EUROPEAN COMMISSION
DIRECTORATE-GENERAL
TAXATION AND CUSTOMS UNION
Digital Delivery of Customs and Taxation Policies
Customs Systems

Interface Control Document

ICS2 Harmonised Trader Interface

Date:	10/07/2020
Status:	Sent for acceptance (SfA)
Version:	2.50 EN
Author:	CUST-DEV3
Approved by:	DG TAXUD
Reference number:	Ares(2019)6516093
Public:	DG TAXUD external
Confidentiality:	Publicly available (PA)

Document control information

Property	Value
Title	Interface Control Document
Subtitle	ICS2 Harmonised Trader Interface
Author	CUST-DEV3
Project owner	Klemen OVEN
Solution provider	ICS2 team
DG TAXUD Project Manager	Bartlomiej BZDELA
Version	2.50 EN
Confidentiality	Publicly available (PA)
Date	10/07/2020

Contractor information

Property	Value
Framework Contract	Framework Contract - TAXUD/2013/CC/124
Specific Contract	Specific Contract n° 23 - TAXUD/2018/DE/148

Document history

The document author is authorised to make the following types of changes to the document without requiring that the document be re-approved:

- Editorial, formatting and spelling;
- Clarification.

To request a change to this document, contact the document author or project owner.
Changes to this document are summarised in the table in reverse chronological order (latest version first).

Version	Date	Description	Action[1]	Section
2.50	10/07/2020	Implementing review cycle comments. Submitted for Acceptance (SfA) to DG TAXUD	I/R	All
2.40	02/07/2020	Implementing Release 1 construction 3 input: • RTC36766 ICS2 message prioritisation • RTC45826 include minor omissions and UUM&DS error codes • Alignment with the currently applicable TEMPO template requirements (all sections). Submitted for Review (SfR) to DG TAXUD	I/R	Document control information, 3.3.2.6, Annex 4 section 5
2.30	21/01/2020	Implementing review cycle comments. Submitted for Acceptance (SfA) to DG TAXUD	I/R	All

[1] Action: I=Insert R=Replace

Version	Date	Description	Action[1]	Section
2.20	31/12/2019	Implementing Release 1 construction 3 input: • Aligned to new TEMPO format; • RTC 36783: the new structure of the partyId has already been updated in the previous version; • RTC 35391: ICS2 CTSS review MS and Trade comments: the change was already implemented. Submitted for Review (SfR) to DG TAXUD	I/R	All
2.10	09/10/2019	Implementing review cycle comments. Submitted for Acceptance (SfA) to DG TAXUD	I/R	All
2.00	20/09/2019	Implemented Release 2 input. Section 4.2.2.1 has been updated to the new structure of the partyId, and section 4.3.3 has the mpc structure updated. Submitted for Review (SfR) to DG TAXUD	I/R	All
1.90	10/05/2019	Implementing review cycle comments. Submitted for Acceptance (SfA) to Taxation and Customs Union DG.	I/R	All
1.80	06/05/2019	RTC35391: Implement the comments raised during the Member State and Trader review of the CTSS package sent to them on the 28/02/2019 in sections 3.1.2. Submitted for Review (SfR) to DG TAXUD	I/R	All
1.71	28/02/2019	Submitted for Review to member States and Trade Representatives.	I/R	All
1.70	25/02/2019	Re-Submitted for Acceptance (SfA) to Taxation and Customs Union DG.	I/R	All
1.60	21/02/2019	Implementing review cycle comments. Submitted for Acceptance (SfA) to Taxation and Customs Union DG.	I/R	All
1.50	06/02/2019	Implemented changes on message level encryption and dynamic receiver profile extension in section 4.6, adding the F17 message, explained binary attachments and maximal message size[2]. Submitted for Review (SfR) to DG TAXUD	I/R	All
1.40	07/11/2018	Implementing QA4 and DG TAXUD review comments. Submitted for Acceptance (SfA) to Taxation and Customs Union DG.	I/R	All
1.30	16/10/2018	Implemented error handling in section 4.5, message level encryption and dynamic receiver profile extension in section 4.6, submitted for SfR to DG TAXUD	I/R	All
1.21	19/09/2018	Submitted for SfI to DG TAXUD	I/R	All
1.20	30/05/2018	Updates following review cycle by Member States	I/R	All

[2] RTC 33193, RTC32675, RTC 32737 and RTC 32972

Version	Date	Description	Action[1]	Section
1.10	27/04/2018	Updates following comments and conclusions of the STI Project Group.	I/R	All
1.00	23/04/2018	Implementing QA and DG TAXUD review comments. Submitted for Acceptance (SfA) to Taxation and Customs Union DG.	I/R	All
0.10	04/04/2018	Implementing DG TAXUD review comments. Submitted for Review (SfR) to Taxation and Customs Union DG.	I/R	All
0.04	14/03/2018	Draft Submitted to STI Project Group (21/03) and for Information to ECCG members.	I/R	All
0.03	13/03/2018	Implementing DG TAXUD review comments. Submitted for Information (SfI3) to Taxation and Customs Union DG.	I/R	All
0.02	22/02/2018	Implementing DG TAXUD initial review comments. Submitted for Information (SfI2) to Taxation and Customs Union DG.	I/R	All
0.01	02/02/2018	First draft. Submitted for Information (SfI) to Taxation and Customs Union DG.	I	All

Configuration management: document location

The latest version of this controlled document is stored on CIRCABC.

Table of contents

List of tables

List of figures

1 INTRODUCTION

1.1 DOCUMENT PURPOSE

The purpose of this document is to describe the overall technical Common System Specifications of the ICS2 System-to-System (S2S) Trader Interfaces. In particular, this document provides specifications and lays out applicable guidelines to support the technical implementation of IT system-to-system interfaces between the ICS2 Trader Interfaces (ICS2 TI) and the connectivity access points used by Economic Operators in the context of the ICS2 system.

Each Member State has the option to develop a National Trader Interface (NTI) or use the Shared Trader Interface (STI) implementation. These implementations must be compliant to the Harmonised Trader Interface specifications (HTI) which are the subject of this document.

1.2 TARGET AUDIENCE

The main target audience for this document is the Economic Operators and/or the IT service providers who are responsible for the implementation and maintenance of interfaces between the EO system and the ICS2 TI, as well as national administrations implementing a NTI or participating in the STI.

Readers are assumed to have a good understanding of general IT architectural concepts and may belong to the following categories:

- Economic Operators;
- EO IT system providers;
- DG TAXUD units responsible for ICS2 TI implementation;
- Member States responsible for ICS2 TI implementation;
- External Contractors involved in ICS2 development or operational activities.

1.3 SCOPE

The scope of this document is to define:

- The technical and operational aspects of the ICS2 system-to-system Trader Interface with a link to the functional specifications;
- The interfaces and services to be implemented at ICS2 TI with a view to be consumed by the access point used by an Economic Operator (EO);
- The interfaces and services to be implemented by the access point used by an EO with a view to be consumed by the ICS2 TI;
- The message exchange protocol between the ICS2 TI and the access point used by an EO, including the technical specificities of its implementation for ICS2;
- The operational aspects of the interface to be applied, e.g. the necessary actions to be taken in order to enroll and register an access point as an ICS2 system actor, the testing, connection and message exchange actions with the ICS2 TI, etc.

In addition, it is in the scope of this document to describe supporting and operational elements of the interfaces, such as security aspects, certain Operational Service Level and Change Management aspects.

The ICS2 system will be implemented in an incremental way: a series of blocks define the roadmap for its implementation along three releases. The scope of this document was originally release 1 and has been updated to include the impact of release 2. The document is applicable to both releases.

1.4 STRUCTURE

The present document contains the following chapters:

- **Chapter 1: Introduction** describes the scope and the objectives of the document;
- **Chapter 2: Overview** provides an overview of the functional, technical and operational aspects of the ICS2 system-to-system Trader Interface, as well as the context of this interface in the ICS2 environment;
- **Chapter 3: Functional Information Exchange Specifications** describes the functional specification of the services, the information exchange messages and the orchestration of information exchange between the access point used by an EO and the ICS2 TI, including the rules and conditions;
- **Chapter 4: Technical Information Exchange Specifications** describes the technical specification of the selected message exchange protocol between the ICS2 TI and the access point used by an EO, including the technical specificities of its implementation;
- **Chapter 5: Operational** describes the operational aspects of enrolling, registering, testing and successfully setting-up an interface between the access point used by an EO and the ICS2 TI;
- **Annex 1: Service operations** provides a list of service operations and their payloads;
- **Annex 2: P-Modes Summary** provides a summary of the P-modes;
- **Annex 3: Sample Message Scenario** provides an example scenario of an information exchange with the help of messages;
- **Annex 4: ebMS Errors** lists the errors returned during problematic message exchanges;
- **Annex 5: Message Layer Security Controls** describes how message level security controls are applied.

