ORGANIZACIÓN MARÍTIMA INTERNACIONAL

S

4 ALBERT EMBANKMENT
LONDRES SE1 7SR
Teléfono: +44(0)20 7735 7611 Facsímil: +44(0)20 7587 3210

FAL.5/Circ.46
1 junio 2022

DIRECTRICES SOBRE LA AUTENTICACIÓN, INTEGRIDAD Y CONFIDENCIALIDAD DE LOS INTERCAMBIOS DE INFORMACIÓN CON LAS VENTANILLAS ÚNICAS MARÍTIMAS Y SERVICIOS CONEXOS

1 El Comité de facilitación, en su 46º periodo de sesiones (9 a 13 de mayo de 2022), aprobó las Directrices sobre la autenticación, integridad y confidencialidad de los intercambios de información con las ventanillas únicas marítimas y servicios conexos, que figuran en el anexo.

2 Se invita a los Estados Miembros y a las organizaciones internacionales a que pongan las Directrices en conocimiento de todas las partes interesadas.

3 Asimismo, se invita a los Estados Miembros y a las organizaciones internacionales a que señalen a la atención del Comité, tan pronto como sea posible, los resultados de la experiencia que hayan adquirido con la utilización de las Directrices, a fin de examinar las medidas que han de adoptarse.

***

ANEXO

DIRECTRICES SOBRE LA AUTENTICACIÓN, INTEGRIDAD Y CONFIDENCIALIDAD DE LOS INTERCAMBIOS DE INFORMACIÓN CON LAS VENTANILLAS ÚNICAS MARÍTIMAS Y SERVICIOS CONEXOS

Índice

1 Resumen

Mediante las presentes directrices se establecen los requisitos generales de una plataforma o sistema digital que puede utilizarse para dotar de funciones de autenticación, integridad y confidencialidad a los intercambios de información por medio de las ventanillas únicas marítimas y servicios conexos. Estos requisitos se elaboran principalmente para los intercambios de información relacionados con el buque, su paso por aguas internacionales y nacionales y sus escalas en los puertos. Con respecto a los intercambios de información que se basan en sistemas de intercambio de datos por VHF (VDES) en el apéndice 3 *(Guidelines to signature system in an international shipping environment)* (Directrices para los sistemas de firma en el marco del transporte marítimo internacional) y el apéndice 4 (*Guidelines to low-bandwidth communication systems*) (Directrices para los sistemas de comunicación de baja anchura de banda) se disponen los requisitos generales para los sistemas de firmas que se han de utilizar en el contexto VDES.

En estas directrices se definirán algunas "pautas" generales de intercambio de mensajes que se utilizan como referencia para las prescripciones relativas a la firma electrónica. Las diferentes pautas tendrán algunas diferencias en las prescripciones.

En las directrices también se definirán algunas prescripciones para el envío de "metadatos". Se trata de datos que no están relacionados con la información transmitida en los mensajes, sino con las prescripciones de los procesos de transmisión. Muchos de los metadatos están directamente relacionados con la seguridad de los mensajes, por ejemplo, los códigos de referencia y la marca de tiempo (*timestamp*), pero para completarlos, también se han incluido elementos administrativos más generales. En el apéndice 1 figura un resumen de los elementos de metadatos.

Las pautas y prescripciones relativas a los mensajes en estas directrices se basan en los datos que envía un remitente a un destinatario cuando el remitente solicita un servicio, es decir, el "empuje de datos" visto desde el remitente. También es posible crear pautas basadas en la "extracción de datos", es decir, que el destinatario obtiene activamente datos de alguna fuente predefinida después de que se haya solicitado el servicio. Sin embargo, este principio aún no es común en el ámbito marítimo, por lo que no se examina en el presente documento. La mayoría de las prescripciones especificadas en las presentes directrices seguirán aplicándose, pero pueden manifestarse de manera diferente en un entorno de extracción de datos.

Las directrices se basan, en la medida de lo posible, en las normas y especificaciones existentes. Por consiguiente, las prescripciones que se presentan en estas directrices serán similares a las que figuran en otros documentos. Sin embargo, el entorno marítimo tiene algunas características especiales que es preciso tener en cuenta y que se han abordado específicamente en las presentes directrices, por ejemplo, el carácter internacional del negocio, el hecho de que los buques no siempre pueden estar conectados a Internet y el costo relativamente alto y/o el bajo ancho de banda de las comunicaciones que se aplica a muchos de los sistemas actuales de comunicación por satélite.

Si bien estas directrices han sido elaboradas por el Comité de facilitación en relación con las prescripciones del Convenio de facilitación, existen también otros intercambios de mensajes obligatorios que podrían beneficiarse de la digitalización, por ejemplo, la notificación obligatoria de buques y los nuevos servicios de navegación electrónica.

2 Términos y definiciones

Interfaz de aplicación de programas (API): un tipo de interfaz de software que ofrece servicios a otras secciones de servicios y facilita una conexión entre aplicaciones y los sistemas.

Cancelación: esta es una forma de solicitud de actualización que cancela la solicitud de un servicio.

Remitente: la parte que solicita un servicio de un destinatario enviando una solicitud inicial y cualquier otra solicitud de actualización que pueda ser requerida por el servicio. El remitente es el iniciador del intercambio de mensajes y puede ser un buque o una entidad terrestre.

Firma digital:[1] datos que, cuando se adjuntan a un mensaje, o que constituyen una transformación criptográfica, permiten al receptor del mismo autenticar su origen e integridad y que protegen contra las falsificaciones por parte de, por ejemplo, el receptor

Firma electrónica:[2]. datos que, cuando se adjuntan a un mensaje, permiten al destinatario del mensaje autenticar su origen e integridad (adaptado del ISO 20415).

