|  |  |
| --- | --- |
| logo_ec_17_colors_300dpi | EUROPEAN COMMISSIONDIGIT – DIRECTORATE GENERAL INFORMATICS |

European Maritime Single Window environment

**Specifications of the Common Addressing Service**

**Document status:**

|  |
| --- |
| **Status** |
| Final |

**Document approver(s):**

|  |  |
| --- | --- |
| **Name** | **Role** |
| Roberto ALONGI (MOVE) | Policy Expert |
| Cristian OSPINA VARGAS (MOVE) | Product Owner |
| Martins ZIEDS (MOVE) | Business Project Manager |

**Document reviewer(s):**

|  |  |
| --- | --- |
| **Name** | **Role** |
| Catherine FOLEY (DIGIT) | IT Programme Manager |
| Laurent KUMMER (DIGIT) | Senior Project Manager |
| Juan Alfonso BARRACA (DIGIT) | Business Analyst |

**Summary of changes:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Created by** | **Short Description of Changes** |
| 1.0 | 25/03/2023 | European Commission (DIGIT) | Initial version of the document |
| 1.1 | 23/08/2024 | European Commission (DIGIT) | Clarification on some requirements following comments from MS (20240425) |

Table of Contents

[1. Figures and tables 4](#_Toc178693973)

[1.1. Table of figures 4](#_Toc178693974)

[1.2. Table of tables 4](#_Toc178693975)

[2. Introduction 5](#_Toc178693976)

[2.1. Purpose 5](#_Toc178693977)

[2.2. Acronyms 5](#_Toc178693978)

[2.3. Glossary 6](#_Toc178693979)

[2.4. Referenced documents 7](#_Toc178693980)

[3. Context 8](#_Toc178693981)

[3.1. Scope 8](#_Toc178693982)

[3.2. Business Requirements 8](#_Toc178693983)

[3.2.1. Dynamic Address Resolution 9](#_Toc178693984)

[3.2.2. Reusability 10](#_Toc178693985)

[3.2.3. Scalability and adaptability 10](#_Toc178693986)

[4. High-level Functional and Technical specifications for the cas 11](#_Toc178693987)

[4.1. Architecture of the CAS 11](#_Toc178693988)

[4.2. Functional and Technical Specifications 12](#_Toc178693989)

[4.2.1. High-level process for address discovery 13](#_Toc178693990)

[4.2.2. Reverse Lookup 14](#_Toc178693991)

[4.2.3. Central Node 14](#_Toc178693992)

[4.2.4. Publisher nodes 15](#_Toc178693993)

[4.2.5. Logging and feedback 18](#_Toc178693994)

Figures and tables

Table of figures

[Figure 1 - CAS in 4-corner architecture 12](#_Toc178693995)

[Figure 2 - Address discovery 13](#_Toc178693996)

[Figure 3 – Recipient address management 16](#_Toc178693997)

[Figure 4 – Participant migration 17](#_Toc178693998)

Table of tables

[Table 1 - Acronyms 5](#_Toc178693999)

[Table 2 - Glossary 7](#_Toc178694000)

[Table 3 - Related documents 7](#_Toc178694001)

[Table 4 - Business requirements - Dynamic Address Resolution 9](#_Toc178694002)

[Table 5 - Business requirements - Reusability 10](#_Toc178694003)

[Table 6 - Business requirements - Scalability and adaptability 10](#_Toc178694004)

[Table 7 - Functional Area - Central Address Lookup 14](#_Toc178694005)

[Table 8 - Functional Area – Central Management of Publisher nodes 15](#_Toc178694006)

[Table 9 - Functional Area - Publisher nodes 17](#_Toc178694007)

[Table 10 - Recipient capabilities 18](#_Toc178694008)

[Table 11- Logging and feedback 18](#_Toc178694009)

Introduction

Purpose

The purpose of this document is to define the high-level functional and technical requirements for the Common Addressing Service (CAS) component, to be used as a basis for drafting the annex to the Implementing Act of the Regulation (EU) 2019/1239 on a European Maritime Single Window environment.

The high-level requirements have been defined with consideration to Article 13 of Regulation (EU) 2019/1239, which serves as the legal basis for the Commission to draft these specifications. Established by the European Parliament and the Council on 20 June 2019, this regulation creates a European Maritime Single Window environment, ensuring that the elaboration of these requirements aligns with its directives.