1.5 REFERENCE DOCUMENTS

Ref.	Title	Originator	Version	Date
R01	eDelivery AS4 Profile	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4	1.14 1.15 (eDelivery Community Draft)	31/10/2018 18/12/2018
R02	ICS2 BPM L4 Process Description	ICS2-CFSS-BPML4 Process Description	1.12 1.22	07/12/2018 31/03/2020
R03	ICS2 Definitions	ICS2-CFSS-Definitions	1.11	16/03/2020
R04	ICS2 Information Exchange Specifications	ICS2-CFSS-IE	1.15 1.22	08/01/2019 31/03/2020
R05	ICS2 EO SSD	CD3-ICS2-STI-SSD-eu_ics2_c2t	4.40	09/10/2019
R06	ICS2 EO TSC	CD3-ICS2-STI-TSC-eu_ics2_c2t	4.40	09/10/2019
R07	OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.html	3.0	01/10/2007

Ref.	Title	Originator	Version	Date
R08	eDelivery AS4 Conformant Solutions	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-SENS+AS4+conformant+solutions	N/A	N/A
R09	XML Schema Part 2: Datatypes	https://www.w3.org/TR/xmlschema-2	2nd Edition	28/10/2004
R10	Internet Message Format	https://www.ietf.org/rfc/rfc2822.txt	N/A	April 2001
R11	e-SENS ebCore Party Id	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-SENS+ebCore+Party+Id+1.3	1.3	18/10/2017
R12	AS4 Profile of ebMS 3.0	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.html	1.0	23/01/2013
R13	Algorithms, Key Sizes and Parameters Report – 2013	https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report	N/A	29/10/2013
R14	Test Design Specifications for Economic Operator Conformance Test Cases	CD3-ICS2-TDS-CTC-EO	1.40	07/07/2020
R15	UUM&DS – Central Certificates Registration Tool Manual for Economic Operators	Manual for EO - Certificate Registration	N/A	N/A

Table 1: Reference documents

1.6 APPLICABLE DOCUMENTS

Ref.	Title	Reference	Version	Date
A01	Framework Contract	TAXUD/2013/CC/124	N/A	11/11/2013
A02	Specific Contract n° 23	TAXUD/2018/DE/128	N/A	01/05/2019
A03	CD3-FQP-Framework Quality Plan	DG TAXUD	1.00	30/04/2015

Table 2: Applicable documents

1.7 ABBREVIATIONS & ACRONYMS

For a better understanding of the present document, the following table provides a list of the principal abbreviations and acronyms used.

See also the ‘list of acronyms’ on TEMPO.

Abbreviation/Acronym	Definition
AEO	Authorised Economic Operator
AEOS	Authorised Economic Operator – Safety and Security
AS4	Applicability Statement 4
CA	Certificate Authority
CR or ICS2 CR	ICS2 Common Repository
DG TAXUD	Directorate-General Taxation and Customs Union
ebMS	ebXML Messaging Services
eIDAS	Electronic Identification Authentication and trust Services
ENS	Entry Summary Declaration
EO	Economic Operator
EORI	Economic Operator Registration and Identification
ERDS	Electronic Registered Delivery Service
HRCM	High Risk Cargo and Mail
HTI	Harmonised Trader Interface
ICS2	Import Control System 2
ITSP	IT Service Provider
LOTL	List of Trusted Lists
LRN	Local reference number
MEP	Message Exchange Pattern
MIME	Multipurpose Internet Mail Extensions
MS	Member State
MSH	Message Service Handler
MRN	Movement Reference Number
NES	National Entry System
NTI	National Trader Interface
NVOCC	Non-Vessel Operating Common Carrier
RMS	Responsible Member State
S2S	System-to-System
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
STI	Shared Trader Interface
TAPAS	DG TAXUD AS4 Access Point
TI or ICS2 TI	ICS2 Trader Interface

Abbreviation/Acronym	Definition
TES	Trans-European System
U2S	User to System
UI	User Interface
UUID	Universal Unique Identifier
UUM&DS	Uniform User Management and Digital Signatures
XML	Extensible Markup Language
XPath	XML Path Language

Table 3: Abbreviations and acronyms

1.8 DEFINITIONS

For a better understanding of the present document, the following table provides a list of the principal terms used.

See also the 'glossary' on TEMPO.

Term	Definition
AS4	AS4 (Applicability Statement 4) is a Conformance Profile of the OASIS ebMS 3.0 specification and represents an open standard for the secure and payload-agnostic exchange of Business-to-business documents using Web services.
AS4 access point	An AS4 access point is an operational IT component that implements the AS4 specifications for the exchange of information with other AS4 access points, be it a Trader Interface (STI/NTI) or an access point used by an Economic Operator (EO).
Carrier	Carrier means in the context of entry, the person who brings the goods, or who assumes responsibility for the carriage of the goods, into the customs territory of the Union. However, (i) in the case of combined transportation, "carrier" means the person who operates the means of transport which, once brought into the customs territory of the Union, moves by itself as an active means of transport; (ii) in the case of maritime or air traffic under a vessel- sharing or contracting arrangement, "carrier" means the person who concludes a contract and issues a bill of lading or air waybill for the actual carriage of the goods into the customs territory of the Union. (Definition is from ICS2 definitions [R03])
Certificate Authority	A Certificate Authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 standard.

Electronic Certificate	An electronic or digital certificate is an attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.
Electronic seal[3]	According to the eIDAS regulation, an electronic seal is a piece of data attached to an electronic document or other data, which ensures data origin and integrity. Technically similar to digital signatures, electronic seals serve as evidence that an electronic document was issued by a specific legal entity, not a natural person.
High Risk Cargo and Mail Screening (HRCM screening)	High Risk Cargo and Mail Screening (HRCM screening) is a notification communicated by the customs authority of the RMS to the person filing (and the carrier under certain conditions) that the goods concerned shall need to be screened as a high risk cargo and mail, in accordance with the point 6.7.3 of the Annex to Commission Decision C (2010) 774 of 13 April 2010, before being loaded on board of an aircraft bound to the customs territory of the Union. (Definition is from ICS2 definitions [R03])
IT Service Provider	An IT Service Provider (ITSP) is a legal person contracted by a Person filing for services involving the delivery and reception of messages to and from ICS2 TI. An IT Service Provider must be identified and registered by Customs to be authorised to exchange messages with TI. Any EO can have its own system or make use of services from one or several ITSPs for the delivery of ICS2 messages to Customs (via STI/NTI). The use of these services must be covered by a contractual arrangement where the EO assumes the responsibility of any information sends by the ITSP to Customs.
Payload	The present document refers to the term “payload” as the XML encoded data-set defined for information exchange as defined in the ICS2 Information Exchange Message definition document [R04]. For the technical realisation of an information exchange between two parties (a Sender and a Trader Interface), a payload is embedded in an AS4 message.
Person filing	Person filing means any person that submits to the customs authority ENS filing in its complete or partial content and other notifications in the prescribed form and manner. This person can be any person that issues a bill of lading or air waybill and can be either

[3] This electronic seal must not be confounded with the physical electronic seals attached to shipping containers.

	carrier, NVOCC (i.e. freight forwarder), or any person identified by the legal provisions obliged to submit required particulars of ENS to the customs and can include postal operator, consignee stipulated in the lowest bill of lading. Person filing also includes a representative of any of the persons mentioned above that submits the ENS filing in its complete or partial content to the customs authority on behalf of the person that it is representing. (Definition is from ICS2 definitions [R03])
Sender	The present document refers to the term "sender" as the system sending the technical messages to the TI. This can be a system implemented by the EO lodging the ENS filings or by an IT Service Provider. The sender is understood as a system actor in the ICS2 system context and is the one authenticated and authorised from the system security point of view.
Signal Message	An AS4 Message is a logical unit which consists of User Messages or Signal Messages or both. A Signal Message is an ebMS message that contains a Signal Message unit (an eb:Messaging/eb:SignalMessage XML structure) and allows transmitting data interpreted by an AS4 Message Service Handler as a signal (e.g. a pull signal).
Trader Interface	Trader Interface: The TI represents the IT system that will be used by Economic Operators to communicate with customs authorities in the context of ICS2. It is an abstraction of: The National Trader Interface (NTI), developed, hosted and operated by a particular Member State; The Shared Trader Interface (STI), developed, hosted and operated by DG TAXUD.
User Message	An AS4 Message is a logical unit which consists of User Messages or Signal Messages or both. A User Message is a message that contains a User Message unit (an eb:Messaging/eb:UserMessageXML structure) and allows transmitting data interpreted by a Consumer.

Table 4: Definitions

2 OVERVIEW

The Interface Control Document of the ICS2 Trader Interface defines the technical and operational aspects of the ICS2 system-to-system Trader Interface with a link to the functional specifications. It also provides guidelines for the adequate implementation of the interfaces.

It is assumed that the reader is aware of the functional context of the ICS2 system as described in;

- The ICS2 Business Process Description [R02];
- The ICS2 Definitions [R03];
- The ICS2 Information Exchange Message Specifications [R04].

More details on the provided services can be found in:

- The ICS2 Service Specification Documents [R05];
- The ICS2 Technical Service Contracts [R06].

Figure 1 defines the context of this interface in the ICS2 environment.