Envío de información: datos o mensajes que el buque o su agente han de enviar, por ejemplo la información previa a la llegada, que no contiene ninguna solicitud. Normalmente será necesario que el sistema o plataforma receptora muestre un API o un servicio web para recibir los datos.

Integridad: característica de un documento cuyo contenido no ha sido alterado.:

Ventanilla única marítima: un sistema o plataforma digital que permite que toda la información requerida por las autoridades públicas en relación con la llegada, permanencia y salida de los buques, las personas y la carga se presente, pero sin duplicación.

Mensaje: serie de campos de datos y/o bloques de campos de datos comunicados de una parte a otra para transmitir información comercial significativa (ISO 15022-1).

Situación del mensaje: debería contener información sobre la forma en que se tramitará la solicitud e indicar, por ejemplo, que la solicitud ya ha sido aceptada y/o que un acuse de recibo de solicitud se enviará más adelante. También puede indicar que la solicitud no era válida, en cuyo caso no podrá seguir tramitándose, o que se necesita información adicional, en cuyo caso debería enviarse una solicitud de actualización.

Solicitud: un mensaje que es enviado por el remitente como una solicitud de servicio al receptor. Durante una sesión pueden enviarse varias solicitudes de actualización, que pueden incluir la cancelación de todo el servicio o de partes del mismo.

Código de referencia de la solicitud: un código único asignado por el remitente a una solicitud, para permitir al receptor hacer una referencia inequívoca a ese mensaje. Un código de referencia puede hacerse único, por ejemplo, combinando el número IMO y/o de viaje de un buque con un número de serie.

---

1 Hay una diferencia entre la firma digital y la electrónica. La diferencia fundamental es que la firma digital se utiliza para dotar de seguridad a un documento/mensaje, mientras que un mensaje electrónico se utiliza para verificar un documento mensaje.

2 La firma electrónica, tal como se define aquí, es la misma que el "sello electrónico", tal como se define en el número de referencia de la bibliografía [3].

Canal seguro: canal de comunicación que proporciona la confidencialidad y la autenticidad de los mensajes intercambiados. Es posible que se disponga de un canal seguro a través de las conexiones de Internet mediante el uso de protocolos como el HTTPS (Protocolo de Transmisión de Hipertexto Seguro).

Receptor: el receptor de una solicitud que proporciona o facilita el servicio asociado. A menudo, se tratará de una entidad terrestre de tipo administrativo, como una ventanilla única marítima, un sistema de notificación de buques u otra instalación portuaria o costera del Estado. Sin embargo, el receptor también puede ser una nave o cualquier otra entidad que reciba una solicitud de un remitente.

*Servicio***:** una solicitud del remitente al receptor (incluido un informe), que el receptor acepta o rechaza. Obsérvese que una sesión puede incluir más de un servicio, por ejemplo que se pida que diversos formularios FAL se acepten en una sesión.

Acuse de recibo de solicitud: un mensaje enviado por el receptor para verificar que se ha recibido una solicitud.

Sesión: una secuencia de mensajes relacionados con una misma solicitud inicial.

Código de referencia de la sesión: un código único asignado por el receptor. Puede ser, por ejemplo, el mismo que el código de referencia de la solicitud inicial. El código de referencia de la sesión es utilizado por el remitente y el receptor para identificar mensajes posteriores relacionados con la misma sesión. "Único" significa que el código no debería ser reutilizado en un intervalo de tiempo razonable.

Dispositivo de firma: se puede utilizar un programa o equipo informático especial, por ejemplo una tarjeta inteligente, para firmar los mensajes salientes o comprobar las firmas entrantes. En estas directrices, esto se llama un dispositivo de firma. Por seguridad física, normalmente solo habrá uno o dos dispositivos de este tipo en un sitio. El acceso al dispositivo desde otras computadoras será normalmente a través de conexiones de red.

Timestamp: fecha y hora, incluido el uso horario en que ocurre un determinado evento (adaptado de la ISO 8601 en formato UTC). En el contexto de este documento, el evento es normalmente la transmisión de un mensaje y la marca de tiempo (*timestamp*) se fija en el mensaje. La marca de tiempo (*timestamp*) debería tener una resolución suficiente para que sea improbable que dos mensajes consecutivos del mismo remitente tengan la misma marca de tiempo (*timestamp*).

Solicitud de actualización: es una solicitud que se envía como actualización de la solicitud inicial. Una forma especial de solicitud de actualización es la cancelación. Normalmente, no se puede enviar una solicitud de actualización después de que el receptor haya generado un acuse de recibo de solicitud, pero esto dependerá de la implementación del servicio.

3 Introducción

Los intercambios de información digital en el sector marítimo son convenientes por muchas razones, por ejemplo

.1 para reducir la carga de trabajo administrativo de las partes involucradas, incluida la gente de mar. Esto se hace utilizando computadoras para automatizar los procesos relacionados con el envío, la recepción y el procesamiento de la información; y

2 para mejorar la calidad de la información utilizada para planificar y ejecutar operaciones marítimas y portuarias. Las transmisiones electrónicas evitan los malentendidos y permiten un intercambio eficiente de información más compleja.

Sin embargo, la comunicación electrónica puede fallar por varias razones, por ejemplo:

.1 los errores técnicos pueden modificar alguna información o pueden hacer que algunos mensajes no se entreguen;

.2 los destinatarios que no son fiables pueden, por ejemplo, falsificar el contenido de los mensajes o negar que se hayan recibido o enviado determinados mensajes; y

.3 los ciberataques malintencionados que pueden tener objetivos comerciales o de amenaza o que son solo intentos aleatorios de irrumpir en sistemas técnicos interesantes, pueden introducir mensajes falsos o cambiar el contenido de los mensajes.

