el certificado: 'X'” (donde 'X' es la razón del error).

**9b.2.** El sistema registra el evento “Importar certificado desde archivo fallido” en el registro de auditoría.

**9b.3.** El administrador del SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.

**9b.3a.** El administrador del SS selecciona terminar el caso de uso.

**9c.** El uso de la clave está indefinido.

**9c.1.** El sistema asigna el uso de la clave según el uso del certificado importado y guarda el certificado en la configuración del sistema.

**9c.2.** El caso de uso continúa desde el paso 10.

**10a.** El administrador del SS intentó importar un certificado que no fue emitido por un servicio de certificación aprobado.

**10a.1.** El sistema muestra el mensaje de error “No se pudo importar el certificado: El certificado no fue emitido por un proveedor de servicio de certificación aprobado”.

**10a.2.** El sistema registra el evento “Importar certificado desde archivo fallido” en el registro de auditoría.

**10a.3.** El administrador del SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.

**10a.3a.** El administrador del SS selecciona terminar el caso de uso.

**11a.** El certificado ha expirado.

**11a.1.** El sistema muestra el mensaje de error “No se pudo importar el certificado: El certificado no es válido”.

**11a.2.** El sistema registra el evento “Importar certificado desde archivo fallido” en el registro de auditoría.

**11a.3.** El administrador del SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.

**11a.3a.** El administrador del SS selecciona terminar el caso de uso.

**13a.** El uso de la clave está indefinido.

**13a.1.** El sistema asigna el uso de la clave según el uso del certificado importado y guarda el certificado en la

configuración del sistema.

**13a.2.** El caso de uso continúa desde el paso 14.

**14a.** El certificado importado es un certificado de autenticación.

**14a.1.** El sistema establece el certificado en estado deshabilitado y establece el estado de registro como “guardado”.

**14a.2.** El caso de uso continúa desde el paso 15.

**15a.** No existe una notificación de solicitud de firma de certificado correspondiente al certificado importado en la configuración del sistema. El caso de uso continúa desde el paso 16.

---

## UC SS\_31: Importar un Certificado desde un Token de Seguridad

**Sistema:** Servidor de seguridad

**Nivel:** Tarea del usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador de SS

**Descripción breve:** El administrador de SS importa un certificado desde un token de seguridad.

**Precondiciones:** -

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

**Disparador:** El administrador de SS quiere importar un certificado desde un token de seguridad.

### Escenario principal de éxito:

1. El administrador de SS selecciona importar un certificado desde un token de seguridad.
2. El sistema verifica que la configuración global no haya expirado.
3. El sistema verifica que el certificado importado sea un certificado de firma y usa el decodificador de identificadores descrito para el servicio de certificación que emitió el certificado para decodificar el identificador de X-Road del cliente del servidor de seguridad para el cual fue emitido el certificado.
4. El sistema verifica que el miembro, a quien se le emitió el certificado, sea el propietario del servidor de seguridad o tenga un subsistema registrado como cliente del servidor de seguridad.
5. El sistema verifica que la clave privada, asociada con la clave pública en el certificado, no haya sido eliminada del token.
6. El sistema verifica que este certificado no esté ya guardado en la configuración del sistema.
7. El sistema verifica que el uso del certificado esté en conformidad con el uso de claves.
8. El sistema verifica que el certificado haya sido emitido por un servicio de certificación aprobado, confirmando que el emisor esté listado en la configuración global.
9. El sistema verifica que el certificado no haya expirado.
10. El sistema verifica que el uso de la clave esté definido y guarda el certificado en la configuración del sistema.
11. El sistema establece el estado de registro del certificado de firma como "registrado".
12. El sistema obtiene la respuesta OCSP para el certificado importado (ver UC MESS\_15 [UC-MESS] para más detalles).

13. El sistema verifica que exista una notificación de solicitud de firma de certificado correspondiente al certificado importado en la configuración del sistema y elimina la información de la solicitud de firma de certificado.
14. El sistema registra el evento “Importar certificado desde token” en el registro de auditoría.

