INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

FAL.5/Circ.46
1 June 2022

GUIDELINES ON AUTHENTICATION, INTEGRITY AND CONFIDENTIALITY OF INFORMATION EXCHANGES VIA MARITIME SINGLE WINDOWS AND RELATED SERVICES

1 The Facilitation Committee, at its forty-sixth session (9 to 13 May 2022), approved the annexed *Guidelines on authentication, integrity and confidentiality of information exchanges via maritime single windows and related services*.

2 Member States and international organizations are invited to bring the Guidelines to the attention of all parties concerned.

3 Member States and international organizations are also invited to bring to the attention of the Committee, at the earliest opportunity, the results of the experience gained from the use of the Guidelines for consideration of action to be taken.

***

ANNEX

GUIDELINES ON AUTHENTICATION, INTEGRITY AND CONFIDENTIALITY OF INFORMATION EXCHANGES VIA MARITIME SINGLE WINDOWS AND RELATED SERVICES

Table of Contents

1 Summary

These Guidelines provide general requirements for a digital system or platform that can be used to provide authentication, integrity and confidentiality in digital information exchanges via maritime single windows and related services. These requirements are developed primarily for information exchanges related to the ship, its passage through international and national waters and its port calls. For information exchanges that rely on VHF Data Exchange System (VDES), appendix 3 (Guidelines to signature system in an international shipping environment) and appendix 4 (Guidelines to low-bandwidth communication systems) provides the general requirements for signature systems to be used in VDES context.

These Guidelines will define some general message exchange "patterns" that are used as reference for the requirements to the electronic signature. Different patterns will have some differences in requirements.

These Guidelines will also define some requirements to message "metadata". This is data that is not related to the information transmitted in the messages, but rather to requirements from the transmission processes. Many of the metadata are directly related to message security and safety, e.g. reference codes and timestamp, but for completeness, also more general administrative elements have been included. A summary of the metadata elements is included in the appendix 1.

The message patterns and requirements in these guidelines are based on data being sent by a sender to a receiver when a service is requested by the sender, i.e. "data push" as seen from the sender. It is also possible to create patterns based on "data pull", i.e. that the receiver actively fetches data from some predefined source after the service has been requested. However, this principle is not yet common in the maritime domain and is not discussed here. Most of the requirements specified in this guideline will still apply but may manifest themselves differently in a data pull environment.

These Guidelines are as far as possible based on existing standards and specifications. Thus, the requirements presented in these guidelines will be similar to what can be found in several other documents. However, the maritime environment has some special features that need consideration that has been specifically addressed in these guidelines, e.g. the international nature of the business, the fact that ships may not always be connected to the Internet and the relatively high cost and/or low bandwidth of communication that applies to many of today's satellite communication systems.

While these Guidelines have been prepared by the Facilitation Committee related to requirements in the Facilitation Convention, there are also other mandatory message exchanges that could benefit from digitalization, e.g. mandatory ship reporting and new e-navigation services.

2 Terminology and definitions

Application Programming Interface (API): A type of software interface offer a services to other pieces of services and provides a connection between applications and systems.

Cancellation: This is a form of update request that cancels the request for a service.

Sender: The party requesting a service from a receiver by sending an initial request and any additional update requests that may be required by the service. The sender is the initiator of the message exchange and can be a ship or a land-based entity.

Digital Signature:[1] Data appended to, or cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the unit and protect against forgery by, for example, the recipient.

Electronic signature:[2] Data which, when appended to a message, enable the receiver of the message to authenticate its origin and integrity (adapted from ISO 20415).

Information Submission: Data or messages that need to be submitted by the ship or agent, for example pre-arrival information, that does not contain any requests. This will usually require the receiving system or platform to expose an API or webservice to receive the data.

Integrity: Attribute of a document whose content is unimpaired.

