ORGANISATION MARITIME INTERNATIONALE

F

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

FAL.5/Circ.46
1er juin 2022

DIRECTIVES SUR L'AUTHENTIFICATION, L'INTÉGRITÉ ET LA CONFIDENTIALITÉ DES ÉCHANGES DE RENSEIGNEMENTS À L'USAGE DES GUICHETS UNIQUES MARITIMES ET DES SERVICES CONNEXES

1 À sa quarante-sixième session (9-13 mai 2022), le Comité de la simplification des formalités a approuvé les Directives sur l'authentification, l'intégrité et la confidentialité des échanges de renseignements à l'usage des guichets uniques maritimes et des services connexes, telles qu'elles figurent en annexe.

2 Les États Membres et les organisations internationales sont invités à porter les présentes Directives à l'attention de toutes les parties intéressées.

3 Les États Membres et les organisations internationales sont également invités à informer le Comité, dans les meilleurs délais, des résultats de l'expérience acquise lors de l'application des Directives, afin qu'il puisse examiner les mesures à prendre.

***

ANNEXE

DIRECTIVES SUR L'AUTHENTIFICATION, L'INTÉGRITÉ ET LA CONFIDENTIALITÉ DES ÉCHANGES DE RENSEIGNEMENTS À L'USAGE DES GUICHETS UNIQUES MARITIMES ET DES SERVICES CONNEXES

Table des matières

1 Résumé

Les présentes Directives énoncent des prescriptions générales applicables à un système ou plateforme numérique qui peut être utilisé pour l'authentification, l'intégrité et la confidentialité des échanges de renseignements électroniques par le biais des guichets uniques maritimes et des services connexes. Ces prescriptions ont été élaborées essentiellement pour les échanges de renseignements relatifs au navire, à ses traversées des eaux nationales et internationales et à ses escales dans les ports. Pour les échanges de renseignements qui reposent sur le système d'échange de données en VHF (VDES), l'appendice 3* (Directives sur le système de signature dans un environnement de transport maritime international) et l'appendice 4* (Directives sur les systèmes de communication à faible bande passante) fournissent les prescriptions générales applicables aux systèmes de signature à utiliser dans le contexte du VDES.

Les présentes Directives définissent certains "modèles" généraux d'échange de messages qui servent de référence pour les prescriptions applicables à la signature électronique. Les prescriptions divergent en fonction des différents modèles.

Les présentes Directives définissent également certaines prescriptions applicables aux "métadonnées" des messages. Ces données ne concernent pas les renseignements communiqués dans les messages, mais plutôt les prescriptions relatives aux processus de transmission. Bon nombre de ces métadonnées concernent directement la sécurité et la sûreté des messages, tels que les codes de référence et l'horodatage. Toutefois, par souci d'exhaustivité, des éléments administratifs plus généraux ont également été intégrés. On trouvera un résumé des éléments de métadonnées à l'appendice 1* du présent document.

Les modèles d'échange de messages et les prescriptions qui figurent dans les présentes Directives sont fondés sur les données qu'un expéditeur transmet à un destinataire lorsqu'il demande un service, c'est-à-dire "la transmission de données" du point de vue de l'expéditeur. Il est également possible de créer des modèles fondés sur "l'extraction de données", c'est-à-dire lorsque le destinataire extrait directement des données à partir d'une source prédéfinie après la demande de service. Toutefois, ce principe n'est pas encore très répandu dans le domaine maritime et il n'est pas examiné dans le cadre du présent document. La plupart des prescriptions énoncées dans les présentes Directives continueront de s'appliquer mais elles pourraient se manifester différemment dans un contexte d'extraction de données.

Dans la mesure du possible, les présentes Directives sont fondées sur des normes et spécifications existantes. Ainsi, les prescriptions énoncées dans les présentes Directives sont semblables à celles qui figurent dans de nombreux autres documents. Toutefois, l'environnement maritime présente certaines caractéristiques spécifiques dont il faut tenir compte et dont les présentes Directives traitent tout particulièrement, comme la dimension internationale du secteur, le fait que les navires ne peuvent pas toujours se connecter à Internet, les coûts relativement élevés des actuels systèmes de communication par satellite et/ou la faible bande passante qui caractérise nombre d'entre eux.

Bien que les présentes Directives aient été élaborées par le Comité de la simplification des formalités sur la base des prescriptions énoncées dans la Convention FAL, d'autres échanges de messages obligatoires pourraient également tirer parti de la numérisation, comme les comptes rendus obligatoires de navires et les nouveaux services d'e-navigation.

* En anglais uniquement.

2 Terminologie et définitions

Interface de programmation d'applications (API) : Type d'interface logicielle offrant un service à d'autres éléments de services et assurant une connexion entre les applications et les systèmes.

Annulation : Type de demande de mise à jour qui annule une demande de service.