**Extensiones:**

- **2a.** La configuración global ha expirado.
  1. El sistema muestra el mensaje de error “La configuración global ha expirado”.
  2. El sistema registra el evento “Importar certificado desde token fallido” en el registro de auditoría.
  3. El administrador de SS selecciona volver a seleccionar el archivo. El caso de uso continúa desde el paso 3.
  4. El administrador de SS selecciona terminar el caso de uso.

---

## UC SS\_32: Activar un Certificado

**Sistema:** Servidor de seguridad

**Nivel:** Tarea del usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador de SS

**Descripción breve:** El administrador de SS activa un certificado. El servidor de seguridad puede usar los certificados activos para establecer un canal seguro de intercambio de datos entre servidores de seguridad (certificados de autenticación) o para firmar mensajes (certificados de firma).

**Precondiciones:** El certificado está en estado deshabilitado.

**Postcondiciones:** El certificado está activado.

**Disparador:** El administrador de SS quiere activar un certificado.

**Escenario principal de éxito:**

1. El administrador de SS selecciona activar un certificado.
2. El sistema activa el certificado y muestra el valor más reciente de la respuesta OCSP (si existe, de lo contrario muestra el valor “desconocido”) como el estado de la respuesta OCSP de este certificado.
3. El sistema registra el evento “Habilitar certificado” en el registro de auditoría.

---

## UC SS\_33: Deshabilitar un Certificado

**Sistema:** Servidor de seguridad

**Nivel:** Tarea del usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador de SS

**Descripción breve:** El administrador de SS desactiva un certificado. Los certificados en estado deshabilitado no se utilizan para la firma ni la autenticación.

**Precondiciones:** El certificado está en estado activo.

**Postcondiciones:** El certificado está deshabilitado.

**Disparador:** El administrador de SS quiere deshabilitar un certificado.

**Escenario principal de éxito:**

1. El administrador de SS selecciona deshabilitar un certificado.
2. El sistema desactiva el certificado y establece el estado de la respuesta OCSP en “deshabilitado”. No se consultan los respondedores OCSP para certificados deshabilitados.
3. El sistema registra el evento “Deshabilitar certificado” en el registro de auditoría.

---

## UC SS\_34: Registrar un Certificado de Autenticación

**Sistema:** Servidor de seguridad

**Nivel:** Tarea del usuario

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

**Actores:** Administrador de SS, servidor central

**Descripción breve:** El administrador de SS envía una solicitud de registro de certificado de autenticación al servidor central.

**Precondiciones:** El certificado está en estado “guardado”.

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

**Disparador:** El administrador de SS quiere registrar un certificado de autenticación para el servidor de seguridad.

**Escenario principal de éxito:**

1. El administrador de SS selecciona registrar un certificado de autenticación no registrado.
2. El sistema solicita el nombre DNS/dirección IP del servidor de seguridad.
3. El administrador de SS inserta el nombre DNS o la dirección IP del servidor de seguridad.
4. El sistema analiza la entrada del usuario: 3.42.
5. El sistema verifica que el nombre DNS o la dirección IP sea válido.
6. El sistema crea la solicitud de registro, encuentra la dirección del servicio de gestión de la configuración global y envía la solicitud al servidor central. El contenido de la solicitud está descrito en [PR-MSERV].
7. El sistema recibe el mensaje de respuesta del servidor central y verifica que la respuesta no sea un mensaje de error.
8. El sistema muestra el mensaje “Solicitud enviada” al administrador de SS y establece el estado de registro del certificado como “registro en progreso”.
9. El sistema registra el evento “Registrar certificado de autenticación” en el registro de auditoría.

**Extensiones:**

- **4a.** El proceso de análisis de la entrada del usuario termina con un mensaje de error.
  1. El sistema muestra el mensaje de terminación del proceso de análisis.
  2. El sistema registra el evento “Registrar certificado de autenticación fallido” en el registro de auditoría.
  3. El administrador de SS selecciona volver a insertar el nombre DNS o la dirección IP. El caso de uso continúa desde el paso 2.
  4. El administrador de SS selecciona terminar el caso de uso.

