Journal officiel
de l'Union européenne

FR
Série L

2023/2790

18.12.2023

RÈGLEMENT D'EXÉCUTION (UE) 2023/2790 DE LA COMMISSION

du 14 décembre 2023

établissant des spécifications fonctionnelles et techniques pour le module d'interface de déclaration des guichets uniques maritimes nationaux

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2019/1239 du Parlement européen et du Conseil du 20 juin 2019 établissant un système de guichet unique maritime européen et abrogeant la directive 2010/65/UE ([1]), et notamment son article 6, paragraphe 1, et son article 12, paragraphe 4,

après consultation du comité sur la facilitation numérique des échanges et des transports,

considérant ce qui suit:

(1) Les spécifications du module d'interface de déclaration devraient reposer sur une technologie d'accès, d'installation et d'intégration faciles dans tous les guichets uniques maritimes nationaux (MNSW) et permettre une intégration et une maintenance aisées à l'avenir.

(2) Les spécifications fonctionnelles et techniques du module d'interface de déclaration devraient être fondées sur les lignes directrices de conception de haut niveau pour l'architecture de solutions pour les exigences d'interopérabilité (HL SAT) afin de permettre la traçabilité entre les exigences de haut niveau et les exigences détaillées en matière d'interopérabilité.

(3) Étant donné que les expéditeurs utilisent des systèmes de déclaration différents et que les MNSW sont mis en œuvre au moyen de technologies différentes, le module d'interface de déclaration devrait s'appuyer sur des technologies qui permettent l'échange d'informations entre différents systèmes d'information utilisant un protocole normalisé, propice à une meilleure interopérabilité.

(4) L'application des obligations de déclaration énumérées à l'annexe du règlement (UE) 2019/1239 peut amener les déclarants à soumettre des données à caractère personnel par l'intermédiaire du module d'interface de déclaration, lequel devrait permettre le traitement de toute donnée à caractère personnel conformément aux règlements (UE) 2018/1725 ([2]) et (UE) 2016/679 ([3]) du Parlement européen et du Conseil lors de l'échange d'informations.

(5) Le module d'interface de déclaration étant développé et actualisé par la Commission et distribué aux États membres en vue de son intégration, la distribution de nouvelles versions du module d'interface de déclaration, le contrôle de la bonne installation du logiciel et la mise à jour du manuel de mise en œuvre des messages devraient être gérés de manière centralisée, en tenant compte, dans la mesure du possible, des exigences de sécurité informatique des MNSW.

(6) Afin de garantir la stabilité, la sécurité et les performances du module d'interface de déclaration, les États membres devraient être en mesure de surveiller le trafic sur le réseau et d'analyser les événements, les erreurs et les exceptions touchant le système, ainsi que d'intégrer ces informations dans leurs systèmes et processus de surveillance existants. À cette fin, le module d'interface de déclaration devrait offrir des fonctionnalités appropriées permettant la journalisation et le stockage des événements et fournir aux États membres des informations concernant le trafic sur le réseau.

([1]) JO L 198 du 25.7.2019, p. 64.

([2]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

([3]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

(7) Afin de garantir un échange d'informations sécurisé par l'intermédiaire du module d'interface de déclaration, les expéditeurs doivent être authentifiés. Le système commun de gestion des accès et du registre des utilisateurs devrait dès lors comporter deux composantes essentielles, à savoir un service central d'authentification et un registre central. Ces composantes devraient fonctionner ensemble pour permettre l'authentification de l'expéditeur dans tous les modules d'interface de déclaration, en fournissant un mécanisme d'authentification unique.

(8) Pour échanger des informations en toute sécurité au moyen du module d'interface de déclaration et garantir que les utilisateurs sont reconnus au niveau de l'Union lorsqu'ils accèdent à l'un des modules d'interface de déclaration, les expéditeurs devraient obtenir un certificat qualifié de cachet électronique conforme aux exigences fixées par le règlement (UE) n° 910/2014 du Parlement européen et du Conseil ([4]).

