

Casos de Uso Trust Service Management

Índice

Introducción	3
Descripción general.....	3
Modelo de caso de uso	4
Actores.....	4
UC TRUST_01: Ver servicios de certificación aprobados	5
UC TRUST_02: Ver los detalles de un certificado CA de servicio de certificación	5
UC TRUST_03: Ver los detalles de un certificado	6
UC TRUST_04: Ver la configuración de un servicio de certificación	7
UC TRUST_05: Ver los respondedores OCSP de un CA	8
UC TRUST_06: Ver los CAs intermedios de un servicio de certificación	8
UC TRUST_07: Ver los detalles de un CA intermedio	9
UC TRUST_08: Añadir un servicio de certificación aprobado	10
UC TRUST_09: Editar la configuración de un servicio de certificación	12
UC TRUST_10: Agregar o editar un respondedor OCSP de una CA.....	13
UC TRUST_11: Eliminar un respondedor OCSP de una CA	14
UC TRUST_12: Agregar una CA Intermedia a un Servicio de Certificación	15
UC TRUST_13: Eliminar una CA Intermedia	16
UC TRUST_14: Eliminar un Servicio de Certificación Aprobado.....	16
UC TRUST_15: Ver Servicios de Sello de Tiempo Aprobados.....	17
UC TRUST_16: Agregar un Servicio de Sellado de Tiempo Aprobado	18
UC TRUST_17: Editar la URL de un Servidor de Sellado de Tiempo	19
UC TRUST_18: Eliminar un Servicio de Sellado de Tiempo Aprobado.....	20
UC TRUST_19: Analizar la Entrada del Usuario.....	21

Introducción

El propósito de este documento es describir los procesos relacionados con la gestión de servicios de confianza aprobados en el servidor central de X-Road.

Los casos de uso incluyen las verificaciones que tienen lugar y las principales condiciones de error que pueden encontrarse durante el proceso descrito. Los errores generales del sistema que pueden ocurrir en la mayoría de los casos de uso (por ejemplo, errores de conexión a la base de datos o errores de memoria) 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.

Los casos de uso que incluyen un actor humano (el nivel del caso de uso es 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.

Descripción general

Los servicios de certificación y los servicios de sellado de tiempo aprobados por la agencia rectora de X-Road proporcionan servicios de confianza para los miembros de una instancia de X-Road.

Los servicios de confianza aprobados están descritos en el servidor central. La información sobre los servicios de confianza aprobados se distribuye a los servidores de seguridad como parte de la configuración global.

Los servidores de seguridad verifican que los certificados, respuestas OCSP y sellos de tiempo utilizados en el proceso de comunicación entre los miembros de X-Road sean proporcionados por los servicios de confianza aprobados.

Modelo de caso de uso

Actores

El modelo de caso de uso para la gestión de servicios de confianza en el servidor central incluye el siguiente actor:

Administrador de CS (administrador del servidor central) – una persona responsable de gestionar el servidor central.

Las relaciones entre el actor, el sistema y los casos de uso se describen en la Figura 1.

