

Casos de Uso

Member

Communication

Índice

Introducción	3
Propósito	3
Visión General	3
Modelo de Casos de Uso	3
Actores.....	4
UC MESS_01: Llamada al servicio X-Road.....	6
UC MESS_02: Procesar solicitud SOAP X-Road	7
UC MESS_03: Procesar mensaje de solicitud X-Road.....	11
UC MESS_04: Verificar mensaje SOAP	16
UC MESS_05: Iniciar una conexión segura.....	18
UC MESS_06: Establecer la conexión segura.....	19
UC MESS_07: Verificar el certificado de autenticación.....	20
UC MESS_08: Crear Firma	22
UC MESS_09: Registrar Mensaje y Firma en el Registro de Mensajes.....	23
UC MESS_10: Estampillar Registros de Log de Mensajes.....	24
UC MESS_11: Verificar la Firma.....	25
UC MESS_12: Verificar la Cadena de Certificados	27
UC MESS_13: Validar una Respuesta OCSP	28
UC MESS_14: Obtener Respuestas OCSP.....	30
UC MESS_15: Obtener y Verificar Respuesta OCSP	31
UC MESS_16: Almacenar Datos de Monitoreo Operacional y Enviar los Datos al	
Anexo A: Diagrama de Secuencia para Mensajería.....	36

Introducción

Propósito

El propósito de este documento es describir los eventos y verificaciones que tienen lugar en los servidores de seguridad durante la comunicación entre un cliente de servicio de X-Road y un proveedor de servicio de X-Road.

Visión General

Los servicios de X-Road son utilizados por los miembros de X-Road que se comunican directamente entre sí a través de los servidores de seguridad, utilizando un patrón de mensajería sincrónico de solicitud-respuesta.

Los servidores de seguridad descargan periódicamente la configuración global desde el servidor central. La configuración global se utiliza para verificar la validez de varios elementos de datos, tales como certificados, respuestas OCSP y sellos de tiempo. Además, la configuración global se usa para verificar que las partes que se comunican están registradas en X-Road.

Los servidores de seguridad aseguran la integridad y la confidencialidad de los mensajes intercambiados firmando los mensajes con la clave de firma del miembro de X-Road y utilizando un canal de Seguridad de Capa de Transporte (TLS) mutuamente autenticado para el transporte. El valor evidencial a largo plazo de los mensajes firmados se asegura mediante el registro de los mensajes intercambiados y la creación periódica de sellos de tiempo en los registros de mensajes.

Los servidores de seguridad interactúan con servicios de confianza para obtener información de validez de los certificados y para sellar de tiempo los mensajes firmados. Las llamadas a los servicios de confianza son asincrónicas con respecto al intercambio de mensajes.

Los servidores de seguridad almacenan datos de monitoreo operativo en un búfer de monitoreo operativo y reenvían los datos al demonio de monitoreo operativo.

El proceso de comunicación entre un cliente de servicio de X-Road y un proveedor de servicio de X-Road se describe detalladamente como casos de uso en el Capítulo 3.

Los pasos generales del proceso de comunicación, excluyendo las acciones que son asincrónicas al proceso de intercambio de mensajes, se representan como un diagrama de secuencia en el Anexo A.

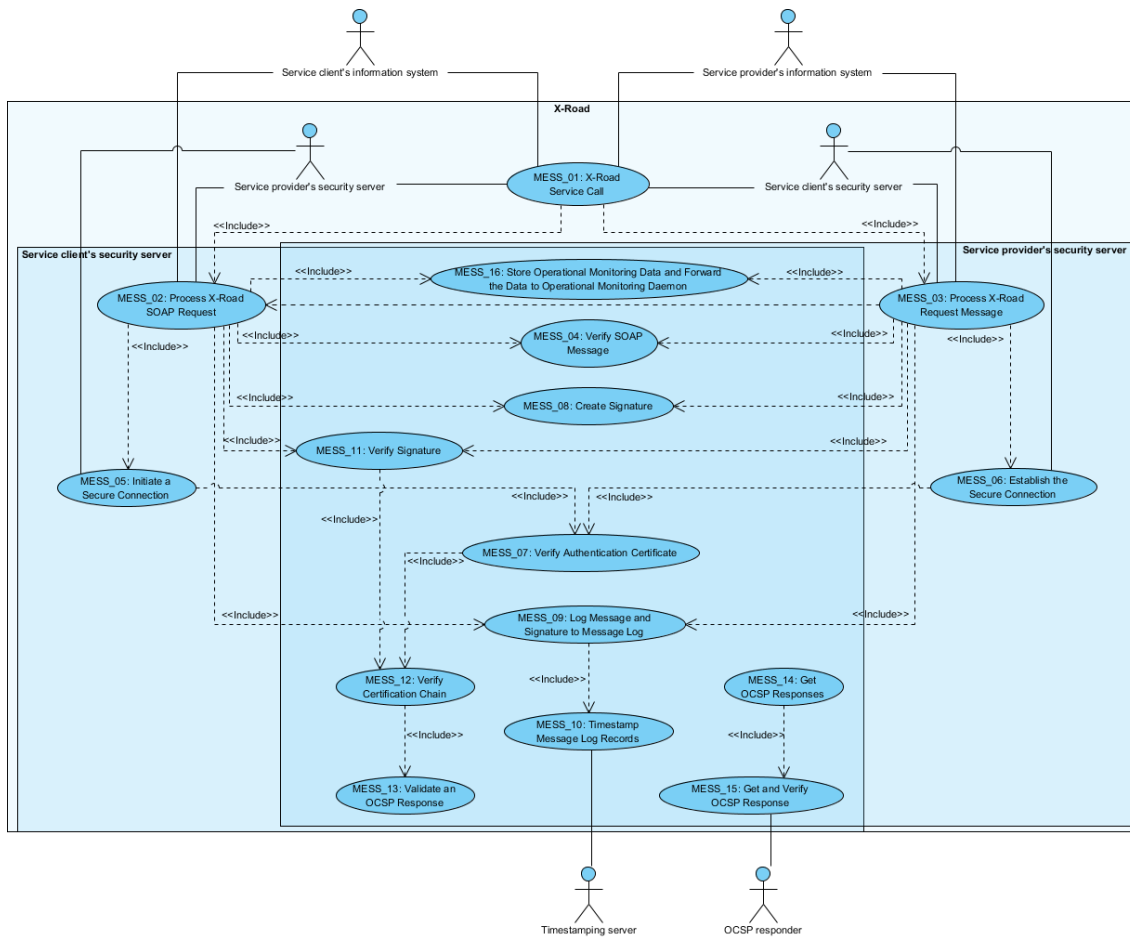
Modelo de Casos de Uso

Actores

El modelo de casos de uso de comunicación de miembros de X-Road incluye los siguientes actores:

- **Cliente IS** (sistema de información del cliente de servicio) – un subsistema de un miembro de X-Road que actúa como cliente de servicio en un evento de llamada a servicio de X-Road.
- **Cliente SS** (servidor de seguridad del cliente de servicio) – servidor de seguridad de X-Road donde el sistema de información del cliente de servicio está registrado como cliente de este servidor de seguridad.
- **Proveedor IS** (sistema de información del proveedor de servicio) – un subsistema de un miembro de X-Road que actúa como proveedor de servicio en un evento de llamada a servicio de X-Road.
- **Proveedor SS** (servidor de seguridad del proveedor de servicio) – servidor de seguridad de X-Road donde el sistema de información del proveedor de servicio está registrado como cliente de este servidor de seguridad.
- **TSS** (servidor de sellado de tiempo) – un servicio de sellado de tiempo aprobado por X-Road y configurado para ser utilizado por el Cliente SS y el Proveedor SS.
- **Respondedor OCSP** – servicio OCSP que proporciona respuestas OCSP para el servicio de certificación aprobado que emitió los certificados utilizados por el Cliente SS y el Proveedor SS.

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



UC MESS_01: Llamada al servicio X-Road

Sistema: X-Road

Nivel: Resumen

Componente: Servidor de seguridad

Actores:

- Client IS
- Client SS
- Provider SS
- Provider IS

Descripción breve: Un cliente de servicio inicia una llamada al servicio y recibe una respuesta. Tanto la solicitud como la respuesta son procesadas por los servidores de seguridad del cliente de servicio y del proveedor de servicio.

Precondiciones:

- El proveedor de servicio y el cliente de servicio están afiliados a X-Road.
- El proveedor de servicio y el cliente de servicio han firmado un contrato de uso del servicio.
- El proveedor de servicio y el cliente de servicio han integrado sus sistemas de información como subsistemas al sistema X-Road.
- El servidor de seguridad del cliente de servicio está en funcionamiento y puede recibir mensajes.

Postcondición: El sistema de información del cliente de servicio ha recibido una respuesta de servicio o un mensaje de error SOAP (SOAP Fault).

Desencadenante: El sistema de información del cliente de servicio inicia una llamada al servicio X-Road.