(9) Afin de disposer d'un enregistrement unique des expéditeurs permettant d'échanger des informations par l'intermédiaire des interfaces de déclaration harmonisées dans les différents États membres, les États membres devraient pouvoir enregistrer les expéditeurs dans le registre central. Cela devrait réduire la charge que représentent les enregistrements multiples dans plusieurs MNSW dans le cas d'opérations transfrontières. Toute donnée à caractère personnel introduite dans le registre central devrait être traitée conformément aux règlements (UE) 2018/1725 et (UE) 2016/679.

(10) Afin de réduire au minimum la dépendance des États membres à l'égard des services centraux et étant donné que les services d'authentification nationaux peuvent déjà accueillir les MNSW, les États membres devraient également être autorisés à réutiliser leurs propres services d'authentification et registres nationaux pour authentifier les expéditeurs souhaitant utiliser le module d'interface de déclaration, en lieu et place du système de gestion des accès et du registre des utilisateurs du système de guichet unique maritime européen (EMSWe).

(11) Pour que États membres puissent intégrer correctement le module d'interface de déclaration et le système de gestion des accès et du registre des utilisateurs aux MNSW, il conviendrait que le présent règlement s'applique à partir de la même date que le règlement (UE) 2019/1239.

(12) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu un avis le 18 octobre 2023,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Définitions

Aux fins du présent règlement, on entend par:

1) «module d'interface de déclaration»: un composant intergiciel du MNSW mentionné à l'article 2, paragraphe 4, du règlement (UE) 2019/1239;

2) «expéditeur»: un déclarant ou un prestataire de services de données exploitant le système informatique qui envoie des messages électroniques au MNSW ou les reçoit par l'intermédiaire du module d'interface de déclaration;

3) «données requises»: les données requises telles que définies à l'article 1er du règlement d'exécution (UE) 2023/204 de la Commission ([5]);

4) «AS4»: un protocole de messagerie fondé sur des services web permettant l'échange sécurisé de messages entre deux parties;

5) «message»: une représentation numérique des données requises ou des messages de réponse utilisée pour les échanges entre l'expéditeur et le MNSW;

6) «point d'accès AS4»: un serveur exploitant des logiciels compatibles avec le protocole de messagerie AS4 et les exigences du module d'interface de déclaration, permettant l'envoi et la réception d'informations au nom d'un expéditeur depuis et vers le module d'interface de déclaration;

([4]) Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

([5]) Règlement d'exécution (UE) 2023/204 de la Commission du 28 octobre 2022 établissant les spécifications techniques, les normes et les procédures applicables au système de guichet unique maritime européen au titre du règlement (UE) 2019/1239 du Parlement européen et du Conseil (JO L 33 du 3.2.2023, p. 1).

7) «MNSW-Core»: un composant technique du MNSW auquel le module d'interface de déclaration est intégré;

8) «validation syntaxique»: le processus consistant à vérifier si un message électronique est exempt d'erreurs de programmation, de structure ou de style;

9) «validation sémantique»: un processus consistant à vérifier la conformité des données aux règles spécifiques en matière de données dans les limites des données requises;

10) «manuel de mise en œuvre des messages»: une spécification fonctionnelle établissant des normes et des messages à échanger entre les expéditeurs et les MNSW par l'intermédiaire du module d'interface de déclaration;

11) «enregistrement»: un processus par lequel une personne physique ou morale s'identifie et crée un compte auprès de l'autorité visée à l'article 12, paragraphe 2, du règlement (UE) 2019/1239;

12) «identification»: une identification électronique telle que définie à l'article 3, point 1, du règlement (UE) nº 910/2014;

13) «moyen d'identification électronique»: un moyen d'identification électronique tel que défini à l'article 3, point 2, du règlement (UE) nº 910/2014;

14) «authentification»: une authentification telle que définie à l'article 3, point 5, du règlement (UE) nº 910/2014;