Es necesario establecer una confianza suficiente en los procesos automatizados para evitar que las personas que tienen la responsabilidad general de que los procesos sean correctos tengan que comprobar dos veces la información y los resultados del procesamiento. Si no se logra esto, la carga de trabajo puede aumentar en lugar de disminuir. Los fallos de transmisión también pueden tener consecuencias para la seguridad y protección, cuya gravedad depende de la importancia de la información contenida en los mensajes.

Esta confianza no puede establecerse a menos que los mecanismos de seguridad inherentes a los sistemas basados en papel se reproduzcan en los intercambios de información digital. Estos servicios son los siguientes:

.1 *integridad* (impreso en papel - difícil de cambiar): el contenido de un mensaje no puede ser manipulado;

.2 *autenticidad* (firmas, sellos, timbres): la identidad del autor del mensaje puede ser verificada; y

.3 *confidencialidad* (sobre sellado): el contenido del mensaje no puede ser leído por otras personas que no sean el destinatario previsto.

Además, se necesitará también un mecanismo adicional que pueda derivarse de los mecanismos anteriores:

.4 *no repudio* (correo certificado, mensajería): proporcionar una prueba de que el mensaje fue entregado al destinatario. En el caso de los intercambios de información digital, esto requiere alguna forma de reconocimiento por parte del receptor de que el mensaje fue entregado.

En las presentes directrices se especificarán los requisitos que debe cumplir un sistema o plataforma digital para aplicar esos mecanismos de seguridad y protección.

4 Interfaz de aplicación de programas (API)

La interfaz de aplicación de programas (API) se ha generalizado y actualmente es el mecanismo más usado para conectar e interoperar con otros sistemas y aplicaciones. Por tanto, se recomienda utilizar API para facilitar la interoperabilidad entre los sistemas, los. MSW

y otros sistemas conexos, dado que es necesario proceder a la autenticación para garantizar que se verifica y valida la solicitud antes de que pueda realizarse el intercambio de información.

Hay tres métodos comunes mediante los que se puede proceder a la autenticación de las API

.1 Autenticación básica HTTP- en este método, un agente que haga uso del HTTP facilitará un nombre de usuario y una contraseña mediante el encabezamiento del HTTP, a los fines de la autenticación.

.2 Clave API- en este método, se asigna a la aplicación de llamada (solicitante) una clave única a fin de denotar que el solicitante es conocido, de forma que cuando envía una solicitud con la clave API como uno de los parámetros de la solicitud, la clave única se utiliza para autenticar al solicitante.

.3 OAuth- en este método, la aplicación que llama (solicitante) en primer lugar envía una solicitud al Sistema para que se le envíe una ficha de acceso. Seguidamente el sistema devuelve la ficha de acceso al solicitante. Seguidamente el solicitante envía otra solicitud junto con la ficha de acceso al sistema para validar la ficha antes de que pueda realizarse el intercambio de información.

No hay reglas o directrices específicas con respecto a cuál de los métodos de autenticación es mejor, dado que depende de la situación en la que se utilice el API.

Téngase presente que la garantía de la autenticación utilizando únicamente mecanismos API no hará posible que el remitente pueda probar que de hecho se ha enviado el contenido de un mensaje específico (integridad). A menos que el mensaje se firme digitalmente, cabe la posibilidad, en la parte del destinatario, de que alguien altere el contenido sin que el remitente pueda probar que este es el caso. Para solventar esto, es necesario proteger las Comunicaciones que se hagan a través de redes de ordenadores. Uno de los protocolos más comunes para firmar digitalmente el mensaje o cifrarlo, incluida la autenticación, integridad y confidencialidad, es "Transport Layer Security (TLS) / Secure Socket Layer (SSL)".

5 Proceso de envío único a nivel internacional

Independientemente del API, tal como se examina en la sección 4, se deberían examinar las posibles ventajas de contar con un certificado clave público internacionalmente reconocido que se utilice para la autenticación del Sistema receptor. Esto permitiría que el buque o su agente utilizasen sus certificados públicos en el proceso de autenticación, sin necesidad de registrar previamente el sistema.

6 Prescripciones generales para todos los mensajes electrónicos

Todos los mensajes han de incluir la marca de tiempo (*timestamp*) de envío a fin de garantizar la existencia y cualidades de un determinado mensaje de datos en un determinado momento.

El mensaje también puede incluir un tiempo de validez para especificar el tiempo máximo en que el contenido del mensaje puede considerarse válido.

Todos los mensajes de cualquier importancia deberían ser encriptados. La encriptación debería proteger la integridad de cada uno de los elementos de datos importantes del mensaje, la marca de tiempo (*timestamp*) de envío, así como cualquier código de referencia.

No basta con confiar en un canal seguro para comprobar la integridad, ya que las personas del lado receptor pueden manipular los datos, o el remitente puede negar haber enviado algunos de los datos. Para una protección total, es necesario incluir una firma electrónica en cada mensaje.

El receptor de un mensaje encriptado debe verificar la autenticidad del remitente, así como la integridad de la información firmada antes de que se procese el contenido del mensaje. Si se detecta un problema, se le debería notificar al remitente y desechar el mensaje.

> NOTA: Para las pautas de mensajes de difusión, puede que no se quiera notificar al remitente, ya que es posible que esté inundado de mensajes. Sin embargo, el mensaje falsificado debería, de ser posible, causar una advertencia al operador del sistema.

Un mensaje con una marca de tiempo (*timestamp*) que sea más antiguo que los mensajes ya recibidos del mismo remitente o que tenga marca de tiempo *timestamp*) que sea "demasiado antigua" debería ser descartado y se le debería notificar al remitente. El valor real de "demasiado antigua" dependerá del servicio solicitado o prestado, así como de los sistemas de comunicación en uso.

