2023/2790

18.12.2023

COMMISSION IMPLEMENTING REGULATION (EU) 2023/2790

of 14 December 2023

laying down functional and technical specifications for the reporting interface module of the Maritime National Single Windows

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU ([1]), and in particular Articles 6(1) and 12(4) thereof,

After consulting the Digital Transport and Trade Facilitation Committee,

Whereas:

(1) The specifications of the reporting interface module should be founded on a technology that is readily accessible, easy to install and easy to integrate in all Maritime National Single Windows (MNSWs) and should allow for smooth integration and maintenance in future.

(2) The functional and technical specifications of the reporting interface module should be based on the high-level Interoperability Requirements Solution Architecture Template (HL SAT) Design Guidelines to allow traceability between high-level and detailed interoperability requirements.

(3) Considering that senders use different reporting systems and the MNSWs are implemented using different technologies, the reporting interface module should be built on technologies that enable information to be exchanged between different information systems that use a standardised protocol, enabling greater interoperability.

(4) The reporting obligations listed in the Annex to Regulation (EU) 2019/1239 may require declarants to submit personal data through the Reporting Interface Module, which should exchange the information in a way that any personal data is processed in accordance with Regulations (EU) 2018/1725 ([2]) and Regulation (EU) 2016/679 ([3]) of the European Parliament and of the Council.

(5) As the reporting interface module is developed and updated by the Commission and distributed to the Member States for integration, distributing new versions of the reporting interface module, monitoring correct installation of the software and updating the message implementation guide should be managed centrally, taking into account the IT security requirements of the MNSWs where possible.

(6) To guarantee stability, security and performance of the reporting interface module, Member States should be able to monitor network traffic and analyse system events, errors and exceptions, as well as integrate this information into their existing monitoring systems and processes. To accomplish this, the reporting interface module should provide suitable functionalities that allow events to be logged and stored and provide network traffic information to the Member States.

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

([2]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

([3]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

(7) To ensure secure information exchange through the reporting interface module, senders require authentication. To this end, the common user registry and access management system should have a central authentication service and a central registry as key components. These components should work together to enable sender authentication across all reporting interface modules, providing a unified authentication mechanism.

(8) To exchange information securely using the reporting interface module and ensure that users are recognised at EU level when they access any of the reporting interface modules, senders should obtain a qualified certificate for electronic seals compliant with the requirements set by Regulation (EU) No 910/2014 ([4]) of the European Parliament and of the Council.

(9) To provide single registration for senders to exchange information through the harmonised reporting interfaces in different Member States, Member States should be able to register senders in the central registry. This should reduce the burden of multiple registrations for cross-border operations in multiple MNSWs. Any personal data in the central registry should be managed in accordance with Regulations (EU) 2018/1725 and (EU) 2016/679.

(10) To minimise Member States' reliance on central services and considering that MNSWs may already be supported by national authentication services, Member States should also be allowed to reuse their own national authentication services and national registries to authenticate senders wishing to use the reporting interface module, as an alternative to the user registry and access management system of the European Maritime Single Window environment (EMSWe).

(11) To allow Member States to correctly integrate the reporting interface module and the user registry and access management system with the MNSWs, this Regulation should apply as of the same date as Regulation (EU) 2019/1239.

(12) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 18 October 2023.

HAS ADOPTED THIS REGULATION:

Article 1

Definitions

For the purpose of this Regulation, the following definitions shall apply:

(1) 'reporting interface module' means a middleware component of the MNSW referred to in Article 2(4) of Regulation (EU) 2019/1239;

(2) 'sender' means a declarant or data service provider operating the IT system that sends electronic messages to MNSW or receives them via the reporting interface module;

(3) 'formality' means the formality as defined in article 1 of Commission Implementing Regulation (EU) 2023/204 ([5]);

(4) 'AS4' means a message protocol based on web services to securely exchange messages between two parties;

(5) 'message' means a digital representation of formalities or response messages used for the exchange between the sender and the MNSW;

(6) 'AS4 access point' means a server operating software that is compatible with the AS4 messaging protocol and the requirements of the reporting interface module, enabling information to be sent and received on behalf of a sender from and to the reporting interface module;

([4]) 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 (OJ L 257, 28.8.2014, p. 73).