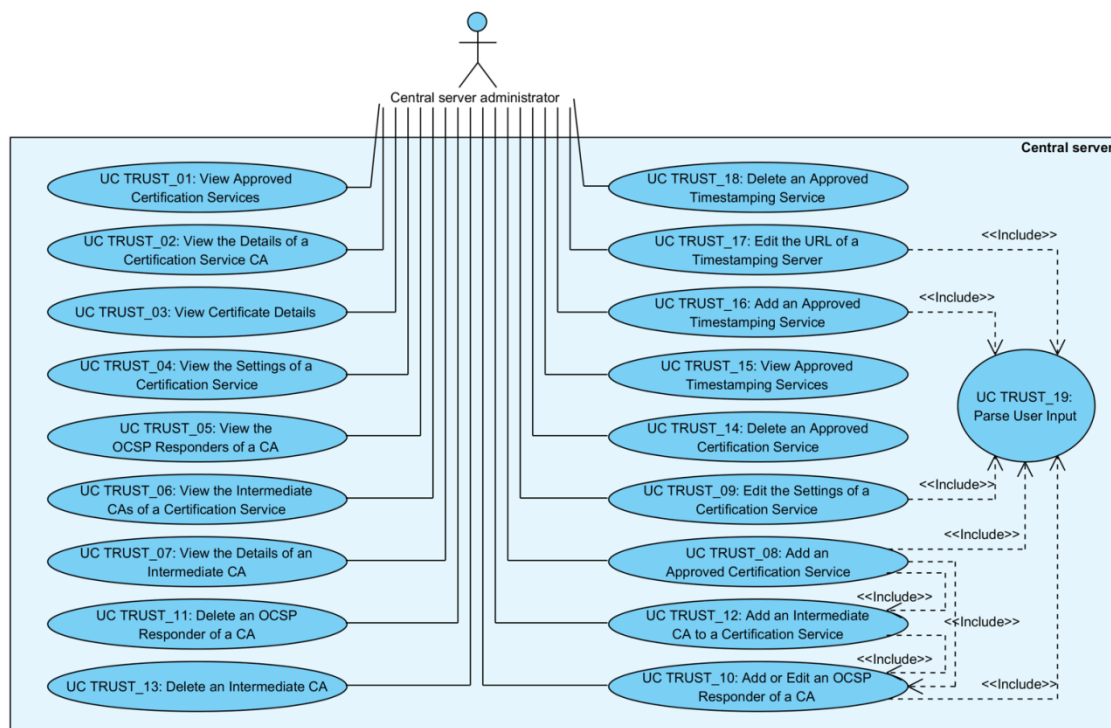


Figura 1. Diagrama de casos de uso para la gestión de servicios de confianza.

UC TRUST_01: Ver servicios de certificación aprobados

Sistema: Servidor central

Nivel: Tarea del usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS ve la lista de servicios de certificación que han sido aprobados y descritos para esta instancia de X-Road.

Precondiciones: -

Postcondiciones: La lista de servicios de certificación aprobados ha sido mostrada al administrador de CS.

Disparador: -

Escenario principal de éxito:

- El administrador de CS selecciona ver la lista de servicios de certificación aprobados.
- El sistema muestra la lista de servicios de certificación aprobados. Se muestra la siguiente información para cada servicio de certificación:
 - El valor del nombre común (CN) del sujeto del certificado CA del servicio de certificación se muestra como el nombre del servicio de certificación.
 - El período de validez del certificado CA del servicio.
 - Las siguientes opciones de acción del usuario son mostradas:
 - añadir un servicio de certificación aprobado: 3.9;
 - ver los detalles de un servicio de certificación aprobado: 3.3;
 - eliminar un servicio de certificación aprobado: 3.15.

UC TRUST_02: Ver los detalles de un certificado CA de servicio de certificación

Sistema: Servidor central

Nivel: Tarea del usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS ve los detalles de un servicio de certificación aprobado.

Precondiciones: -

Postcondiciones: Los detalles del servicio de certificación han sido mostrados al administrador de CS.

Disparador: -

Escenario principal de éxito:

- El administrador de CS selecciona ver los detalles de un servicio de certificación aprobado.
- El sistema muestra la siguiente información:
 - El nombre distinguido (DN) del sujeto del certificado CA del servicio de certificación;
 - El nombre distinguido (DN) del emisor del certificado CA del servicio de certificación;
 - El período de validez del certificado CA del servicio de certificación.
 - Las siguientes opciones de acción del usuario son mostradas:
 - ver los detalles del certificado CA del servicio de certificación: 3.4;
 - ver la configuración del CA del servicio de certificación: 3.5;
 - ver los respondedores OCSP configurados para el CA del servicio de certificación: 3.6;
 - ver los CAs intermedios configurados para el servicio de certificación: 3.7.

UC TRUST_03: Ver los detalles de un certificado

Sistema: Servidor central

Nivel: Tarea del usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS ve el contenido de un certificado.

Precondiciones: -

Postcondiciones: El contenido del certificado ha sido mostrado al administrador de CS.

Disparador: -

Escenario principal de éxito:

- El administrador de CS selecciona ver un certificado.
- El sistema muestra la siguiente información:
 - El contenido del certificado;
 - El valor del hash SHA-1 del certificado.

UC TRUST_04: Ver la configuración de un servicio de certificación

Sistema: Servidor central

Nivel: Tarea del usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS ve la configuración de un servicio de certificación.

Precondiciones: -

Postcondiciones: La configuración del servicio de certificación ha sido mostrada al administrador de CS.