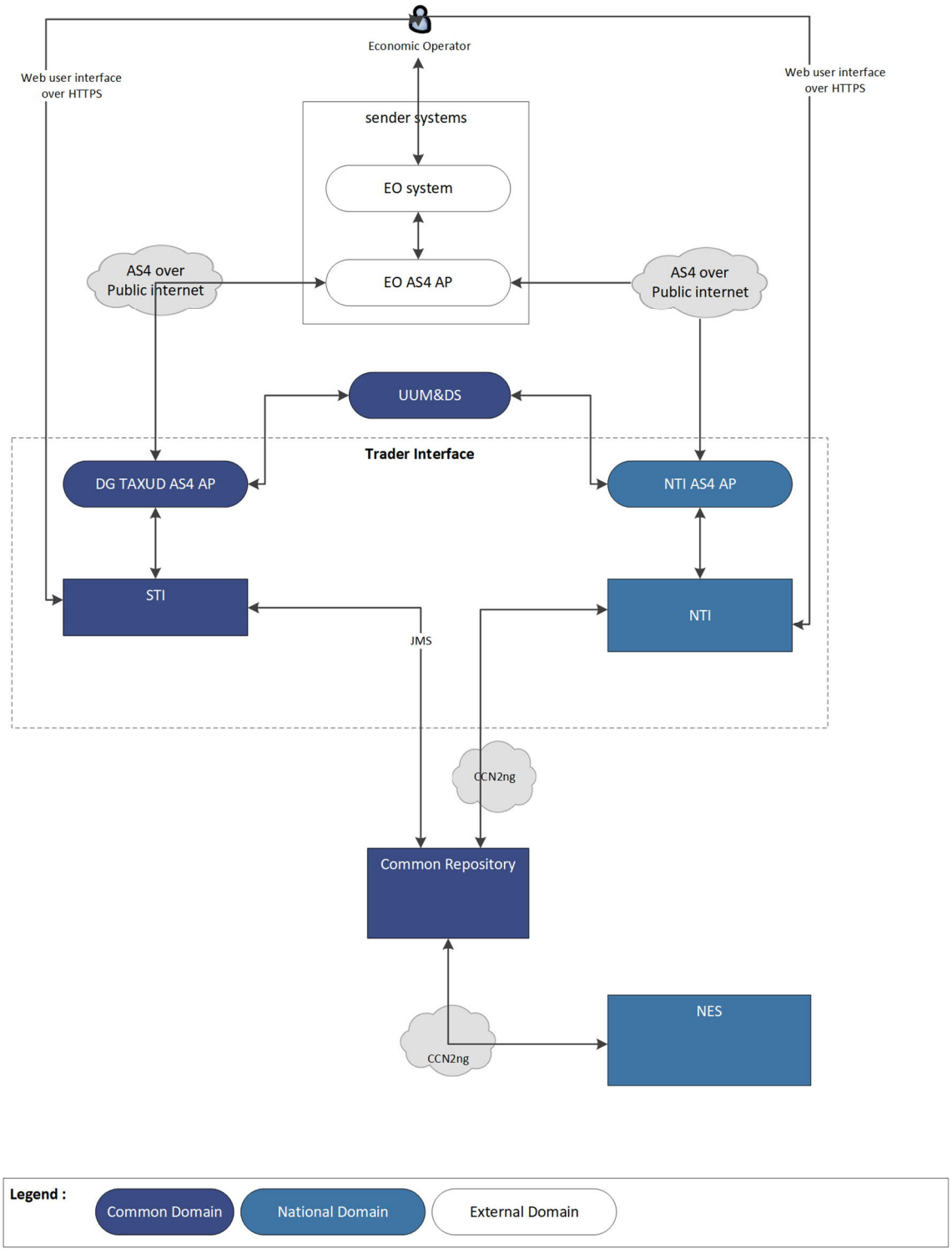

Figure 1: ICS2 overview

In the context of the ICS2 programme, an Economic Operator must interact with the various ICS2 components through the ICS2 Trader Interface. Each Member State has the option to develop a National Trader Interface (NTI) or use the Shared Trader Interface (STI) implementation. These implementations must be compliant with the Harmonised Trader Interface specifications.

A trader must connect to a specific Trader Interface system (National or Shared) according to the Member State of the Customs Office of First Entry (COFE) specified inside the ENS Filing or (if unknown) to the Member State to which the ENS Filing will be addressed.

The ICS2 Trader Interfaces (National or Shared) interact with the ICS2 Common Repository (CR) which is responsible for the ENS lifecycle management (i.e. linking all relevant ENS filings) as well as for orchestrating the risk management process with the relevant NES systems.

The interactions between the ICS2 Common Repository and NES systems occur over the Common Communication Network (CCN2ng). The Uniform User Management and Digital Signatures system (UUM&DS) will support the security measures with registration, identification and authorisation functionality.

The Economic Operator has the choice to interact with a Trader Interface through a web user interface[4], or through a system-to-system interface. Only the latter interface is in scope of this document. The interfaces will be implemented according to the Connecting Europe Facility (CEF) eDelivery building block specifications which are aligned with the eIDAS requirements for ERDS (Electronic Registered Delivery Service) as defined in Article 3(36)[5].

For the technical realisation of these system-to-system interfaces, AS4 access points have to be used accordingly to the eDelivery building block specifications. From a trade perspective, such an access point can be implemented and operated by an Economic Operator himself or can be delivered by an IT Service Provider (ITSP) as a service to an Economic Operator.

As described in more details in the document, the system-to-system interaction occurs over a secure HTTPS connection on the public internet using the AS4 secure and reliable messaging protocol.

[4] Web user interface for trade will only be available from ICS2 Release 2 onwards.

[5] The eIDAS regulation (EU regulation № 910/2014 of 23 July 2014 on electronic identification and repeals directive 1999/93/EC with effect from 30 June 2016) oversees electronic identification and trust services for electronic transactions in the European Union's internal market and regulates electronic signatures, electronic transactions, involved bodies and their embedding processes to provide a safe way for users to conduct business online. Article 3(36) reads as follows: "(36) 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;".

3 FUNCTIONAL INFORMATION EXCHANGE SPECIFICATIONS

The ICS2 TI provides the interface to support information exchanges between a Person filing or if different a Carrier and the Customs Authorities in the scope of ICS2 system. In the case of the System-to-system interaction as described in the current document, the Sender IT system technically fulfils EO requirements to lodge full or partial ENS filings, respond to requests for missing or additional information from National Customs Authorities and receive notifications that they have requested or that are required to be provided in response to their submitted ENS filings. An EO can connect to the ICS2 TI via its own IT system or by using the contracted services of an IT Service Provider (ITSP). In case the latter is true, the ITSP itself must be identified and registered by Customs (see section 4.6.3).

The functional specifications of the prescribed information exchanges are detailed in the ICS2 Business Process Description document [R02] and will not be repeated here in their full extent. In this chapter, a high-level description of the asynchronous communication between the Sender access point used by an EO and the ICS2 TI will be provided, focused on the services implementing the business processes, the message exchanges and the consequent system operations.

Only the S2S interactions will be described in the current document. For the traders using the provided web UI, a user manual will be provided separately.

3.1 INFORMATION EXCHANGES

In this section, the asynchronous S2S interaction between the ICS2 TI and the access point used by an EO is described with the help of high-level sequence diagrams as a set of prescribed information exchanges. These sequence diagrams focus on showing the correlation between services, related message exchanges and system operations which support business processes defined in ICS2 Business Process Description document [R02]. Therefore, they cover functionalities and actions which are initiated by or require the response of the IT system through which the EO is connected to the TI.

In the sequence diagrams provided unterhalb, the mapping of services to system operations (actions) is provided to the reader using the “service_name (ACTION)” convention. The action names used to invoke each operation are aligned with the corresponding message ID of the BPM L4 functional specifications and related ICS2 Information Exchange Message Specifications document [R04]. The list of ICS2 services and the correlation to messages and actions are detailed further below in **Annex 1**.

To assure completeness of information flow and accuracy of high-level description of the system, the high-level sequence diagrams include the ICS2 Common Repository system and the Responsible Member State NES systems, even though there is no direct interaction between access point used by an EO and those systems for the purpose of ICS2.

3.1.1 General Context

In the context of the communication between the EO system and the ICS2 TI, there are four categories of business interaction between the Person filing or if different the Carrier and the ICS2 system:

- Lodge (full or partial)/amend/invalidate an ENS filing;
- Lodge an arrival notification for the means of transport (in case of air and maritime transport);
- Respond to request for additional information from National Customs Authorities;
- Receive information or error notifications relevant to the submitted lodgings.

The Person filing, or if different the Carrier, can be an actor in three of the four categories of business interaction above. A Person filing is responsible for registering a full or partial ENS filing, completing all necessary details according to the type of ENS filing. The types of ENS filing are divided into the following main categories:

- 'sea and inland waterways';
- 'air cargo';
- 'express consignments';
- 'postal consignments';
- 'road mode of transport';
- 'rail mode of transport'.

More information can be found in Annex 1.

The Person filing can submit a request to amend or invalidate a previously registered ENS filing.

The carrier that is the operator of the vessel or aircraft entering the EU from a foreign origin must lodge an arrival notification to the customs office of first entry except where such information is available to the customs authorities (Article 133 UCC).

The Person filing can receive a request to provide additional information and consequently respond to this request. There are two types of request:

- a request to provide additional information;
- a request to perform a HRCM screening (aviation only).

The Person filing can receive information or error notifications relevant to previously submitted ENS filing(s), e.g. notification of an ENS filing for which the ENS is deemed not complete.

Some notifications can be also sent by the TI to the Carrier if different from the filer, when under certain circumstances a Carrier must be notified about an action performed on the system by a Person filing. The carrier is to be notified when:

- The carrier is different from the Person filing and has expressed the preference to also receive the notifications concerning these filings;
- A Do Not Load (message) is issued for cargo transported by that carrier;
- One or more of the parties that the Carrier has indicated as obliged to lodge ENS filings, have not yet filed;
- The carrier is connected to the TI.

Furthermore, there is one notification (in particular, a notification of an ENS filing for which the ENS is deemed not complete) sent by the TI to the 'Person not yet filed', a role which is also defined in the ICS2 Business Process Model [R02]. The Person that has not yet filed is to be notified when:

- This person was indicated in an ENS filing (master or house level) as a person that has an obligation to file a lower level ENS filing;
- The person is connected to the TI.

As mentioned above, the IT system connectivity to the TIs can be implemented by the trader (a Person filing or if different a Carrier) themselves or it can be provided as a service by a contracted IT Service Provider (ITSP). Such ITSP assumes responsibility as system owner of the connecting system (system actor) which must be registered and authorised by Customs; this of course on top of its contractual responsibilities towards the trader as his client.

In the case a trader contracts the use of ITSP services, it will not release him from his responsibility towards Customs Authorities (as Person filing or Carrier).

The access point operated by an ITSP is delivering messages on behalf of a Person filing or if different the Carrier. From a system perspective this is just the intermediary for sending messages containing ENS Filings and receiving/dispatching replies and notifications.

In all cases, in order to be able to send or receive messages from a TI, a party (either an ITSP or the trader himself) must be registered and authorised by the Customs Authorities and registered in the TI to establish system connectivity to ICS2 Trader Interfaces and act as system actor.

The high-level sequence diagrams in the following paragraphs correspond to the following scenarios:

- Register ENS filing (Person filing and Carrier);
- Amend ENS filing (Person filing);
- Invalidate ENS filing (Person filing);
- Submit arrival notification (Person filing);
- Additional information response (Person filing and Carrier);
- HRCM screening response (Person filing and Carrier);
- Notifications received from TI (Person filing, Person not yet filed and Carrier).