Escenario de éxito principal:

1. Client IS forma y envía una solicitud SOAP X-Road al Client SS.
2. Client SS procesa la solicitud SOAP X-Road y la reenvía como mensaje de solicitud X-Road al Provider SS: 3.3 (pasos 1-14).
3. Provider SS procesa el mensaje de solicitud X-Road y lo reenvía como solicitud SOAP X-Road al Provider IS: 3.4 (pasos 1-14).
4. Provider IS procesa la solicitud recibida, forma una respuesta SOAP X-Road y envía la respuesta al Provider SS.
5. Provider SS procesa la respuesta SOAP X-Road y la reenvía como mensaje de respuesta X-Road al Client SS: 3.4 (pasos 15-20).
6. Client SS procesa el mensaje de respuesta X-Road y lo reenvía como respuesta SOAP X-Road al Client IS: 3.3 (pasos 15-22).
7. Client IS recibe y procesa la respuesta.

Extensiones:

2-6a. El procesamiento o reenvío del mensaje resulta en un error. Client IS recibe un mensaje de error SOAP Fault. El caso de uso termina.

UC MESS_02: Procesar solicitud SOAP X-Road

Sistema: Servidor de seguridad del cliente de servicio

Nivel: Sistema

Componente: Servidor de seguridad

Actores:

- Client IS
- Provider SS

Descripción breve: El sistema recibe un mensaje de solicitud de Client IS; verifica que la configuración del sistema permita el intercambio de mensajes X-Road y que la composición del mensaje de solicitud cumpla con el protocolo de mensajes X-Road; establece una sesión de conexión segura con Provider SS; firma el mensaje de solicitud; registra el mensaje de solicitud y la firma; envía el mensaje de solicitud y la firma a Provider SS y espera la respuesta. Después de recibir la respuesta de Provider SS, el sistema valida la composición del mensaje y la firma; registra el mensaje de respuesta y la firma y envía la respuesta al Client IS. Si ocurre un error de verificación o validación, el sistema envía un mensaje de error (SOAP Fault) a Client IS.

Precondiciones:

- El servidor de seguridad del cliente de servicio está en funcionamiento y puede recibir mensajes.

Postcondiciones: -

Desencadenante: Client IS envía una solicitud al sistema.

Escenario de éxito principal:

1. El sistema recibe la solicitud y verifica que la solicitud se haya enviado utilizando el método POST.
2. El sistema verifica que la configuración del sistema contenga una configuración global válida.
3. El sistema verifica que la configuración del sistema contenga un certificado de autenticación que pueda usarse para intercambiar mensajes con otro servidor de seguridad (el certificado debe estar activo y válido).
4. El sistema verifica que la solicitud contenga un mensaje SOAP y verifica el mensaje SOAP: 3.5.
5. El sistema verifica que el encabezado de la solicitud SOAP contenga el identificador de servicio X-Road.

6. El sistema verifica que el Client IS esté en estado Registrado en la configuración del sistema.
7. El sistema verifica que el tipo de comunicación para el Client IS en la configuración del sistema esté configurado como "HTTPS" y que el Client IS haya realizado la conexión para enviar la solicitud utilizando el protocolo HTTPS.
8. El sistema verifica que el Client IS haya proporcionado un certificado TLS que coincida con un certificado guardado para Client IS en la configuración del sistema.
9. El sistema busca las direcciones de Provider SS en la configuración global.
10. El sistema prepara la información de autenticación que se enviará a Provider SS mientras se establece la conexión segura.
11. El sistema verifica que no existan sesiones de comunicación en caché con las direcciones encontradas e inicia una conexión segura con el servidor más rápido: 3.6.
12. El sistema firma el mensaje de solicitud: 3.9.
13. El sistema registra el mensaje de solicitud y la firma en el registro de mensajes: 3.10.
14. El sistema envía la solicitud firmada y las respuestas OCSP necesarias para verificar el certificado de autenticación a Provider SS y espera la respuesta.
15. El sistema recibe una respuesta de Provider SS y analiza la respuesta para verificar que las partes del mensaje estén bien formadas.
16. El sistema verifica que la respuesta no sea un mensaje de error SOAP Fault.
17. El sistema verifica que la respuesta contenga un mensaje SOAP y una firma.
18. El sistema verifica la firma: 3.12.
19. El sistema verifica que los encabezados de la respuesta SOAP sean consistentes con los encabezados de la solicitud SOAP.
20. El sistema verifica que el hash del mensaje de solicitud esté incluido en la respuesta y que el hash coincida con el mensaje de solicitud.
21. El sistema registra el mensaje de respuesta y la firma en el registro de mensajes: 3.10.
22. El sistema almacena los datos de monitoreo operativo en el búfer de monitoreo operativo: 3.17.
23. El sistema envía el mensaje de respuesta a Client IS.

Extensiones:

- 1a. La solicitud se envió utilizando un método diferente a POST.
 - 1a.1. El sistema envía un mensaje SOAP Fault con la cadena de error "Must use POST request method instead of X" (donde "X" es el método utilizado) a Client IS. El caso de uso termina.
- 2a. La configuración global ha expirado.
 - 2a.1. El sistema envía un mensaje SOAP Fault con la cadena de error "Global configuration is expired" a Client IS. El caso de uso termina.
- 3a. El servidor de seguridad no tiene certificados de autenticación utilizables.
 - 3a.1. El sistema envía un mensaje SOAP Fault con la cadena de error "Security server has no valid authentication certificate" a Client IS. El caso de uso termina.
- 4a. La solicitud no contiene un mensaje SOAP.
 - 4a.1. El sistema envía un mensaje SOAP Fault con la cadena de error "Request does not contain SOAP message" a Client IS. El caso de uso termina.
- 4b. El proceso de validación termina con un mensaje de excepción.
 - 4b.1. El sistema envía un mensaje SOAP Fault con la cadena de error que contiene el mensaje de excepción a Client IS. El caso de uso termina.
- 6a. Client IS no está en estado Registrado.
 - 6a.1. El sistema envía un mensaje SOAP Fault con la cadena de error "Client 'X' not

found” (donde “X” es el identificador X-Road de Client IS) a Client IS. El caso de uso termina.

7a. El tipo de conexión de Client IS en la configuración del sistema es “HTTP” y Client IS ha realizado una conexión HTTP.

7a.1. El caso de uso continúa desde el paso 9.

7b. El tipo de conexión de Client IS en la configuración del sistema es “HTTP”, pero Client IS ha realizado una conexión HTTPS.

7b.1. El caso de uso continúa desde el paso 9.

7c. El tipo de conexión de Client IS en la configuración del sistema es “HTTPS NO AUTH”, pero Client IS ha realizado una conexión HTTP.

7c.1. El sistema envía un mensaje SOAP Fault con la cadena de error “Client (X) specifies HTTPS NO AUTH but client made plaintext connection” (donde “X” es el identificador X-Road de Client IS) a Client IS. El caso de uso termina.

7d. El tipo de conexión de Client IS en la configuración del sistema es “HTTPS”, pero Client IS ha realizado una conexión HTTP.

7d.1. El sistema envía un mensaje SOAP Fault con la cadena de error “Client (X) specifies HTTPS but did not supply TLS certificate” (donde “X” es el identificador X-Road de Client IS) a Client IS. El caso de uso termina.

8a. No se encuentran certificados TLS para Client IS en la configuración del sistema.

8a.1. El sistema envía un mensaje SOAP Fault con la cadena de error “Client (X) has no IS certificates” (donde “X” es el identificador X-Road de Client IS) a Client IS. El caso de uso termina.

8b. No se encuentran certificados TLS correspondientes para Client IS en la configuración del sistema.

8b.1. El sistema envía un mensaje SOAP Fault con la cadena de error “Client (X) TLS certificate does not match any IS certificates” (donde “X” es el identificador X-Road de Client IS) a Client IS. El caso de uso termina.

9a. No se encuentran direcciones de Provider SS para el servicio solicitado.

9a.1. El sistema envía un mensaje SOAP Fault con la cadena de error “Could not find addresses for service provider ‘X’” (donde “X” es el identificador X-Road del proveedor de servicio) a Client IS. El caso de uso termina.

10a. El sistema no puede encontrar una clave de autenticación que se pueda usar para establecer una conexión segura.

10a.1. El sistema envía un mensaje SOAP Fault con la cadena de error “Could not find active authentication key for security server ‘X’” (donde “X” es el identificador del servidor de seguridad) a Client IS. El caso de uso termina.

11a. El sistema encuentra una sesión en caché con uno de los servidores de seguridad encontrados.

11a.1. El sistema reutiliza la información de la sesión en caché para establecer la conexión: 3.6 desde el paso 3.

11a.1a. El proceso de iniciar una conexión segura utilizando la información de la sesión en caché termina con un mensaje de excepción.

11a.1a.1. El sistema envía un mensaje SOAP Fault con la cadena de error que contiene el mensaje de excepción a Client IS. El caso de uso termina.

11a.2. El caso de uso continúa desde el paso 12.

11b. El proceso de iniciar una conexión segura termina con un mensaje de excepción.

11b.1. El sistema envía un mensaje SOAP Fault con la cadena de error que contiene el mensaje de excepción a Client IS. El caso de uso termina.

11c. El sistema no pudo iniciar contacto con ninguna de las direcciones de Provider SS encontradas.