Disparador: -

Escenario principal de éxito:

- El administrador de CS selecciona ver la configuración de un servicio de certificación.
- El sistema muestra la siguiente configuración:
 - Restricciones de uso para los certificados emitidos por el servicio de certificación. Los certificados emitidos por el servicio de certificación pueden ser usados para firmas y autenticación, o solo para autenticación.
 - El nombre completamente calificado de la clase Java que describe el perfil del certificado para los certificados emitidos por el servicio de certificación.
 - Las siguientes opciones de acción del usuario son mostradas:
 - editar la configuración del servicio de certificación: 3.10.

UC TRUST_05: Ver los respondedores OCSP de un CA

Sistema: Servidor central

Nivel: Tarea del usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS ve los respondedores OCSP configurados para un CA.

Precondiciones: -

Postcondiciones: Los respondedores OCSP configurados para un CA han sido mostrados al administrador de CS.

Disparador: -

Escenario principal de éxito:

- El administrador de CS selecciona ver los respondedores OCSP de un CA.
- El sistema muestra la lista de respondedores OCSP configurados. Para cada respondedor OCSP, se muestra la siguiente información:
 - La URL del servidor OCSP.
- Las siguientes opciones de acción del usuario son mostradas:
 - añadir un respondedores OCSP para el CA: 3.11;
 - ver los detalles del certificado del respondedor OCSP (si se ha subido un certificado para este respondedor OCSP): 3.4;
 - editar la información de un respondedor OCSP: 3.11;
 - eliminar un respondedor OCSP del CA: 3.12.

UC TRUST_06: Ver los CAs intermedios de un servicio de certificación

Sistema: Servidor central

Nivel: Tarea del usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS ve los CAs intermedios configurados para un servicio de certificación.

Precondiciones: -

Postcondiciones: La lista de CAs intermedios ha sido mostrada al administrador de CS.

Disparador: -

Escenario principal de éxito:

- El administrador de CS selecciona ver los CAs intermedios configurados para un servicio de certificación.
- El sistema muestra la lista de CAs intermedios. Para cada CA intermedio, se muestra la siguiente información:
 - El valor del nombre común (CN) del sujeto del certificado CA intermedio se muestra como el nombre del CA intermedio.
 - El período de validez del certificado CA intermedio.
- Las siguientes opciones de acción del usuario son mostradas:
 - añadir un CA intermedio: 3.13;
 - ver los detalles de un CA intermedio: 3.8;
 - eliminar un CA intermedio: 3.14.

UC TRUST_07: Ver los detalles de un CA intermedio

Sistema: Servidor central

Nivel: Tarea del usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS ve los detalles de un CA intermedio.

Precondiciones: -

Postcondiciones: Los detalles de un CA intermedio han sido mostrados al administrador de CS.

Disparador: -

Escenario principal de éxito:

- El administrador de CS selecciona ver los detalles de un CA intermedio.
- El sistema muestra la siguiente información:
 - El nombre distinguido (DN) del sujeto del certificado CA intermedio;
 - El nombre distinguido (DN) del emisor del certificado CA intermedio;
 - El período de validez del certificado CA intermedio.
- Las siguientes opciones de acción del usuario son mostradas:
 - ver los detalles del certificado CA intermedio: 3.4;

- ver los respondedores OCSP configurados para el CA intermedio: 3.6.

UC TRUST_08: Añadir un servicio de certificación aprobado

Sistema: Servidor central

Nivel: Tarea del usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS añade un servicio de certificación a la lista de servicios de certificación aprobados.

Precondiciones:

- El servicio de certificación ha sido aprobado por la agencia reguladora de X-Road.
- El administrador de CS ha recibido los certificados e información del respondedor OCSP del proveedor del servicio de certificación que son necesarios para configurar el servicio de certificación en el servidor central.
- Se ha desarrollado una clase Java que describe el perfil del certificado para el servicio de certificación.

Postcondiciones: -

Disparador: Un servicio de certificación es aprobado por la agencia reguladora de X-Road para proporcionar servicios de certificación a los miembros de X-Road.