Maritime Single Window (MSW): A system or digital platform that enables all the information required by public authorities in connection with the arrival, stay and departure of ships, persons and cargo, to be submitted without duplication

Message: Series of data fields and/or blocks of data fields communicated from one party to another to convey meaningful business information (ISO 15022-1).

Message status: The message status should contain information as to how the request will be further processed, e.g. that the request was already accepted and/or that a service request status will be sent later. It may also return that the request was invalid, in which case it may not be processed further or that additional information is needed, in which case an update request should be sent.

Request: A message that is sent by the sender as a request for a service to the receiver. Several update requests, possibly including a cancellation of the whole or parts of the service, may be sent during a session.

Request reference code: A unique code assigned by the sender to a request, to allow the receiver to make an unambiguous reference to that message. A reference code may be made unique, e.g. by combining the ship's IMO and/or voyage number with a serial number.

Secure channel: Communication channel providing the confidentiality and authenticity of exchanged messages. A secure channel may be available over internet connections through use of protocols such as HTTPS (Secure Hypertext Transmission Protocol).

Receiver: The receiver of a request which provides or facilitates the associated service. Often, this will be an administration type land-based entity, such as a maritime single window, a ship reporting system or another port or coastal state facility. However, the receiver can also be a ship or any other entity that receives a request from a sender.

Service: A request from the sender to the receiver (including a report), that the receiver accepts or rejects. Note that a session may include more than one service, e.g. that a number of FAL forms are requested to be accepted in one session.

Service request status: A message sent by the receiver to verify that a request was received.

---

1 There is a difference between digital signature and electronic signature. The key difference is: digital signature is used to secure a document/message while an electronic message is used to verify a document/message.

2 Electronic signature, as defined here, is the same as "electronic seal", as defined in the bibliography reference number [3].

Session: A sequence of messages that is related to one and the same initial request.

Session reference code: A unique code assigned by the receiver. It can, e.g. be the same as the initial request reference code. The session reference code is used by the sender and receiver to identify later messages related to the same session. "Unique" means that the code should not be reused within a reasonable time interval.

Signature device: Special software or hardware, e.g. a smart card, can be used to sign outgoing messages or check incoming signatures. In this guideline, this is called a signature device. For physical security, there will normally only be one or two such devices on a site. Access to the device from other computers will normally be via network connections.

Timestamp: Date and time, including the time zone at which a certain event occurs (adapted from ISO 8601 in UTC format). In the context of this document, the event is normally the transmission of a message and the timestamp is affixed to the message. The timestamp should have sufficient resolution to make it unlikely that two consecutive messages from the same sender have the same timestamps.

Update request: This is a request that is sent as an update to the initial request. A special form of update request is a cancellation. Normally, an update request cannot be sent after a service request status has been generated by the receiver, but this will depend on the service implementation.

3 Introduction

Digital information exchanges in the maritime sector are desirable for many reasons, e.g.:

.1 to reduce the administrative workload for the involved parties, including the seafarers. This is done by using computers to automate the processes related to information sending, reception and processing; and

.2 to improve the quality of information used to plan and execute maritime and port operations. Electronic transmissions avoid misunderstandings and allow more complex information to be exchanged efficiently.

However, electronic communication may fail for several reasons, e.g.:

.1 technical errors may change some information or may cause some messages not to be delivered;

.2 unfaithful servants may, e.g. falsify message content or deny that certain messages were received or sent; and

.3 malicious cyberattacks that may have commercial or threat objectives or are just random attempts to break into interesting technical systems, may introduce false messages or change the content of messages.

It is necessary to establish enough trust in the automated processes to avoid that the persons with overall responsibility for the correctness of the processes need to double-check the information and the results of the processing. If this is not achieved, the workload may be increased rather than decreased. Transmission failures may also have safety or security consequences, the severity being dependent on the criticality of the information contained in the messages.