15) «certificat»: un certificat qualifié de cachet électronique au sens de l'article 3, point 30, du règlement (UE) nº 910/2014 délivré par un prestataire de services de confiance qualifié au sens de l'article 3, point 20, du règlement (UE) nº 910/2014;

16) «numéro EORI» (numéro d'enregistrement et d'identification des opérateurs économiques): un numéro d'identification tel que défini à l'article 1er, point 18, du règlement délégué (UE) 2015/2446 de la Commission ([6]);

17) «système de gestion des accès et du registre des utilisateurs de l'EMSWe»: un système géré par la Commission qui comprend un registre central et un service central d'authentification, et qui garantit la reconnaissance mutuelle des moyens d'identification électronique et l'authentification aux fins de l'échange transfrontière sécurisé de données entre les expéditeurs et les MNSW au moyen du module d'interface de déclaration;

18) «registre central»: un registre géré par la Commission qui détient les données d'enregistrement des expéditeurs fournies par les États membres dans le but de faciliter l'authentification des expéditeurs;

19) «registre national»: un registre géré par un État membre qui détient les données d'enregistrement des expéditeurs et qui peut être utilisé pour faciliter l'authentification des expéditeurs s'il est conforme aux exigences du service central d'authentification;

20) «service central d'authentification»: un service exploité par la Commission pour authentifier les expéditeurs qui utilisent le module d'interface de déclaration;

21) «service national d'authentification»: un service exploité par un État membre pouvant être utilisé pour authentifier les expéditeurs qui utilisent le module d'interface de déclaration.

Article 2

Le module d'interface de déclaration est conforme aux spécifications fonctionnelles et techniques énoncées dans la partie I de l'annexe.

Afin de contribuer à l'intégration du module d'interface de déclaration dans les MNSW, la Commission, en étroite collaboration avec les coordinateurs nationaux de l'EMSWe:

— définit des lignes directrices pour tester et configurer le module d'interface de déclaration en vue de son intégration dans les MNSW respectifs,

— définit et tient à jour, avec l'aide de l'Agence européenne pour la sécurité maritime, le manuel de mise en œuvre des messages.

([6]) Règlement délégué (UE) 2015/2446 de la Commission du 28 juillet 2015 complétant le règlement (UE) nº 952/2013 du Parlement européen et du Conseil au sujet des modalités de certaines dispositions du code des douanes de l'Union (JO L 343 du 29.12.2015, p. 1).

Article 3

Le registre central et le service central d'authentification sont établis conformément aux spécifications techniques, normes et procédures énoncées dans la partie II de l'annexe.

Article 4

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il est applicable à partir du 15 août 2025.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 14 décembre 2023.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

PARTIE I

MODULE D'INTERFACE DE DÉCLARATION (RIM)

ARCHITECTURE ET CHAMP D'APPLICATION

Le RIM fait partie d'un modèle à quatre angles pour les messages échangés entre les expéditeurs (angle 1) et le MNSW-Core (angle 4), relayés par les points d'accès AS4 (angles 2 et 3) de chaque côté, mettant en œuvre le protocole AS4 pour le transport et la sécurité, comme suit:

Angle 1: le back office de l'expéditeur prépare, envoie et reçoit les messages depuis et vers le MNSW-Core.

Angle 2: point d'accès AS4 de l'expéditeur.

Angle 3: RIM.

Angle 4: le MNSW-Core reçoit les messages et envoie des messages de réponse à l'expéditeur.