Escenario principal de éxito:

- El administrador de CS selecciona añadir un servicio de certificación aprobado.
- El administrador de CS selecciona y sube el archivo del certificado CA del servicio de certificación desde el sistema de archivos local.
- El sistema verifica que el archivo subido está en formato DER o PEM.
- El sistema muestra el mensaje “Certificado importado con éxito” y solicita la configuración del servicio de certificación.
- El administrador de CS: a. selecciona si los certificados emitidos por el servicio de certificación pueden ser utilizados solo para autenticación o también para firmas; b. inserta el nombre completamente calificado de la clase Java que describe el perfil del certificado para el servicio de certificación.
- El sistema analiza la entrada del usuario: 3.20.
- El sistema verifica que la clase Java que describe el perfil del certificado existe en el classpath del sistema y guarda los cambios.

- El sistema guarda el certificado seleccionado como el certificado CA del servicio de certificación y las configuraciones insertadas para el servicio, mostrando el mensaje “Servicio de certificación añadido con éxito”.
- El sistema registra el evento “Añadir servicio de certificación” en el registro de auditoría.
- El administrador de CS añade respondedores OCSP para el certificado CA del servicio de certificación (si la información del respondedor OCSP no está incluida en el certificado CA del servicio de certificación): 3.11.
- El administrador de CS añade CAs intermedios para el servicio de certificación: 3.13.

Extensiones:

3a. El archivo subido no está en formato DER o PEM.

3a.1. El sistema muestra el mensaje de error: “No se pudo subir el certificado del servicio CA: Formato de archivo incorrecto. Solo se permiten archivos PEM y DER.”

3a.2. El administrador de CS selecciona volver a seleccionar y subir el certificado CA del servicio de certificación. El caso de uso continúa desde el paso 3. 3a.2a. El administrador de CS selecciona terminar el caso de uso. 5a. El administrador de CS selecciona no editar la configuración del servicio de certificación y termina el caso de uso.

6a. El análisis de la entrada del usuario terminó con un mensaje de error.

6a.1. El sistema muestra el mensaje de terminación del proceso de análisis. 6a.2. El sistema registra el evento “Añadir servicio de certificación fallido” en el registro de auditoría. 6a.3. El administrador de CS selecciona volver a insertar el nombre de la clase del perfil del certificado. El caso de uso continúa desde el paso 6. 6a.3a. El administrador de CS selecciona terminar el caso de uso. 7a. El sistema no encontró la clase del perfil del certificado insertada en el classpath.

7a.1. El sistema muestra el mensaje de error “El perfil de certificado con el nombre 'X' no existe”, donde “X” es el nombre de la clase insertada. 7a.2. El sistema registra el evento “Añadir servicio de certificación fallido” en el registro de auditoría. 7a.3. El administrador de CS selecciona volver a insertar el nombre de la clase del perfil del certificado. El caso de uso continúa desde el paso 6. 7a.3a. El administrador de CS selecciona terminar el caso de uso. 10a. El administrador de CS selecciona no añadir respondedores OCSP para el certificado CA del servicio de certificación (la información del respondedor OCSP está incluida en el certificado CA del servicio de certificación).

10a.1. El administrador de CS termina el caso de uso. 10a.1a. El administrador de CS selecciona añadir CAs intermedios para el servicio de certificación. El caso de uso continúa desde el paso 11. 11a. El administrador de CS selecciona no añadir CAs intermedios para el servicio de certificación y termina el caso de uso.

UC TRUST_09: Editar la configuración de un servicio de certificación

Sistema: Servidor central

Nivel: Tarea de usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS edita la configuración de un servicio de certificación.

Precondiciones: -

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

Desencadenante: Se necesitan establecer o cambiar las restricciones de uso para los certificados emitidos por el servicio de certificación, o el nombre de la clase que describe el perfil de certificado para el servicio de certificación.

Escenario principal de éxito:

1. El administrador de CS selecciona editar la configuración de un servicio de certificación.
2. El administrador de CS:
 - selecciona si los certificados emitidos por el servicio de certificación solo pueden ser utilizados para autenticación o también para firmas;
 - inserta el nombre completo de la clase de Java que describe el perfil de certificado para el servicio de certificación.
3. El sistema analiza la entrada del usuario: **3.20**.
4. El sistema verifica que la clase de Java que describe el perfil del certificado existe en el classpath del sistema y guarda los cambios.
5. El sistema registra el evento "Editar configuración del servicio de certificación" en el registro de auditoría.