3.1.2 ENS filing (IE3Fxx)

A Person filing is responsible for lodging a full or partial ENS filing, providing all necessary details according to the type of ENS filing. The types of ENS filing are divided into the following main categories:

- ‘sea and inland waterways’;
- ‘air cargo’;
- ‘express consignments’;
- ‘postal consignments’;
- ‘road mode of transport’;
- ‘rail mode of transport’.

The types of ENS filing are distinguished using a Specific Circumstance Indicator which can take a code value of the type FXX, where XX are two numeric digits, e.g. ‘F10’. The mapping of the code values to the types of ENS filing can be found in **Annex 1**. In Figure 2, the reader can see actions which include the FXX code value, i.e. IE3FXX. The sequence diagram in the current section represents the message exchange pattern for the submission of any type of ENS filing.

After the submission of an ENS filing via the access point of the Person filing, the Person filing will receive a single reply with an MRN via this same access point.

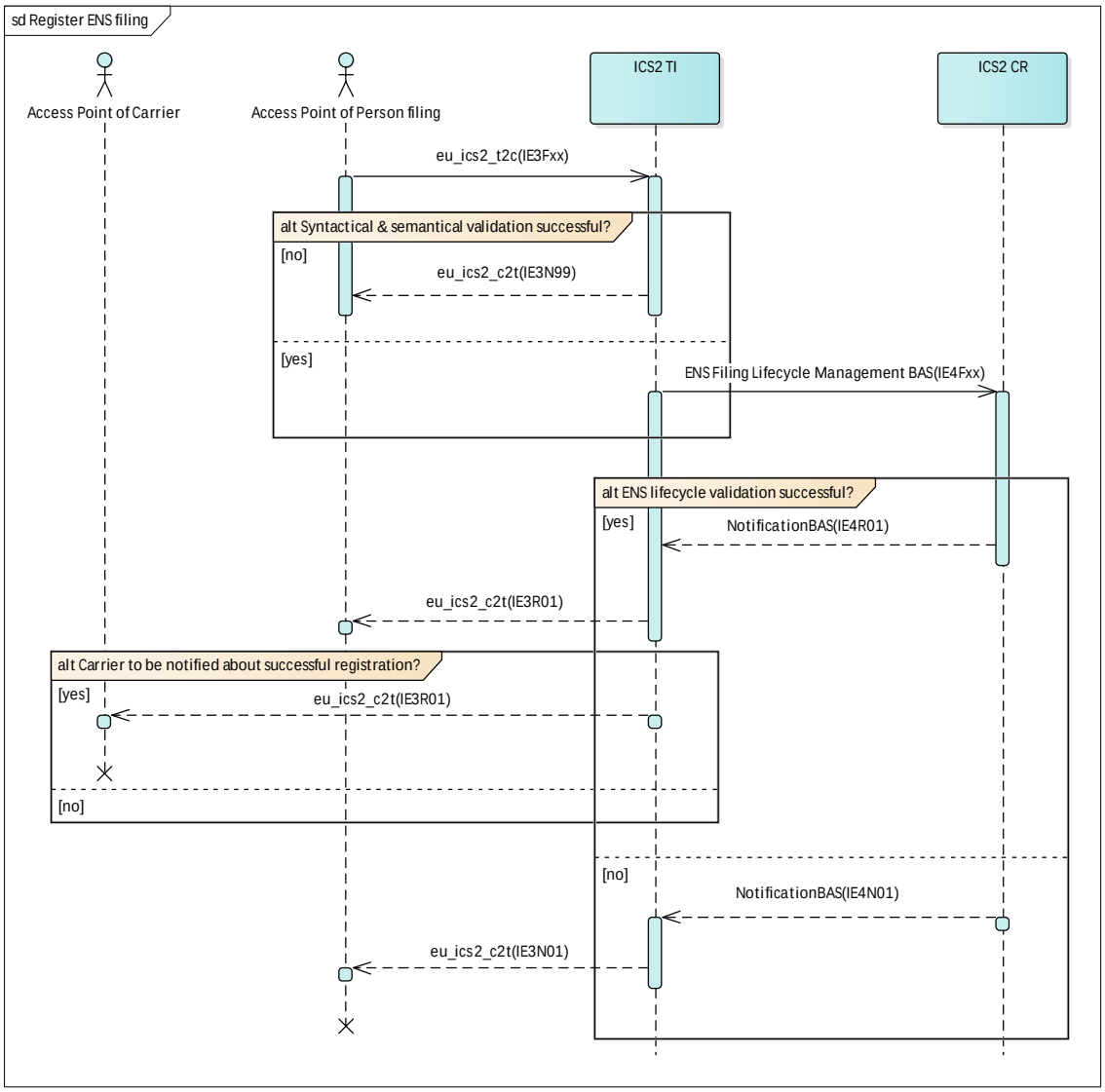

Figure 2: ‘Register ENS filing’ information exchange

3.1.3 ENS filing amendment (IE3Axx)

A Person filing may request to amend a full or partial ENS filing, by submitting a new data-set, according to the type of ENS filing. The updated data-set submitted by this amendment completely replaces the data-set previously associated with the MRN and submitted in a previous ENS filing or amendment. The types of ENS filing amendment are distinguished by their message ID which can take a code value of the type IE3AXX, where XX are two numerical digits, e.g. 'IE3A10'. The mapping of the code values to the types of ENS filing amendment can be found in **Annex 1**. In the figure below, the reader can see actions which include the IE3AXX code value. The sequence diagram in the current section represents the message exchange pattern for the amendment of any type of ENS filing.

After the submission of an amendment to an ENS filing from the filer's access point and successful semantic, syntactical and lifecycle validation, the Person filing will receive a single reply via this access point. Alternatively, an error message will be received by the person filing giving the reason for the message rejection.

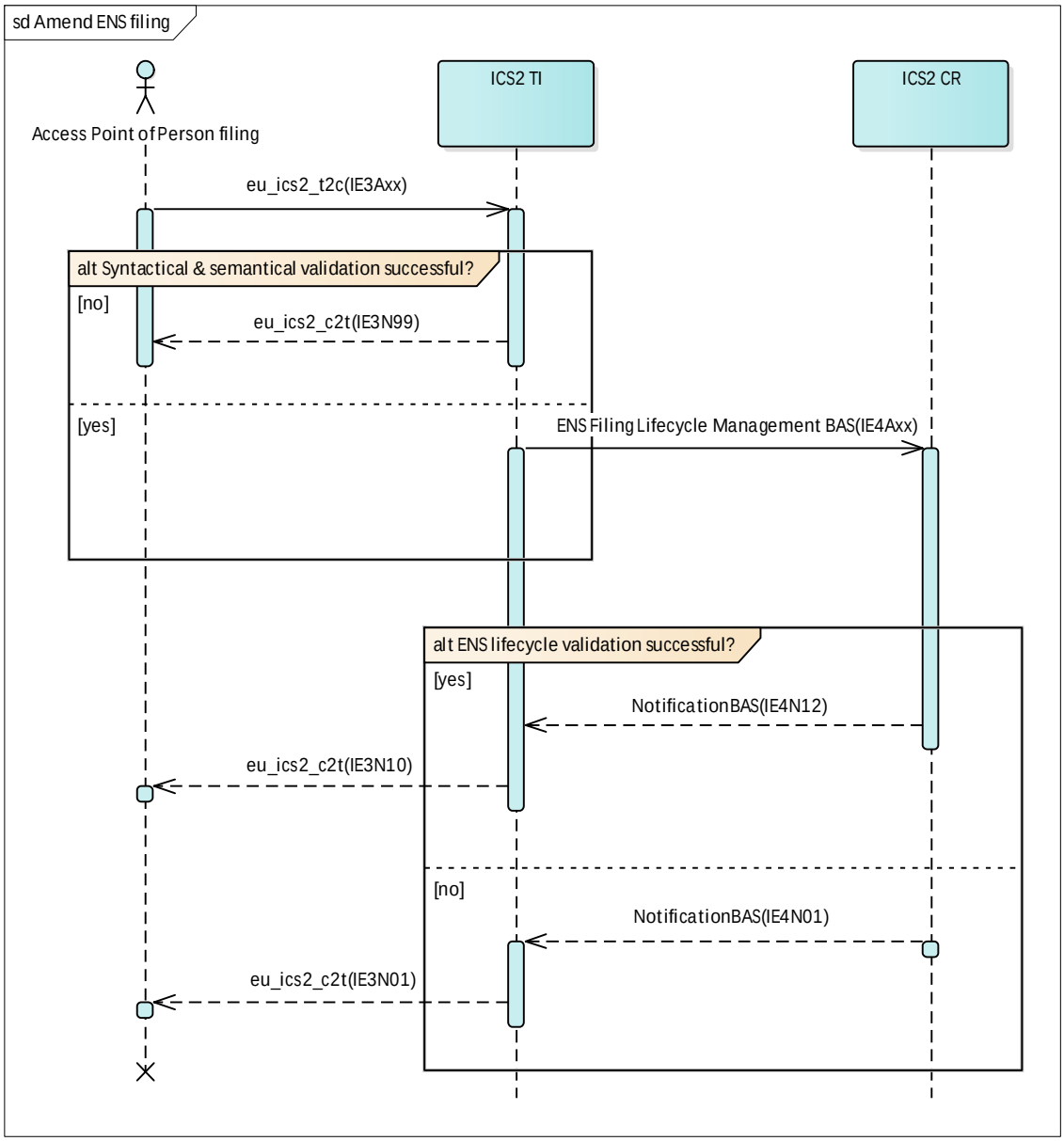

Figure 3: 'Amend ENS filing' information exchange

3.1.4 Invalidation request (IE3Q04)

A Person filing can submit an electronic request to invalidate an ENS filing. The following sequence diagram describes how the system enables the Person filing to electronically request the invalidation of an ENS filing. After the submission of an invalidation request for an ENS filing via the access point of the Person filing, the Person filing will receive a single reply via this same access point.