---

## UC SS\_35: Eliminar una clave de la configuración del sistema y de un token

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del SS

**Breve descripción:** El administrador del SS elimina una clave, incluyendo los certificados y/o notificaciones de solicitud de firma de certificado asociadas, si existen, de la configuración del sistema y de un token.

**Precondiciones:** La información sobre la clave está guardada en la configuración del sistema.

**Postcondiciones:** -

**Disparador:** El administrador del SS desea eliminar una clave.

**Escenario de éxito principal:**

1. El administrador del SS selecciona eliminar una clave de la configuración del sistema.
2. El sistema verifica si la clave está asociada con certificados de autenticación que tengan el estado de registro “registrado” o “registro en progreso” importados para la clave y, de ser así, solicita confirmación para continuar con la desregistración y eliminación de los certificados asociados, las notificaciones de solicitud de firma de certificado y la clave.
3. El administrador del SS confirma las acciones de desregistración y eliminación.
4. El sistema desregistra cada uno de los certificados de autenticación: ver UC 3.43.
5. El sistema elimina la clave y los certificados y/o notificaciones de solicitud de firma de certificado de la configuración del sistema y del token.

6. El sistema registra el evento “Eliminar clave de token y configuración” en el registro de auditoría.

**Extensiones:**

**2a.** No existen certificados de autenticación que tengan el estado de registro “registrado” o “registro en progreso” importados para la clave.

**2a.1.** El sistema solicita confirmación para la eliminación.

**2a.2.** El administrador del SS confirma.

**2a.2a.** El administrador del SS termina el caso de uso.

**2a.3.** El caso de uso continúa desde el paso 5.

**3a.** El administrador del SS termina el caso de uso.

**4a.** El proceso de desregulación de los certificados de autenticación terminó con un mensaje de error.

**4a.1.** El sistema muestra el mensaje: “Error al eliminar la clave: X”, donde “X” es el mensaje de terminación del proceso de desregulación.

**4a.2.** El sistema registra el evento “Eliminación de clave fallida” en el registro de auditoría.

**4a.3.** El caso de uso termina.

---

## UC SS\_36: Eliminar una clave de un token de software

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del SS

**Breve descripción:** El administrador del SS elimina una clave de un token de software.

**Precondiciones:** La información sobre la clave no está guardada en la configuración del sistema.

**Postcondiciones:** -

**Disparador:** El administrador del SS desea eliminar una clave.

**Escenario de éxito principal:**

1. El administrador del SS selecciona eliminar una clave.
2. El sistema solicita confirmación.
3. El administrador del SS confirma.



4. El sistema elimina la clave y los certificados asociados y las notificaciones de solicitud de firma de certificado del token.
5. El sistema registra el evento “Eliminar clave de token y configuración” en el registro de auditoría.

**Extensiones:**

- 3a. El administrador del SS termina el caso de uso.
- 

## UC SS\_37: Eliminar una clave de un token de hardware

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del SS

**Breve descripción:** El administrador del SS elimina una clave de un token de hardware.

**Precondiciones:**

- Existe una clave en un token de seguridad hardware.
- La información de la clave no está guardada en la configuración del sistema.
- El token es accesible para el sistema.

**Postcondiciones:** -

**Disparador:** El administrador del SS desea eliminar una clave.

**Escenario de éxito principal:**

1. El administrador del SS selecciona eliminar una clave.
2. El sistema solicita confirmación.
3. El administrador del SS confirma.
4. El sistema elimina la clave y los certificados asociados y las notificaciones de solicitud de firma de certificado del token.
5. El sistema registra el evento “Eliminar clave de token y configuración” en el registro de auditoría.

**Extensiones:**

- 3a. El administrador del SS termina el caso de uso.
-

**4a.** La eliminación falló (por ejemplo, la eliminación de la clave no es compatible con el token).

**4a.1.** El sistema muestra el mensaje de error: “Error al eliminar la clave: 'X'”, donde “X” es el código de error del interfaz criptográfico PKCS #11 (ver [PKCS11]).