11c.1. El sistema envía un mensaje SOAP Fault con la cadena de error “Could not connect to any target host (X)” (donde X es la lista de direcciones de Provider SS) a Client IS. El caso de uso termina.

12a. El proceso de creación de la firma termina con un mensaje de excepción.

- 12a.1. El sistema envía un mensaje SOAP Fault con la cadena de error que contiene el mensaje de excepción a Client IS. El caso de uso termina.
- 13a. El proceso de registro termina con un mensaje de excepción.
- 13a.1. El sistema envía un mensaje SOAP Fault con la cadena de error que contiene el mensaje de excepción a Client IS. El caso de uso termina.
- 15a. El sistema no recibe una respuesta dentro del período de tiempo de espera establecido por el parámetro del sistema proxy.client-timeout.
- 15a.1. El sistema envía un mensaje SOAP Fault con los detalles del error a Client IS. El caso de uso termina.
- 15b. El análisis del mensaje de respuesta resultó en un error.
- 15b.1. El sistema envía un mensaje SOAP Fault con la cadena de error que contiene los detalles del error encontrado a Client IS. El caso de uso termina.
- 16a. La respuesta es un mensaje de error.
- 16a.1. El sistema envía un mensaje SOAP Fault con la cadena de error que contiene el mensaje de error recibido a Client IS. El caso de uso termina.
- 17a. La respuesta no contiene un mensaje SOAP.
- 17a.1. El sistema envía un mensaje SOAP Fault con la cadena de error "Response does not have SOAP message" a Client IS. El caso de uso termina.
- 17b. La respuesta no contiene una firma.
- 17b.1. El sistema envía un mensaje SOAP Fault con la cadena de error "Response does not have signature" a Client IS. El caso de uso termina.
- 18a. El proceso de verificación de la firma termina con un mensaje de excepción.
- 18a.1. El sistema envía un mensaje SOAP Fault con la cadena de error que contiene el mensaje de excepción a Client IS. El caso de uso termina.
- 19a. Los encabezados de la respuesta no son consistentes con los encabezados de la solicitud.
- 19a.1. El sistema envía un mensaje SOAP Fault con la cadena de error "Response from server proxy is not consistent with request" a Client IS. El caso de uso termina.
- 20a. El hash del mensaje de solicitud contenido en la respuesta no coincide con el mensaje de solicitud.
- 20a.1. El sistema envía un mensaje SOAP Fault con la cadena de error "Request message hash does not match request message" a Client IS. El caso de uso termina.
- 20b. La respuesta no contiene el hash del mensaje de solicitud.
- 20b.1. El sistema envía un mensaje SOAP Fault con la cadena de error "Response from server proxy is missing request message hash" a Client IS. El caso de uso termina.
- 21a. El proceso de registro termina con un mensaje de excepción.
- 21a.1. El sistema envía un mensaje SOAP Fault con la cadena de error que contiene el mensaje de excepción a Client IS. El caso de uso termina.
- 22a. El tamaño del búfer de monitoreo operativo definido con un parámetro del sistema es 0.
- 22a.1. Los datos de monitoreo operativo no se almacenan en el búfer de monitoreo operativo y no se enviarán al demonio de monitoreo operativo.

Aquí tienes la traducción al español del texto, con las palabras antes de los dos puntos en **negrita**:

UC MESS_03: Procesar mensaje de solicitud X-Road

Sistema: Servidor de seguridad del proveedor de servicios

Nivel: Sistema

Componente: Servidor de seguridad

Actores:

- Cliente SS
- Proveedor IS

Descripción breve:

El sistema recibe una solicitud de comunicación del Cliente SS; verifica que la configuración del sistema permita el intercambio de mensajes X-Road; establece una sesión de conexión segura con el Cliente SS; recibe la solicitud del servicio X-Road; verifica la firma de la solicitud; registra el mensaje de la solicitud y su firma en el registro de mensajes; reenvía el mensaje de la solicitud al Proveedor IS o al demonio de monitoreo operativo (si la solicitud es de datos de monitoreo operativo o de salud del servidor de seguridad) y espera la respuesta. Al recibir la respuesta del Proveedor IS, el sistema verifica que la composición del mensaje de respuesta cumpla con el protocolo de mensajes X-Road; firma el mensaje de respuesta; registra el mensaje de respuesta y su firma en el registro de mensajes y reenvía el mensaje y la firma al Cliente SS. En caso de que falle una verificación o validación o si el sistema encuentra una condición de error, el sistema envía un mensaje de error SOAP Fault al Cliente SS.

Precondiciones:

El servidor de seguridad del proveedor de servicios está en funcionamiento y es capaz de recibir mensajes.

Postcondiciones:

Disparador:

El servidor de seguridad del cliente de servicio envía una solicitud de servicio X-Road al servidor de seguridad del proveedor de servicios.

Escenario de éxito principal:

1. El sistema recibe la solicitud y verifica que la solicitud se haya enviado utilizando el método POST.
2. El sistema verifica que la configuración del sistema contenga una configuración global válida.
3. El sistema verifica que el Proveedor IS esté en estado Registrado en la configuración del sistema.
4. El sistema encuentra la información de firma para el proveedor de servicios. (El sistema no acepta la solicitud si no es posible firmar la respuesta respectiva.)
5. El sistema establece la conexión segura iniciada por el Cliente SS: 3.7.

6. El sistema analiza la solicitud para verificar que las partes del mensaje estén bien formadas.
7. El sistema verifica que la solicitud no contenga un mensaje SOAP Fault.
8. El sistema verifica que la solicitud contenga un mensaje SOAP y una firma.
9. El sistema verifica que el servicio solicitado esté configurado en el sistema, permitido para el sistema de información solicitante y habilitado.
10. El sistema verifica la firma: 3.12.
11. El sistema registra el mensaje de la solicitud y la firma en el registro de mensajes: 3.10.
12. El sistema busca la dirección del Proveedor IS en la configuración del sistema.
13. El sistema verifica que el Proveedor IS deba conectarse utilizando el protocolo HTTP. El sistema inicia una conexión con el Proveedor IS.
14. El sistema envía la solicitud y espera la respuesta.
15. El sistema recibe una respuesta del Proveedor IS o del demonio de monitoreo operativo y verifica el mensaje SOAP: 3.5.
16. El sistema verifica que la respuesta no sea un mensaje SOAP Fault.
17. El sistema agrega el hash del mensaje de solicitud al encabezado del mensaje de respuesta.
18. El sistema firma el mensaje de respuesta: 3.9.
19. El sistema registra el mensaje de respuesta y su firma en el registro de mensajes: 3.10.
20. El sistema almacena los datos de monitoreo operativo en el búfer de monitoreo operativo: 3.17.
21. El sistema envía el mensaje de respuesta al Cliente SS.

Extensiones:

1a. La solicitud se envió utilizando un método distinto a POST.

1a1. El sistema envía un mensaje SOAP Fault con el mensaje de error “Debe usar el método POST en lugar de X” (donde “X” es el método utilizado) al Cliente SS. El caso de uso termina.

2a. La configuración global ha expirado.

2a1. El sistema envía un mensaje SOAP Fault con el mensaje de error “La configuración global ha expirado” al Cliente SS. El caso de uso termina.

3a. El sistema de información del cliente no está en estado Registrado.

3a1. El sistema envía un mensaje SOAP Fault con el mensaje de error “Cliente 'X' no encontrado” (donde “X” es el identificador X-Road del sistema de información del proveedor) al Cliente SS. El caso de uso termina.

4a. El sistema no pudo encontrar la información de firma para el miembro X-Road.

4a1. El sistema envía un mensaje SOAP Fault con el mensaje de error “No se pudo obtener la información de firma para el miembro 'X': Y” (donde “X” es el identificador del miembro X-Road y “Y” es la descripción del error encontrado) al Cliente SS. El caso de uso termina.

5a. El establecimiento del canal seguro termina con un mensaje de excepción.

5a1. El sistema envía un mensaje SOAP Fault con el mensaje de error que contiene los detalles de la excepción al Cliente SS. El caso de uso termina.

6a. El análisis del mensaje de solicitud resultó en un error.

6a1. El sistema envía un mensaje SOAP Fault con el mensaje de error que contiene los detalles del error encontrado al Cliente SS. El caso de uso termina.

7a. La solicitud contiene un mensaje de error.

7a1. El sistema descarta el mensaje recibido. El caso de uso termina.

8a. La solicitud no contiene un mensaje SOAP.

8a1. El sistema envía un mensaje SOAP Fault con el mensaje de error “La solicitud no tiene mensaje SOAP” al Cliente SS. El caso de uso termina.

8b. La solicitud no contiene una firma.

8b1. El sistema envía un mensaje SOAP Fault con el mensaje de error “La solicitud no tiene firma” al Cliente SS. El caso de uso termina.

9a. El servicio solicitado no se encuentra en la configuración del sistema.

9a1. El sistema envía un mensaje SOAP Fault con el mensaje de error “Servicio desconocido: X” (donde “X” es el identificador X-Road del servicio solicitado) al Cliente SS. El caso de uso termina.

9b. El sistema de información solicitante no tiene derechos de acceso para el servicio solicitado.