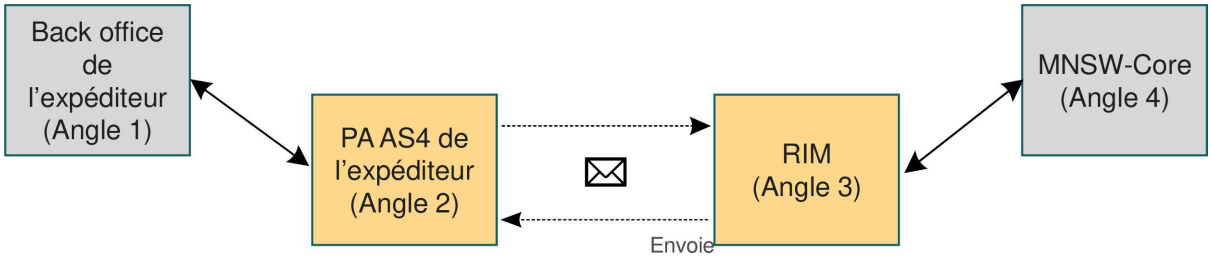

Figure 1 — Architecture RIM de haut niveau

Le RIM ne procède plus à la validation sémantique des messages au-delà des spécifications du manuel de mise en œuvre des messages, ne traite plus leur séquence ni ne stocke plus les messages après qu'ils ont été transférés avec succès au MNSW-Core ou à l'expéditeur.

Conformément à l'article 5, paragraphe 3, point c), du règlement (UE) 2019/1239, une fois que le message est transféré du RIM au MNSW-Core, les États membres, s'il y a lieu, traduisent, valident et transfèrent les données requises vers les systèmes des autorités compétentes conformément aux spécifications de ces systèmes.

SPÉCIFICATIONS FONCTIONNELLES DU RIM

ID	Fonction	Description
LR1	Journalisation et suivi	La fonction assure la journalisation et le stockage des événements (échec d'envoi, retard et erreur de destinataire).
LR2	Stockage de métadonnées	La fonction assure le stockage des métadonnées des messages échangés.
OA1	Stockage et consultation des données techniques	La fonction assure le stockage et permet la consultation des données techniques nécessaires à la configuration et au fonctionnement du RIM au moyen d'une interface (par exemple, adresses techniques des points d'accès AS4 des expéditeurs, schémas de message du manuel de mise en œuvre des messages, etc.).
OA2	Traitement des exceptions	La fonction fournit des notifications de détection d'erreurs de traitement et/ou de conditions anormales par l'intermédiaire d'une interface utilisateur.
OA3	Accès à la journalisation et au suivi des informations et métadonnées	La fonction permet au MNSW-Core d'accéder à la journalisation et au suivi des informations et métadonnées des messages échangés par l'intermédiaire d'une interface système à système.

OA4	Authentification de l'expéditeur	La fonction déclenche le processus d'authentification d'un expéditeur utilisant un service d'authentification central ou national.
OA5	Validation du message	La fonction assure la validation syntaxique et sémantique des messages reçus conformément aux spécifications techniques des messages définies dans le manuel de mise en œuvre des messages. Le manuel de mise en œuvre des messages précise quelles validations sont effectuées par le RIM. Le RIM notifie les erreurs en conséquence.
MF1	Traitement des messages	La fonction garantit que le contenu des messages reçus (données requises ou réponse) est transféré sans modification dans l'angle correspondant si les validations ont abouti.

SPÉCIFICATIONS TECHNIQUES DU RIM

Intégration

ID	Nom	Description
IA1	Norme de protocole de messagerie	Le RIM utilise le protocole de messagerie AS4 pour faciliter l'interopérabilité avec différentes technologies et différents systèmes de déclaration des expéditeurs.

Échange de messages

ID	Nom	Description
AP1	Schéma d'échange de messages asynchrone	Le RIM prend en charge la transmission asynchrone des messages à destination et en provenance (données requises et réponse) du MNSW-Core au moyen d'un mécanisme «push/pull».

Sécurité

ID	Nom	Description
SA1	Confidentialité et sécurité des échanges d'informations	Le RIM garantit la confidentialité des informations et la protection de toute donnée à caractère personnel en cryptant les informations échangées entre le point d'accès AS4 de l'expéditeur et le RIM. Le RIM décrypte et met les messages envoyés par un expéditeur à la disposition du MNSW-Core. Le RIM utilise le protocole Web Service Security (WSS) comme norme pour permettre l'échange sécurisé de messages entre le point d'accès AS4 de l'expéditeur et le RIM.
SA2	Non-répudiation des messages	La communication et la validation des messages par l'intermédiaire du RIM intègrent des mesures de sécurité visant à garantir l'authenticité des messages et à éviter leur répudiation.