Extensiones:

- **3a.** El análisis de la entrada del usuario termina con un mensaje de error.
 - **3a.1.** El sistema muestra el mensaje de terminación del proceso de análisis.
 - **3a.2.** El sistema registra el evento "Fallo al editar la configuración del servicio de certificación" en el registro de auditoría.
 - **3a.3.** El administrador de CS selecciona volver a insertar el nombre de la clase del perfil de certificado. El caso de uso continúa desde el paso 3.
 - **3a.3a.** El administrador de CS selecciona terminar el caso de uso.
- **4a.** El sistema no encuentra la clase de perfil de certificado insertada en el classpath.
 - **4a.1.** El sistema muestra el mensaje de error: "El perfil de certificado con el nombre 'X' no existe", donde "X" es el nombre de la clase insertada.
 - **4a.2.** El sistema registra el evento "Fallo al editar la configuración del servicio de certificación" en el registro de auditoría.
 - **4a.3.** El administrador de CS selecciona volver a insertar el nombre de la clase del perfil de certificado. El caso de uso continúa desde el paso 3.

- **4a.3a.** El administrador de CS selecciona terminar el caso de uso.

UC TRUST_10: Agregar o editar un respondedor OCSP de una CA

Sistema: Servidor central

Nivel: Tarea de usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS describe la información del servicio de un respondedor OCSP para una CA.

Precondiciones: El administrador de CS ha recibido la información del respondedor OCSP (URL y/o certificado) del proveedor de servicios de certificación.

Postcondiciones: -

Desencadenantes:

- Se necesita describir un respondedor OCSP para una CA.
- Paso 8 de **3.9**.
- Paso 6 de **3.13**.

Escenario principal de éxito:

1. El administrador de CS selecciona agregar o editar un respondedor OCSP de una CA.
2. El administrador de CS inserta la URL del servidor OCSP.
3. El administrador de CS selecciona y carga el archivo del certificado utilizado por el servidor OCSP para firmar las respuestas OCSP desde el sistema de archivos local.
4. El sistema verifica que el archivo cargado esté en formato DER o PEM.
5. El sistema analiza la entrada del usuario: **3.20**.
6. El sistema verifica que la URL insertada esté en el formato correcto.
7. El sistema guarda la información del respondedor OCSP.
8. El sistema registra el evento "Agregar respondedor OCSP de servicio de certificación" o "Editar respondedor OCSP", dependiendo de si el respondedor OCSP fue agregado o editado, en el registro de auditoría.

Extensiones:

- **3a.** El administrador de CS selecciona no cargar un certificado para el respondedor OCSP. El caso de uso continúa desde el paso 5.
- **4a.** El archivo cargado no está en formato DER o PEM.
 - **4a.1.** El sistema muestra el mensaje de error: "Fallo al cargar el certificado del respondedor OCSP: Formato de archivo incorrecto. Solo se permiten archivos PEM y DER."
 - **4a.2.** El administrador de CS selecciona volver a seleccionar y cargar el archivo del certificado. El caso de uso continúa desde el paso 4.
 - **4a.2a.** El administrador de CS selecciona terminar el caso de uso.
- **5a.** El análisis de la entrada del usuario termina 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 "Fallo al agregar el respondedor OCSP del servicio de certificación" o "Fallo al editar el respondedor OCSP", dependiendo de si el respondedor OCSP fue agregado o editado, en el registro de auditoría.
- **5a.3.** El administrador de CS selecciona volver a insertar la URL. El caso de uso continúa desde el paso 3.
- **5a.3a.** El administrador de CS selecciona terminar el caso de uso.
- **6a.** La URL está mal formada.
 - **6a.1.** El sistema muestra el mensaje de error: "'X' es una URL no válida, ejemplos de URL válidas: '<http://www.ejemplo.com>', '<https://www.ejemplo.com>', donde 'X' es la URL insertada.
 - **6a.2.** El sistema registra el evento "Fallo al agregar el respondedor OCSP del servicio de certificación" o "Fallo al editar el respondedor OCSP", dependiendo de si el respondedor OCSP fue agregado o editado, en el registro de auditoría.
 - **6a.3.** El administrador de CS selecciona volver a insertar la URL. El caso de uso continúa desde el paso 3.
 - **6a.3a.** El administrador de CS selecciona terminar el caso de uso.

UC TRUST_11: Eliminar un respondedor OCSP de una CA

Sistema: Servidor central

Nivel: Tarea de usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS elimina la información de un respondedor OCSP de una CA.