This trust cannot be established unless the safety and security mechanisms inherent in the paper-based systems are replicated in the digital information exchanges. These mechanisms are:

.1 *Integrity* (printed on paper – difficult to change): The content of a message cannot be tampered with;

.2 *Authenticity* (signatures, stamps, seals): The identity of the originator of the message can be verified; and

.3 *Confidentiality* (sealed envelope): The contents of the message cannot be read by others than the intended receiver.

In addition, one will also need an additional mechanism that can be derived from the above mechanisms:

.4 *Non-repudiation* (registered mail, courier): Providing proof that the message was delivered to the recipient. For digital information exchanges, this requires some form of acknowledgement from the receiver that the message was delivered.

These guidelines will specify requirements to a system or digital platform that implement these security and safety mechanisms.

4 Application Programming Interface (API)

The use of Application Programming Interfaces (APIs) has become widespread and is the most common mechanism in use today to connect and interoperate with other systems and applications. It is therefore recommended to use API to facilitate interoperability between systems, MSW and other related services, and there is a need to perform authentication to ensure that the request is verified and validated before information exchange can take place.

There are three common methods how API can be authenticated:

.1 HTTP Basic Authentication – In this approach, an HTTP user agent will provide a username and password via the HTTP header for the authentication.

.2 API Keys – In this approach, a unique generated value will be assigned to the calling application (requester), to signify that the requestor is known, so that when the requestor sends a request with the API keys as one of the request parameters, the unique key is used to authenticate the requestor.

.3 OAuth – In this approach, the calling application (requestor) will first send a request to the system for an access token. The system will then return the access token to the requestor. Thereafter, the requestor will then send another request together with the access token to the system to validate the token before information exchange can take place.

There are no specific rules or guidelines on which API authentication method is the best, as it depends on the situation and environment where the APIs are implemented.

Note that authentication ensured using API mechanisms alone will not make it possible for the sender to prove that a specific message content was sent (integrity). Unless the actual message was digitally signed, there is a possibility for someone on the receiver side to tamper with the content without the sender being able to prove that this was the case. To overcome this, there is a need to provide communications security over a computer network. One of the widely used protocols to digitally sign the message or provide cryptography, including the authentication, integrity and confidentiality is the Transport Layer Security (TLS)/Secure Socket Layer (SSL).

5 Single sign-on internationally

Independent of the use of an API as discussed in section 4, one should also consider the possible benefit of having an internationally recognized public key certificate used in authentication to the receiving system. This would allow the ship or its agent to use their public certificate in the authentication process without any prior registration to the system.

6 General requirements for all electronic messages

All messages should include a timestamp to provide assurance of the existence and qualities of a certain data message at a certain point in time.

The message may also include a valid-to time to specify the maximum time the message content can be considered valid.

All messages of any importance should be encrypted. The encryption should protect the integrity of every important data element in the message, the sending timestamp as well as any reference codes.

It is not sufficient to rely on a secure channel for integrity checks, as persons at the receiving side can tamper with the data, or the sender may deny having sent some of the data. For full protection, it is necessary to have an electronic signature included in each message.

The receiver of an encrypted message must verify the authenticity of the sender as well as the integrity of the signed information before the message content is processed. If a problem is detected, the sender should be notified, and the message should be discarded.

> NOTE: For broadcast message patterns, one may not want to notify the sender as the sender may be flooded by messages. However, the falsified message should, if possible, cause a warning to a system operator.

A message with a timestamp that is older than already received messages from the same sender or which has a time stamp that is "too old" should be discarded and the sender notified. The actual value of "too old" will depend on the service requested or provided as well as the communication systems in use.

The receiver and the sender should store copies of all outgoing and incoming messages as proof of transmission and reception. These copies should not be deleted until the further message exchange proves that the messages were indeed received and processed by the other party.

All senders and receivers of electronic messages need to have their time sufficiently synchronized to detect timestamp problems as shown above.

7 Requirements for sender

The sender must specify the service requested, e.g. reporting, port clearance, port service etc., if any.

The sender should generate and add a unique request reference code to all outgoing requests, so that the receiver can provide a message status for each unique request. Thus, all update requests should get a new request reference code.