**4a.2.** El sistema registra el evento “Eliminación de clave fallida de token” en el registro de auditoría.

**4a.3.** El caso de uso termina.

---

## UC SS\_38: Desregistrar un certificado de autenticación

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del SS, servidor de seguridad del servicio de gestión

**Breve descripción:** El administrador del SS desregistra un certificado de autenticación registrado.

**Precondiciones:** El estado de registro del certificado de autenticación es “registrado” o “registro en progreso”.

**Postcondiciones:** -

**Disparador:**

- El administrador del SS desea desregistrar el certificado de autenticación registrado.
- El administrador del SS desea eliminar una clave de la configuración del sistema.

**Escenario de éxito principal:**

1. El administrador del SS selecciona desregistrar un certificado de autenticación.
2. El sistema solicita confirmación.
3. El administrador del SS confirma.
4. El sistema verifica que existe un certificado de autenticación válido para el servidor de seguridad.
5. El sistema crea una solicitud SOAP de X-Road que contiene la solicitud de eliminación del certificado de autenticación.
6. El sistema envía la solicitud al servidor de seguridad del servicio de gestión: ver UC MESS\_02 [UC-MESS], donde este sistema actúa como el Cliente IS y el Sistema; el propietario de este servidor de seguridad actúa como el cliente del servicio; y el servidor central actúa como el proveedor IS.

7. El sistema recibe la respuesta del servidor de seguridad del servicio de gestión y verifica que la respuesta no sea un mensaje de error.
8. El sistema muestra el mensaje “Solicitud enviada” al administrador del SS.
9. El sistema establece el estado de registro del certificado de autenticación como “eliminación en progreso”.
10. El sistema registra el evento “Desregistrar certificado de autenticación” en el registro de auditoría.

**Extensiones:**

**3a.** El administrador del SS termina el caso de uso.

**4a.** No existe un certificado de autenticación válido para el servidor de seguridad.

**4a.1.** El sistema muestra el mensaje de error “Error al desregistrar el certificado: El servidor de seguridad no tiene un certificado de autenticación válido”.

**4a.2.** El sistema registra el evento “Desregistrar certificado de autenticación fallido” en el registro de auditoría.

**4a.3.** El caso de uso termina.

**5-7a.** El proceso de creación o envío de la solicitud de eliminación falló, o la respuesta fue un mensaje de error.

**5-7a.1.** El sistema muestra el mensaje de advertencia: “Error al enviar solicitud de eliminación de certificado. ¿Desea continuar con la eliminación del certificado de todas maneras?” y el mensaje de error “Error al desregistrar certificado: 'X'”, donde “X” es la descripción del error

encontrado, y solicita confirmación.

**5-7a.2.** El sistema registra el evento “Desregistrar certificado de autenticación fallido” en el registro de auditoría.

**5-7a.3.** El administrador del SS confirma.

**5-7a.3a.** El administrador del SS termina el caso de uso.

**5-7a.4.** El sistema establece el estado de registro del certificado de autenticación como “eliminación en progreso”.

**5-7a.5.** El sistema registra el evento “Omitir desregistro de certificado de autenticación” en el registro de auditoría.

**5-7a.6.** El caso de uso termina.

---

## UC SS\_39: Eliminar un certificado o una notificación de solicitud de firma de certificado de la configuración del sistema

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

---

**Actores:** Administrador del SS

**Breve descripción:** El administrador del SS elimina un certificado o una notificación de solicitud de firma de certificado de la configuración del sistema.

**Precondiciones:**

- Los certificados de autenticación pueden eliminarse si el estado de registro es “guardado”, “error global” o “eliminación en progreso”.
- El certificado o la notificación de solicitud de firma de certificado está guardado en la configuración del sistema.

**Postcondiciones:** -

**Disparador:** El administrador del SS desea eliminar un certificado o una notificación de solicitud de firma de certificado de la configuración del sistema.