SA3	Intégrité	Des mesures techniques sont mises en place pour garantir l'intégrité des données échangées.
SA4	Sécurité des applications	Le RIM s'appuie sur les meilleures pratiques en matière de développement de logiciels qui permettent de détecter les activités malveillantes et de transférer en toute sécurité des informations sensibles.
SA5	Disponibilité du service	Pour une communication et une diffusion fiables des informations entre les expéditeurs et les guichets uniques maritimes nationaux, le RIM met en œuvre des mécanismes qui garantissent que les messages échangés par son intermédiaire ne sont pas perdus en cas d'indisponibilité du service.

Performances et évolutivité

ID	Nom	Description
PS1	Performances et évolutivité	Le RIM a la capacité d'atteindre les objectifs de performance existants et futurs, tels que le temps de réponse, le nombre d'expéditeurs simultanés et le volume/la taille des messages échangés.

Portabilité et déploiement

ID	Nom	Description
PD1	Indépendance de la plateforme	Le RIM est compatible avec l'architecture matérielle et les systèmes d'exploitation les plus courants à l'intérieur desquels il sera déployé. Le RIM ne devrait pas nécessiter de matériel ou de logiciel propriétaires pour son installation ou sa configuration.
PD2	Application auto-installable	Le RIM est fourni sous la forme d'un ensemble de logiciels comprenant tous les composants de l'application requis par le RIM. Les dépendances fournies et requises sont énumérées dans chaque note de version du RIM.

PARTIE II

SYSTÈME DE GESTION DES ACCÈS ET DU REGISTRE DES UTILISATEURS DE L'EMSWE (URAM)

REGISTRE CENTRAL

À la demande de l'expéditeur, les États membres qui ne fournissent pas de registre national conforme aux spécifications du registre central énoncées dans la présente annexe enregistrent le numéro EORI et le certificat de l'expéditeur dans le registre central et sont responsables de la vérification, de l'exactitude et de la gestion des données conformément à l'article 12, paragraphe 2, du règlement (UE) 2019/1239. Le registre central fournit une interface aux États membres pour l'enregistrement et la gestion des expéditeurs.

SERVICE CENTRAL D'AUTHENTIFICATION

Le diagramme ci-dessous illustre les étapes séquentielles de l'authentification d'un expéditeur qui prépare et envoie un message au RIM (étapes 1, 2).

Le RIM exécute la fonction d'«authentification de l'expéditeur» ([1]) en utilisant le service central d'authentification (étape 3.a).

Étape 3.a: le service central d'authentification authentifie l'expéditeur en interrogeant le registre central et en vérifiant l'enregistrement correspondant (3.a.i) ou, si l'expéditeur ne figure pas dans le registre central, en interrogeant le registre national du pays de l'expéditeur, le cas échéant, et en vérifiant l'enregistrement correspondant (étape 3.a.ii).

Étape 3.b: lorsqu'un service national d'authentification est créé et mis à disposition dans un État membre, le RIM exécute la fonction «authentification de l'expéditeur» en utilisant ce service national d'authentification uniquement pour l'authentification des expéditeurs au moyen d'un certificat délivré dans cet État membre.

Étape 4: le résultat de l'authentification est renvoyé au RIM. En cas d'authentification réussie, le message est mis à la disposition de l'angle 4 (MNSW-Core) (étape 5). Si l'authentification échoue, un message d'échec est renvoyé à l'angle 2.