9b1. El sistema envía un mensaje SOAP Fault con el mensaje de error “La solicitud no está permitida: X” (donde “X” es el identificador X-Road del servicio solicitado) al Cliente SS. El caso de uso termina.

9c. El servicio solicitado está deshabilitado.

9c1. El sistema envía un mensaje SOAP Fault con el mensaje de error “Servicio X está deshabilitado: Y” (donde “X” es el identificador X-Road del servicio solicitado y “Y” es un mensaje de notificación ingresado por la persona que deshabilitó el servicio) al Cliente SS. El caso de uso termina.

10a. El proceso de verificación de la firma termina con un mensaje de excepción.

10a1. El sistema envía un mensaje SOAP Fault con el mensaje de error que contiene los detalles de la excepción al Cliente SS. El caso de uso termina.

11a. El proceso de registro termina con un mensaje de excepción.

11a1. El sistema envía un mensaje SOAP Fault con el mensaje de error que contiene los detalles de la excepción al Cliente SS. El caso de uso termina.

12a. El sistema no puede encontrar la dirección del Proveedor IS en la configuración del sistema.

12a1. El sistema envía un mensaje SOAP Fault con el mensaje de error “Dirección de servicio no especificada para 'X'” (donde “X” es el identificador X-Road del servicio solicitado) al Cliente SS. El caso de uso termina.

12b. La dirección del sistema de información del proveedor encontrada en la configuración del sistema está malformada.

12b1. El sistema envía un mensaje SOAP Fault con el mensaje de error “Dirección del servicio malformada 'X': Y” (donde “X” es el identificador X-Road del servicio solicitado y “Y” es un mensaje de excepción) al Cliente SS. El caso de uso termina.

12c. La solicitud es una solicitud de datos de monitoreo operativo o de salud del servidor de seguridad. El sistema busca la dirección del demonio de monitoreo operativo desde el archivo de configuración del demonio de monitoreo operativo.

12c1. El caso de uso continúa desde el paso 13.

12c.1a. La dirección del demonio de monitoreo operativo encontrada en el archivo de configuración está malformada.

12c.1a1. El sistema envía un mensaje SOAP Fault con el mensaje de error al Cliente SS. El caso de uso termina.

13a. El sistema no pudo iniciar una conexión con el Proveedor IS.

13a1. El sistema envía un mensaje SOAP Fault con el mensaje de error que contiene los detalles del error al Cliente SS. El caso de uso termina.

13b. El Proveedor IS debería conectarse utilizando HTTPS y no se debe verificar el certificado del Proveedor IS.

13b1. El sistema encuentra el certificado TLS del Proveedor IS desde la conexión, pero no verifica el certificado. El caso de uso continúa desde el paso 14.

13b.1a. El sistema no pudo encontrar el certificado TLS.

13b.1a1. El sistema envía un mensaje SOAP Fault con el mensaje de error “No se pudieron obtener los certificados del par” al Cliente SS. El caso de uso termina.

13c. El Proveedor IS debería conectarse utilizando HTTPS y se debe verificar el certificado del Proveedor IS.

13c.1. El sistema encuentra el certificado TLS del Proveedor IS desde la conexión.

13c.1a. El sistema no pudo encontrar el certificado TLS.

13c.1a1. El sistema envía un mensaje SOAP Fault con el mensaje de error “No se pudieron obtener los certificados del par” al Cliente SS. El caso de uso termina.

13c.2. El sistema verifica que el certificado TLS enviado por el Proveedor IS coincida con uno de los certificados TLS configurados para el Proveedor IS en la configuración del sistema. El caso de uso continúa desde el paso 14.

13c.2a. El sistema no encuentra ningún certificado TLS para el Proveedor IS en la configuración del sistema.

13c.2a1. El sistema envía un mensaje SOAP Fault con el mensaje de error “Cliente 'X' no tiene certificados IS” (donde “X” es el identificador del Proveedor IS) al Cliente SS. El caso de uso termina.

13c.2b. Ninguno de los certificados TLS configurados para el Proveedor IS coincide con el certificado que el Proveedor IS presentó para la autenticación TLS.

13c.2b1. El sistema envía un mensaje SOAP Fault con el mensaje de error “El certificado del servidor no es de confianza” al Cliente SS. El caso de uso termina.

13d. La solicitud es una solicitud de datos de monitoreo operativo o de salud del servidor de seguridad. El sistema verifica que el demonio de monitoreo operativo debería conectarse utilizando el protocolo HTTP. El sistema inicia una conexión con el demonio de monitoreo operativo.

13d1. El caso de uso continúa desde el paso 14.

13d.1a. El sistema no pudo iniciar una conexión con el demonio de monitoreo operativo.

13d.1a1. El sistema envía un mensaje SOAP Fault con el mensaje de error que contiene los detalles del error al Cliente SS. El caso de uso termina.

13e. La solicitud es una solicitud de datos de monitoreo operativo o de salud del servidor de seguridad. El sistema verifica que el demonio de monitoreo operativo debería conectarse utilizando HTTPS y que se debe verificar el certificado del demonio de monitoreo operativo.

13e.1. El sistema usa el certificado TLS interno del servidor de seguridad para la conexión.

13e.2. El sistema encuentra el certificado TLS del demonio de monitoreo operativo en la conexión.

13e.2a. El sistema no pudo encontrar el certificado TLS.

13e.2a1. El sistema envía un mensaje SOAP Fault con el mensaje de error al Cliente SS. El caso de uso termina.

13e.3. El sistema verifica que el certificado TLS enviado por el demonio de monitoreo operativo coincida con el certificado TLS configurado para el demonio de monitoreo operativo en la configuración del sistema. El caso de uso continúa desde el paso 14.

13e.3a. El sistema no encuentra un certificado TLS para el demonio de monitoreo operativo en la configuración del sistema.

13e.3a1. El sistema envía un mensaje SOAP Fault con el mensaje de error al Cliente SS. El caso de uso termina.

13e.3b. El certificado TLS configurado para el demonio de monitoreo operativo no coincide con el certificado que el demonio de monitoreo operativo presentó para la autenticación TLS.

13e.3b1. El sistema envía un mensaje SOAP Fault con el mensaje de error al Cliente SS. El caso de uso termina.

14a. El sistema no recibe una respuesta dentro del período de tiempo configurado para el servicio en la configuración del sistema.

14a1. El sistema envía un mensaje SOAP Fault con los detalles del error al Cliente SS. El caso de uso termina.

15a. El proceso de validación termina con un mensaje de excepción.

15a1. El sistema envía un mensaje SOAP Fault con el mensaje de error que contiene los detalles de la excepción al Cliente SS. El caso de uso termina.

16a. La respuesta es un mensaje SOAP Fault.

16a1. El sistema envía un mensaje SOAP Fault con el mensaje de error que contiene el contenido del mensaje Fault recibido al Cliente SS. El caso de uso termina.

18a. El proceso de creación de la firma termina con un mensaje de excepción.

18a1. El sistema envía un mensaje SOAP Fault con el mensaje de error que contiene los detalles de la excepción al Cliente SS. El caso de uso termina.

19a. El proceso de registro termina con un mensaje de excepción.

19a1. El sistema envía un mensaje SOAP Fault con el mensaje de error que contiene los detalles de la excepción al Cliente SS. El caso de uso termina.

20a. El tamaño del búfer de monitoreo operativo definido con un parámetro del sistema es 0.

20a1. Los datos de monitoreo operativo no se almacenan en el búfer de monitoreo operativo y no se enviarán al demonio de monitoreo operativo.

UC MESS_04: Verificar mensaje SOAP

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actores: -

Descripción breve: El sistema verifica que el mensaje SOAP recibido de un sistema de información (IS Cliente o IS Proveedor) se ajuste al protocolo de mensajes de X-Road [PR-MESS].

Precondiciones: -

Postcondiciones: -

Disparadores:

Paso 4 de 3.3.

Paso 14 de 3.4.

Escenario principal de éxito:

El sistema verifica que el tipo de contenido base del mensaje sea **text/xml** o **multipart/related**.

El sistema verifica que el mensaje SOAP esté bien formado.

Extensiones:

- 1a. El sistema no puede obtener el tipo de contenido base del mensaje.
 - 1a.1. El sistema crea un mensaje de excepción: "No se pudo obtener el tipo de contenido de la solicitud". El caso de uso termina.
- 1b. El tipo de contenido base del mensaje no es **text/xml** ni **multipart/related**.
 - 1b.1. El sistema crea un mensaje de excepción: "Tipo de contenido inválido: X" (donde "X" es el tipo de contenido base). El caso de uso termina.
- 2a. El elemento **SOAP body** falta en el mensaje.
 - 2a.1. El sistema crea un mensaje de excepción: "Mensaje SOAP malformado: falta cuerpo". El caso de uso termina.
- 2b. La validación del sobre SOAP contra el esquema del sobre SOAP (<http://schemas.xmlsoap.org/soap/envelope/>) falla.
 - 2b.1. El sistema crea un mensaje de excepción que contiene el mensaje de error de validación. El caso de uso termina.
- 2c. El mensaje no es un **SOAP Fault** y el elemento **SOAP header** falta en el mensaje.
 - 2c.1. El sistema crea un mensaje de excepción: "Mensaje SOAP malformado: falta encabezado". El caso de uso termina.
- 2d. El mensaje no es un **SOAP Fault** y el encabezado del mensaje está vacío.
 - 2d.1. El sistema crea un mensaje de excepción: "El encabezado del mensaje debe contener el **service id**". El caso de uso termina.
- 2e. El mensaje no es un **SOAP Fault** y el **SOAP header** contiene campos duplicados.
 - 2e.1. El sistema crea un mensaje de excepción: "El encabezado SOAP contiene el campo duplicado 'X'" (donde "X" es el nombre del elemento de encabezado duplicado). El caso de uso termina.
- 2f. El mensaje contiene **adjuntos** y el sistema no puede obtener el tipo de contenido de una parte adjunta.