Update requests should include the session reference code.

If a message status fails to arrive after a reasonable time, normally defined by the type of request, the sender should resend the message with the same request reference and session reference codes if already obtained. The timestamp should be updated.

If a service request status to a request fails to arrive within the time limit defined by the last received message status, the sender should send a renewed request to the receiver. This may use the same request reference code or a new one, dependent on the content of the repeat request. The timestamp should be updated.

For technical and/or security reasons, a sender and ships in particular, may have restrictions on how a receiver can deliver messages to the sender. It may be necessary that the sender specifies how the message status and service request status should be sent to the sender when it sends a request. In this case, also the method of delivery should be encrypted.

8 Requirements for receiver

In many cases, proof of the receiver's reception of a request is required. Thus, the receiver should send a message status for any received request to the client. The message status must contain the request reference code. The receiver may provide the functionality to generate the unique request reference code and send it to the sender.

In general, the receiver should acknowledge all received messages unless, e.g. a service request status is sent immediately after the reception of a request. In this case, the service request status can include the message status.

For requests that require a later service request status, the message status should specify the maximum time the sender needs to wait for the service request status. When the sender sends updates to the request, this time limit may be updated in the message status to the update request.

Unless the first message status is also the final service request status, the first message status from the receiver should include a unique session reference code that can be used by later update requests to identify the session that the update request refers to.

The receiver must return a service status code in message status and service request status to inform the sender about the status of the request, e.g. error in data, denies, in progress, successfully completed, etc. If there are errors, more specific error service request status information should also be included.

9 Patterns for message exchanges

Message exchanges are often executed in an asynchronous manner as shown in the diagrams below. Asynchronous message exchanges are any type of communication where one entity submits data or a request, and then there is a time lag before the recipients validates the data and offer the service request status, if any.

In general, digital information exchanges consist of more than one message as illustrated in the following figures. Each of the figures illustrates a message "pattern", i.e. a typical way to exchange messages, independently of the functionality that the exchange implements or represents.

The message patterns discussed in this section are included to provide guidance on how messages are normally used in longer sequences of message exchanges or "sessions". This has implications for secure and safe transmission of messages as the integrity and authenticity must be protected throughout the whole session. This requires, e.g. that messages should include timestamps as well as reference codes so that one message from one session cannot be taken out of its context and used to interfere with the same session at a later time or in another session altogether.

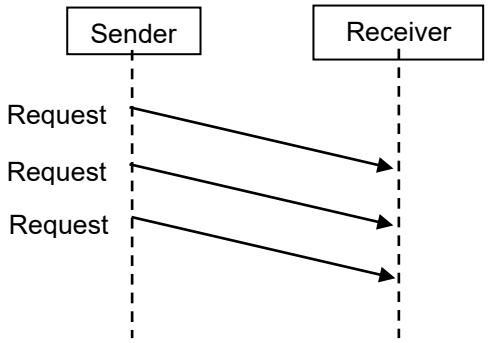

Figure 1 – Simple information distribution

Figure 1 shows the simplest message exchange. The sender sends information to one or more receivers without expecting any service request status or message status. An example of such a pattern is the transmission of Automatic Identification System (AIS) position reports or static ship information messages. As for AIS, this pattern will often use a broadcast mechanism to distribute the information to all parties in geographic vicinity. The pattern will also normally rely on periodic retransmission of the request to avoid problems in cases where one or more messages are lost. The sender repeats the information regularly and does not generally have to worry about loss of data or messages. However, depending on the criticality of the information sent, it may be necessary to add an electronic signature and a timestamp to verify the identity of the sender and to avoid that hostile parties interfere with the information exchanges, e.g. by repeating old messages at a later time.