Expéditeur : Partie qui formule une demande de service auprès d'un destinataire en lui adressant une demande initiale ainsi que toutes les autres demandes de mise à jour qui pourraient être requises dans le cadre de ce service. L'expéditeur est l'initiateur de l'échange de messages et il peut être un navire ou une entité à terre.

Signature numérique[1] : Données ajoutées à une unité de données ou transformation cryptographique de celle-ci, qui permettent à un destinataire de l'unité de données de prouver la source et l'intégrité de l'unité et de se protéger contre la falsification par le destinataire, par exemple.

Signature électronique[2] : Données qui, lorsqu'elles sont jointes à un message, permettent au destinataire du message de vérifier son origine et son intégrité (texte adapté à partir de la norme ISO 20415).

Soumission de renseignements : données ou messages qui doivent être soumis par le navire ou l'agent, par exemple des informations préalables à l'arrivée, et qui ne contiennent aucune demande. Pour cela, il faut généralement que le système ou la plateforme de réception expose une API ou un service Web pour recevoir les données.

Intégrité : Attribut d'un document dont le contenu n'est pas altéré.

Guichet unique maritime (MSW) : Système ou plateforme numérique permettant de soumettre sans double emploi toutes les informations requises par les autorités publiques en rapport avec l'arrivée, le séjour et le départ des navires, des personnes et des cargaisons.

Message : Ensemble de champs de données et/ou de blocs de champs de données qui, échangés d'une partie à une autre, permettent de communiquer des informations significatives (norme ISO 15022-1).

État du message : L'état du message doit contenir des informations sur la manière dont la demande sera traitée ultérieurement, par exemple que la demande a déjà été acceptée et/ou qu'un état de la demande de service sera envoyé ultérieurement. Il peut également indiquer que la demande n'est pas valide, auquel cas elle ne sera pas traitée ou que des informations supplémentaires sont nécessaires, auquel cas une demande de mise à jour doit être envoyée.

Demande : Message envoyé au serveur par l'expéditeur sous la forme d'une demande de service. Il est possible d'envoyer plusieurs demandes de mise à jour au cours d'une même session, y compris éventuellement une demande d'annulation partielle ou totale du service.

---

1 Il existe une différence entre la signature numérique et la signature électronique. La différence essentielle est la suivante : la signature numérique est utilisée pour sécuriser un document/message tandis que le message électronique est utilisé pour vérifier un document/message.

2 Le concept de signature électronique, tel que défini dans le présent document, est le même que le concept de "scellé électronique" défini dans la référence bibliographique [3].

Code de référence de la demande : Code unique attribué à une demande par l'expéditeur afin que le destinataire puisse se référer à un message de manière non équivoque. Il est possible de rendre un code de référence unique en combinant par exemple le numéro OMI et/ou du voyage du navire et un numéro de série.

Canal sécurisé : Canal de communication permettant de garantir la confidentialité et l'authenticité des messages échangés. Dans le cadre d'une connexion Internet, l'utilisation de protocoles tels que le protocole HTTPS (Secure Hypertext Transmission Protocol) permet d'accéder à un canal sécurisé.

Destinataire : Destinataire d'une demande qui assure ou facilite le service correspondant. Il s'agira souvent d'une entité de type administratif à terre, telle qu'un guichet unique maritime, un système de comptes rendus de navires ou une autre installation portuaire ou relevant d'un État côtier. Toutefois, le destinataire peut aussi être un navire ou toute autre entité qui reçoit une demande de la part d'un expéditeur.

Service : demande de l'expéditeur au destinataire (y compris un rapport), que le destinataire accepte ou rejette. Notez qu'une session peut inclure plus d'un service, par exemple qu'un certain nombre de formulaires FAL sont demandés pour être acceptés dans une session.

État de la demande de service : message envoyé par le destinataire pour vérifier qu'une demande a été reçue.

Session : Série de messages se rapportant à une seule et même demande initiale.

Code de référence de la session : Code unique attribué par le destinataire. Ce code peut, à titre d'exemple, être le même que le code de référence de la demande initiale. Le code de référence de la session est utilisé par l'expéditeur et le destinataire afin d'identifier les derniers messages envoyés dans le cadre de ladite session. Le terme "unique" signifie que le code ne devrait pas être réutilisé pendant un intervalle de temps suffisant.

Dispositif de signature : Logiciel spécial ou matériel informatique, comme une carte à puce, pouvant être utilisé pour signer les messages sortants ou procéder à la vérification des signatures reçues. Dans le cadre des présentes Directives, ce logiciel ou ce matériel informatique est appelé "dispositif de signature". Pour la sécurité physique, il n'y aura normalement qu'un ou deux dispositifs de ce type sur un site. L'accès au dispositif depuis d'autres ordinateurs se fait normalement via des connexions réseau.