Acronyms

|  |  |
| --- | --- |
| Acronym | Description |
| CAS | Common Addressing Service |
| DIGIT | Directorate-General for Informatics |
| EC | European Commission  |
| EMSWe | European Maritime Single Window environment |
| RIM | Harmonised **R**eporting **I**nterface **M**odule |
| MNSW | Maritime National Single Window |
| URAM | EMSWe **U**ser **R**egistry and **A**ccess **M**anagement System  |
| DNS | Domain Name System  |
| SAT  | Solution Architecture Template |

Table 1 - Acronyms

Glossary

|  |  |
| --- | --- |
| Term | Definition |
| Declarant | Any natural or legal person who is subject to reporting obligations or any duly authorised natural or legal person acting on that person’s behalf within the limits of the relevant reporting obligation as defined in Article 2 of the EMSWe Regulation (Regulation (EU) 2019/1239). |
| Direct system-to-system data connection | It is a method of exchanging data between two computer systems without the need for human intervention or involvement. The data exchange is automated and operates in real-time or near real-time. In this type of connection, the two systems are usually configured to communicate with each other through a specific protocol or interface, which allows them to exchange data seamlessly. The data can be transmitted in various formats such as files, messages, or API calls, depending on the specific needs of the systems involved. |
| Message | Digital representation of a formality or a response in a exchange between Sender and Member State. |
| Sender | The legal entity operating the IT system sending and receiving electronic messages to maritime national single windows via the harmonised reporting interface module. That legal entity can be a declarant or a data service provider as defined in Article 2 of the EMSWe Regulation (Regulation (EU) 2019/1239).  |
| Sender endpoint | Senders’ systems technical address. Refers in this context to the technical address of the AS4 AP which is used by a sender and is connected to the senders’ Backoffice. Such a technical address could be a URL or an IP address. This endpoint is accessible over the Internet by other technical services. |
| AS4 AP | AS4 (Applicability Statement 4) is a message protocol based on web services to securely exchange B2B messages between trading partners. **AP** is the Access Point providing AS4 exchange. |
| Participant | A (sending or receiving) party. It refers to an entity that initiates or receives a transmission of a message through an AS4 Access Point (AP) – could be a Sender or a Member State |
| Recipient | Unless stated otherwise, the recipient corresponds to the business message destination – the Member State RIM |
| Domain Name System (DNS) | Hierarchical system that translates human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on the network. It acts as the "phonebook" of the internet, enabling users to access websites using easily remembered names instead of numerical addresses. |

Table 2 - Glossary

Referenced documents

|  |  |  |
| --- | --- | --- |
| **Ref** | **Document name** | **Location** |
| REF\_D1 | Regulation (EU) 2019/1239 | <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R1239&from=EN> |
| REF\_D2 | Functional and technical specifications for the reporting interface module of the MNSWs. | <https://eur-lex.europa.eu/eli/reg_impl/2023/2790>  |
| REF\_D3 | High-level Interoperability Requirements Solution Architecture Template (HL SAT) Design Guidelines v1.0.0 | <https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/document/high-level-interoperability-requirements-solution-architecture-template-hl-sat-design-guidelines> |

Table 3 - Related documents

Context

Scope

According to the definitions in Article 2 of Regulation (EU) 2019/1239 REF\_D1, common addressing service (CAS) means “*an additional voluntary service for declarants for initiating direct system-to-system data connections between the system of a declarant and the harmonised reporting interface module (RIM) of the respective maritime National Single Window*”. More specifically, according to Article 13, the CAS is a component of the European Maritime Single Window environment (EMSWe), that the Commission shall develop in close cooperation with the Member States, provided that the harmonised reporting interface module (RIM) has been implemented fully in accordance with Article 6.

The Commission, in joint collaboration with the Member States, shall adopt implementing acts to provide details and guidelines on the following aspects:

* The functional and technical specifications.
* Quality control mechanisms.
* Procedures for deploying, maintaining, and employing the common addressing service.

The present document focuses on the **functional and technical specifications of the CAS,** that need to be in place to effectively support the predefined business requirements. This document provides a comprehensive overview of the technical specifications for the CAS, outlining its requirements, technical architecture, and specifications. This document is intended for Member States and technical stakeholders, including software providers interested in implementing the CAS component, and data service providers and declarants who are exploring integration with the CAS component.

Requirements are listed based on the template and related attributes described in the HL SAT GuidelinesREF\_D3. The specifications have been structured according to the mentioned guidelines, keeping the most relevant attributes for the EMSWe implementation.