**Escenario de éxito principal:**

1. El administrador del SS selecciona eliminar un certificado o una notificación de solicitud de firma de certificado.
2. El sistema solicita confirmación.
3. El administrador del SS confirma.
4. El sistema verifica si la clave tiene más certificados y/o notificaciones de solicitud de firma de certificado guardados en la configuración del sistema y elimina el certificado o CSR de la configuración del sistema.
5. El sistema registra el evento “Eliminar certificado de configuración” o “Eliminar CSR”, según el objeto eliminado, en el registro de auditoría.

**Extensiones:**

**3a.** El administrador del SS termina el caso de uso.

**4a.** La clave no tiene más certificados y/o notificaciones de solicitud de firma de certificado guardados en la configuración del sistema.

**4a.1.** El sistema elimina el certificado o CSR y la clave de la configuración del sistema.

**4a.2.** El caso de uso continúa desde el paso 5.

**4b.** La clave no tiene más certificados y/o notificaciones de solicitud de firma de certificado guardados en la configuración del sistema y el token no tiene más claves guardadas en la configuración del sistema.

**4b.1.** El sistema elimina el certificado o CSR, la clave y el token de la configuración del sistema.

**4b.2.** El caso de uso continúa desde el paso 5.

## UC SS\_40: Eliminar un certificado de un token de hardware

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador del SS

**Breve descripción:** El administrador del SS elimina un certificado de un token de hardware.

**Precondiciones:**

- El certificado no está guardado en la configuración del sistema.
- El token de hardware está en estado conectado.

**Postcondiciones:** -

**Disparador:** El administrador del SS desea eliminar un certificado de un token de hardware.

**Escenario de éxito principal:**

1. El administrador del SS selecciona eliminar un certificado de un token de hardware.
2. El sistema solicita confirmación.
3. El administrador del SS confirma.
4. El sistema elimina el certificado del token.
5. El sistema registra el evento "Eliminar certificado de token" en el registro de auditoría.

**Extensiones:**

**3a.** El administrador del SS termina el caso de uso.

**4a.** La eliminación falló (por ejemplo, la operación de eliminación de certificados no es compatible con el token).

**4a.1.** El sistema muestra el mensaje de error: "Error al eliminar el certificado: 'X'", donde "X" es el código de error del interfaz criptográfico PKCS #11 (ver [PKCS11]).

**4a.2.** El sistema registra el evento "Eliminación de certificado fallida de token" en el registro de auditoría.

**4a.3.** El caso de uso termina.

---

## UC SS\_41: Analizar la Entrada del Usuario

**Sistema:** Servidor de seguridad

**Nivel:** Subfunción

**Componente:** Servidor de seguridad

**Actores:** -

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

**Precondiciones:** -

**Postcondiciones:** -

**Disparador:**

- Paso 2 de 3.23.
- Paso 2 de 3.24.
- Paso 3 de 3.25.
- Paso 3 de 3.26.
- Paso 4 de 3.29.
- Paso 5 de 3.30.
- Paso 2 de 3.35.

**Escenario de éxito principal:**

1. El sistema elimina los espacios en blanco al principio y al final de la entrada.
2. El sistema verifica que los campos obligatorios estén completos.
3. 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 caracteres.

**3a.1.** El caso de uso termina con el mensaje de error “El parámetro 'X' excede los 255 caracteres” (donde “X” es el nombre del parámetro).

## UC SS\_42: Desregistrar un Certificado de Autenticación al Eliminar la Clave

**Sistema:** Servidor de seguridad

**Nivel:** Subfunción

**Componente:** Servidor de seguridad

**Actores:** -

**Breve descripción:** El sistema crea y envía una solicitud de eliminación de certificado de autenticación al servidor de seguridad de los servicios de gestión, espera la respuesta y establece el estado del certificado de autenticación como "eliminación en progreso".

**Precondiciones:** -

**Postcondiciones:** -

**Disparador:** Paso 2 de 3.36.

**Escenario de éxito principal:**

1. El sistema crea una solicitud SOAP de X-Road que contiene la solicitud de eliminación del certificado de autenticación para el certificado. El contenido de la solicitud se describe en [PR-MSERV].
2. El sistema envía la solicitud al servidor de seguridad de los servicios de gestión: ver UC MESS\_02 [UC-MESS], donde este sistema actúa tanto como Cliente IS como Sistema; el propietario de este servidor de seguridad actúa como cliente del servicio; y el servidor central actúa como Provider IS.
3. El sistema recibe la respuesta del servidor de seguridad de los servicios de gestión y verifica que la respuesta no sea un mensaje de error.
4. El sistema establece el estado de registro del certificado de autenticación como "eliminación en progreso".