Horodatage : Date et heure, y compris le fuseau horaire, auxquelles se produit un événement donné (texte adapté à partir de la norme ISO 8601 au format UTC). Dans le contexte du présent document, l'événement est normalement la transmission d'un message et l'horodatage est apposé sur le message. L'horodatage doit avoir une résolution suffisante pour qu'il soit peu probable que deux messages consécutifs provenant du même expéditeur aient le même horodatage.

Demande de mise à jour : il s'agit d'une demande qui est envoyée en tant que mise à jour de la demande initiale. Une forme particulière de demande de mise à jour est l'annulation. En règle générale, une demande de mise à jour ne peut être envoyée après que le destinataire a généré un état de la demande de service, mais cette condition dépendra de la mise en œuvre du service.

3 Introduction

Les échanges de renseignements électroniques dans le secteur maritime sont souhaitables à plus d'un titre, notamment pour :

.1 réduire les charges administratives qui pèsent sur les parties concernées, y compris les gens de mer. Ce résultat peut être atteint en utilisant des ordinateurs pour automatiser les processus liés à la transmission, à la réception et au traitement des renseignements; et

.2 améliorer la qualité des renseignements utilisés pour planifier et exécuter les opérations maritimes et portuaires. Les transmissions électroniques permettent d'éviter les malentendus et d'échanger des renseignements plus complexes de manière efficace.

Toutefois, il est possible que les communications électroniques échouent, et ce pour plusieurs raisons :

.1 les erreurs techniques sont susceptibles de modifier certains renseignements ou d'entraîner la non-transmission de certains messages;

.2 les personnes malintentionnées peuvent par exemple falsifier le contenu des messages ou nier qu'elles ont reçu ou transmis certains messages; et

.3 les cyberattaques malveillantes dont les objectifs peuvent être de nature commerciale ou menaçante, ou celles qui sont simplement des tentatives visant à pénétrer de façon aléatoire dans des systèmes techniques d'intérêt, sont susceptibles d'introduire de faux messages ou de modifier le contenu des messages.

Il est nécessaire d'établir un niveau de confiance suffisant à l'égard des procédures automatisées pour faire en sorte que les personnes chargées d'assurer l'exactitude des procédures n'aient à revérifier les renseignements et les résultats issus du traitement des données. Dans le cas contraire, il se pourrait que la charge de travail augmente plutôt qu'elle ne diminue. Les défauts de transmission peuvent aussi avoir des conséquences en matière de sécurité ou de sûreté, dont la gravité dépend du degré de criticité des renseignements qui figurent dans les messages.

Ce niveau de confiance ne peut être établi qu'en reproduisant les mécanismes de sécurité et de sûreté propres aux systèmes papier dans les échanges de renseignements électroniques. Les mécanismes en question sont les suivants :

.1 *Intégrité* (messages imprimés sur papier et donc difficilement modifiables) : le contenu du message ne peut être falsifié;

.2 *Authenticité* (signatures, cachets, scellés) : l'identité de l'expéditeur du message peut être vérifiée; et

.3 *Confidentialité* (enveloppe scellée) : le contenu du message ne peut être lu par d'autres personnes que le destinataire prévu.

En outre, il faudra également prévoir un mécanisme supplémentaire qui pourra s'appuyer sur les mécanismes susmentionnés :

.4 *Non-répudiation* (envoi recommandé, service de messagerie) : preuve que le message a été transmis au destinataire. Dans le cas des échanges de renseignements électroniques, il faudra que le destinataire puisse accuser réception du message, sous une forme ou sous une autre.

Les présentes Directives énoncent des prescriptions applicables à un système ou une plateforme électronique qui tiennent compte de ces mécanismes de sécurité et de sûreté.

4 Interface de programmation d'applications (API)

L'utilisation des interfaces de programmation d'applications (API) s'est généralisée et constitue le mécanisme le plus courant utilisé aujourd'hui pour se connecter et interagir avec d'autres systèmes et applications. Il est donc recommandé d'utiliser l'API pour faciliter l'interopérabilité entre les systèmes, les guichets uniques maritimes et d'autres services connexes, et il est nécessaire de procéder à une authentification pour s'assurer que la demande est vérifiée et validée avant que l'échange de renseignements puisse avoir lieu.

Il existe trois méthodes courantes d'authentification des API :

.1 Authentification de base HTTP - Dans cette approche, l'agent utilisateur HTTP fournit un nom d'utilisateur et un mot de passe via l'en-tête HTTP pour l'authentification.

.2 Clés API - Dans cette approche, une valeur unique générée sera attribuée à l'application appelante (demandeur), pour signifier que le demandeur est connu, de sorte que lorsque le demandeur envoie une demande avec les clés API comme l'un des paramètres de la demande, la clé unique est utilisée pour authentifier le demandeur.

.3 OAuth - Dans cette approche, l'application appelante (le demandeur) envoie d'abord une demande au système pour obtenir un jeton d'accès. Le système renvoie alors le jeton d'accès au demandeur. Par la suite, le demandeur enverra une autre demande accompagnée du jeton d'accès au système pour valider le jeton avant que l'échange de renseignements puisse avoir lieu.