Precondiciones: -

Postcondiciones:

- Un respondedor OCSP ha sido eliminado de una CA.
 - Se ha creado un registro en el registro de auditoría para el evento.
- Desencadenante:** Se necesita eliminar la información de un respondedor OCSP de la configuración de un servicio de certificación aprobado.

Escenario principal de éxito:

1. El administrador de CS selecciona eliminar un respondedor OCSP de una CA.
2. El sistema elimina la información del respondedor OCSP de la configuración del sistema.
3. El sistema registra el evento "Eliminar respondedor OCSP" en el registro de auditoría.

Extensiones: -

UC TRUST_12: Agregar una CA Intermedia a un Servicio de Certificación

Sistema: Servidor central

Nivel: Tarea de usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS configura una CA intermedia para un servicio de certificación.

Precondiciones: -

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

Desencadenantes:

- Se necesita describir una CA intermedia para el servicio de certificación.
- Paso 9 de **3.9**.

Escenario principal de éxito:

1. El administrador de CS selecciona agregar una CA intermedia a un servicio de certificación.
2. El administrador de CS selecciona y carga el archivo del certificado de la CA intermedia desde el sistema de archivos local.
3. El sistema verifica que el archivo seleccionado esté en formato DER o PEM.
4. El sistema guarda el certificado seleccionado como el certificado de la CA intermedia y muestra el mensaje "CA intermedia agregada con éxito".
5. El sistema registra el evento "Agregar CA intermedia" en el registro de auditoría.
6. El administrador de CS agrega los respondedores OCSP para la CA intermedia (si la información del respondedor OCSP no está incluida en el certificado de la CA intermedia): **3.11**.

Extensiones:

- **3a.** El archivo seleccionado no está en formato DER o PEM.
 - **3a.1.** El sistema muestra el mensaje de error: "Fallo al cargar el certificado de la CA intermedia: Formato de archivo incorrecto. Solo se permiten archivos PEM y DER."
 - **3a.2.** El sistema registra el evento "Fallo al agregar la CA intermedia" en el registro de auditoría.
 - **3a.3.** El administrador de CS selecciona volver a seleccionar y cargar el certificado de la CA intermedia. El caso de uso continúa desde el paso 3.
 - **3a.3a.** El administrador de CS selecciona terminar el caso de uso.
- **6a.** El administrador de CS selecciona no agregar respondedores OCSP a la CA intermedia (la información del respondedor OCSP está incluida en el certificado de la CA intermedia) y termina el caso de uso.

UC TRUST_13: Eliminar una CA Intermedia

Sistema: Servidor central

Nivel: Tarea de usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS elimina una CA intermedia de un servicio de certificación.

Precondiciones: -

Postcondiciones:

- Se ha eliminado la información sobre una CA intermedia.
- Se ha creado un registro en el registro de auditoría para el evento.

Desencadenante: Se necesita eliminar una CA intermedia de un servicio de certificación.

Escenario principal de éxito:

1. El administrador de CS selecciona eliminar una CA intermedia de un servicio de certificación.
2. El sistema elimina la información de la CA intermedia de la configuración del sistema.
3. El sistema registra el evento "Eliminar CA intermedia" en el registro de auditoría.

UC TRUST_14: Eliminar un Servicio de Certificación Aprobado

Sistema: Servidor central

Nivel: Tarea de usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS elimina un servicio de certificación aprobado.

Precondiciones: -

Postcondiciones: -

Desencadenante: Se necesita eliminar un servicio de certificación aprobado de la configuración del sistema.

Escenario principal de éxito:

1. El administrador de CS selecciona eliminar un servicio de certificación aprobado.
2. El sistema solicita confirmación.
3. El administrador de CS confirma.
4. El sistema elimina la información del servicio de certificación aprobado de la configuración del sistema.

5. El sistema registra el evento "Eliminar servicio de certificación" en el registro de auditoría.

Extensiones:

- **3a.** El administrador de CS selecciona no eliminar el servicio de certificación aprobado y termina el caso de uso.

UC TRUST_15: Ver Servicios de Sello de Tiempo Aprobados

Sistema: Servidor central

Nivel: Tarea de usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS visualiza los servicios de sellado de tiempo aprobados configurados para esta instancia de X-Road.

Precondiciones: -

Postcondiciones: La lista de servicios de sellado de tiempo aprobados ha sido mostrada al administrador de CS.