El receptor y el remitente deberían almacenar copias de todos los mensajes salientes y entrantes como prueba de transmisión y recepción. Estas copias no deberían borrarse hasta que el nuevo intercambio de mensajes demuestre que los mensajes fueron efectivamente recibidos y procesados por la otra parte.

Todos los remitentes y receptores de mensajes electrónicos deben tener su tiempo suficientemente sincronizado para detectar problemas de marca de tiempo (*timestamp*), como se muestra arriba.

7 Prescripciones para el remitente

El remitente ha de especificar el servicio que se solicita, por ejemplo, notificación, despacho portuario, servicio portuario, etc.

El remitente debería generar e incluir un Código específico de referencia para todas las solicitudes que se envíen, de modo que el destinatario pueda facilitar una situación del mensaje en relación a cada solicitud. Por lo tanto, todas las solicitudes de actualización deberían obtener un nuevo código de referencia de la solicitud.

Las solicitudes de actualización deberían incluir el código de referencia de la sesión.

Si no llega una situación del mensaje después de un plazo razonable, normalmente definido por el tipo de solicitud, el remitente debería volver a enviar el mensaje con los mismos códigos de referencia de solicitud y sesión si ya se han obtenido. La marca de tiempo (*timestamp*) debería ser actualizada.

Si el acuse de recibo de solicitud no llega en el plazo definido por la última situación del mensaje recibida, el remitente debería enviar una nueva solicitud al receptor. Puede utilizar el mismo código de referencia de la solicitud o uno nuevo, dependiendo del contenido de la solicitud repetida. La marca de tiempo (*timestamp*) debería ser actualizada.

Por razones técnicas y/o de seguridad, los remitentes y los buques en particular pueden tener restricciones en cuanto a la forma en que un receptor puede entregar los mensajes al remitente. Puede ser necesario que el remitente especifique cómo deberían enviarse los

acuses de recibo de solicitud y la situación del mensaje al remitente cuando se envíe una solicitud. En este caso, también el método de entrega debería estar encriptado.

8 Prescripciones para el receptor

En muchos casos, se requiere una prueba de la recepción de una solicitud por parte del receptor. Por lo tanto, el receptor debería enviar una situación del mensaje de cualquier solicitud recibida al remitente. La situación del mensaje debe contener el código de referencia de la solicitud. El receptor podía proporcionar la funcionalidad para generar el código único de referencia de la solicitud y enviarlo al remitente.

En general, el receptor debería acusar recibo de todos los mensajes recibidos, a menos que, por ejemplo, se envíe un acuse de recibo de solicitud inmediatamente después de la recepción de una solicitud. En este caso, el acuse de recibo de solicitud podría incluir la situación del mensaje.

En el caso de los acuses de recibo de solicitud que requieran un acuse de recibí de solicitud posterior, en la situación del mensaje debería especificarse el tiempo máximo que el remitente debe esperar por el acuse de recibo de solicitud. Cuando el remitente envía actualizaciones a la solicitud, este plazo puede actualizarse en la situación del mensaje de la solicitud de actualización.

A menos que la primera situación del mensaje sea también el acuse de recibo de solicitud definitivo, la primera situación del mensaje del receptor debería incluir un código de referencia de sesión único que pueda ser utilizado por las solicitudes de actualización posteriores para identificar la sesión a la que se refiere la solicitud de actualización.

El receptor ha de devolver un código de estado de servicio en los acuses de recibo de solicitud y la situación del mensaje para informar al remitente sobre el estado de la solicitud, por ejemplo, error en los datos, denegaciones, en curso, completado con éxito, etc. Si hay errores, también se debería incluir información más específica de los acuses de recibo de solicitud.

9 Pautas para el intercambio de mensajes

Los intercambios de mensajes frecuentemente se realizan asincrónicamente tal como se muestra en el diagrama infra. Por intercambio asincrónico de mensajes se entiende cualquier tipo de comunicación en la que una entidad envía datos o cursa una petición y seguidamente hay un lapso antes de que el destinatario valida el dato e informa del acuse de recibo de solicitud.

En general, los intercambios de información digital constan de más de un mensaje, como se ilustra en las siguientes figuras. Cada una de las figuras ilustra una "pauta" de mensaje, es decir, una forma típica de intercambiar mensajes, independientemente de la funcionalidad que el intercambio implemente o represente.

Las pautas de los mensajes que se examinan en esta sección se incluyen para orientar sobre la forma en que los mensajes se utilizan normalmente en secuencias más largas de intercambios de mensajes o "sesiones". Esto tiene implicaciones para la transmisión segura y protegida de los mensajes, ya que la integridad y la autenticidad deben ser protegidas durante toda la sesión. Esto requiere, por ejemplo, que los mensajes incluyan marcas de tiempo (*timestamp*s), así como códigos de referencia, de modo que un mensaje de una sesión no pueda sacarse de su contexto y utilizarse para interferir en la misma sesión en un momento posterior o en otra sesión en conjunto.

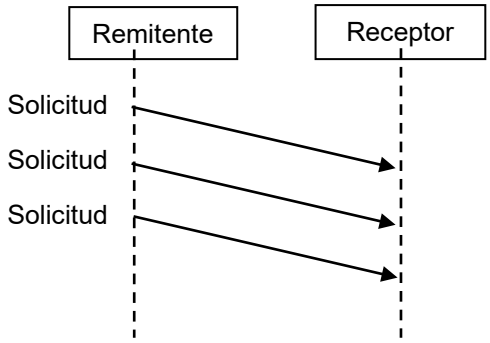

Figura 1: Distribución simple de información

La figura 1 muestra el intercambio de mensajes más simple. El remitente envía información a uno o más receptores sin esperar ningún acuse de recibo de solicitud o situación del mensaje. Un ejemplo de este tipo de pauta es la transmisión de notificaciones de la situación del Sistema de Identificación Automática (SIA) o de mensajes de información estática de buques. En cuanto al SIA, esta pauta utilizará a menudo un mecanismo de difusión para distribuir la información a todas las partes que se encuentren en las proximidades geográficas. La pauta también dependerá normalmente de la retransmisión periódica de la solicitud para evitar problemas en los casos en que se pierdan uno o más mensajes. El remitente repite la información con regularidad y, por lo general, no tiene que preocuparse por la pérdida de datos o mensajes. Sin embargo, dependiendo de la importancia de la información enviada, puede ser necesario añadir una firma electrónica y una marca de tiempo (*timestamp*) para verificar la identidad del remitente y evitar que partes hostiles interfieran en los intercambios de información, por ejemplo, repitiendo mensajes antiguos en un momento posterior.