Il n'existe pas de règles ou de directives spécifiques concernant la meilleure méthode d'authentification des API, car cela dépend de la situation et de l'environnement dans lequel les API sont mises en œuvre.

Il y a lieu de noter que l'authentification assurée par les seuls mécanismes de l'API ne permettra pas à l'expéditeur de prouver qu'un contenu spécifique du message a été envoyé (intégrité). Si le message n'est pas signé numériquement, il est possible que quelqu'un du côté du destinataire en altère le contenu sans que l'expéditeur puisse le prouver. Pour remédier à ce problème, il est nécessaire d'assurer la sécurité des communications sur un réseau informatique. L'un des protocoles les plus utilisés pour signer numériquement le message ou fournir une cryptographie, y compris l'authentification, l'intégrité et la confidentialité, est le Transport Layer Security (TLS)/Secure Socket Layer (SSL).

5 Authentification unique à l'échelle internationale

Indépendamment de l'utilisation d'une API, comme indiqué à la section 4, il convient également d'envisager l'avantage éventuel de disposer d'un certificat de clé publique reconnu au niveau international pour l'authentification du système récepteur. Cela permettrait au navire ou à son agent d'utiliser son certificat public dans le processus d'authentification sans inscription préalable auprès du système.

6 Prescriptions générales applicables à tous les messages électroniques

Tous les messages doivent comporter un horodatage afin de garantir l'existence et les qualités d'un certain message de données à un moment donné.

On pourrait également attribuer une date et une heure de fin de validité à chaque message afin d'indiquer le délai maximum pendant lequel le contenu du message peut être considéré comme valide.

Tous les messages, quelle que soit leur importance, devraient être codés. L'encodage devrait permettre de préserver l'intégrité de chaque élément de données essentiel qui figure dans le message, de la date et de l'heure auxquelles le message a été envoyé et de tous les codes de référence.

Il ne suffit pas d'avoir recours à un canal sécurisé pour procéder aux vérifications de l'intégrité, car des tierces parties pourraient intercepter le message adressé au destinataire et falsifier les données qui y figurent ou l'expéditeur pourrait nier avoir transmis certaines données. Pour assurer une protection complète, il est indispensable que chaque message soit signé électroniquement.

Le destinataire d'un message codé est tenu de procéder à une authentification de l'expéditeur et de vérifier l'intégrité des renseignements signés avant de traiter le contenu du message. Au cas où un problème serait détecté, il faudrait en informer l'expéditeur et rejeter le message.

> NOTE : S'agissant des modèles de diffusion de messages, il pourrait être décidé de ne pas informer l'expéditeur car il pourrait être submergé de messages. Toutefois, dans la mesure du possible, un message d'alerte devrait être transmis à un opérateur du système en cas de falsification d'un message.

Un message dont l'horodatage est plus ancien que les messages déjà reçus du même expéditeur ou dont l'horodatage est "trop ancien" doit être écarté et l'expéditeur doit en être informé. La valeur réelle de "trop ancien" dépendra du service demandé ou fourni ainsi que des systèmes de communication utilisés.

Le destinataire et l'expéditeur devraient conserver une copie de tous les messages entrants et sortants comme preuve de leur transmission et de leur réception. Il ne faudrait pas supprimer ces copies tant que les échanges de messages ultérieurs n'ont pas prouvé que les messages en question ont bien été reçus et traités par l'autre partie.

Le niveau de synchronisation temporelle entre tous les expéditeurs et destinataires de messages électroniques devrait être suffisant pour qu'ils soient en mesure de détecter les problèmes d'horodatage susmentionnés.

7 Prescriptions relatives à l'expéditeur

L'expéditeur est tenu d'indiquer le service demandé, par exemple les services ayant trait aux comptes rendus et à l'accomplissement des formalités portuaires, et les services portuaires, etc., le cas échéant.

L'expéditeur devrait générer et attribuer un code de référence unique à toutes les demandes sortantes afin que le destinataire puisse envoyer état du message pour chaque demande. Par conséquent, un nouveau code de référence devrait être attribué à toutes les demandes de mise à jour.

Les demandes de mise à jour devraient inclure le code de référence de la session.

Dans l'hypothèse où un état du message n'aurait pu être transmis à l'issue d'un délai raisonnable, lequel dépend généralement du type de demande, l'expéditeur devrait retransmettre le message en utilisant les mêmes codes de référence de la demande et de la session s'ils sont disponibles. L'horodatage devrait alors être mis à jour.

Dans l'hypothèse où une demande de service n'aurait pu recevoir de réponse à l'issue du délai prévu dans l'état du message le plus récent, l'expéditeur devrait transmettre une nouvelle demande au destinataire. En pareil cas, il serait possible d'utiliser le même code de référence que celui de la demande initiale ou d'en utiliser un nouveau, en fonction de la teneur de cette nouvelle demande. L'horodatage devrait alors être mis à jour.