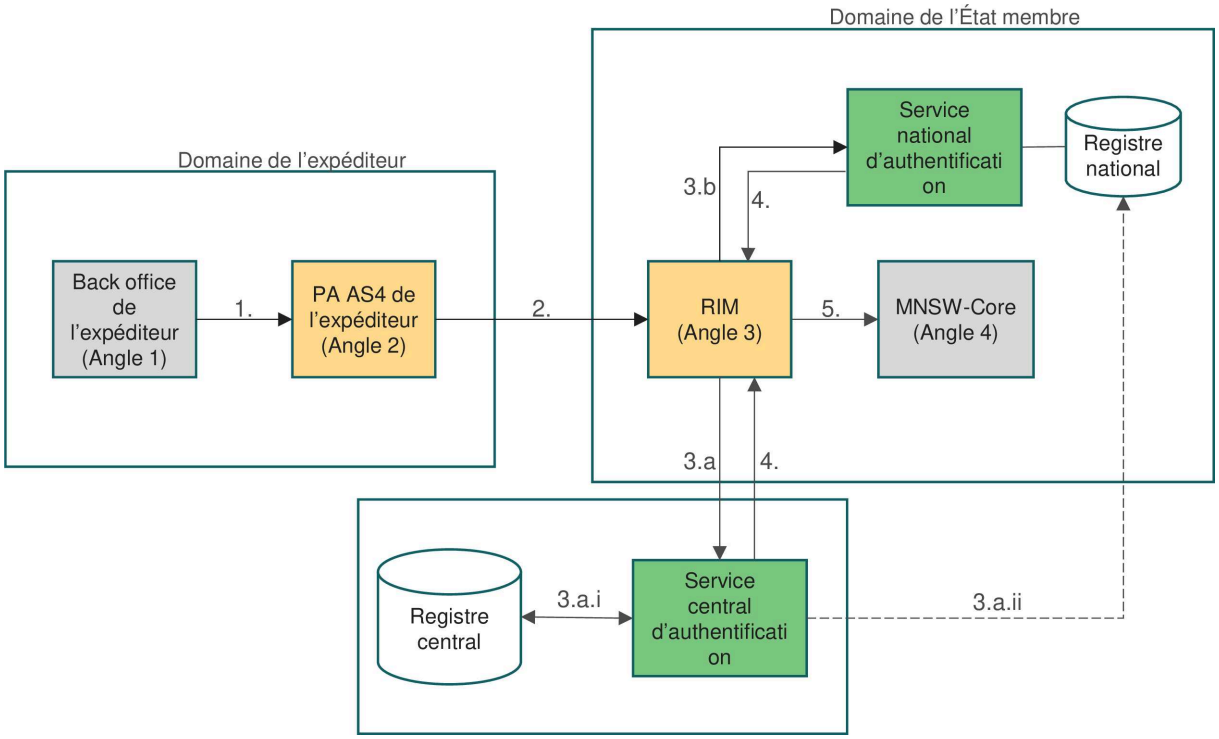

Figure 2

SPÉCIFICATIONS TECHNIQUES URAM

Intégration

ID	Nom	Description
URAM.01	Normes interopérables	Le logiciel URAM respecte des protocoles normalisés et utilise des éléments de sécurité solides lorsqu'il expose ses interfaces et se combine avec d'autres composants.

([1]) Identifiée comme OA4 dans la section «Spécifications fonctionnelles du RIM» de la partie I de la présente annexe.

URAM.02	Conformité à l'eIDAS	Le logiciel URAM utilise des normes et solutions ouvertes de l'UE et met en œuvre les mécanismes de contrôle nécessaires pour vérifier les certificats de l'expéditeur par rapport aux listes de confiance publiées par les États membres conformément à l'article 22 du règlement (UE) nº 910/2014 et à la décision d'exécution (UE) 2015/1505 de la Commission ([2]), y compris les informations relatives aux prestataires de services de confiance qualifiés délivrant des certificats de cachet électronique.