Desencadenante: -

Escenario principal de éxito:

1. El administrador de CS selecciona ver los servicios de sellado de tiempo aprobados.
2. El sistema muestra la lista de servicios de sellado de tiempo. La siguiente información es mostrada para cada servicio de sellado de tiempo:
 - El valor del elemento common name (CN) del certificado TSA se muestra como el nombre del servicio de sellado de tiempo.
 - El período de validez del certificado del TSA.
3. Se muestran las siguientes opciones de acción del usuario:
 - Agregar un servicio de sellado de tiempo aprobado: **3.17**;
 - Ver los detalles de un certificado TSA: **3.4**;
 - Editar la URL del servidor de sellado de tiempo de un servicio de sellado de tiempo aprobado: **3.18**;
 - Eliminar un servicio de sellado de tiempo aprobado: **3.19**.

UC TRUST_16: Agregar un Servicio de Sellado de Tiempo Aprobado

Sistema: Servidor central

Nivel: Tarea de usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS agrega un servicio de sellado de tiempo a la lista de servicios de sellado de tiempo aprobados.

Precondiciones:

- El servicio de sellado de tiempo ha sido aprobado por la agencia gobernante de X-Road.
- El administrador de CS ha recibido la información del proveedor del servicio de sellado de tiempo necesaria para configurar el servicio de sellado de tiempo en el servidor central.

Postcondiciones: -

Desencadenante: Un servicio de sellado de tiempo ha sido aprobado por la agencia gobernante de X-Road para proporcionar servicios de sellado de tiempo a los miembros de X-Road.

Escenario principal de éxito:

1. El administrador de CS selecciona agregar un servicio de sellado de tiempo aprobado.
2. El administrador de CS inserta la URL del servidor de sellado de tiempo.
3. El administrador de CS selecciona y carga el archivo del certificado TSA desde el sistema de archivos local.
4. El sistema verifica que el archivo cargado esté en formato DER o PEM y muestra el mensaje "Certificado importado con éxito".
5. El sistema analiza la entrada del usuario: **3.20**.
6. El sistema verifica que la URL insertada esté en el formato correcto.
7. El sistema verifica que un servicio de sellado de tiempo aprobado con la URL y el certificado insertados no exista ya en la configuración del sistema.
8. El sistema guarda la información del servicio de sellado de tiempo.
9. El sistema registra el evento "Agregar servicio de sellado de tiempo" en el registro de auditoría.

Extensiones:

- **4a.** El archivo cargado no está en formato DER o PEM.
 - **4a.1.** El sistema muestra el mensaje de error: "Fallo al cargar el certificado TSA aprobado: Formato de archivo incorrecto. Solo se permiten archivos PEM y DER."
 - **4a.2.** El administrador de CS selecciona volver a seleccionar y cargar el archivo del certificado. El caso de uso continúa desde el paso 4.
 - **4a.2a.** El administrador de CS selecciona terminar el caso de uso.
- **5a.** El análisis 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 “Fallo al agregar el servicio de sellado de tiempo” en el registro de auditoría.
 - **5a.3.** El administrador de CS selecciona volver a insertar la URL. El caso de uso continúa desde el paso 5.
 - **5a.3a.** El administrador de CS selecciona terminar el caso de uso.
- **6a.** La URL está malformada.
 - **6a.1.** El sistema muestra el mensaje de error: “La URL del servidor de sellado de tiempo 'X' es una URL inválida, ejemplos de URL válidas: '<http://www.example.com>', '<https://www.example.com>”, donde "X" es la URL insertada.
 - **6a.2.** El sistema registra el evento “Fallo al agregar el servicio de sellado de tiempo” en el registro de auditoría.
 - **6a.3.** El administrador de CS selecciona volver a insertar la URL. El caso de uso continúa desde el paso 5.
 - **6a.3a.** El administrador de CS selecciona terminar el caso de uso.
- **7a.** Ya existe un servicio de sellado de tiempo aprobado con la URL y el certificado insertados.
 - **7a.1.** El sistema muestra el mensaje de error: “Ya existe un servicio de sellado de tiempo aprobado con la URL y el certificado insertados.”
 - **7a.2.** El sistema registra el evento “Fallo al agregar el servicio de sellado de tiempo” en el registro de auditoría.
 - **7a.3.** El administrador de CS selecciona volver a insertar la URL. El caso de uso continúa desde el paso 5.
 - **7a.3a.** El administrador de CS selecciona volver a seleccionar y cargar el archivo del certificado. El caso de uso continúa desde el paso 4.
 - **7a.3b.** El administrador de CS selecciona terminar el caso de uso.