Pour des raisons techniques et/ou de sécurité, les expéditeurs et les navires en particulier pourraient notamment décider d'imposer des restrictions au destinataire concernant les moyens à utiliser pour leur transmettre des messages. Il faudrait sans doute qu'au moment d'envoyer une demande, l'expéditeur précise les moyens qui devraient être utilisés pour lui transmettre des états du message et des réponses. Dans ce cas, le mode de livraison devrait également être codé.

8 Prescriptions relatives au destinataire

Dans de nombreux cas, le destinataire doit apporter la preuve qu'il a reçu une demande. Ainsi, le destinataire doit envoyer au client un état du message pour toute demande reçue. L'état du message doit contenir le code de référence de la demande. Le destinataire pourrait générer le code de référence unique de la demande et l'envoyer à l'expéditeur.

En règle générale, le destinataire devrait accuser réception de tous les messages reçus, à moins que par exemple un état de la demande de service soit envoyé immédiatement après la réception d'une demande. Dans ce cas, l'état de la demande de service peut inclure l'état du message.

Pour les demandes qui requièrent un état de la demande de service ultérieur, l'état du message doit spécifier le temps maximum que l'expéditeur doit attendre pour l'état de la demande de service. Lorsque l'expéditeur transmet des demandes de mise à jour, ce délai d'exécution peut être actualisé dans l'état du message.

À moins qu'il ne constitue aussi un état de la demande de service définitif, le premier état du message envoyé par le destinataire devrait inclure un code de référence de session unique qui puisse être utilisé dans le cadre des demandes de mise à jour ultérieures en vue d'identifier la session à laquelle se réfère la demande de mise à jour.

Le destinataire doit renvoyer un code sur l'état du service dans l'état du message et l'état de la demande de service afin d'informer l'expéditeur de l'état de la demande, en indiquant par exemple qu'il existe des erreurs dans les données ou que la demande a été refusée, est en cours ou a été traitée avec succès, etc. En cas d'erreur, il faudrait également inclure un message sur l'état de la demande de service plus spécifique sur l'erreur en question.

9 Modèles d'échange de messages

Les échanges de messages sont souvent exécutés de manière asynchrone comme le montrent les schémas ci-dessous. Les échanges de messages asynchrones sont tout type de communication où une entité soumet des données ou une demande, puis il y a un décalage avant que les destinataires valident les données et communiquent l'état de la demande de service, le cas échéant.

En règle générale, les échanges de renseignements électroniques se composent de plusieurs messages, comme le montrent les figurent ci-après. Chacune de ces figures illustre un "modèle" d'échange de messages, c'est-à-dire un moyen particulier d'échanger des messages, quelle que soit la fonctionnalité mise en œuvre ou représentée par l'échange.

Les modèles d'échange de messages examinés dans la présente section ont été retenus afin de donner des indications sur l'utilisation qui est généralement faite des messages dans le cadre de séries d'échange de messages plus longues ou de "sessions". Cette utilisation a des incidences sur la sûreté et la sécurité de la transmission des messages, en gardant à l'esprit que l'intégrité et l'authenticité des messages doivent être préservées tout au long de la session. Pour ce faire, il faudrait par exemple horodater les messages et leur attribuer un code de référence, de sorte qu'un message transmis dans le cadre d'une session ne soit pas sorti de son contexte et utilisé dans le but de perturber la même session à un stade ultérieur ou une autre session dans son ensemble.

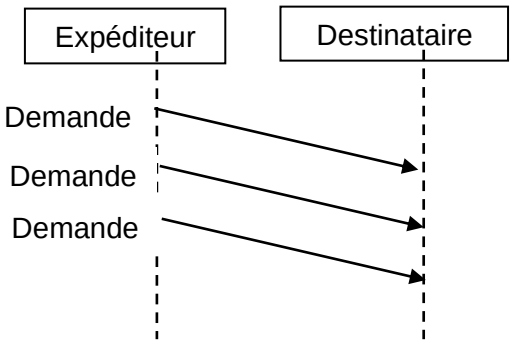

Figure 1 – Diffusion simple de renseignements

La figure 1 illustre le modèle d'échange de messages le plus simple. L'expéditeur transmet des renseignements à un ou plusieurs destinataires sans attendre d'état de la demande de service et d'état du message. Les comptes rendus de position ou les données statiques relatives aux navires transmis dans le cadre du système d'identification automatique (AIS) sont un exemple de ce type de modèle. Dans le cas de l'AIS, il n'est pas rare que ce modèle s'appuie sur un mécanisme de diffusion permettant de transmettre les renseignements à toutes les parties qui se trouvent à proximité. Le modèle s'appuie aussi normalement sur la retransmission périodique de la demande pour éviter les problèmes en cas de perte d'un ou plusieurs messages. L'expéditeur répète régulièrement les renseignements et ne doit généralement pas s'inquiéter de la perte de données ou de messages. Toutefois, selon le degré de criticité des renseignements communiqués, il pourrait être nécessaire de prévoir un dispositif de signature électronique et un horodatage afin de vérifier l'identité de l'expéditeur et

d'éviter que des parties hostiles ne perturbent les échanges de renseignements, notamment en retransmettant d'anciens messages à un stade ultérieur.