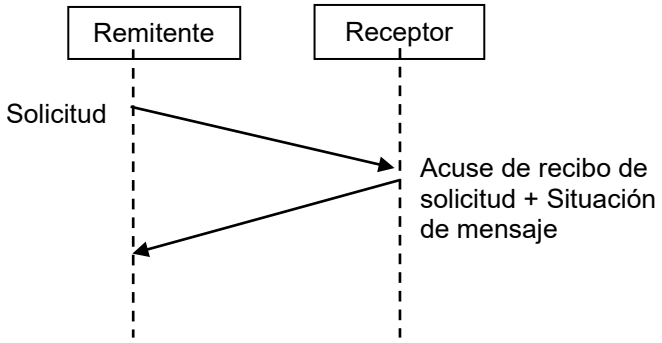

Figura 2: Pauta simple de acuse de recibo de solicitud

La figura 2 muestra otro intercambio de mensajes relativamente simple. El remitente envía alguna información al receptor y recibe inmediatamente un acuse de recibo de solicitud de la recepción del mensaje, así como un acuse de recibo de solicitud del servicio solicitado.

La figura 3 ilustra una solicitud de información o una solicitud de situación del servicio algo más complicada. La figura muestra un caso típico en el que el receptor acusa primero la recepción del mensaje de solicitud, sin responder directamente a la solicitud, y más tarde el acuse de recibo de solicitud al servicio solicitado.

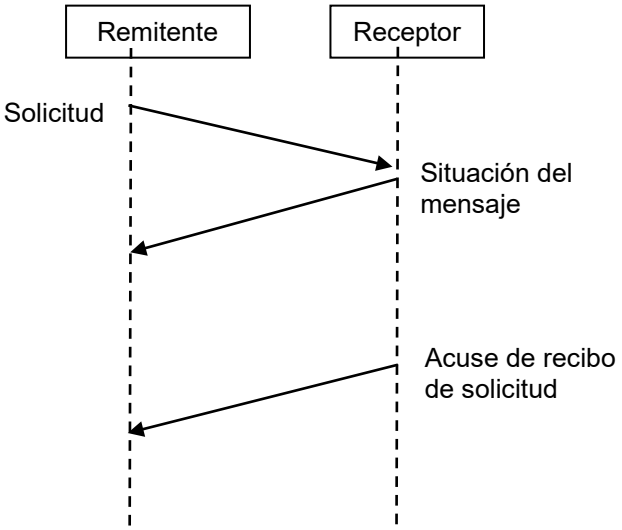

Figura 3: Diagrama de secuencia básica para la solicitud de información o servicio

En algunos casos, el remitente puede enviar solicitudes de actualización en momentos posteriores hasta que se reciba un acuse de recibo de solicitud definitivo a las solicitudes. En la figura 4 se ilustra este concepto.

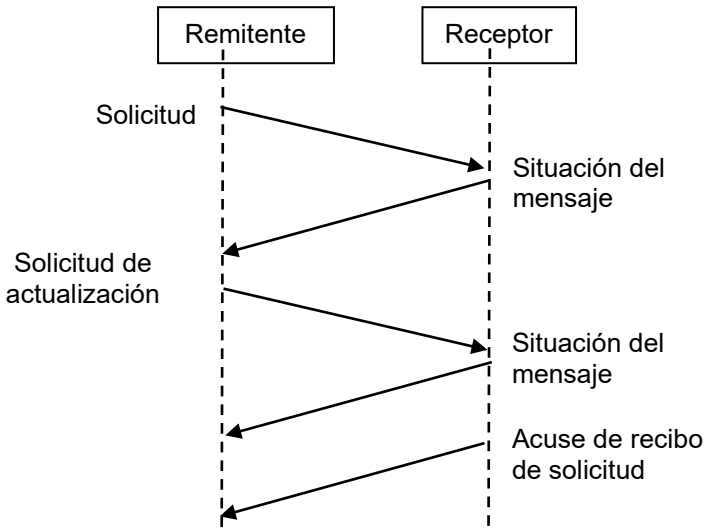

Figura 4: Diagrama de secuencia con solicitud actualizada

Una de estas solicitudes de actualización también puede ser una cancelación de la solicitud inicial. En la mayoría de los casos se responderá a una cancelación con una combinación de situación del mensaje y acuse de recibo de solicitud, mediante los cuales se informa al remitente de que se ha recibido el mensaje y que se acepta la cancelación. Sin embargo, en algunos casos puede ser necesario un acuse de recibo de solicitud tardío también para la cancelación.