**Extensiones:**

**1-2a.** La creación o envío de la solicitud de eliminación falló.

**1-2a.1.** El caso de uso termina con el mensaje de error que describe el fallo.

**3a.** La respuesta fue un mensaje de error.

**3a.1.** El caso de uso termina con el mensaje de error recibido.

## UC SS\_43: Crear una Nueva Clave API

**Sistema:** Servidor de seguridad

**Nivel:** Tarea de usuario

**Componente:** Servidor de seguridad

**Actores:** Administrador SS

**Breve descripción:** El administrador crea una nueva clave API, que se usará para autenticación al ejecutar llamadas REST API para actualizar la configuración del servidor.

**Precondiciones:** -

**Postcondiciones:** -

**Disparador:** El administrador SS desea crear una nueva clave API.

**Escenario de éxito principal:**

1. El administrador SS decide a qué roles debe estar vinculada la nueva clave API. Los roles posibles son:  
**XROAD\_SECURITY\_OFFICER,**  
**XROAD\_REGISTRATION\_OFFICER,**  
**XROAD\_SERVICE\_ADMINISTRATOR,**  
**XROAD\_SYSTEM\_ADMINISTRATOR,**  
**XROAD\_SECURITYSERVER\_OBSERVER**
2. El administrador SS envía la solicitud HTTP POST para crear una nueva clave API. El cliente REST debe:
  - 2.1 Enviar la solicitud localmente desde el servidor de seguridad, el acceso remoto está prohibido (por defecto).
  - 2.2 Enviar la solicitud a la URL <https://localhost:4000/api/v1/api-keys>
  - 2.3 Aceptar el certificado SSL autofirmado de la API REST
  - 2.4 Proporcionar las credenciales de un administrador SS con el rol **XROAD\_SYSTEM\_ADMINISTRATOR**, utilizando autenticación básica.
  - 2.5 Proporcionar los roles para vincular a la clave API, con un cuerpo de mensaje que contenga los nombres de los roles en una matriz JSON de cadenas.
  - 2.6 Definir el tipo de contenido correcto con el encabezado HTTP  
**Content-Type: application/json**  
Ejemplo utilizando el comando "curl":  
curl -X POST -u <username>:<password>  
https://localhost:4000/api/v1/api-keys --data  
['XROAD\_SERVICE\_ADMINISTRATOR','XROAD\_REGISTRATION\_O  
FFICER'] --header "Content-Type: application/json" -k



3. El sistema crea una nueva clave API y responde con un mensaje JSON que contiene los detalles de la clave:
  - 3.1 ID de la clave API con el nombre **id**
  - 3.2 Roles vinculados a la clave, con el nombre **roles**, en una matriz de cadenas
  - 3.3 Clave API actual con el nombre **key**

Ejemplo:

```
1. {  
2. "roles": [  
3. "XROAD_REGISTRATION_OFFICER",  
4. "XROAD_SERVICE_ADMINISTRATOR"  
5. ],  
6. "id": 63,  
7. "key": "4366c766-cfd0-423f-84d5-ae1932d00b6a"  
8. }
```

4. El administrador SS guarda la clave API en un lugar seguro. La clave solo se muestra en esta respuesta y no se puede recuperar más tarde. La clave API debe mantenerse segura, ya que proporciona acceso a todos los usuarios de la API REST que conozcan la clave.

**Extensiones:**

**2a.** El administrador SS proporciona credenciales inválidas o credenciales para un usuario que no tiene el rol **XROAD\_SYSTEM\_ADMINISTRATOR**

**2a.1.** El sistema responde con HTTP 401 o HTTP 403

**2b.** El administrador SS envía la solicitud desde un servidor remoto

**2b.1.** El sistema responde con HTTP 401