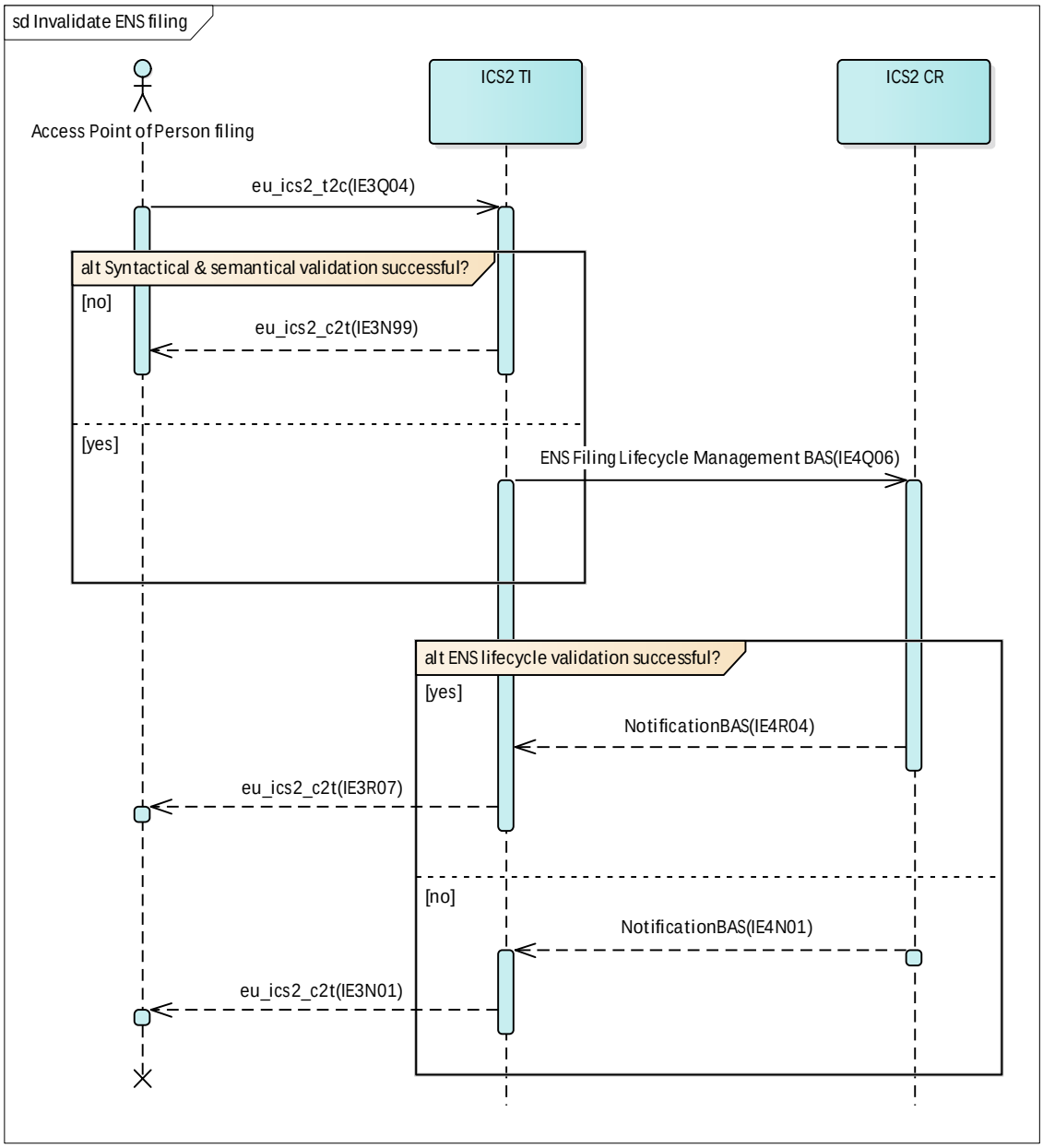

Figure 4: 'Invalidate ENS filing' information exchange

3.1.5 Arrival notification (IE3N06)

In case of air and maritime transport, an arrival notification for the means of transport can be lodged, either via TI or a national arrival system, by a Person filing (a carrier operating the means of transport). The arrival notification identifies the Member State of Actual First Entry and triggers controls on goods which were identified being a risk requiring a control at the first point of entry in the EU (i.e. security and safety threat of such nature that immediate action is required upon arrival).

The following sequence diagram (Figure 5) describes how an arrival notification can be lodged via the EO system.

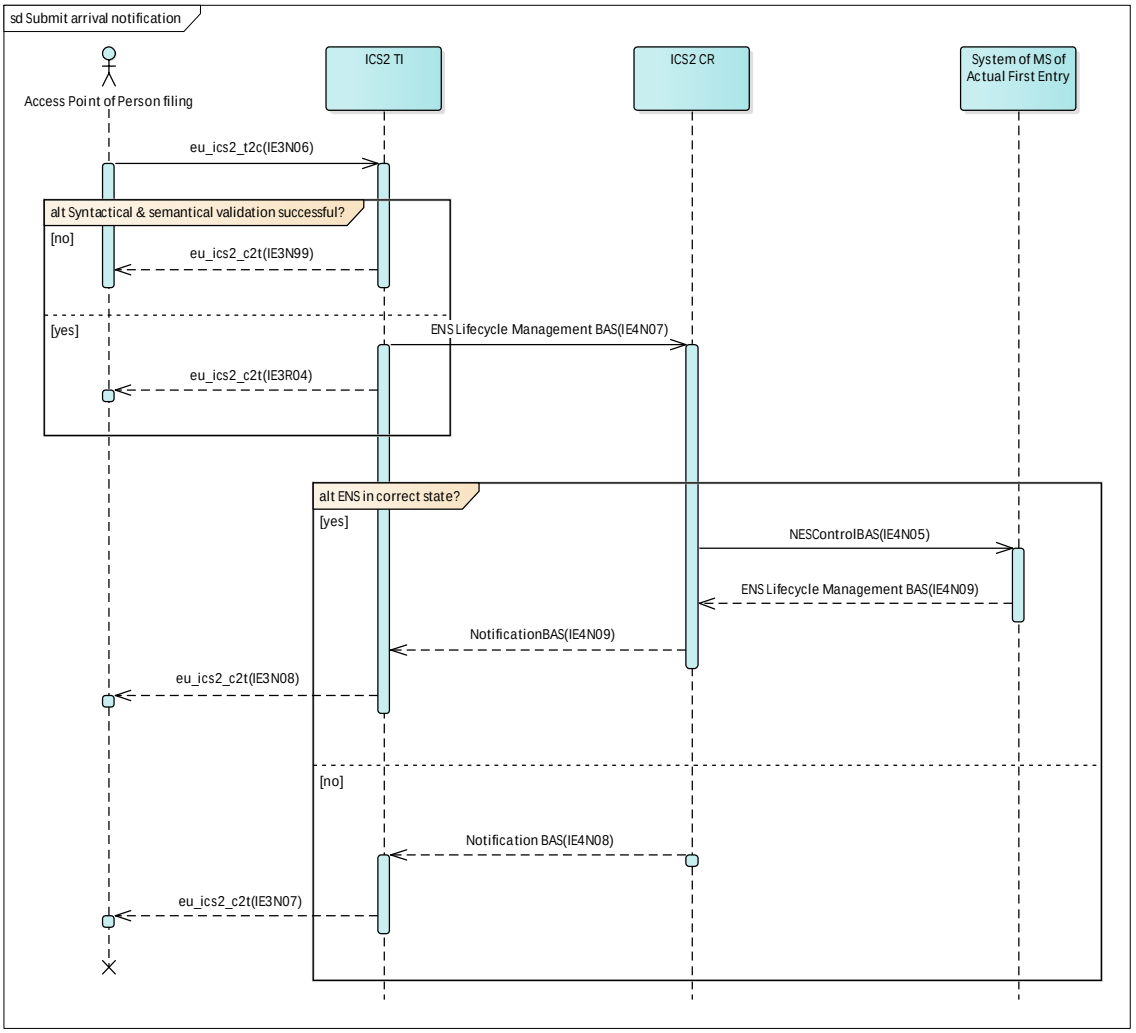

Figure 5: 'Submit arrival notification' information exchange

3.1.6 Additional information request (IE3Q02)

Under certain circumstances, the Person filing may be requested to provide additional information regarding one or more already submitted ENS filing(s). The following sequence diagram describes where the request for additional information originates from and how it reaches the Person filing, who in turn responds to the request. The Carrier may also request to be notified about the request to provide additional information when it is not the Person filing.