Hereafter is the description of the specification attributes:

* **ID**: unique identifier for the interoperability specification.
* **Name:** short, descriptive name.
* **Description**: complete description.

Business Requirements

The anticipated benefits of the CAS include the dynamic address resolution of a receiving participant in an AS4 network. A sender which needs to send an AS4 message may not know the technical address of the recipient (which would be a Member State’s RIM in the network).

A CAS dynamic discovery service is provided to the sender by the European Commission, a service that uses DNS lookups to find the appropriate recipient information in the network – this is the main functional requirement of the CAS and will be described below as BR1. This service is voluntary for the sender. A static configuration in the RIM technical address may be still used as alternative.

The same service may be used the other way around (in reverse), where the RIM lookups the sender address – this is voluntary as well. This reverse lookup provides an additional layer of flexibility in communication handling and can support more complex scenarios if necessary.

The CAS dynamic discovery service will function in a similar manner as the Domain Name Service (DNS), where the service will respond to system-to-system queries against its key-value database in order to provide the endpoint of the Access Point in question.

A **sender** queries a metadata publisher service that provides information related to the recipient including IP address, message format and transmission protocol – which are often referenced as **capabilities** throughout the document.

A metadata publisher node is a service that interacts with a database of capabilities of participants.

The CAS will introduce increased scalability, interoperability, and reusability among the different domains in the network: the sender and the member state domains. Rather than having a fixed, pre-determined address for the recipient, the sender retrieves the recipient’s details dynamically at the time of communication. This makes the network more flexible and scalable, as the sender does not need to maintain a static list of addresses for all possible recipients.

Outlined below are the business requirements which the CAS is expected to fulfil to ensure it is an effective solution.

Dynamic Address Resolution

|  |  |  |
| --- | --- | --- |
|  | Name | Description |
| BR1 | Dynamic Address Resolution | Mechanism by which a sender dynamically discovers the communication endpoint and capabilities of a RIM – this is a voluntary mechanism to the sender. This requirement fulfils the regulation REF\_D1 |
| BR2 | Reverse Lookup | Same mechanism as above but on Member State level which lookups the endpoint and capabilities of the sender. Some capabilities and participant structure might differ from BR1. This requirement is not mentioned in the regulation, but it is considered advantageous for MSs on the long term, making use of the existing structure created for the CAS to manage address lookup of senders. |

Table 4 - Business requirements - Dynamic Address Resolution

Dynamic Address Resolution introduces flexibility and scalability to the network. It is particularly important in large, distributed networks where changes in participants communication endpoints and capabilities are more frequent and unpredictable.

To achieve this, the network must have a mechanism in place that allows senders to retrieve the latest address information for a given recipient. This will be done through a dedicated service that maintains up-to-date information about all the participants in the network.

Reusability

|  |  |  |
| --- | --- | --- |
|  | Name | Description |
| BR3 | Reusability | Mandates that any piece of information provided by a participant must be reusable. |

Table 5 - Business requirements - Reusability

After initial provision, the participant’s data must be internally reusable across different access points in the network to prevent users from being asked for the same information multiple times. This requirement is critical for improving efficiency and reducing administrative burden.

Scalability and adaptability

|  |  |  |
| --- | --- | --- |
|  | Name | Description |
| BR4 | Adaptability | The service should be designed to handle changing participants and their capabilities. |
| BR5 | Scalability | The service should maintain its ability to adapt and perform efficiently despite changes in the environment and respond quickly to those changes to minimize the risk of errors and increase efficiency. |

Table 6 - Business requirements - Scalability and adaptability

The common addressing service is best suited for evolving networks where the participants and their capabilities may change frequently.

This service will minimise the need for extensive human interventions and will, therefore, proportionally reduce costs and risks of errors. By using the common addressing service, the network will adapt to changes in the capabilities of its participants, ensuring that it remains flexible.

The common addressing service will provide the system with the scalability and adaptability it needs to evolve and grow with the changing needs of its participants, avoiding the costs and risks associated with manual interventions.

High-level Functional and Technical specifications for the cas

This chapter contains an overview of the scope and describes the high-level functional and technical specifications for the Common Addressing Service (CAS).

Architecture of the CAS

The CAS can be used as an extension to the 4-corner model architecture to enable dynamic discovery of participants’ capabilities.

The 4-corner model describes the structure of secure and reliable electronic data interchange in an eDelivery AS4 network. The eDelivery AS4 Profile, developed under the direction of the European Commission, is a set of technical specifications and requirements that standardizes the use of AS4 messaging protocol.