Sécurité

ID	Nom	Description
URAM.03	Confidentialité de l'échange d'informations	Afin de garantir la sécurité des logiciels URAM et de l'échange de données à caractère personnel, les protocoles et méthodes de cryptage suivants sont mis en œuvre: — Sécurité de la couche de transport (TLS): tous les logiciels au sein d'URAM sont sécurisés par TLS pour assurer le cryptage et l'intégrité des données au niveau du réseau afin de contribuer à protéger les données pendant leur transmission, pour empêcher tout accès non autorisé ou toute manipulation. — Pour communiquer avec le logiciel URAM, une configuration TLS est mise en œuvre.
URAM.04	Sécurité des applications	Le logiciel URAM garantit la détection des activités malveillantes et le transfert en toute sécurité des informations sensibles.
URAM.05	Protection des données à caractère personnel	Des droits d'accès sont accordés aux autorités des États membres conformément à l'article 12, paragraphe 2, du règlement (UE) 2019/1239 aux fins de l'enregistrement des expéditeurs. Le logiciel URAM met en œuvre des mécanismes de contrôle d'accès afin de garantir la protection des informations relatives à l'utilisateur constituant des données à caractère personnel, qui sont traitées uniquement aux fins de la création de comptes d'utilisateur et de la gestion des droits d'accès correspondants. Le service central d'authentification conserve les données à caractère personnel des expéditeurs pour une durée n'excédant pas celle nécessaire aux fins de l'authentification. Le registre central conserve les données à caractère personnel des expéditeurs pour une durée n'excédant pas celle nécessaire aux fins de la gestion du compte.

Durabilité et portabilité

ID	Nom	Description
URAM.06	Indépendance technologique	Le logiciel URAM permet des interactions avec le RIM et d'autres services utiles sans nécessiter de logiciels ou de matériel propriétaires et permet la combinaison avec le RIM quel que soit l'environnement technologique dans lequel le RIM est déployé.

([2]) Décision d'exécution (UE) 2015/1505 de la Commission du 8 septembre 2015 établissant les spécifications techniques et les formats relatifs aux listes de confiance visées à l'article 22, paragraphe 5, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 235 du 9.9.2015, p. 26).

URAM.07	Déploiement indépendant	Le logiciel URAM n'impose pas au RIM de respecter une exigence de déploiement spécifique. Le RIM ne devrait garantir qu'une connectivité internet et le respect des normes relatives à la sécurité et aux protocoles du logiciel URAM.

Fonctions du service central d'authentification

Le service central d'authentification met les services suivants à la disposition du RIM.

ID	Nom	Description
URAM.08	Service d'authentification	Le service central d'authentification est chargé d'authentifier les expéditeurs en vérifiant la validité du certificat, le numéro EORI et l'association entre le numéro EORI de l'expéditeur et son certificat. Il traite les demandes d'authentification envoyées par le RIM et fournit des réponses indiquant si une authentification a réussi ou échoué.

Spécifications du registre central

ID	Nom	Description
URAM.09	Enregistrement de l'expéditeur	Le registre central fournit une interface utilisateur graphique aux États membres pour l'enregistrement des données de l'expéditeur. Une fois enregistré dans le registre central, l'expéditeur est enregistré dans tous les États membres.
URAM.10	Visualisation et recherche de l'expéditeur	Le registre central permet à un État membre de visualiser toutes les données des expéditeurs qu'il a précédemment enregistrés. Il fournit également une fonctionnalité de recherche permettant d'extraire les données de ses expéditeurs enregistrés sur la base de différents critères de recherche.
URAM.11	Mise à jour de l'expéditeur	Le registre central permet à un État membre de modifier toutes les données de ses expéditeurs précédemment enregistrés afin de garantir l'exactitude et la validité des données.
URAM.12	Désactivation de l'expéditeur	Le registre central permet à un État membre de désactiver ses expéditeurs précédemment enregistrés.
URAM.13	Audit et déclaration	Le registre central offre des capacités de déclaration permettant à un État membre d'analyser les données spécifiques de ses expéditeurs précédemment enregistrées, telles que la date d'enregistrement et la validité du certificat.
URAM.14	Notifications	Le registre central offre aux États membres la possibilité de recevoir une notification du registre central chaque fois qu'un expéditeur précédemment enregistré par cet État membre est enregistré, mis à jour ou désactivé, ainsi qu'à l'expiration de son certificat.