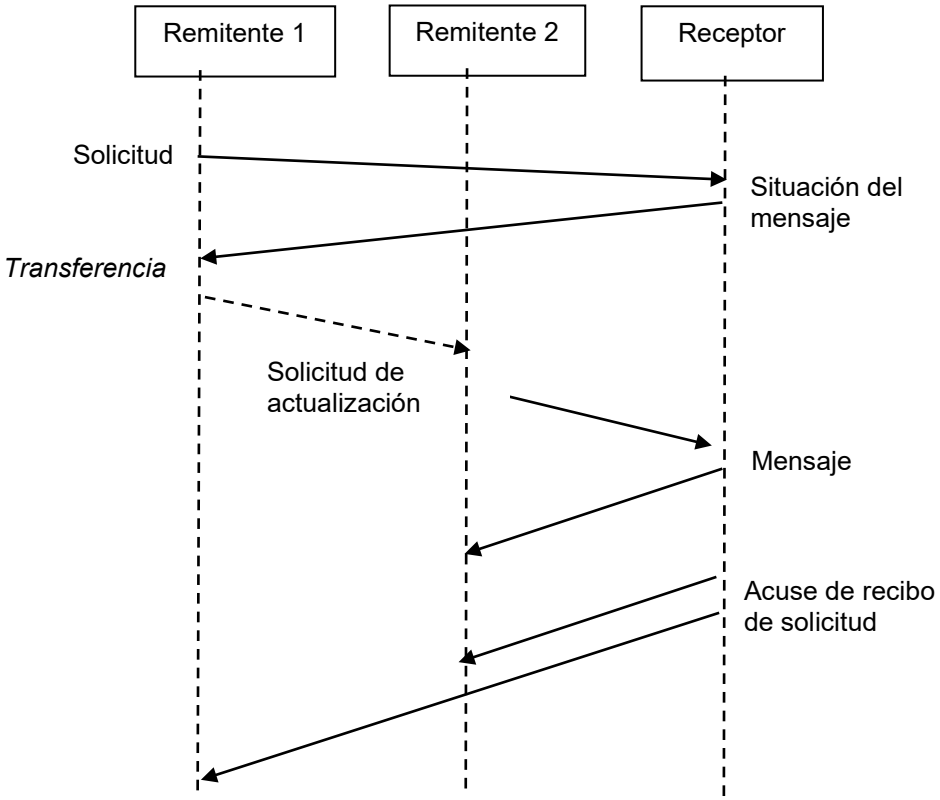

Figura 5: Diagrama de secuencia con más de un remitente

En la figura 5 se puede observar una pauta más compleja. En este caso, varios remitentes cooperan para suministrar al receptor la información requerida. Este podría ser el caso cuando un buque envía alguna información a una ventanilla única marítima y luego pide, por ejemplo, al agente o a la empresa gestora que proporcione detalles adicionales. En este supuesto, todos los remitentes deben utilizar el mismo código de referencia de sesión, lo que requiere alguna forma de comunicación entre ellos (véase la flecha punteada de "transferencia"). El receptor debería enviar un acuse de recibo de solicitud a todos los remitentes a menos que si se define un remitente principal, entonces puede enviar solo al remitente principal.

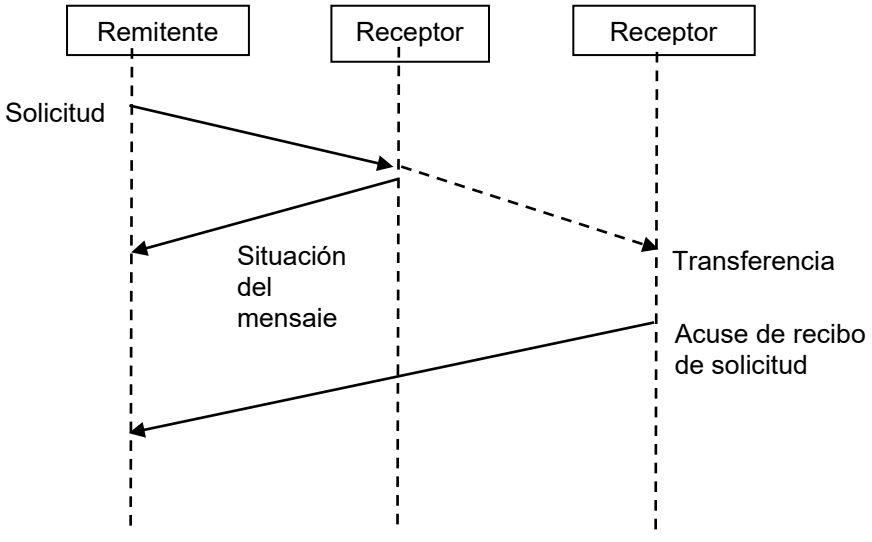

Figura 6: Diagrama secuencial a través de la ventanilla única marítima

La pauta en la figura 6 se utiliza específicamente en el entorno de los sistemas de ventanilla única marítima en el que la ventanilla es el sistema que recibe una solicitud y acusa recibo de la solicitud, siendo el receptor una entidad diferente. La figura 7 es una ampliación de un servicio solicitado a través de una ventanilla única marítima, en un entorno en el que en un momento dado el servicio solicitado se entregará por parte de más de un receptor/proveedor de servicios.