([5]) Commission Implementing Regulation (EU) 2023/204 of 28 October 2022 laying down technical specifications, standards and procedures for the European Maritime Single Window environment pursuant to Regulation (EU) 2019/1239 of the European Parliament and of the Council (OJ L 33, 3.2.2023, p. 1).

(7) ‘MNSW core’ means a MNSW technical component with which the reporting interface module is integrated;

(8) ‘syntax validation’ means the process of checking whether an electronic message is free of programming, structural or stylistic errors;

(9) ‘semantic validation’ means a process in which data conformity with specific data rules within a formality is checked;

(10) ‘message implementation guide’ means a functional specification laying down standards and messages to be exchanged between senders and MNSWs through the reporting interface module;

(11) ‘registration’ means a process where a natural or legal person identifies themselves and creates an account with the authority referred to in Article 12(2) of Regulation (EU) 2019/1239;

(12) ‘identification’ means electronic identification as defined in point (1) of Article 3 of Regulation (EU) No 910/2014;

(13) ‘electronic identification means’ means an electronic identification as defined in point (2) of Article 3 of Regulation (EU) No 910/2014;

(14) ‘authentication’ means an authentication as defined in point (5) of Article 3 of Regulation (EU) No 910/2014;

(15) ‘certificate’ means a qualified certificate for electronic seal defined in Article 3(30) of Regulation (EU) No 910/2014 issued by a qualified trust service provider as defined in Article 3(20) of Regulation (EU) No 910/2014;

(16) ‘EORI number’ means an identification number as defined in point (18) of Article 1 of Commission Delegated Regulation (EU) 2015/2446 ([6]);

(17) ‘EMSWe user registry and access management system’ means a system operated by the Commission that encompasses a central registry and a central authentication service, and ensures the mutual recognition of electronic identification means and authentication for secure cross-border data exchange between senders and MNSWs through the reporting interface module;

(18) ‘central registry’ means a registry operated by the Commission that holds senders’ registration data provided by the Member States with the purpose of facilitating the authentication of senders;

(19) ‘national registry’ means a registry operated by a Member State that holds senders’ registration data and can be used to facilitate the authentication of senders if compliant with the requirements of the central authentication service;

(20) ‘central authentication service’ means a service operated by the Commission that authenticates senders that use the reporting interface module;

(21) ‘national authentication service’ means a service operated by a Member State that may be used to authenticate senders that use the reporting interface module.

Article 2

The reporting interface module shall comply with the functional and technical specifications set out in Part I of the Annex.

To help integrate the reporting interface module into the MNSWs, the Commission, in close collaboration with the national coordinators for EMSWe, shall:

— define guidelines for testing and configuring the reporting interface module for integration into the respective MNSWs;

— define and maintain, with the assistance of the European Maritime Safety Agency, the message implementation guide.

([6]) Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code (OJ L 343, 29.12.2015, p. 1)

Article 3

The central registry and the central authentication service shall be set up in accordance with the technical specifications, standards and procedures set out in Part II of the Annex.

Article 4

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 15 August 2025.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 14 December 2023.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

PART I

REPORTING INTERFACE MODULE

ARCHITECTURE AND SCOPE

The RIM shall be part of a four-corner model for the messages exchanged between senders (corner 1) and the MNSW-Core (corner 4) relayed through AS4 Access Points (corners 2 and 3) on each side implementing AS4 protocol for transport and security as follows:

Corner 1: sender's back-office preparing, submitting and receiving the messages from and to the MNSW-Core;

Corner 2: sender's AS4 Access Point;

Corner 3: RIM;

Corner 4: MNSW-Core receiving the messages and sending response messages to the sender.