- 2f.1. El sistema crea un mensaje de excepción: “No se pudo obtener el tipo de contenido de la parte”. El caso de uso termina.
- 2g. El **objectType** del cliente de servicio es **MEMBER**, pero el **SOAP header** contiene el elemento **subsystemCode**.
- 2g.1. El sistema crea un mensaje de excepción: “Código de subsistema redundante”. El caso de uso termina.
- 2h. El **objectType** del cliente de servicio es **SUBSYSTEM**, pero el **SOAP header** no contiene el elemento **subsystemCode**.
- 2h.1. El sistema crea un mensaje de excepción: “Falta el código de subsistema requerido”. El caso de uso termina.
-

UC MESS_05: Iniciar una conexión segura

Sistema: Servidor de seguridad del cliente de servicio

Nivel: Subfunción

Componente: Servidor de seguridad

Actor: Proveedor SS

Descripción breve: El sistema inicia una conexión segura con el **Proveedor SS** y valida la información de autenticación del **Proveedor SS**.

Precondiciones: -

Postcondiciones: -

Disparador: Paso 11 de 3.3.

Escenario principal de éxito:

El sistema inicia un apretón de manos **TLS** con el **Proveedor SS**.

El sistema intercambia la información de autenticación de sesión con el **Proveedor SS**.

El sistema obtiene el identificador del proveedor de servicios y el certificado de autenticación de la información de autenticación de la sesión.

El sistema verifica que el certificado de autenticación fue emitido por un proveedor de servicios de certificación aprobado y construye la cadena de certificados desde el certificado de autenticación hasta un certificado de autoridad de certificación confiable (**CA**).

El sistema encuentra que algunas de las respuestas **OCSP** necesarias para verificar la cadena de certificados no están en caché (de una sesión anterior). El sistema usa el certificado de autenticación y el enlace registrado entre el certificado de autenticación y el **Proveedor SS** para encontrar la dirección del **Proveedor SS** desde la

configuración global. El sistema envía una solicitud para las respuestas **OCSP** faltantes al **Proveedor SS**.

El sistema recibe y guarda en caché las respuestas **OCSP**.

El sistema verifica el certificado de autenticación: 3.8.

El sistema guarda en caché la información de la sesión.

Extensiones:

3a. El sistema no puede encontrar certificados utilizables en la información de autenticación de la sesión.

3a.1. El sistema crea un mensaje de excepción: “El proveedor de servicios no envió el certificado de autenticación correcto”. El caso de uso termina.

3b. El sistema no puede encontrar certificados en la información de autenticación de la sesión.

3b.1. El sistema crea un mensaje de excepción: “No se pudieron obtener los certificados del contexto”. El caso de uso termina.

4a. El emisor del certificado de autenticación no está listado como un servicio de certificación aprobado en la configuración global.

4a.1. El sistema crea un mensaje de excepción: “El certificado no fue emitido por un proveedor de servicios de certificación aprobado”. El caso de uso termina.

5a. El sistema no puede encontrar un enlace entre el **Proveedor SS** y el certificado de autenticación recibido del **Proveedor SS** en la configuración global (el certificado de autenticación no está registrado en el servidor central de X-Road como un certificado utilizado por el **Proveedor SS**).

5a.1. El sistema crea un mensaje de excepción: “No se puede encontrar la dirección del proveedor para el certificado de autenticación X (proveedor de servicios: Y)” (donde “X” es el número de serie del certificado de autenticación enviado por el **Proveedor SS** y “Y” es el identificador del proveedor de servicios). El caso de uso termina.

6a. El sistema no recibió todas las respuestas **OCSP** necesarias para verificar la cadena de certificados.

6a.1. El sistema crea un mensaje de excepción: “No se pudieron obtener todas las respuestas **OCSP** del servidor (se esperaban X, pero se recibieron Y)” (donde “X” es el número de certificados en la cadena de certificados y “Y” es el número de respuestas **OCSP** recibidas del **Proveedor SS**). El caso de uso termina.

7a. El proceso de verificación del certificado de autenticación termina con un mensaje de excepción.

7a.1. El caso de uso termina con el mensaje de excepción.

UC MESS_06: Establecer la conexión segura

Sistema: Servidor de seguridad del proveedor de servicios

Nivel: Subfunción

Componente: Servidor de seguridad

Actor: Cliente SS

Descripción breve: El sistema finaliza la configuración de la conexión segura iniciada por el **Cliente SS** validando la información de autenticación recibida del **Cliente SS**.

Precondiciones: El **Cliente SS** ha iniciado la conexión segura y el sistema ha recibido la información de validación del **Cliente SS**.

Postcondiciones: -

Disparador: Paso 5 de 3.4.

Escenario principal de éxito:

El sistema verifica que el mensaje de solicitud recibido del **Cliente SS** contiene respuestas **OCSP**.

El sistema verifica que el certificado de autenticación del **Cliente SS** fue emitido por un proveedor de servicios de certificación aprobado.

El sistema verifica el certificado de autenticación del **Cliente SS**: 3.8.

Extensiones:

1a. El sistema no puede encontrar la respuesta **OCSP** necesaria para verificar el certificado de autenticación.

1a.1. El sistema crea un mensaje de excepción: "No se puede verificar el certificado TLS, falta la respuesta **OCSP** correspondiente". El caso de uso termina.

2a. El emisor del certificado de autenticación no está listado como un servicio de certificación aprobado en la configuración global.

2a.1. El sistema crea un mensaje de excepción: "El certificado no fue emitido por un proveedor de servicios de certificación aprobado". El caso de uso termina.

3a. El proceso de verificación termina con un mensaje de excepción.

3a.1. El caso de uso termina con el mensaje de excepción.

UC MESS_07: Verificar el certificado de autenticación

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actores: -

Descripción breve: El sistema valida el certificado de autenticación y verifica que el servidor de seguridad remoto tiene derecho a usar el certificado de autenticación que presentó y que tiene derecho a enviar mensajes en nombre del cliente de servicio (si el

Proveedor SS realiza la verificación) o del proveedor de servicios (si el **Cliente SS** realiza la verificación).

Precondiciones: -

Postcondiciones: La validez del certificado de autenticación se verifica o refuta.

Disparadores:

Paso 7 de 3.6.

Paso 3 de 3.7.

Escenario principal de éxito:

El sistema verifica que el certificado es un certificado de autenticación (El certificado es un certificado de autenticación si tiene una extensión **ExtendedKeyUsage** que contiene **ClientAuthentication** o si tiene una extensión **keyUsage** que tiene los bits **digitalSignature**, **keyEncipherment** o **dataEncipherment** establecidos).

El sistema construye la cadena de certificados desde el certificado de autenticación hasta un certificado de autoridad de certificación confiable (**CA**).

El sistema verifica la cadena de certificados: 3.13.

El sistema verifica (usando la configuración global) que el certificado de autenticación está registrado para el servidor de seguridad que proporcionó el certificado de autenticación y que el servidor de seguridad tiene derecho a enviar mensajes en nombre del cliente de servicio/proveedor de servicios (el proveedor de servicios/cliente de servicio está registrado como cliente del servidor de seguridad).

Extensiones:

1a. El certificado no es un certificado de autenticación.

1a.1. El sistema crea un mensaje de excepción: "El certificado del par no es un certificado de autenticación". El caso de uso termina.

2a. El sistema no encuentra suficientes certificados para construir la cadena de certificados.

2a.1. El sistema crea un mensaje de excepción: "La cadena debe tener al menos el certificado del usuario y el certificado de la autoridad de certificación raíz". El caso de uso termina.

2b. El sistema encuentra un error mientras construye el camino de certificados desde el certificado de firma hasta el certificado raíz confiable.

2b.1. El sistema crea un mensaje de excepción que contiene los detalles del error encontrado. El caso de uso termina.

3a. El proceso de validación de la cadena de certificados termina con un mensaje de excepción.

3a.1. El caso de uso termina con el mensaje de excepción.

4a. El servidor de seguridad no tiene derecho a enviar mensajes en nombre del cliente de servicio/proveedor de servicios.

4a.1. El sistema crea un mensaje de excepción: "El cliente 'X' no está registrado en el servidor de seguridad Y" (donde "X" es el identificador del cliente de servicio o

proveedor de servicios y “Y” es el identificador del servidor de seguridad que proporcionó el certificado de autenticación). El caso de uso termina.

4b. El certificado de autenticación presentado no está registrado en el servidor central.