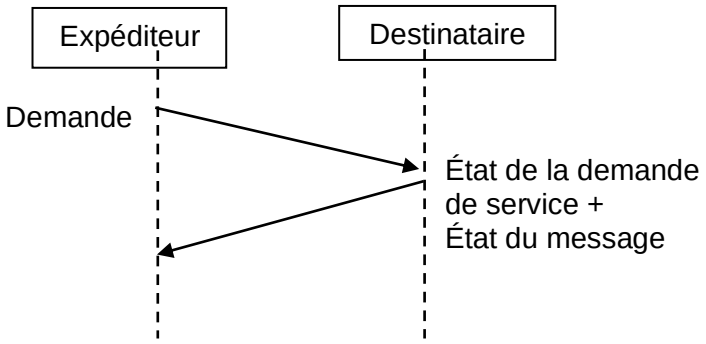

Figure 2 – Modèle simple de demande et d'état de la demande de service

La figure 2 illustre un autre modèle relativement simple d'échange de messages. L'expéditeur transmet certains renseignements au destinataire et reçoit immédiatement un état de la demande de service à la réception du message et aux renseignements ou au service demandé.

La figure 3 illustre une demande de renseignements ou de service légèrement plus complexe. Elle présente un cas typique dans lequel le destinataire accuse réception du message de demande dans un premier temps, sans répondre directement à la demande, pour ensuite indiquer un état de la demande de service au service demandé.

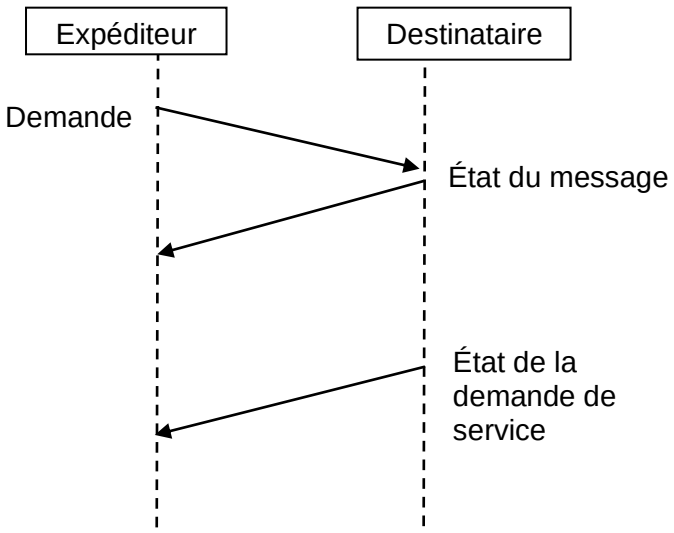

Figure 3 – Schéma de séquence élémentaire d'une demande de renseignements ou de service

Dans certains cas, l'expéditeur peut transmettre une demande de mise à jour à un stade ultérieur avant qu'un état de la demande de service ne soit apportée aux demandes. La figure 4 illustre ce type de cas.

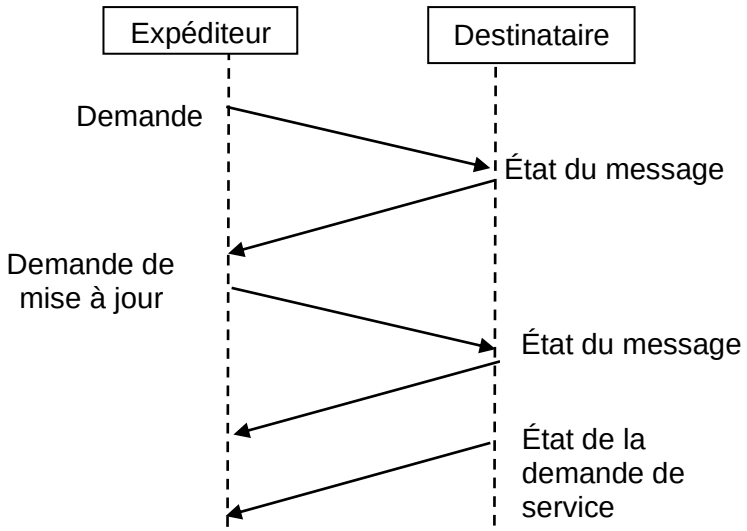

Figure 4 – **Schéma de séquence d'une demande de mise à jour**

Il est possible qu'une de ces demandes de mise à jour constitue aussi une annulation de la demande initiale. Dans la plupart des cas, la réponse apportée à une annulation comprendra à la fois un état du message et un état de la demande de service informant l'expéditeur que le message a bien été reçu et que la demande d'annulation a été acceptée. Toutefois, s'agissant de l'annulation, il pourrait également être nécessaire d'apporter un état de la demande de service différé dans certains cas.