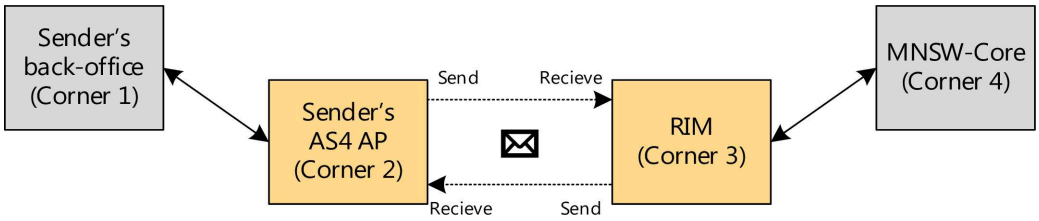

Figure 1 – High–level RIM architecture

The RIM shall not perform semantic validation of messages beyond the specifications of message implementation guide, handle their sequence nor store messages any longer than they have been successfully transferred to the MNSW-Core or the sender.

In accordance with Article 5(3) point (c) of Regulation (EU) 2019/1239, once the message is transferred from the RIM to the MNSW-Core, the Member States, where appropriate, shall translate, validate and transfer the formality data to the systems of the relevant authorities in compliance with the specifications of those systems.

RIM FUNCTIONAL SPECIFICATIONS

ID	Function	Description
LR1	Logging and monitoring	The function shall ensure logging and storage of events (delivery failures, delays, and recipient's error).
LR2	Metadata storing	The function shall ensure the storage of metadata of exchanged messages.
OA1	Technical data storage and lookup	The function shall ensure storage and lookup of technical data required for the configuration and functioning of the RIM through an interface (e.g. technical addresses of the senders' AS4 access points, message schemas of message implementation guide, etc.).
OA2	Exception handling	The function shall provide notifications of detected processing errors and/or anomalous conditions through a user interface.
OA3	Access to logging and monitoring information and metadata	The function shall provide the MNSW-Core access to logging and monitoring information and metadata of exchanged messages through a system-to-system interface.

OA4	Sender authentication	The function shall trigger the authentication process of a sender using a central or national authentication service.
OA5	Message validation	The function shall perform the syntax and semantic validation of received messages in accordance with the technical message specifications defined in the message implementation guide. The message implementation guide shall specify which validations shall be done by the RIM. The RIM shall notify errors accordingly.
MF1	Message handling	The function shall ensure that the content of the messages received (formality or response) is transferred without modifications to the relevant corner if the validations have been successful.

RIM TECHNICAL SPECIFICATIONS

Integration

ID	Name	Description
IA1.	Messaging protocol standard	The RIM shall use AS4 messaging protocol to facilitate interoperability with different technologies and reporting systems of senders.

Message Exchange

ID	Name	Description
AP1.	Asynchronous message exchange pattern	The RIM shall support asynchronous transmission of messages to and from (formality and response) the MNSW-Core by push and pull mechanism.

Security

ID	Name	Description
SA1.	Information exchange confidentiality and security	The RIM shall ensure confidentiality of information and protection of any personal data exchanged by encrypting the information exchanged between senders AS4 Access Point and RIM. The RIM shall decrypt and make the messages sent by a sender available to the MNSW-Core. The RIM shall use a Web Service Security (WSS) as standard to allow the secure exchange of messages between sender's AS4 Access Point and RIM.
SA2.	Non-repudiation of messages	The communication and validation of messages via the RIM shall include security measures to ensure message authenticity and avoid repudiation of messages.

SA3.	Integrity	Technical measures shall be put in place to ensure the integrity of data exchanged.
SA4.	Application Security	The RIM shall rely on software development best practices that enable the detection of malicious activities, and the secure transfer of sensitive information.
SA5.	Service Availability	For reliable communication and distribution of information between senders and Maritime National Single Windows, the RIM shall implement mechanisms that ensures messages exchanged with the RIM are not lost in case of service unavailability.

Performance and Scalability

ID	Name	Description
PS1.	Performance and scalability	The RIM shall be able to meet existing and future performance targets such as response time, number of concurrent senders and amount/size of exchanged messages.