4b.1. El sistema crea un mensaje de excepción: “El certificado de autenticación X no está asociado con ningún servidor de seguridad” (donde “X” es el nombre del sujeto del certificado de autenticación). El caso de uso termina.

UC MESS_08: Crear Firma

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actores: -

Descripción breve: El sistema firma el mensaje utilizando la clave de firma y el certificado del cliente de servicio (en caso de que el Cliente SS cree la firma) o del proveedor de servicio (en caso de que el Proveedor SS cree la firma).

Precondiciones: -

Postcondiciones: -

Desencadenantes:

Paso 12 de 3.3.

Paso 18 de 3.4.

Escenario principal de éxito:

- El sistema encuentra la información de firma (clave, certificado, respuestas OCSP) para el miembro X-Road que envió el mensaje a firmar.
- El sistema crea la firma. Consulte los documentos “Perfil para Firma Digital de Alto Rendimiento” [HPDS] y “Uso de Hashing por Lotes para Firmar y Sello de Tiempo” [BATCH] para una descripción detallada de las firmas de X-Road.

Extensiones:

1a. El sistema no pudo encontrar la información de firma para el miembro de X-Road.

1a.1. El sistema crea un mensaje de excepción: “No se pudo obtener la información de firma para el miembro 'X': Y” (donde “X” es el identificador del miembro de X-Road y “Y” es la descripción del error encontrado). El caso de uso termina.

1b. El sistema no pudo encontrar ningún certificado de firma (activo, válido) para el miembro de X-Road.

1b.1. El sistema crea un mensaje de excepción: “No se pudo obtener la información de firma para el miembro 'X': El miembro 'X' no tiene certificados adecuados” (donde “X” es el identificador del miembro de X-Road). El caso de uso termina.

2a. El sistema no pudo construir la cadena de certificados para el certificado de firma.

2a.1. El sistema crea un mensaje de excepción: “Cadena de certificados vacía para el certificado X” (donde X es el número de serie del certificado). El caso de uso termina.

2b. El sistema no encontró una respuesta OCSP para uno o más certificados en la cadena de certificados.

2b.1. El sistema crea un mensaje de excepción: “No se pudieron obtener respuestas OCSP para los certificados (X)” (donde “X” es la lista de certificados). El caso de uso termina.

UC MESS_09: Registrar Mensaje y Firma en el Registro de Mensajes

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actores: -

Descripción breve: El sistema verifica que el registro esté permitido (si el tiempo de la última estampilla de tiempo exitosa es más antiguo que el especificado por la política de seguridad, entonces no se aceptan más mensajes en el registro de mensajes) y crea un registro de log que contiene el mensaje y la firma. Si el sistema está configurado para estampillar tiempos de manera síncrona, entonces el proceso de registro incluye la estampilla de tiempo del registro creado.

Precondiciones: -

Postcondiciones: -

Desencadenantes:

Pasos 13 y 21 de 3.3.

Pasos 11 y 19 de 3.4.

Escenario principal de éxito:

- El sistema verifica que al menos exista un servicio de estampillado de tiempo en la configuración del sistema.
- El sistema verifica que el estampillado de tiempo no ha fallado durante más tiempo que el período establecido por el parámetro del sistema del servidor de seguridad **acceptable-timestamp-failure-period**.
- El sistema crea un registro de log que consiste en el mensaje SOAP (los archivos adjuntos no se registran) y la firma y guarda el registro en el registro de mensajes.
- El sistema verifica que el registro de log debe ser estampillado sincrónicamente con el proceso de mensajería (si el parámetro del sistema del servidor de seguridad **timestamp-immediately** está configurado como verdadero).
- El sistema estampilla el registro del log: 3.11 del paso 2.

Extensiones:

1a. No se encuentran servicios de estampillado de tiempo en la configuración del sistema.

1a.1. El sistema crea un mensaje de excepción: "No se puede estampillar mensajes: no hay servicios de estampillado de tiempo configurados". El caso de uso termina.

2a. El estampillado de tiempo ha estado fallando durante más tiempo que el período permitido.

2a.1. El sistema crea un mensaje de excepción: "No se puede estampillar mensajes". El caso de uso termina.

3a. Crear o guardar el registro de log encuentra un error.

3a.1. El sistema crea un mensaje de excepción que contiene los detalles del error encontrado. El caso de uso termina.

4a. El parámetro del sistema del servidor de seguridad **timestamp-immediately** está configurado como falso.

4a.1. El sistema estampilla el registro de log de manera asíncrona, en el próximo momento en que el estampillado de tiempo sea activado por el temporizador definido por el parámetro del servidor central **timeStampingIntervalSeconds**. El caso de uso termina.

5a. El estampillado de tiempo termina con un mensaje de excepción.

5a.1. El caso de uso termina con el mensaje de excepción.

UC MESS_10: Estampillar Registros de Log de Mensajes

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actor: TSS

Descripción breve: El sistema encuentra registros de log que necesitan ser estampillados, crea una solicitud de estampillado de tiempo y la envía al TSS. Al recibir la respuesta del TSS, el sistema valida la respuesta y la registra en el registro de mensajes.

Precondiciones: -

Postcondiciones: -

Desencadenantes:

Paso 5 de 3.10 si el parámetro del servidor de seguridad **timestamp-immediately** está configurado como verdadero.

Temporizador definido por el parámetro del servidor central

timeStampingIntervalSeconds si el parámetro del servidor de seguridad **timestamp-immediately** está configurado como falso.

Escenario principal de éxito:

- El sistema verifica que existen registros de log de mensajes que necesitan ser estampillados.
- El sistema verifica que la configuración del sistema contiene una configuración global válida.
- El sistema consulta las direcciones de los servicios de estampillado de tiempo desde la configuración del sistema.
- El sistema crea la solicitud de estampillado de tiempo, la envía al primer servicio de estampillado de tiempo encontrado en la configuración del sistema y recibe la respuesta.
- El sistema lee la respuesta y verifica que la estampilla de tiempo fue concedida (el estado de la respuesta es **concedido** o **concedidoConModificaciones**).
- El sistema verifica que la respuesta corresponde a la solicitud.
- El sistema verifica que la estampilla de tiempo está firmada por una autoridad de estampillado de tiempo aprobada.
- El sistema crea un registro de estampillado de tiempo que contiene la estampilla de tiempo y guarda el registro de estampillado en la base de datos. El sistema asocia los registros de mensajes estampillados con el registro de estampillado.

Extensiones:

- 1a. No se encuentran registros de log de mensajes que necesiten estampillado.
- 1a.1. El caso de uso termina.
- 2a. La configuración global ha expirado.
- 2a.1. El sistema crea un mensaje de excepción: “La configuración global ha expirado”. El caso de uso termina.
- 3a. No se encuentran servicios de estampillado de tiempo en la configuración del sistema.
- 3a.1. El sistema crea un mensaje de excepción: “No se puede estampillar, no hay URLs de TSP configuradas”. El caso de uso termina.
- 4a. El sistema no pudo obtener una respuesta del servicio de estampillado de tiempo.
- 4a.1. El sistema envía la solicitud de estampillado al siguiente servicio de estampillado de tiempo encontrado en la configuración del sistema.
- 4a.1a. El sistema no pudo obtener una respuesta. El caso de uso continúa desde el paso 4a.1.
- 4a.1b. El sistema ha intentado y fallado en obtener una respuesta de todos los servicios de estampillado de tiempo listados en la configuración del sistema.
- 4a.1b.1. El sistema crea un mensaje de excepción: “No se pudo obtener estampilla de tiempo de ningún proveedor de estampillado de tiempo”. El caso de uso termina.
- 5a. El sistema no pudo leer la respuesta.
- 5a.1. El sistema crea un mensaje de excepción: “No se pudo leer la respuesta de estampillado de tiempo”. El caso de uso termina.
- 5b. No se concedió la estampilla de tiempo.
- 5b.1. El sistema crea un mensaje de excepción que contiene la información del estado de la respuesta. El caso de uso termina.
- 6a. La verificación resultó en un error (la respuesta no corresponde a la solicitud).
- 6a.1. El sistema crea un mensaje de excepción que contiene los detalles del error encontrado. El caso de uso termina.
- 7a. El sistema no encuentra el certificado de la autoridad de estampillado de tiempo en la lista de servicios de estampillado de tiempo aprobados.
- 7a.1. El sistema crea un mensaje de excepción: “No se pudo encontrar el certificado de TSP para el estampillado de tiempo”. El caso de uso termina.
- 7b. El sistema no pudo obtener información sobre el firmante de la estampilla de tiempo.
- 7b.1. El sistema crea un mensaje de excepción: “No se pudo obtener información sobre el firmante para X” (donde “X” es el número de serie del certificado utilizado para firmar la estampilla de tiempo). El caso de uso termina.
- 7c. La verificación de la firma falla.
- 7c.1. El sistema crea un mensaje de excepción: “No se pudo verificar la estampilla de tiempo”. El caso de uso termina.
- 8a. La creación o guardado del registro de log falla o asociar los registros de log con el registro de estampillado falla.
- 8a.1. El sistema crea un mensaje de excepción que contiene la información del error. El caso de uso termina.

UC MESS_11: Verificar la Firma

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actores: -

Descripción breve: El sistema verifica que la firma sea válida.