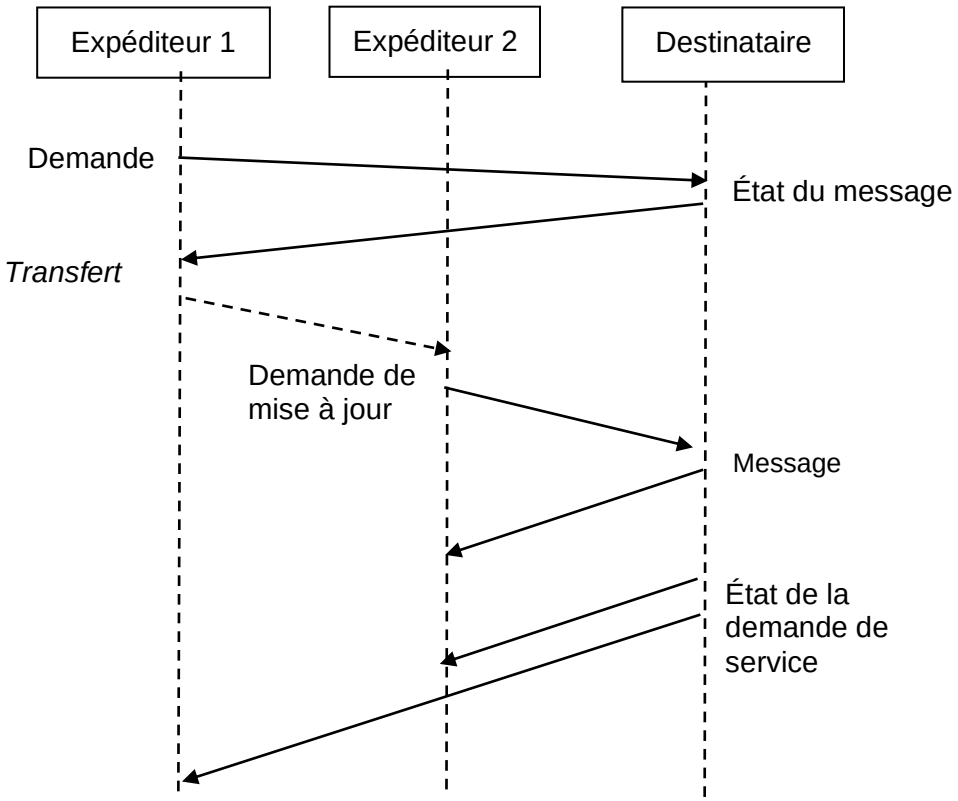

Figure 5 – Schéma de séquence pour les cas impliquant plusieurs expéditeurs

La figure 5 illustre un modèle plus complexe. Dans le cadre de ce modèle, plusieurs expéditeurs collaborent pour transmettre les renseignements requis au destinataire. Ce modèle pourrait concerner les cas où un navire transmet certains renseignements à un guichet unique maritime pour ensuite demander à l'agent ou à la compagnie maritime de transmettre des renseignements supplémentaires. Dans ce scénario, tous les expéditeurs doivent utiliser le même code de référence que celui de la session, ce qui nécessite une certaine forme de communication entre eux (voir la flèche en pointillés "transfert"). Le destinataire devrait envoyer un état de la demande de service à tous les expéditeurs, à moins qu'un expéditeur principal ait été désigné, auquel cas la réponse ne devrait être envoyée qu'à l'expéditeur principal.