Portability and Deployment

ID	Name	Description
PD1.	Platform independence	The RIM shall be compatible with the most common hardware architecture and operating systems where the RIM would be deployed. The RIM should not require proprietary hardware or software for installation or configuration.
PD2	Self-installing application	The RIM shall be provided as a package of software that includes all the application components required by the RIM. The provided and required dependencies shall be listed in each RIM release note.

PART II

EMSWE USER REGISTRY AND ACCESS MANAGEMENT SYSTEM

CENTRAL REGISTRY

Upon request from the sender, Member States that do not provide a national registry compliant to the specifications of the central registry laid out in this Annex, shall register the EORI number and the sender's certificate in the central registry and shall be responsible for data verification, accuracy, and management in accordance with Article 12(2) of Regulation (EU) 2019/1239. The central registry shall provide an interface to Member States to perform the registration and management of the senders.

CENTRAL AUTHENTICATION SERVICE

The diagram below illustrates the sequential steps for authenticating a sender that prepares and sends a message to the RIM (step 1, 2).

The RIM shall perform the 'sender authentication' function ([1]) using the central authentication service (step 3.a).

Step 3.a: The central authentication service shall authenticate the sender by querying the central registry and checking the relevant record (3.a.i), or, if the sender is not present in the central registry, by querying the national registry of the sender's country, if available, and checking the relevant record (step 3.a.ii).

Step 3.b: Where a national authentication service is established and made available in a Member State, the RIM shall perform the 'sender authentication' function using this national authentication service only for the authentication of senders using a certificate issued in that Member State

Step 4: The result of the authentication shall be sent back to the RIM. In case of successful authentication, the message shall be made available to corner 4 (MNSW-core) (step 5). If the authentication fails, a failure message shall be sent back to corner 2.