Precondiciones: -

Postcondiciones: -

Disparadores:

Paso 18 de 3.3.

Paso 10 de 3.4.

Escenario principal de éxito:

- El sistema valida la firma contra el esquema XAdES [UC-OPMON].
- El sistema verifica que la firma sea una firma por lotes y verifica la cadena de hash (los pasos para la verificación de la cadena de hash se describen en el documento "Using Batch Hashing for Signing and Time-Stamping" [BATCH]).
- El sistema verifica que la firma contenga un certificado de firma (la extensión keyUsage del certificado tiene el bit nonRepudiation activado).
- El sistema verifica que el certificado de firma fue emitido por un servicio de certificación aprobado.
- El sistema verifica que el certificado de firma fue emitido para el miembro de X-Road que (o cuyo subsistema) envió el mensaje al que se adjuntó la firma.
- El sistema verifica el valor de la firma.
- El sistema verifica la cadena de certificados utilizando el certificado de firma, las respuestas OCSP y cualquier certificado adicional.

Extensiones:

1a. La validación contra el esquema falla.

1a.1. El sistema genera un mensaje de excepción con los errores de validación. El caso de uso termina.

2a. La firma no es una firma por lotes.

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

2b. La verificación de la cadena de hash falla.

2b.1. El sistema genera un mensaje de excepción con el error encontrado en la verificación. El caso de uso termina.

3a. El sistema no encontró un certificado de firma en la firma.

3a.1. El sistema genera un mensaje de excepción: "La firma no contiene un certificado de firma". El caso de uso termina.

3b. El certificado de firma no califica como certificado de firma.

3b.1. El sistema genera un mensaje de excepción: “El certificado X no es un certificado de firma” (donde "X" es el nombre del sujeto del certificado). El caso de uso termina.

4a. El sistema no encontró el emisor del certificado en la lista de servicios de certificación aprobados en la configuración global.

4a.1. El sistema genera un mensaje de excepción: “El certificado no fue emitido por un proveedor de servicio de certificación aprobado”. El caso de uso termina.

5a. El sistema no puede leer el identificador del sujeto del certificado del certificado de firma.

5a.1. El sistema genera un mensaje de excepción con el error encontrado. El caso de uso termina.

5b. El nombre común del sujeto no coincide con el identificador del remitente del mensaje.

5b.1. El sistema genera un mensaje de excepción: “El nombre en el certificado (X) no coincide con el nombre en el mensaje (Y)” (donde "X" es el nombre común de la persona a la que se le emitió el certificado y "Y" es el identificador del miembro de X-Road que envió el mensaje). El caso de uso termina.

6a. La verificación del valor de la firma falló.

6a.1. El sistema genera un mensaje de excepción: “La firma no es válida”. El caso de uso termina.

7a. El proceso de validación de la cadena de certificados termina con un mensaje de excepción.

7a.1. El caso de uso termina con el mensaje de excepción.

UC MESS_12: Verificar la Cadena de Certificados

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actores: -

Descripción breve: El sistema verifica la cadena de certificados.

Precondiciones: -

Postcondiciones: -

Disparadores:

Paso 3 de 3.8.

Paso 8 de 3.12.

Escenario principal de éxito:

- El sistema construye la cadena de certificados desde el certificado de firma o de autenticación (dependiendo del disparador de este caso de uso) hasta un certificado de una autoridad de certificación (CA) confiable.
- El sistema valida la cadena de certificados.
- El sistema encuentra y valida las respuestas OCSP para cada certificado en la cadena de certificados.

Extensiones:

2a. La validación de la cadena de certificados falló.

2a.1. El sistema genera un mensaje de excepción con los detalles del error de validación. El caso de uso termina.

3a. El sistema no puede encontrar una respuesta OCSP para un certificado en la cadena de certificados.

3a.1. El sistema genera un mensaje de excepción: "No se pudo encontrar la respuesta OCSP para el certificado X" (donde "X" es el nombre del sujeto del certificado). El caso de uso termina.

3b. El proceso de validación de la respuesta OCSP termina con un mensaje de excepción.

3b.1. El caso de uso termina con el mensaje de excepción.

UC MESS_13: Validar una Respuesta OCSP

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actores: -

Descripción breve: El sistema verifica que la respuesta OCSP sea válida y que el estado de la respuesta OCSP sea bueno.

Precondiciones: -

Postcondiciones: -

Disparador: Paso 3 de 3.13.

Escenario principal de éxito:

- El sistema verifica que el certificado identificado en una respuesta recibida del respondedor OCSP corresponda al que se identificó en la solicitud correspondiente.
- El sistema verifica que la firma en la respuesta OCSP sea válida.
- El sistema verifica que el firmante esté actualmente autorizado para firmar las respuestas OCSP para la autoridad de certificación que emitió el certificado al que se entregó la respuesta OCSP.
- El sistema verifica que la respuesta OCSP no sea más antigua de lo permitido por la configuración global. El período de validez de las respuestas OCSP está definido por el parámetro del sistema del servidor central `ocspFreshnessSeconds`.
- El sistema verifica (cuando está disponible) que el tiempo en el que se dispondrá de información más reciente sobre el estado del certificado sea posterior a la hora actual.
- El sistema verifica que el estado de la respuesta OCSP sea bueno.

Extensiones:

1a. El certificado en la respuesta OCSP no coincide con el de la solicitud.

1a.1. El sistema genera un mensaje de excepción: “La respuesta OCSP no se aplica al certificado (sn = X)” (donde “X” es el número de serie del certificado). El caso de uso termina.

2a. El sistema no puede encontrar el certificado del respondedor OCSP necesario para validar la firma.

2a.1. El sistema genera un mensaje de excepción: “No se pudo encontrar el certificado OCSP para el ID del respondedor”. El caso de uso termina.

2b. La validación de la firma falla.

2b.1. El sistema genera un mensaje de excepción: “La firma en la respuesta OCSP no es válida”. El caso de uso termina.

3a. El respondedor OCSP no está autorizado para firmar respuestas OCSP para la autoridad de certificación que emitió el certificado.

3a.1. El sistema genera un mensaje de excepción: “El respondedor OCSP no está autorizado para la CA indicada”. El caso de uso termina.

4a. El estado de la respuesta OCSP es demasiado antiguo.

4a.1. El sistema genera un mensaje de excepción: “La respuesta OCSP es demasiado antigua (thisUpdate: X)”, donde “X” es la fecha que representa el inicio de la validez de esta respuesta. El caso de uso termina.

5a. Se debería disponer de información más reciente sobre el estado del certificado.

5a.1. El sistema genera un mensaje de excepción: “La respuesta OCSP es demasiado antigua: debería estar disponible información más reciente”. El caso de uso termina.

6a. El estado de la respuesta OCSP no es bueno.

6a.1. El sistema genera un mensaje de excepción: “La respuesta OCSP indica que el estado del certificado es X”, donde “X” es el estado (posibles valores: desconocido, revocado (fecha: <hora de revocación>), inválido) de la respuesta OCSP. El caso de uso termina.

Aquí tienes la traducción del texto al español con las palabras clave antes de los dos puntos en negrita:

UC MESS_14: Obtener Respuestas OCSP

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actores: -

Descripción Breve: El sistema obtiene y almacena en caché las respuestas OCSP para los certificados utilizables utilizando los respondedores OCSP definidos en la configuración global.

Precondiciones: -

Postcondiciones: -

Disparador: Temporizador. El sistema calcula el intervalo del temporizador dividiendo el valor del parámetro del servidor central ocsFreshnessSeconds por 10.

El valor de ocsFreshnessSeconds determina el período de validez de las respuestas OCSP almacenadas en caché. Para compensar malfuncionamientos temporales del servicio del respondedores OCSP o fallos del sistema, el intervalo de actualización de las respuestas se ajusta a 10 veces menos que el período de validez.

Escenario Principal de Éxito:

- El sistema verifica que la configuración del sistema contiene una configuración global válida.
- El sistema encuentra certificados en la configuración del sistema que están en estado registrado y no están deshabilitados ni expirados.
- El sistema obtiene una respuesta OCSP para cada certificado encontrado:
3.16.
- El sistema almacena en caché las respuestas OCSP recibidas.

Extensiones:

1a. La configuración global ha expirado.

1a.1. El sistema crea un mensaje de excepción: "La configuración global ha expirado". El caso de uso termina.

2a. El sistema no encuentra certificados que no estén deshabilitados o expirados.

2a.1. El caso de uso termina.

UC MESS_15: Obtener y Verificar Respuesta OCSP

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actor: Respondedor OCSP

Descripción Breve: El sistema encuentra respondedores OCSP para un certificado, realiza una solicitud OCSP y valida la respuesta recibida.

Precondiciones: -

Postcondiciones: -

Disparadores:

- Paso 3 de **3.15**.
- Importación de certificado (ver **[UC-SS]**).