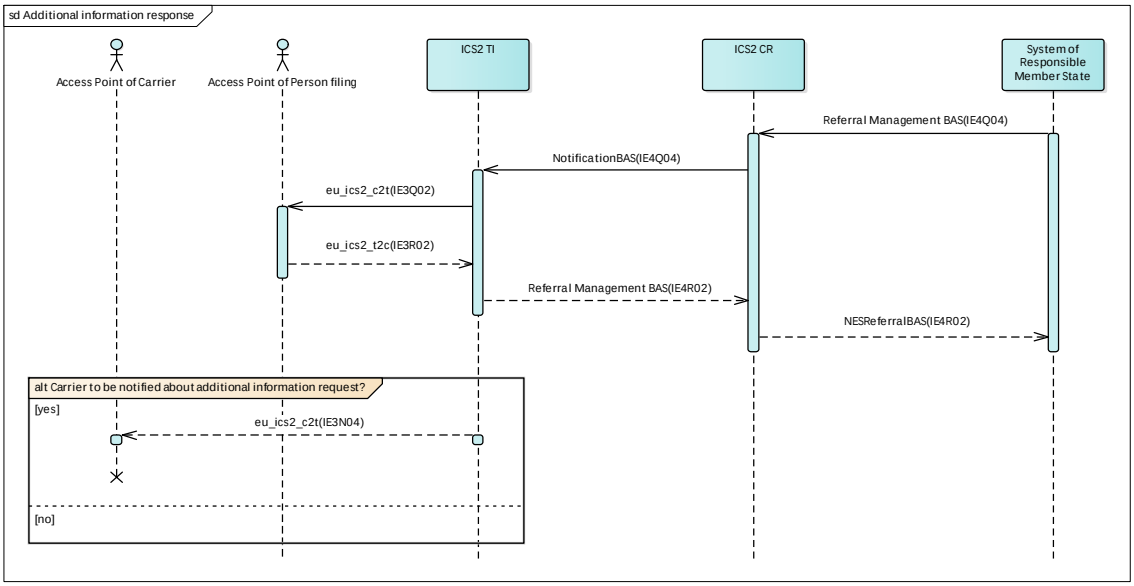

Figure 6: 'Additional information response' information exchange

3.1.7 High Risk Cargo & Mail screening request (IE3Q03)

Under certain circumstances, the Person filing may be requested to execute HRCM screening during the air cargo pre-loading phase. The following sequence diagram describes where the request for HRCM screening execution originates from and how it reaches the Person filing, who in turn responds with the HRCM screening outcome. The Carrier if different may be also notified that the Person filing was requested to provide HRCM screening outcome.

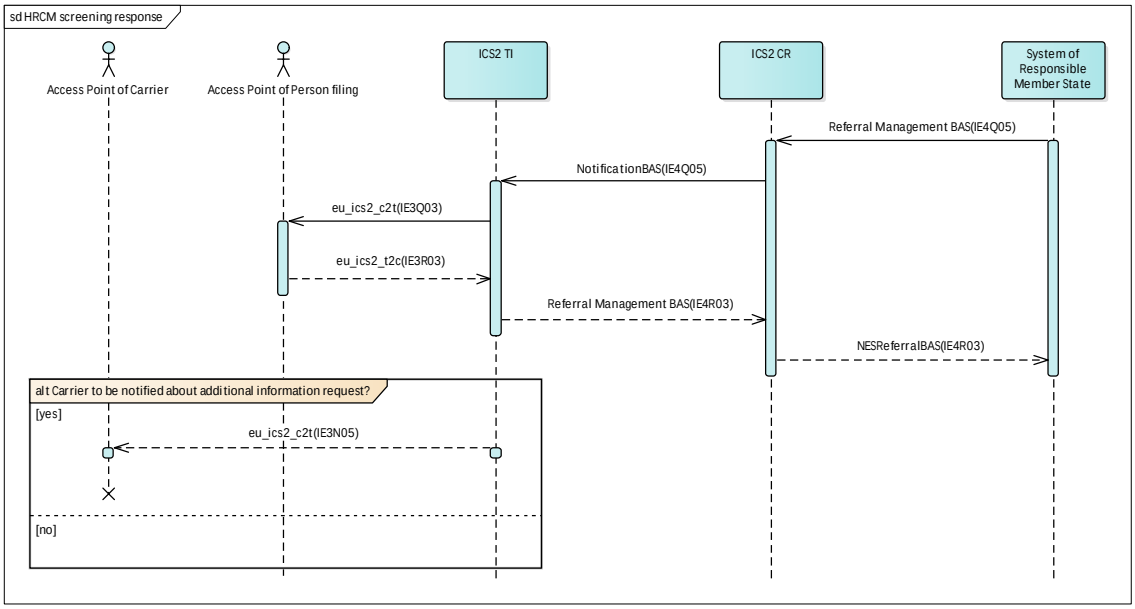

Figure 7: 'HRCM screening response' information exchange

3.1.8 Notifications received from ICS2 TI

The "Person filing", the "Person having not yet filed" and the "Carrier" may receive notifications from ICS2 TI, in the following cases:

- **(AEOS) Control Notification (IE3N09)** - The Authorised Economic Operator will be notified about the controls that will be performed on the goods that are under his responsibility. The ICS2 TI sends an (AEOS) Control Notification with ID IE3N09 to the

Person filing. This notification may be also communicated to the Carrier whenever applicable;

- **ENS Not Complete Notification (IE3N02)** - An ENS is marked as not complete after: either the timer for ENS completion has expired or completeness did not derive from the "Relate ENS filings" sub process. The ICS2 TI sends the ENS Not Complete Notification with ID IE3N02 to the Person filing. This notification may be also communicated to the Carrier whenever applicable;
- **Do Not Load Request (IE3Q01)** - The risk assessment of an ENS filing is complete. The Economic Operator will be requested to not load a part of his initially declared consignment. The ICS2 TI sends the Do Not Load Request with ID IE3Q01 to the Person filing. This notification must be also communicated to the Carrier when the Carrier is different from the Person filing. The specific parts that are not to be loaded will be indicated through the message;
- **Assessment Complete Notification (IE3N03)** - The risk assessment of an ENS filing is complete. The ICS2 TI sends the Assessment Complete Notification with ID IE3N03 to the Person filing when that person has requested to be informed. This notification may be also communicated to the Carrier when it has requested to be informed and is different from the person filing; and
- **ENS Pending Notification (IE3N11)** - The Person that has not yet filed is informed that he is obliged to file an ENS filing. The ICS2 TI sends the ENS Pending Notification with ID IE3N11 to the Person that has not yet filed.

The Person filing's system and the Carrier's system to be notified are identified as defined in the technical rule on routing in section 3.3.2.3.

The following sequence diagram describes how the above notifications reach the Person filing and if different the Carrier.

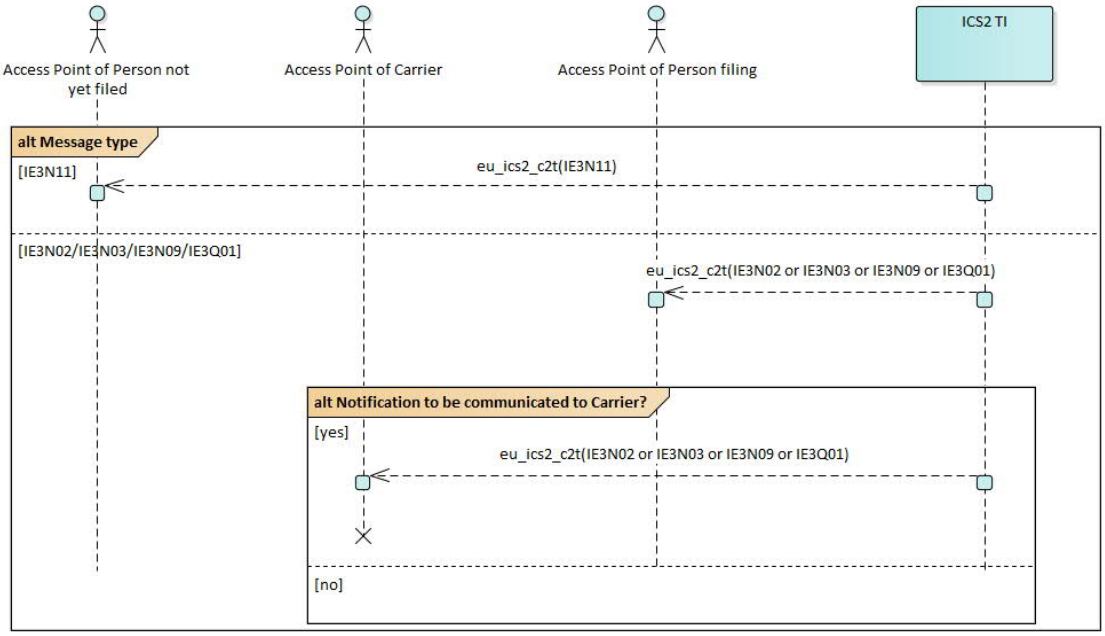

Figure 8: 'Notifications received from ICS2 TI' information exchange

3.1.9 Error handling

In the case of asynchronous interaction as described above, validation of a received message can result in errors being detected. In that case an error message is sent to the sender. This message is defined as IE3N99 for a general validation error, and as IE3N01 in case of a lifecycle validation error.

The technical definition of these error messages and the correlation mechanism to identify the original message are described in section 4.5 unterhalb.

3.1.10 Attachments

Some messages contain binary attachments of files, which must be treated in a particular way. The following messages contain possibly such files:

- ENS filings and amendments: IE3F32, IE3F28, IE3F26, IE3F24, IE3F23, IE3F20, IE3A32, IE3A28, IE3A26, IE3A24, IE3A23, IE3A20;
- Additional information response and High Risk Cargo & Mail screening response: IE3R02, IE3R03.

The files must be sent as attachments using the features of AS4 protocol as explained below in section 4.2.5 and referred to in the IE3xx message using an identification element.

3.2 SERVICE DEFINITIONS

The ICS2 TI application provides the necessary service to receive **Information Exchange messages** from Economic Operators. Operations of this service must be used by the Economic Operator (EO) IT system – either their own IT system or that of the IT Service Provider they use – to send information to the ICS2 TI application.

It is important to understand that the services of the ICS2 TI application are not exposed as web services but as services implemented in the business to the business protocol defined by the eDelivery AS4 specifications, as explained in detail in chapter 4 Technical Information Exchange Specifications.

The following service is provided:

Service
eu_ics2_t2c (trader to customs submission service) A single service is defined to identify the flow from traders to customs and is responsible for providing functionalities related to the reception of information from Economic Operators by ICS2 Trader Interface in the form of Information Exchange messages.

Table 5: List of services implemented by ICS2 TI application

The following service must be implemented by the Economic Operator (EO) system:

Service
eu_ics2_c2t (customs to trader notification service) A single service is defined to identify the flow from customs to traders and is responsible for providing functionalities related to the reception of information from ICS2 Trader Interface by an Economic Operator in the form of Information Exchange messages.