The CAS foresees the concept of distributed nodes that contain the metadata information representing the capabilities (including technical address of recipient, messaging protocol, message format) of each participant in the network – called publisher nodes.. Each receiving participant publishes its capabilities in only one publisher node. The Member State hosts one of these nodes and publishes its own information there as a participant.

A centrally, EC maintained node (central locator node) will index and provide lookup services to dynamically retrieve the distributed publisher nodes. To do this, it stores and manages both the participant information and the corresponding metadata of the distributed publisher nodes in the DNS.

Below, a high-level diagram of the system in the 4-corner model with the introduction of the CAS elements.

1. A sender needs to send a message to the RIM, but it does not know the technical address and/or other capabilities of it.
2. A DNS query is performed, using the RIM’s known business identifier, to retrieve the node that contains the metadata. The node is defined as a publisher node.
3. Corner 2 then retrieves all the necessary metadata from the publisher node to locate the message recipient’s address and capabilities.
4. With the data retrieved from the publisher node it prepares and sends the AS4 message to Corner 3.
5. Corner 4 processes the message.

The dashed connections happen before the workflow above and show that it is the recipient – the Member State – that has registered their capabilities and endpoint information within the publisher node (*a)*) and, later, configured the lookup in the DNS through the central address lookup node (*b)*).

The Member State hosts its own publisher node.



Figure 1 - CAS in 4-corner architecture

Since CAS is a voluntary service (as stated in the Regulation REF\_D1), the dynamic discovery is typically triggered by the sender in the absence of pre-configured technical address information in the AS4 Access Point.

A sender, who actively exchanges an AS4 message described in arrow 4, requests to a central address lookup node to retrieve the endpoint of the message destination. The central node will then find the appropriate distributed publisher node that contains the physical address of the RIM AS4 access point message destination.

Functional and Technical Specifications

Following 3.2 requirements we can infer below functional and technical specifications.

High-level process for address discovery

The Address Lookup is the key component that enables dynamic discovery. This component uses the DNS decentralised system to lookup information concerning a given participant.



Figure 2 - Address discovery

1. When a sender wants to exchange data with a recipient (a Member State RIM), it first queries the DNS with the recipient's electronic address.
	1. This electronic address is derived from the recipient’s unique identifier (that the sender – and everyone – knows) following specific domain name conventions.
2. It performs a DNS query from the derived domain name.
	1. The Central address lookup node is responsible for managing DNS records of participants (but not the DNS system itself). The DNS system returns the record, which resolves to the URL of the corresponding distributed Publisher node of the recipient (Member State).
3. The sender then requests to the publisher node.
4. The publisher node then returns the capabilities and, specifically, the endpoint of the recipient.
5. The Sender has the technical address and all the necessary capabilities of the recipient, including the public certificate, to establish a secure connection and exchange documents with the recipient (the Member State).

Reverse Lookup

The process illustrated in Figure 2 - Address discovery outlines the dynamic discovery of any participant within an AS4 network. By simply reversing the flow direction from sender to receiver, the process remains the same. In other words, when a Member State's RIM initiates a message to the sender, the discovery process should function in a similar manner.

Although not foreseen in the regulation, this feature is technically possible and could be added in the future if there was a need for it. This feature could add flexibility to the network, especially in large, distributed networks where the amount of senders create complexity, keeping track of so many technical addresses.

The Member State is, in any case, responsible for registering and maintaining the sender’s information.

Central Node

The Central Address Lookup node’s main goals are to perform DNS-based lookups for participant business identifiers to identify the associated publisher node, and to manage the records of the endpoints of these publisher nodes.

The Central Address Lookup node is used to create or update the participant’s records in the Domain Name System (DNS) so that the senders can discover the corresponding publisher metadata node of the recipient. As a result, these infrastructures can scale up without being affected by the management of an increasing number of participants. Instead of having to centrally manage a list of Access Points (known as 'static discovery') which all of them must be able to access and download, the discovery of participants becomes dynamic and possibly fully distributed and consequently much more scalable.

| **ID** | **Name** | **Description** |
| --- | --- | --- |
| **C1** | Central Address Lookup | This node enables discovery (via DNS lookup) of a publisher node that contains the address and capabilities of the recipient. |
| **C2** | Central management of publisher nodes  | The node allows for the registration, update, deletion and visualization of the metadata publisher nodes.. |
| **C3** | Central management of participants | The node allows for the creation, listing, deletion or migration of participant records in the DNS. |
| **C4** | Trust and Security | The node will only allow the registration of trusted publisher nodes, i.e., the publisher endpoint is trusted by a known chain of trust. |

Table 7 - Functional Area - Central Address Lookup

The central node is operated by the European Commission and facilitates address resolution via the decentralised and redundant DNS service. The central node does not store the addresses of the AS4 recipients in the network – it stores the information about the distributed publisher node’s location.