Escenario Principal de Éxito:

- El sistema encuentra direcciones de respondedores OCSP en la configuración global.
- El sistema obtiene una respuesta OCSP de uno de los respondedores OCSP encontrados.
- El sistema verifica la respuesta OCSP:
 - El sistema verifica que el certificado identificado en la respuesta recibida del respondedores OCSP corresponda al certificado de la solicitud correspondiente.
 - El sistema verifica que la firma de la respuesta OCSP es válida.
 - El sistema verifica que el firmante está autorizado para firmar las respuestas OCSP para la autoridad certificadora que emitió el certificado al que se dio la respuesta OCSP.
 - El sistema verifica que la respuesta OCSP no es más antigua de lo permitido por la configuración global. El período de validez de las respuestas OCSP está definido por el parámetro del servidor central `ocspFreshnessSeconds`.
 - El sistema verifica (cuando está disponible) que el tiempo antes del cual debe estar disponible nueva información sobre el estado del certificado sea mayor que el tiempo actual.

Extensiones:

1a. El sistema no encuentra respondedores OCSP para un certificado.

1a.1. El sistema registra un mensaje de error: “No hay URIs de respondedores OCSP disponibles”. El caso de uso termina.

2a. El sistema no puede obtener una respuesta de un respondedores OCSP.

2a.1. El sistema registra un mensaje de error: “No se puede obtener respuesta del respondedores en X” (donde X es la dirección del respondedores OCSP).

2b. El sistema no puede obtener una respuesta OCSP de ningún respondedores.

2b.1. El sistema registra un mensaje de error: “No se puede obtener respuesta OCSP válida de ningún respondedores”. El caso de uso termina.

3a. La validación de la respuesta OCSP falla.

3a.1. El sistema registra un mensaje de advertencia: “Respuesta OCSP recibida que falló en la verificación”. El caso de uso termina.

UC MESS_16: Almacenar Datos de Monitoreo Operacional y Enviar los Datos al Demonio de Monitoreo Operacional

Sistema: Servidor de seguridad

Nivel: Subfunción

Componente: Servidor de seguridad

Actores: -

Descripción Breve: El servidor de seguridad almacena los datos de monitoreo operacional en el búfer de monitoreo operacional. Se crea un registro de datos de monitoreo operacional para cada solicitud durante el intercambio de mensajes. El servidor de seguridad envía los datos operacionales almacenados en el búfer de monitoreo operacional al demonio de monitoreo operacional. Los registros enviados con éxito se eliminan del búfer de monitoreo operacional.

Precondiciones: -

Postcondiciones: -

Disparadores:

- Paso 22 de **3.3**.
- Paso 20 de **3.4**.
- Ha pasado el intervalo de tiempo para el envío periódico de datos de monitoreo operacional.

Escenario Principal de Éxito:

- El sistema almacena los siguientes datos en el búfer de monitoreo operacional (los campos no marcados como obligatorios son opcionales):
 - La IP interna del servidor de seguridad (obligatorio);
 - Tipo del servidor de seguridad (ya sea Cliente o Productor, obligatorio);
 - Marca de tiempo de la solicitud de entrada (En el servidor de seguridad del cliente: la marca de tiempo Unix en milisegundos cuando la solicitud fue recibida por el servidor de seguridad del cliente. En el servidor de seguridad del proveedor de servicios: la marca de tiempo Unix en milisegundos cuando la solicitud fue recibida por el servidor de seguridad del proveedor de servicios. Obligatorio);
 - Marca de tiempo de salida de la solicitud (En el servidor de seguridad del cliente: la marca de tiempo Unix en milisegundos cuando la solicitud fue enviada desde el servidor de seguridad del cliente al sistema de información del cliente. En el servidor de seguridad del proveedor de servicios: la marca de tiempo Unix en milisegundos cuando la solicitud fue enviada desde el servidor de seguridad del proveedor de servicios. Si la solicitud es una solicitud de metadatos o una solicitud de datos de monitoreo proxy, el valor del parámetro es igual a 'marca de tiempo de entrada de solicitud');
 - Marca de tiempo de entrada de respuesta (En el servidor de seguridad del cliente: la marca de tiempo Unix en milisegundos cuando la respuesta fue recibida por el servidor de seguridad del cliente. En el servidor de seguridad del proveedor de servicios: la marca de tiempo Unix en milisegundos cuando la respuesta fue recibida por el servidor de seguridad del proveedor de servicios. Si la solicitud es una solicitud de metadatos o una solicitud de datos de monitoreo proxy, el valor del parámetro es igual a 'marca de tiempo de salida de respuesta');
 - Marca de tiempo de salida de respuesta (En el servidor de seguridad del cliente: la marca de tiempo Unix en milisegundos cuando la respuesta fue enviada desde el servidor de seguridad del cliente al sistema de información del cliente. En el servidor de seguridad del proveedor de servicios: la marca de tiempo Unix en milisegundos cuando la respuesta fue enviada desde el servidor de seguridad del proveedor de servicios. Obligatorio);
 - El identificador de instancia de X-Road de la instancia utilizada por el cliente;
 - La clase de miembro del miembro de X-Road (cliente);
 - El código del miembro del miembro de X-Road (cliente);
 - El código del subsistema del miembro de X-Road (cliente);
 - El identificador de instancia de X-Road de la instancia utilizada por el proveedor de servicios;
 - La clase de miembro del miembro de X-Road (proveedor de servicios);
 - El código del miembro del miembro de X-Road (proveedor de servicios);
 - El código del subsistema del miembro de X-Road (proveedor de servicios);
 - El código del servicio;
 - El número de versión del servicio;
 - La clase de la parte representada;
 - El código de la parte representada;
 - El identificador único del mensaje;
 - El código personal del cliente que inició la solicitud;
 - El identificador interno del cliente del mensaje;
 - La versión del protocolo de mensajes de X-Road;

- La dirección externa del servidor de seguridad del cliente (IP o nombre de host) definida en la configuración global;
- La dirección externa del servidor de seguridad del proveedor de servicios (IP o nombre de host) definida en la configuración global;
- El tamaño de la solicitud (bytes);
- El tamaño del contenedor MIME de la solicitud (bytes);
- El número de archivos adjuntos de la solicitud;
- El tamaño de la respuesta (bytes);
- El tamaño del contenedor MIME de la respuesta (bytes);
- El número de archivos adjuntos de la respuesta;
- La indicación de mediación de solicitud exitosa/no exitosa (booleano; obligatorio);
- El código de error SOAP;
- La razón del error SOAP.
- El sistema verifica cuántos registros hay en el búfer de monitoreo operacional y compone un mensaje JSON.
- El sistema verifica que el demonio de monitoreo operacional debe estar conectado usando el protocolo HTTP. El sistema inicia una conexión con el demonio de monitoreo operacional.
- El sistema envía el registro(s) de datos operacionales al demonio de monitoreo operacional. El número de registros incluidos en un mensaje está definido por un parámetro del sistema.
- El sistema recibe una confirmación del demonio de monitoreo operacional.
- El sistema elimina los registros enviados con éxito del búfer de monitoreo operacional.
- El sistema verifica que no hay más registros en el búfer de monitoreo operacional.

Extensiones:

1a. Se ha excedido el límite de tamaño del búfer de monitoreo operacional.

1a.1. El sistema elimina el registro más antiguo del búfer de monitoreo operacional y registra un mensaje de advertencia: "Desbordamiento del búfer de monitoreo operacional, eliminando el registro más antiguo 'X'", donde "X" es el índice del registro en el búfer de monitoreo operacional.

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

1b. Ha pasado el intervalo de tiempo para el envío periódico de datos de monitoreo operacional (definido por un parámetro del sistema).

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

2a. El sistema verifica que el proceso de envío de datos operacionales al demonio de monitoreo operacional no ha terminado.

2a.1. El caso de uso termina.

2b. El sistema verifica que no hay registros de monitoreo operacional en el búfer de monitoreo operacional.

2b.1. El caso de uso termina.

3a. El sistema no puede iniciar una conexión con el demonio de monitoreo operacional.

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

3b. El sistema verifica que el demonio de monitoreo operacional debe estar conectado utilizando HTTPS y que el certificado del demonio de monitoreo operacional debe ser verificado.

3b.1. El sistema usa el certificado TLS interno del servidor de seguridad para la conexión.

3b.2. El sistema encuentra el certificado TLS del demonio de monitoreo operacional en la conexión.

3b.2a. El sistema no puede encontrar el certificado TLS.

3b.2a.1. El sistema registra un mensaje de error. El caso de uso termina.

3b.3. El sistema verifica que el certificado TLS enviado por el demonio de monitoreo operacional coincide con el certificado TLS configurado para el demonio de monitoreo operacional en la configuración del sistema. El caso de uso continúa desde el paso 4.

3b.3a. El sistema no encuentra el certificado TLS para el demonio de monitoreo operacional en la configuración del sistema.

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

3b.3b. El certificado TLS configurado para el demonio de monitoreo operacional no coincide con el certificado que el demonio presentó para la autenticación TLS.

3b.3b.1. El sistema registra un mensaje de error. El caso de uso termina.

5a. El almacenamiento de datos de monitoreo operacional en el demonio de monitoreo operacional falló.

5a.1. El caso de uso termina.

6a. El sistema verifica que hay más registros en el búfer de monitoreo operacional.

6a.1. El caso de uso continúa desde el paso 3.

Anexo A: Diagrama de Secuencia para Mensajería