Table 6: List of services to be implemented by EO system

The above services provide a number of operations allowing a trader to interact with the ICS2 system and vice versa. The payload of these operations is the information exchange messages that are defined in the ICS2 Information Exchange Message Specifications document [R04].

In the table found in **Annex 1**, the reader can find the description of ICS2 TI services, the operations (or actions[6]) of those services and the user messages payload of those operations.

3.3 RULES AND CONDITIONS

The messages must conform to several rules and conditions, and to IT technical rules as described in 3.3.2.

3.3.1 Message validation

All messages will be validated syntactically and semantically. The format of the messages and the rules and conditions to which the messages must conform to are defined in the ICS2 Information Exchange Specifications [R04].

3.3.2 IT Technical rules

3.3.2.1 Single message payload

It is not allowed to send bulk messages containing multiple information exchange messages as defined above. One message will include a single message payload, sent by a single Person filing (e.g. in the case of filing messages each message can only contain one ENS Filing).

3.3.2.2 Single message interface[7]

All operations on an ENS filing must be sent over the same message channel (system-to-system or web user interface). This means it is not possible to send an ENS filing registration over the system-to-system interface and amend it over the web user interface.

3.3.2.3 Response and notification routing

The routing mechanism of replies and notifications to traders regarding a particular ENS submission (filing, amendment, invalidation or arrival notification) must identify the AS4 endpoint (Access Point of destination) and the channel (NTI, STI or UI) to be used.

The rules below will apply by order of priority:

- If the message is the initial reply to an ENS Filing or Arrival Notification, it will be addressed to the access point used by the person that submitted this ENS Filing or Arrival Notification following the channel of reception of the initial submission;
- If the message, having an MRN as subject, is addressed to the person that obtained the given MRN via a TI in a previous filing (ENS Filing or Arrival Notification), it will be addressed to the access point used by this person for that previous filing following the channel of the message attributing the MRN;
- If the message, having a given MRN in its content, is addressed to EOs other than the person filing (to which the given MRN is attributed) and:
    - If this economic operator has recorded a preference in the TI system (channel) used for the incoming messages, the notification is sent to the access point registered in the preference;
    - If the EO has not recorded a preference, he is considered as not connected to the system and hence the notification is not sent.

[6] Service operations are called ‘actions’ in the context of the AS4 protocol. We will use this terminology from here onwards.

[7] A request was raised by some participants of the STI Project Group to allow the multiple channel for an ENS Filing and amendment. This request is being assessed.

3.3.2.4 Selection of ICS2 Trader Interface

Each Member State has a single associated ICS2 Trader Interface. Either this is the ICS2 Shared Trader Interface (STI) or the National Trader Interface (NTI) of this Member State. For each filing delivered by a Sender access point used by the EO, the trader interface of the Member State that is addressed in the filing must be used.

This Sender access point must connect to the relevant Trader Interface system (National or Shared) according to the location of the Customs Office of First Entry (COFE) or (if unknown) to the Member State to which the ENS Filing will be addressed.

3.3.2.5 Support for multiple message versions

A Trader Interface (TI) must support two distinct versions of any specified message. This in order to guarantee the flexible evolution of the TI and the specified messages in particular (section 4.2.3.1 details the support at HTI level).

3.3.2.6 Priority messages

EO systems, DG TAXUD and Member States will size their infrastructure to meet the performance requirements of ICS2 operations. It might happen though that messages start to be buffered in exceptional circumstances such as:

- unexpectedly high peak of messages;
- unexpected downtime of a given service (either the EO system or the ICS2 TI).

In such circumstances, an internal mechanism to prioritise messages is implemented by ICS2 in order to handle specific messages with higher priority according to their message type. It is recommended that a similar operational mechanism may also be implemented by EO systems, at least by those impacted by larger volumes.

The messages in ICS2 have been categorised in three different categories taking into account the mode of transport, the state which a given business process has obtained and its urgency of information exchanges with regard to the potential process disruption and the consequent practical damage this may have for traders and administration. The categories are defined as follows:

- **Category A – high priority:** messages required to ensure the timely application of measures already decided by the customs authorities. Messages to trade to avoid business damage are also in this category;
- **Category B – normal priority:** messages required for a proper execution of the given business process regarding the process' time sequence and constraints;
- **Category C – low priority**: messages which are notifications for information and transparency reasons only.

Table 7 defines the category for all ICS2 messages. The messages IE3R03 (HRCM) and IE3N06 (Arrival notification) are high priority messages sent by the EO systems. In case of temporary system unavailability, it is recommended that those messages are sent prior to other messages.

Message ID	Category A	Category B	Category C
IE3Q01	X		
IE3Q03	X		
IE3R03	X		
IE3N03	X		
IE3N06	X		
IE3N08	X		
IE3Fxx		X	
IE3Axx		X	
IE3Q02		X	

Message ID	Category A	Category B	Category C
IE3R01		X	
IE3R02		X	
IE3R04		X	
IE3R08		X	
IE3N01		X	
IE3N99		X	
IE3Q04			X
IE3Q05			X
IE3R07			X
IE3N02			X
IE3N04			X
IE3N05			X
IE3N07			X
IE3N09			X
IE3N10			X

Table 7: Message prioritisation

4 TECHNICAL INFORMATION EXCHANGE SPECIFICATIONS

The ICS2 Trader Interface (TI) uses AS4 as a message exchange protocol as profiled in the eDelivery AS4 specifications (formerly known as e-SENS AS4). The following sections give an overview of the high-level messaging functionality of the eDelivery AS4 profile used by the ICS2 Trader Interface.

The first section introduces the protocol based on the eDelivery AS4 specifications. More information can be found in eDelivery AS4 specifications ([R01]), the OASIS ebXML Messaging Services specifications ([R07]) and AS4 Profile of ebMS 3.0 ([R07]). The second section details all elements of the user message, while the subsequent sections cover the signal message, routing and finally security aspects.

4.1 EDELIVERY AS4 OVERVIEW

4.1.1 Features

AS4 defines a standardized, secure and reliable exchange of messages, containing one (or multiple) payload(s). The following are the key features of the eDelivery AS4 profile used by the Trader Interface:

- **Interoperable**: AS4 is defined as an OASIS standard. It is built on top of existing standards, which have proven interoperability in the past: MIME, SOAP and WS-Security;
- **Secure**: AS4 uses a subset of the WS-Security features including digital certificate sealing in order to assure message non-repudiation and data confidentiality;
- **Reliable**: AS4 guarantees once-and-only-once delivery, via the exchange of acknowledgments and additional requirements on both send and receive side;
- **Payload agnostic**: AS4 can exchange any kind of payloads and supports multiple payloads being sent in one AS4 message. In the case of TI message exchanges will be limited to **one XML payload per message**.

The eDelivery AS4 Profile defines a mandatory Common Profile that selects, extends and profiles the AS4 ebHandler Conformance Profile and AS4 Additional Features and provides a common Usage Profile. The ICS2 Trader Interface further constrains these by following the eDelivery profile as described in the sections below. This profile can be implemented using open source or closed source AS4 software implementations that conform to eDelivery specifications [R08].

On top of the AS4 ebHandler Conformance Profile, the eDelivery AS4 profile used as a baseline by ICS2 updates or adds some functionality:

- Algorithms specified for securing messages at the Message Layer are updated to current guidelines and use of electronic signature for sealing is mandatory;
- There is an added requirement to support Two Way Message Exchange Patterns (MEPs);
- Transport Layer Security, if handled in the AS4 handler, is profiled and is mandatory;
- The WS-Security version is the 1.1.1;
- Support for IPv4 and IPv6 is explicitly required.

It also adapts some requirements:

- The **Pull** mode is profiled in the eDelivery AS4 profile and ICS2 will support it;

- The single XML payload is exchanged in a separate MIME part, never in the SOAP body;
- Technical receipts and errors are reported synchronously only;
- Electronic sealing is using the WS-Security specification using the X.509 Token Profile, which allows certificates to be used to seal the payload to ensure the data origin and integrity. Throughout the remainder of the document the term sealing will be used as representing the AS4 signature mechanism defined in the AS4 documentation;
- Message encryption is currently mandatory in the eDelivery AS4 profile. ICS2 will deviate from the eDelivery AS4 profile on this aspect and not apply AS4 encryption as it relies already on encryption at the transport level (TLS/SSL)[8].

In the context of the Trader Interface of the ICS2 system, the **eDelivery AS4 profile** is further specified through the definition of Processing Mode (P-Mode) configuration values with the aim of clarifying and removing any ambiguity. Refer to **Annex 2**.

4.1.2 Messaging Model

The following key concepts and terminology from the ebMS 3 core specification ([R07]) are used to model message exchanges as shown in the figure below. The message flow is reversed when the exchange is initiated by Customs.

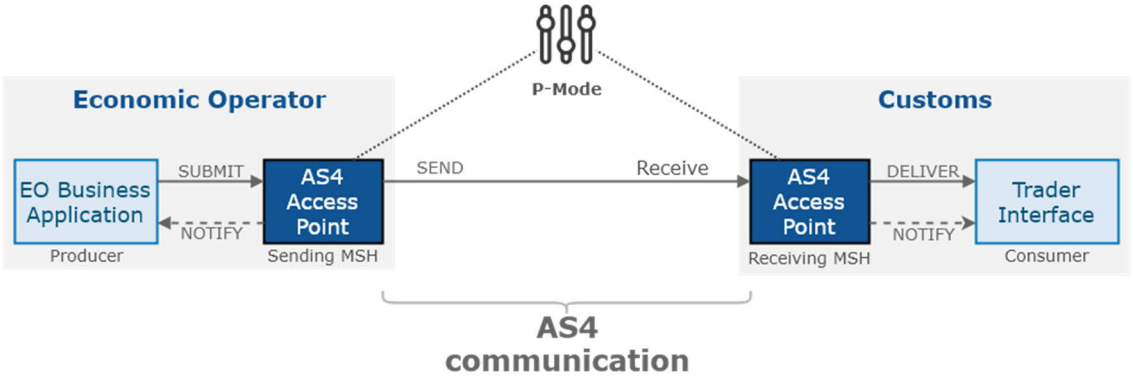

Figure 9: Message model

- A **Messaging Service Handler (MSH)** is an entity that is able to generate or process messages that conform to the ebMS specification, and to act as a sender or receiver role. This can be any eDelivery conformant AS4 access point [R08] on the Economic Operator's side;
- A **Producer** is an entity (e.g. business application) that constructs the functional payload and interacts with a Sending MSH (i.e. an MSH in the Sending role) to initiate the sending of a user message;
- A **Consumer** is an entity that interacts with a Receiving MSH (i.e. an MSH in the Receiving role) to consume the functional payload from a received user message.