The central node interacts with the DNS to find the address of the participant’s metadata publisher. It provides controlled access to the management of entries in the DNS. This means that the dynamic discovery (the actual lookup) relies on a highly resilient and decentralised service.

| **ID** | **Name** | **Description** |
| --- | --- | --- |
| **D1** | Publisher Node registration | The MS Administrator registers the Publisher node’ metadata in the central node. |
| **D2** | Update Node metadata | The Publisher node’s metadata (endpoint) is updated |
| **D3** | Delete Node  | A publisher node is decommissioned via central node.  |

Table 8 - Functional Area – Central Management of Publisher nodes

In addition to these tasks, the MS administrator has another responsibility during the event of a migration of participants from one publisher node to another. When a participant migrates, it is imperative to update the DNS entry through the central address lookup to reflect the new publisher node. This update ensures a smooth transition by enabling other participants to discover the new publisher seamlessly. If all participants migrate to a new node, the administrator can delete the previous publisher entry from the central node, maintaining the integrity and accuracy of the network's metadata information.

Publisher nodes

The Publisher node – an individual metadata publisher node – contains the capabilities (such as message format, the transport protocol, security requirements, and the technical address of the recipient’s Access Point). This metadata is essential for establishing secure and efficient communication between different entities in the network. The sender can then use this metadata to establish a secure connection and exchange messages with the recipient.

To make the network distributed, dynamic and resilient, each Member State sets up their own Publisher node where addresses and capabilities of their RIM and senders are registered.



Figure 3 – Recipient address management

As portrayed in the figure above, a Member State administrator has the authority to carry out several important operations involving the Publisher Node in conjunction with the Central Node. They can register a new participant in the DNS via the Central Node, effectively making the participant discoverable.

The administrator also has the capacity to migrate the location of the participant’s publisher node in the DNS, ensuring the correct and current address is accessible for communication.

If necessary, the administrator can also delete the participant entry from the DNS with the help of the Central Node

 

Figure 4 – Participant migration

In the table below are listed the typical features that a Publisher node makes available for the sender when it obtains the publisher’s endpoint.

| **ID** | **Name** | **Description** |
| --- | --- | --- |
| **D4** | Request handling  | The publisher node provides the recipient’s capabilities metadata upon request. A database is hosted to store the capabilities metadata of each participant. |
| **D5** | Trust and Security | Publisher nodes are accessible over the internet and use HTTPS with a valid certificate containing a trusted chain. |
| **D6** | Manage Capabilities | APIs are exposed to manage sender’s capabilities in the database. This include adding participant’s capabilities, updating or removing them. |

Table 9 - Functional Area - Publisher nodes

In more detail, expanding D6 , the Publisher Node maintains information about the capabilities of each participant registered in its domain, which is important for ensuring interoperability among different participants. These capabilities typically include:

| **ID** | **Name** | **Description** |
| --- | --- | --- |
| **E1** | Endpoint information  | The recipient endpoint where the sender transmits the message |
| **E2** | Document formats | This refers to the types of documents that a sender can transmit. This can be related to formality business types. |
| **E3** | Transport protocols | This indicates the communication protocols that a participant can use to send and receive messages. For the EMSWe, it will be AS4 protocol. |
| **E4** | Public certificate | Publisher nodes can also supply the public certificate (with trusted chain) associated with a recipient. In that way the sender can encrypt the message knowing only the recipient can decrypt it. |

Table 10 - Recipient capabilities

In reverse lookups, when a publisher node contains the capabilities of the sender, it is the Member State responsibility to manage these details in the node and to maintain its freshness.

Logging and feedback

| **ID** | **Name** | **Description** |
| --- | --- | --- |
| **L1** | Logging information | The (central and distributed) nodes provide logging capabilities for auditing and reporting purposes to the member states that host them and to the EC.  |
| **L2** | Monitoring | The (central and distributed) nodes provide monitoring capabilities as well, they provide responsive insights into the usage and traffic of the network. |
| **L3** | Exception handling | The nodes have exception and error-handling capabilities to inform their operators of anomalous conditions and errors. |

Table 11- Logging and feedback