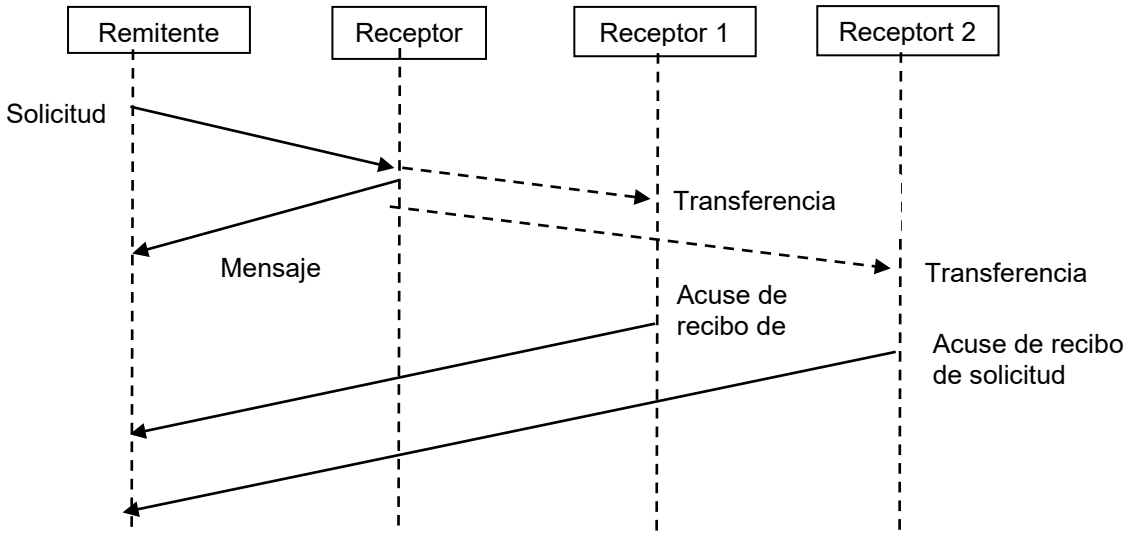

Figura 7: Diagrama secuencial a través de la ventanilla única marítima (receptores múltiples y acuse de recibo de solicitud)

Cabe señalar que se pueden definir otras pautas, que combinen dos o más de las pautas mostradas. Ejemplos típicos son la fusión de acuse de recibo de solicitud y situación del mensaje, la posibilidad de actualizar las solicitudes después de que se haya enviado el acuse de recibo de solicitud o la posibilidad de que haya varios destinatarios de una misma solicitud, en cuyo caso puede requerirse más de un acuse de recibo de solicitud y situación del mensaje. Sin embargo, las pautas que se muestran aquí deberían ser lo suficientemente generales para estas directrices.

10 Prescripciones relacionadas con la confidencialidad

La confidencialidad requiere que el contenido del mensaje sea cifrado con una clave de cifrado robusta.

La transmisión de mensajes por un canal seguro proporcionará confidencialidad, sin que el remitente tenga que cifrar el contenido del mensaje en sí. Sin embargo, puede que todavía sea necesario cifrar el contenido del mensaje si es preciso protegerlo para que no sea leído por algunas partes que pueden acceder al mensaje en el lado receptor.

Los sistemas digitales y las plataformas suelen basarse en la criptografía de clave pública y en claves asimétricas que pueden no ser adecuadas para la codificación de mensajes de mayor tamaño. Un sistema de firma digital o plataforma debe, de ser necesario, contener disposiciones para la generación e intercambio de, por ejemplo, claves simétricas que puedan utilizarse para cifrar mensajes de los tamaños máximos utilizados entre remitentes y receptores.

Referencias y bibliografía

[1] ISO 20415: *Trusted mobile e-document framework — Requirements, functionality and criteria for ensuring reliable and safe mobile e-business*.

[2] ISO 15022-1: *Securities -- Scheme for messages (Data Field Dictionary) -- Part 1: Data field and message design rules and guidelines*.

[3] Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

[4] Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005).

APPENDIX 1

Summary of metadata elements

The following table lists the metadata elements that have been identified in the guidelines. The first column is a short name, the second column specifies in what messages it can be used, the third column gives notes if necessary and the last column provides a short description. The message codes used are:

.1 A: Used in message status and/or service request status messages

.2 R: Used in request messages, including update requests.

.3 U: Used in update request messages.

The list of metadata does not include the electronic signature, as this should be implicit from the guidelines.

Element name	Msg	Note	Description
Message sender identifier	A, R	1	The identifier of the party transmitting the message. Identification of the physical sender of the message (the system). This may be an intermediate, e.g. a message from the ship.
Message receiver identifier	A, R		The identifier of the party receiving the message (the system). Identification of specific receiver the message is intended for. This field should include the possibility of "any" or "all" to identify a message that have no special receiver.
Message date time	A, R	2	The date and time the message is sent
Message validity period	A, R	3	Validity period of the message after it is sent. After this period, the sender and receiver should cancel any outstanding actions at this point, and if appropriate, restart the request sequence.
Message type, coded	A, R	4	Code specifying the name of a message type.
Message function code	A, R		Code providing the function of a message.
Message identifier	A, R		Unique identifier of a message. Used for asynchronous error messages or message status related to this message.
Message return contact point text	A, R		Address to which message status shall be delivered. This can be for instance an URI, and e-mail address. If the ship chooses to poll the receiver, no text is given.
Type of message return contact point method, coded	A, R		This code represents the method by which the sender wants to get the replies from the receiver.
Reference message identifier	A, R		This is the reference to the sender's message identifier to which the message is providing a service request status.

Element name	Msg	Note	Description
Service request status, coded	A		This code represents the status of the service request that the receiver returns to the sender in message status and service request status to the request, e.g. error in data, port call denied, port call in progress, clearance successfully completed etc. If there are errors, a more specific error service request status information is given in the service status explanation, text.
Service request status description	A		This is a free text description of the status of the service request.
Session reference	U, A		Identifier for a session.
Message status, coded	A	5	This code represents the status of received message.
Message status description	A		This is a free text description of the details of why a message failed to be accepted.
Error information	A		Information about why a request was denied.
Authenticator party identification number	A, R		An identifying number, such as an agent identifier, of the party attesting to the validity of the transmitted information.
Authenticator role, coded	A, R		A code providing the role of the person attesting to the validity of the transmitted information.
Authenticator name	A, R		The name of the person attesting to the validity of the transmitted information.
Authentication date	A, R		[1] The date of authentication.
Arrival/departure code	A, R		A code in the message to show whether the information is submitted for the ship arrival or departure.

Comments to the notes:

.1 The sender identity is normally used to find relevant information about the electronic signature used and needs to be identical to the identity codes used in the context of signatures.