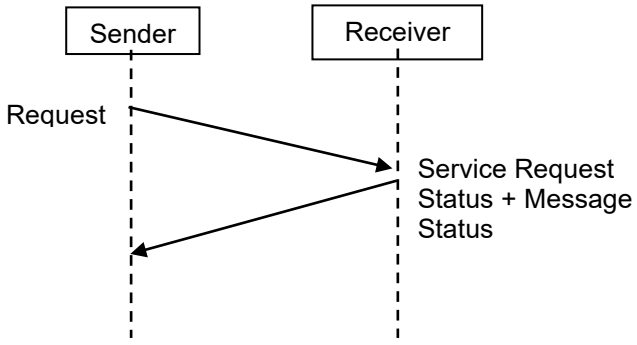

Figure 2 – Simple request and service request status pattern

Figure 2 shows another relatively simple message exchange. The sender sends some information to the receiver and immediately receives a service request status of message reception as well as a service request status to the information or service requested.

Figure 3 illustrates a somewhat more complicated information or service request. The figure shows a typical case where the receiver first acknowledges the receipt of the request message, without answering directly to the request, and later gives the service request status to the requested service.

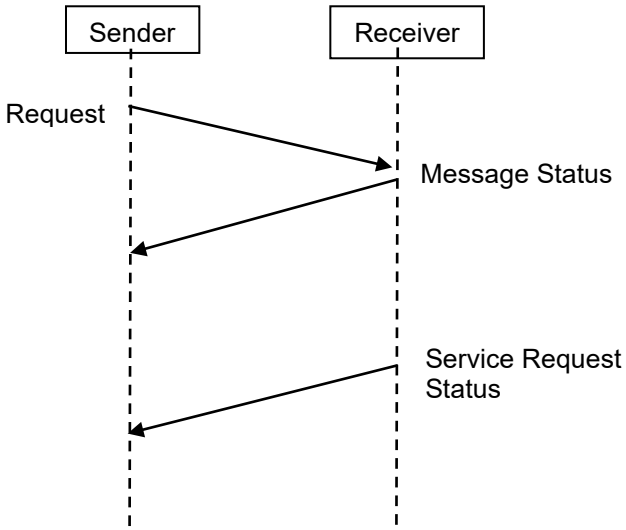

Figure 3 – Basic sequence diagram for information or service request

In some cases, the sender can send update requests at later points in time until a final service request status to the requests is received. This is illustrated in figure 4.

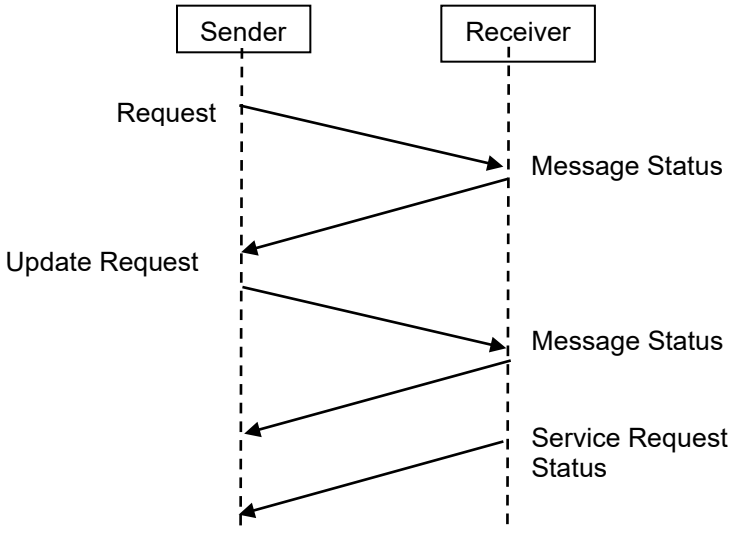

Figure 4 – Sequence diagram with updated request

One of these update requests may also be a cancellation of the initial request. In most cases a cancellation will be answered with a combined message status and service request status, informing the sender that the message was received, and that the cancellation is accepted. However, in some cases a delayed service request status may be required also for the cancellation.