UC TRUST_17: Editar la URL de un Servidor de Sellado de Tiempo

Sistema: Servidor central

Nivel: Tarea de usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS edita la URL de un servidor de sellado de tiempo.

Precondiciones: -

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

Desencadenante: La URL en la que se está proporcionando el servicio de sellado de tiempo ha cambiado.

Escenario principal de éxito:

1. El administrador de CS selecciona editar la URL de un servidor de sellado de tiempo.
2. El administrador de CS inserta la URL.
3. El sistema analiza la entrada del usuario: **3.20**.
4. El sistema verifica que la URL insertada esté en el formato correcto.

5. El sistema guarda la URL del servicio de sellado de tiempo, reemplazando el valor anterior.
6. El sistema registra el evento “Editar servicio de sellado de tiempo” en el registro de auditoría.

Extensiones:

- **3a.** El análisis de la entrada del usuario terminó 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 “Fallo al editar el servicio de sellado de tiempo” en el registro de auditoría.
 - **3a.3.** El administrador de CS selecciona volver a insertar la URL. El caso de uso continúa desde el paso 3.
 - **3a.3a.** El administrador de CS selecciona terminar el caso de uso.
- **4a.** La URL está malformada.
 - **4a.1.** El sistema muestra el mensaje de error: “La URL del servidor de sellado de tiempo 'X' es una URL inválida, ejemplos de URL válidas: '<http://www.example.com>', '<https://www.example.com>”, donde "X" es la URL insertada.
 - **4a.2.** El sistema registra el evento “Fallo al editar el servicio de sellado de tiempo” en el registro de auditoría.
 - **4a.3.** El administrador de CS selecciona volver a insertar la URL. El caso de uso continúa desde el paso 3.
 - **4a.3a.** El administrador de CS selecciona terminar el caso de uso.

UC TRUST_18: Eliminar un Servicio de Sellado de Tiempo Aprobado

Sistema: Servidor central

Nivel: Tarea de usuario

Componente: Servidor central

Actor: Administrador de CS

Descripción breve: El administrador de CS elimina un servicio de sellado de tiempo aprobado.

Precondiciones: -

Postcondiciones: -

Desencadenante: Se necesita eliminar un servicio de sellado de tiempo aprobado de la configuración del sistema.

Escenario principal de éxito:

1. El administrador de CS selecciona eliminar un servicio de sellado de tiempo aprobado.
2. El sistema solicita confirmación.
3. El administrador de CS confirma.
4. El sistema elimina la información del servicio de sellado de tiempo aprobado de la configuración del sistema.

5. El sistema registra el evento “Eliminar servicio de sellado de tiempo” en el registro de auditoría.

Extensiones:

- **3a.** El administrador de CS selecciona no eliminar el servicio de sellado de tiempo aprobado y termina el caso de uso.

UC TRUST_19: Analizar la Entrada del Usuario

Sistema: Servidor central

Nivel: Subfunción

Componente: Servidor central

Actores: -

Descripción breve: El sistema elimina los espacios en blanco al principio y al final de la entrada del usuario y verifica que los campos requeridos no estén vacíos.

Precondiciones: -

Postcondiciones: -

Desencadenantes:

- Paso 6 de **3.9**.
- Paso 3 de **3.10**.
- Paso 5 de **3.11**.
- Paso 5 de **3.17**.
- Paso 3 de **3.18**.

Escenario principal de éxito:

1. El sistema elimina los espacios en blanco al principio y al final.
2. El sistema verifica que los campos obligatorios estén llenos.
3. El sistema verifica que la entrada del usuario no exceda los 255 caracteres.

Extensiones:

- **2a.** Uno o más campos obligatorios no están llenos.
 - **2a.1.** El caso de uso termina con el mensaje de error “Parámetro faltante: 'X'”, donde “X” es el nombre del parámetro faltante.
- **3a.** La entrada del usuario excede los 255 símbolos.
 - **3a.1.** El caso de uso termina con el mensaje de error “La entrada del parámetro X excede los 255 caracteres”, donde “X” es el nombre del parámetro que tiene más de 255 caracteres insertados.