.2 This needs to be accurate enough so that two outgoing messages from the same sender do not get the same timestamp. Sender and receiver need to be sufficiently time synchronized to detect problems related to timestamps.

.3 A 'Message Validity Period' field may be included to limit the time the message can be considered valid.

.4 This indicates what service is requested, e.g. pre-arrival notification, mandatory ship reporting, etc.

.5 This indicates status of request and can be transmitted in message status and service request status, e.g. request is successful, pending, denied, etc.

APPENDIX 2

Suggested cryptographic algorithms and key lengths.

Strong cryptographic algorithms and secure protocol standards are vital for protecting maritime communication. While quantum resistant cryptography has by many been advertised as a silver bullet for future security, the standardization and commercial availability of such algorithms are likely to be many years away. In the meantime, the National Security Agency has released the CNSA: Commercial National Security Algorithm Suite [1], which is a set of well-established and thoroughly tested cryptographic algorithms recommended for products developed and deployed during the transition phase to a quantum safe future.

Regarding choice of algorithms for an electronic signature system, there are two main candidates: Rivest-Shamir-Adleman (RSA) [2] and Elliptic Curve Cryptography (ECC) [3]. Of these two, we strongly recommend ECC, because it provides the same cryptographic strength as RSA, but with much smaller keys. For example, a 256-bit ECC key will be as strong as a 3072-bit RSA key. With ECC there will hence be significantly less data that needs to be transmitted when vessels are to exchange cryptographic certificates with other nearby vessels while out at sea. NSA also recommends selecting ECC over RSA: "*Elliptic Curve Cryptography provides greater security and more efficient performance than the first-generation public key techniques (RSA and Diffie-Hellman) now in use. As vendors look to upgrade their systems, they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security.*" [4]

Regarding choice of key length for an electronic signature system, the choice depends on the value and expected lifetime of the data that is to be protected. The longer the keys, the longer they can be assumed to be secure, but longer keys will cause a larger overhead on the network and they also require more processing power. In the maritime domain, the Root CA and Intermediate ("Issuing") CA certificates should have relatively long lifetimes, to avoid having to re-key and re-issue their certificates, while certificates issued to the end entities (vessels, VTS shore stations, etc) can have shorter keys (corresponding to the value of the information they are intended to protect).

The following signature algorithms and key lengths are hence suggested for the electronic signature system. The choice is in line with the recommendations from NSA.

Root CA: Elliptic Curve Digital Signature Algorithm (ECDSA) with message digest algorithm SHA-384, using key size 384 bits and the curve P-384. The validity of the Root CA certificate should be set to 20 years.

Intermediate CA ("Issuing CA"): Elliptic Curve Digital Signature Algorithm (ECDSA) with message digest algorithm SHA-384, using key size 384 bits and the curve P-384. The validity of the Intermediate CA certificate should be set to 10 years.

End entities (vessels, VTS shore stations, etc): Elliptic Curve Digital Signature Algorithm (ECDSA) with message digest algorithm SHA-256, using key size 256 bits and the curve P-256. The validity of the end entity certificates should be set to 3 years.

The electronic signature system must also be designed by in a way that enables both easy and cost-efficient deployment and usage of cryptographic certificates for vessels and other maritime users, which are expected to be offshore with limited bandwidth and network connectivity for longer periods of time. The electronic signature system should also be

designed to enable migration from ECC to future quantum resistant cryptography without excessive costs or effort.

References

[1] National Security Agency | Central Security Service (NSA|CSS). Commercial National Security Algorithm Suite. Available: https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm [Accessed: 2021-02-226].

[2] Public Key Cryptography Standard (PKCS) #1, RSA Encryption Standard .

[3] ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). .

[4] NSA, "The Case for Elliptic Curve Cryptography," 2009. [Online]. Available: http://web.archive.org/web/20090117023500/http://www.nsa.gov/business/programs/elliptic_curve.shtml [Accessed: 2021-02-226].

APPENDIX 3

Guidelines for signature system in an international shipping environment

The digital system or platform should not rely on the receiver of a message having access to an Internet connection when the signature check is performed. This is particularly relevant for ship-to-ship messages or messages received over a message-based communication channel but may also be necessary in cases where the Internet connection bandwidth is limited, or the connection is of low quality.

There should be one or more internationally known and available repositories for the information needed to verify a signature. The repositories should as a minimum include all ships with an IMO number, all VTS, all mandatory ship reporting systems and all maritime single windows and all port community systems that the ships may be required to communicate with.

The repository could also include information about how the entities can be contacted.

Ships should be able to copy all the information from the repositories when in port, either through the Internet, when they have access to this, or by other means.

The strength of the electronic signature should be sufficient for its intended usage, i.e. in common ship communication related to safety and security.

The technology used on board the ship should make it impossible to copy or steal the signature device without the ship crew noticing it.

The technology used should allow the ship to have backup signature devices in case one is broken or misplaced.

The signature technology should allow distribution of signature devices to the ships through commonly available channels such as mail or courier. It should not be necessary to have specialist personnel installing the signature device.

The technology used should allow a suitable minimum usage time for the signature device before it needs replacement.

NOTE – It is normally necessary to change the electronic signature at regular intervals to avoid that hostile parties over time gain enough information to replicate the function of the signature device.

APPENDIX 4

Guidelines for low-bandwidth communication systems

The size of the service requests should be as small as possible, preferably small enough to make it useful in the emerging VHF Data Exchange System (VDES) or similar narrowband channels.

References and bibliography

[5] ISO 20415: Trusted mobile e-document framework — Requirements, functionality and criteria for ensuring reliable and safe mobile e-business.

[6] ISO 15022-1: Securities -- Scheme for messages (Data Field Dictionary) -- Part 1: Data field and message design rules and guidelines.

[7] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[8] United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005).