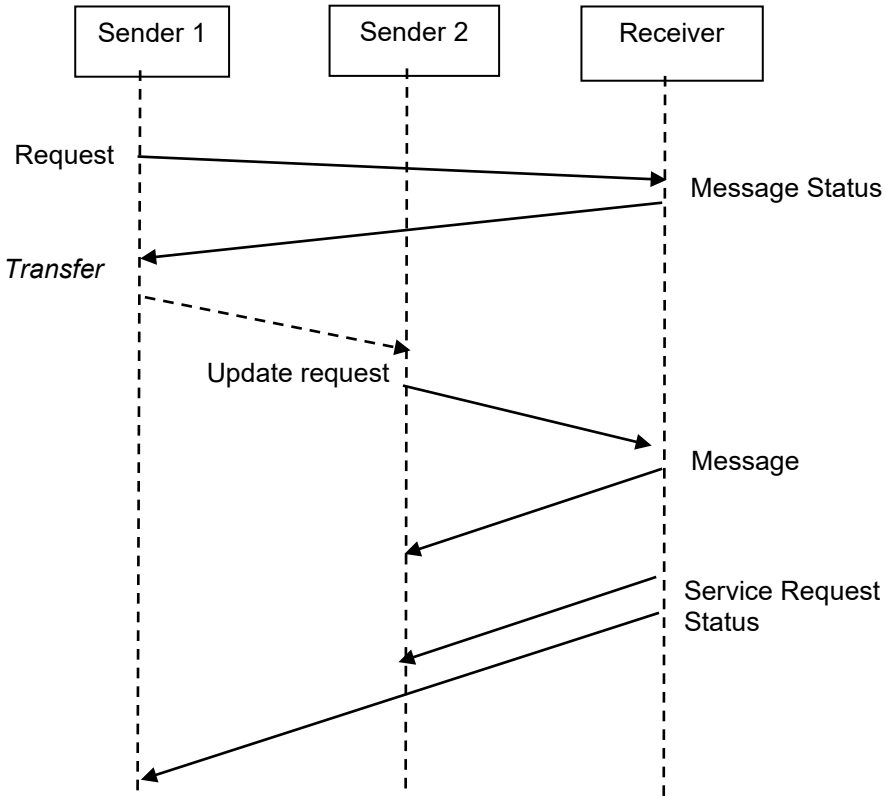

Figure 5 – Sequence diagram with more than one sender

A more complex pattern can be seen in figure 5. Here, several senders cooperate to supply the receiver with the required information. This could be the case where a ship sends some information to a maritime single window and then asks, e.g. the agent or the management company to provide additional details. In this scenario, all senders need to use the same session reference code, which requires some form of communication between them (see "transfer" dashed arrow). The receiver should send a service request status to all senders, unless a main sender is defined, then it may send only to the main sender.