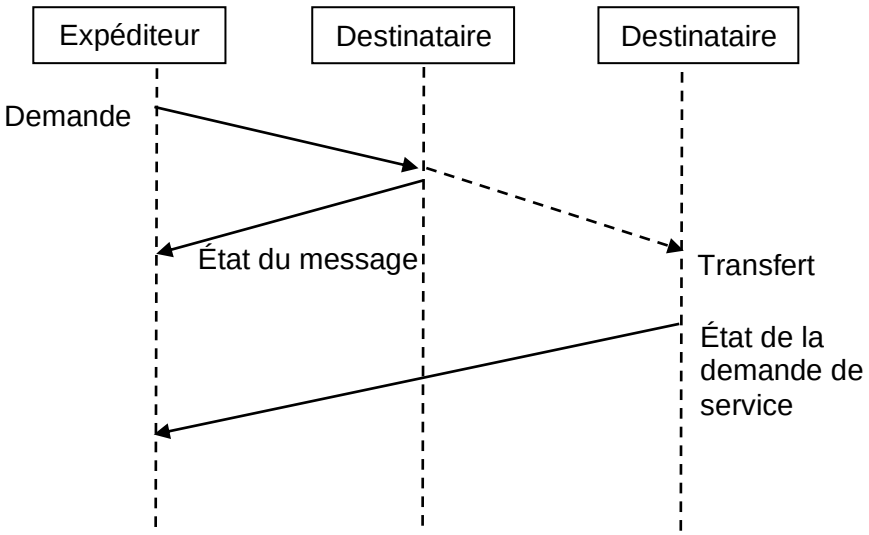

Figure 6 – **Schéma de séquence par l'intermédiaire du guichet unique maritime**

Le modèle de la figure 6 est utilisé spécifiquement par les guichets uniques maritimes où le guichet est le système qui reçoit une demande, et accuse réception de la demande, alors que le destinataire est une entité différente. La figure 7 est une extension d'un service demandé par le biais d'un guichet unique maritime lorsque le service demandé sera, en fin de compte, fourni par plus d'un destinataire/prestataire de services.

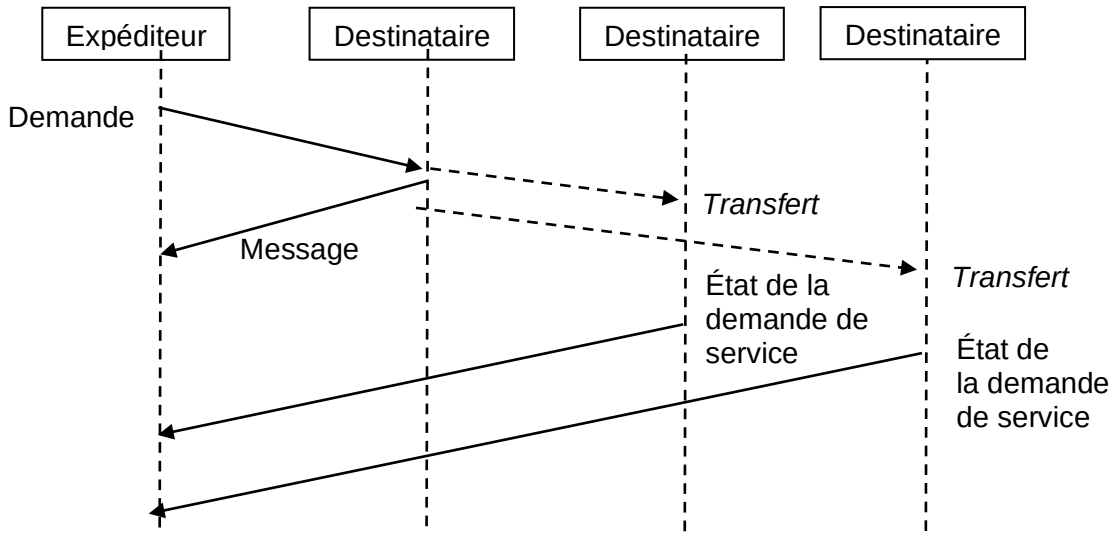

Figure 7 – **Schéma de séquence par l'intermédiaire d'un guichet unique maritime (destinataires multiples et état de la demande de service)**

Il convient de noter qu'il est possible de définir plusieurs autres modèles, en combinant deux ou plusieurs des modèles exposés ci-dessus. Les possibilités de fusionner l'état du message et l'état de la demande de service, permettant de transmettre des demandes de mise à jour après l'envoi de l'état de la demande de service, ou de désigner plusieurs destinataires pour une même demande, auquel cas il faudrait prévoir l'envoi de états du message et d'état de la demande de service, constituent des exemples types. Les modèles exposés dans la présente section devraient toutefois suffire dans le cadre des présentes Directives.

10 Prescriptions en matière de confidentialité

Afin d'assurer la confidentialité du contenu du message, il est nécessaire qu'il soit chiffré au moyen d'une clé de chiffrement au minimum.

L'utilisation d'un canal sécurisé pour la transmission des messages permettra d'assurer la confidentialité du contenu du message, sans que l'expéditeur n'ait à le chiffrer lui-même. Il pourrait toutefois être nécessaire de chiffrer le contenu du message s'il faut éviter que ce dernier soit lu par des tierces parties susceptibles d'intercepter le message adressé au destinataire.

Les systèmes et les plateformes numériques reposent souvent sur la cryptographie à clé publique et les clés asymétriques, qui peuvent ne pas convenir au cryptage de messages plus importants. Un système ou une plateforme numérique doit, si nécessaire, contenir des dispositions permettant de générer et d'échanger, par exemple, des clés symétriques pouvant être utilisées pour chiffrer des messages de la taille maximale utilisée entre les expéditeurs et les destinataires.

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).

* En anglais uniquement.

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.

* En anglais uniquement.

Element name	Msg	Note	Description
			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.
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 inline 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

* En anglais uniquement.

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.

* En anglais uniquement.

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.

---

* En anglais uniquement.