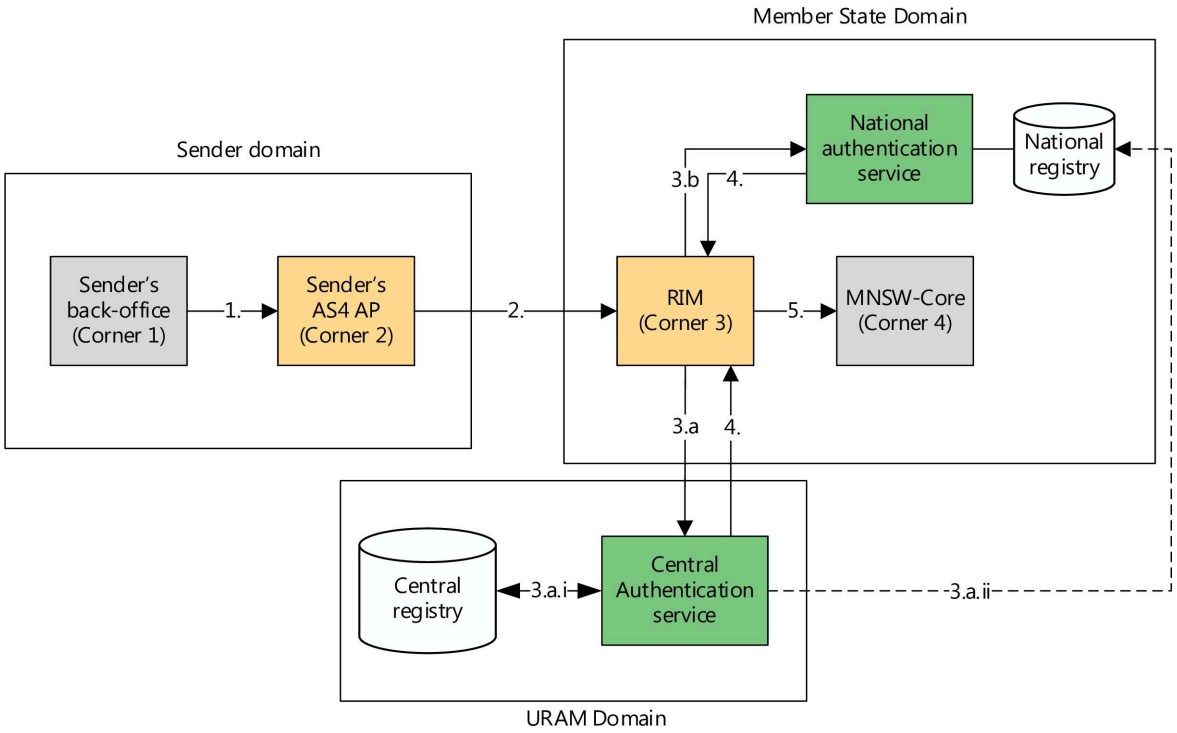

Figure 2

URAM TECHNICAL SPECIFICATIONS

Integration

ID	Name	Description
URAM.01	Interoperable standards	The URAM software shall adhere to standard protocols and employ robust security features when exposing its interfaces and integrating with other components.

([1]) Identified as OA4 in the RIM functional specifications section in Part I of this Annex.

URAM.02	eIDAS compliance	The URAM software shall make use of open EU standards and solutions and shall implement necessary control mechanisms to check sender's certificates against the trusted lists published by Member States in accordance with Article 22 of Regulation (EU) No 910/2014 and Commission Implementing Decision (EU) 2015/1505 ([2]) including information related to qualified trust service providers issuing certificates used for electronic seals.

Security

ID	Name	Description
URAM.03	Information exchange confidentiality	To ensure the security of URAM software and exchange of any personal data, the following protocols and encryption methods shall be implemented: — Transport Layer Security (TLS): all software within URAM shall be secured using TLS to provide network-level encryption and integrity of data to help protect data during transmission, preventing unauthorised access or tampering. — To communicate with the URAM software an TLS configuration shall be implemented.
URAM.04	Application security	The URAM software shall guarantee the detection of malicious activities and the secure transfer of sensitive information.
URAM 05	Personal data protection	Access rights shall be granted to the authorities of the Member States as per Article 12(2) of Regulation (EU) 2019/1239 for the purpose of registering senders. The URAM software shall implement access control mechanisms to ensure the protection of user information that is personal data, which shall be processed solely for the purpose of creating user accounts and managing the corresponding access rights. The central authentication service shall retain personal data of the senders no longer than it is needed for the purpose of the authentication. The central registry shall retain personal data of the senders no longer than necessary for the management of the account.

Sustainability & portability

ID	Name	Description
URAM.06	Technology independence	The URAM software shall allow interactions with the RIM and other relevant services without the need of proprietary software or hardware and shall allow for integration with the RIM regardless of the technological environment in which the RIM is deployed.

([2]) Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 235, 9.9.2015, p. 26).

URAM.07	Independent deployment	The URAM software shall not enforce a specific deployment requirement on the RIM. The RIM should only ensure an internet connectivity and the respect of standards related to security and protocols of the URAM software.

Central authentication service functions

The following services shall be made available to the RIM from the central authentication service.

ID	Name	Description
URAM.08	Authentication service	The central authentication service shall be responsible for the authentication of senders by verifying the validity of the certificate, the EORI number and the association between senders' EORI number and its certificate. It shall process authentication requests sent by the RIM and provide responses indicating successful or unsuccessful authentication.

Central Registry specifications

ID	Name	Description
URAM.09	Sender Registration	The central registry shall provide a graphical user interface to the Member States for registering sender's data. Once registered in the central registry, the sender shall be registered in all Member States.
URAM.10	Sender view and search	The central registry shall allow a Member State to view all data of the senders that it has previously registered. It shall also provide a search functionality for retrieving its registered senders' data based on various search criteria.
URAM.11	Sender update	The central registry shall allow a Member State to modify all its previously registered senders' data to ensure data accuracy and validity.
URAM.12	Sender deactivation	The central registry shall allow a Member State to deactivate its previously registered senders.
URAM.13	Audit and reporting	The central registry shall offer reporting capabilities enabling a Member State to analyse its previously registered specific senders' data, such as registration date and certificate validity.
URAM.14	Notifications	The central registry shall offer Member States the possibility to receive a notification from the central registry each time a sender previously registered by that Member State is registered, updated or deactivated as well as when its certificate expires.