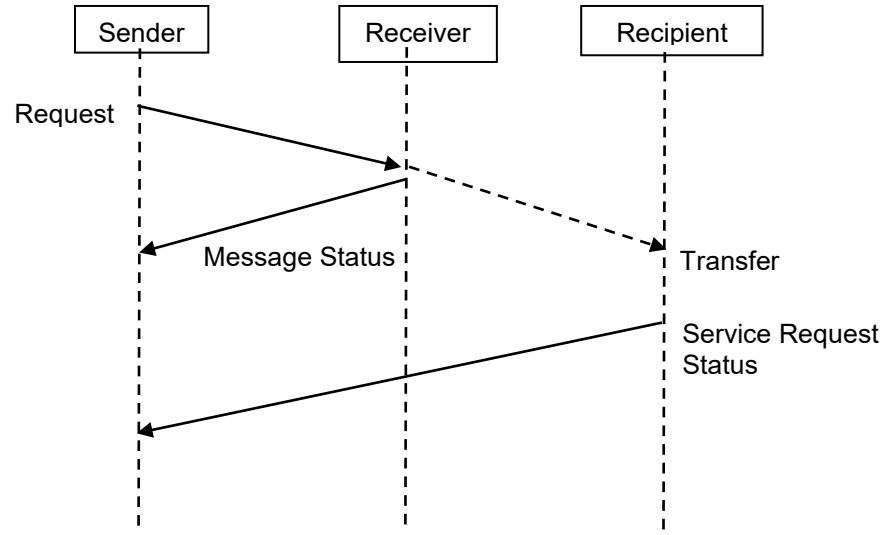

Figure 6 – Sequence diagram through MSW

The pattern in figure 6 is being used specifically by MSW systems where the MSW is the system receiving a request, and acknowledging the request, while the recipient is a different entity. Figure 7 is an expansion of a service requested through a MSW when the service requested will be, eventually, delivered by more than one recipient/service provider.

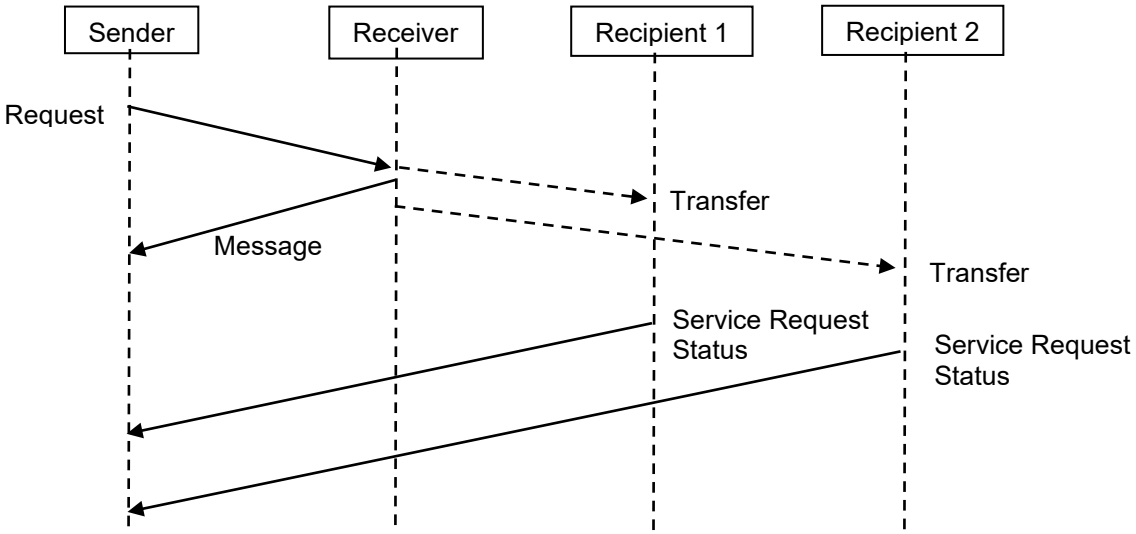

Figure 7 – Sequence diagram through MSW (Multiple recipients and service request status)

Note that several other patterns can be defined, combining two or more of the shown patterns. Typical examples are merging message status and service request status, allowing update requests after the service request status have been sent or allowing multiple receivers of a single request, in which case more than one message status and service request status may be required. However, the patterns shown here should be general enough for these guidelines.

10 Requirements related to confidentiality

Confidentiality requires that the content of the message is encrypted with a minimum encryption key.

Transmission of messages over a secure channel will provide confidentiality, without the sender having to encrypt the message content itself. However, it may still be necessary to encrypt the message content if it needs to be protected from being read by some parties that can get access to the message at the receiving side.

Digital systems and platforms often rely on public-key cryptography and asymmetric keys which may not be suitable for encryption of larger messages. A digital system or platform must, if necessary, contain provisions for generation and exchange of, e.g. symmetric keys that can be used to encrypt messages of the maximum sizes used between senders and receivers.

References and bibliography

[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] 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.

[4] United Nations Convention on the Use of Electronic Communications in International Contracts (New 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 havs 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 three 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.