The interaction between these components is defined in abstract operations, such as Submit, Send, Receive, Deliver and Notify. The communication between a Producer/Consumer and an MSH can be done in an implementation specific way, which is out of scope for the AS4 usage profile.

A **Message** is a logical unit which consists of User Messages or Signal Messages.

[8] In the context of the STI Project Group it was concluded that double encryption was an unnecessary and redundant measure adding a burden to the performance of the system and that it would be enough to rely on encryption at Transport level only. An additional operational complexity would also arise due to the fact that it requires the management of the certificates used for encryption at the receiving access point.

- The **User Message** contains the actual business payload that is exchanged amongst the business applications of two parties (an eb:Messaging/eb:UserMessageXML structure). From a business application perspective, only these categories of messages must be specified;
- **Signal Messages** (an eb:Messaging/eb:SignalMessage XML structure) have a supporting role in establishing message exchange patterns, non-repudiation and reliability. They are restricted to the sending and receiving MSH. There are 3 types of Signal Messages:
    - The **Receipt** is a positive acknowledgment. It indicates that the receiving MSH could parse the incoming message without an exception. This ensures the Received operation was successful;
    - The **Error** is a negative acknowledgment. It indicates that the receiving MSH encountered an issue during the parsing of the incoming message;
    - The **Pull Request** is in support of the pull message exchange pattern described below. While part of the AS4 specifications, the current version of the eDelivery AS4 profile does not use the Pull pattern.

4.1.3 Message Exchange Pattern

4.1.3.1 General Definition

An ebMS Message Exchange Pattern (**MEP)** defines a typical choreography of ebMS **User Messages** which are all related using the referencing feature (RefToMessageId). Each message of an MEP instance refers to a previous message of the same instance, unless it is the first one to occur. Messages are associated with a label (e.g. "request", "reply") that precisely identifies their direction between the parties involved and their role in the choreography.

The ICS2 system will only use **One-Way MEP**s which govern the exchange of a single User Message Unit unrelated to other User Messages. Its label is "oneway" and is identified by the URI http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay.

It should be noted that MEP definitions are primarily concerned with the transfer of **ebMS User Message** Units. Instances of such MEPs may involve or cause the transfer of additional messages (e.g. ebMS signal messages or units such as errors, receipts) but these are not taken into account in the MEP definition.

A message exchange pattern binds with the underlying transport channel to transfer messages, and this dictates how each message transfer is initiated over the underlying protocol. The current eDelivery AS4 profile only uses push binding (where the sender initiates the exchange). It is anticipated that a subsequent version of the profile will add support for the pull.

4.1.3.2 One-Way/Push MEP

This transport-channel-bound MEP involves the transfer of a single ebMS User Message unit (label: "oneway"). When performed over a Two-way underlying transport protocol (HTTP request/response), the response message MAY carry an ebMS Signal Message, such as an error message. However, the response message MUST NOT carry an ebMS User Message that refers to the request message.

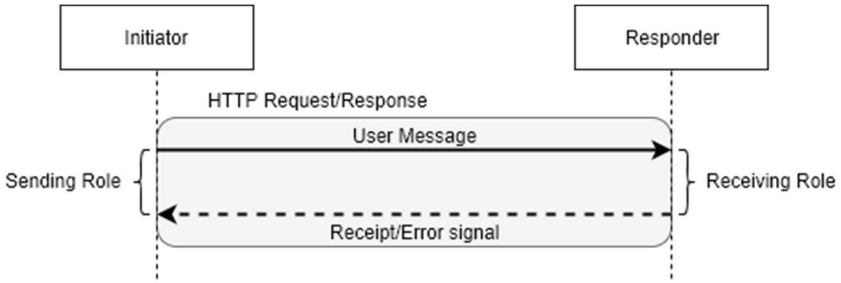

Figure 10: One-way/Push MEP

The only binding supported by the eDelivery AS4 profile is **Push,** which maps an MEP User message to the 1st leg of an underlying 2-way transport protocol or of a 1-way protocol. This binding is identified by the URI:

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push**.**

4.1.3.3 One-way/Pull MEP

This transport-channel-bound MEP involves the transfer of a single ebMS User Message unit (label: "oneway"). This MEP is initiated by the Receiving MSH, over a two-way underlying transport protocol. The first leg of the protocol exchange carries a Pull Signal message. The second leg returns the pulled User Message unit. The pulled User Message unit does not include an eb:RefToMessageId element. This MEP is identified by the URI:

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/pull.

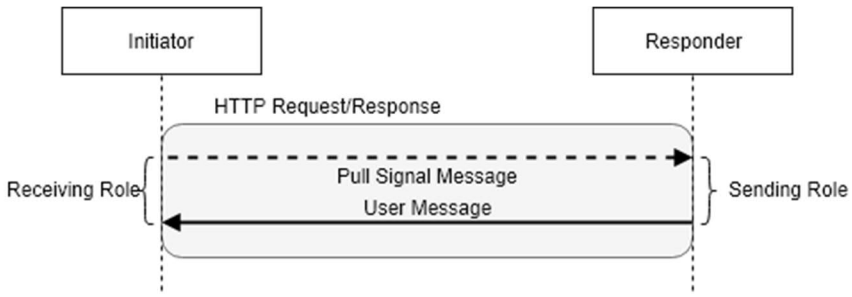

Figure 11: One-way/Pull MEP

Message Partition Channels (MPC) allow for partitioning the flow of messages from the sender MHS (DG TAXUD) to the receiving MSH (the trader system). The sending DG TAXUD MSH MUST be able to determine whether a submitted message should be pulled or pushed, and to which Message Partition Channel (MPC) it must be assigned. Similarly, the Receiving Trader MSH is aware of which MPC(s) should be pulled from, and which ones will be used for push. This knowledge is based on an agreement shared between parties prior to the exchanges, and modelled in this specification as the P-Mode operation set (see Annex 2 P-Modes Summary).

The processing model for a pulled message is as follows, for a typical and successful instance of One-Way/Pull MEP:

- The TI submits message data to the DG TAXUD MSH, intended for the trader system. The message is associated with an MPC. If no MPC name is provided by the submitter, or if the MSH implementation has not been provided with a way to determine this association by itself, the default MPC is used. The MEP associated with this message is a One-Way/Pull;
- On the trader system MSH side: Sending of a PullRequest signal by the MSH. The PullRequest signal specifies the MPC from which to pull messages;
- On the DG TAXUD responding MSH side: Reception of the PullRequest signal. For every PullRequest signal received it selects a previously submitted message according to a FIFO policy with respect to the Submit operation. If there is no user message available in the specified MPC for sending, a warning signal with short description: "EmptyMessagePartitionChannel" (see Annex 4 ebMS Errors) will be sent back instead. The selected message is sent over the SOAP Response to the PullRequest;
- On the trader system MSH side: the pulled message is available for processing by the MSH. The header @mpc attribute indicates from which MPC it has been pulled and is the same as the value of @mpc in the corresponding PullRequest signal.

4.1.3.4 ICS2 Scenarios

The Trader Interface allows using both types of MEPs. The **One-Way/Push** Message Exchange Pattern is used when the responding MSH is a permanently connected AS4 access point. The **One-Way/Pull** Message Exchange Pattern is used to allow intermittently connected Trader

Access Points to have full control to initiate asynchronous transfers with the Trader Interface in both directions, engaging in a client-server type of interaction.

A Trader Sender Party has to declare its choice as a configuration asset to the TI with regards to the mode of operation for the eu_ics2_ct2 service. It is configured One Way/Push or One-Way/Pull.

4.1.4 Processing Mode

A **Processing Mode** (**P-Mode**) is the contextual information that governs the processing of a particular message (this is basically a set of configuration parameters). The P-Mode associated with a message determines, among other things, which security and/or which reliability protocol and parameters, as well as which MEP is being used when sending a message. The technical representation of the P-Mode configuration is implementation-dependent.

The MSH implementing the Harmonised Trader Interface will be REQUIRED to use the P-Mode parameters defined in the current document (see **Annex 2**). Many of these are set as part of the eDelivery AS4 profile and the remaining ones are specific to the Trader Interface exchanges.

4.1.5 Message Packaging

AS4 uses **SOAP with Attachments** as a message format. This is a MIME payload (multi-part), which contains a SOAP envelope as the first MIME part. This SOAP envelope holds the User Message, Receipt or Error. In the case of ICS2 User Messages, the single business payload is in a SOAP Attachment (read MIME part), The SOAP body is always empty. Gzip compression of the payloads in the SOAP Attachments will be used as supported by AS4.

A User Message consists of:

- **MessageInfo** contains the unique MessageId and the timestamp of the message;
- **PartyInfo** identifies the sender and receiver of the message;
- **CollaborationInfo** describes the business context through a service and action parameter;
- **MessageProperties** offer an extension point to add additional business information;
- **PayloadInfo** makes a reference to the payloads in the Attachments.

A Signal Message consists of:

- **MessageInfo** contains the unique MessageId, the MessageId of the referenced User Message and the timestamp of the message.

For a more detailed description of the message packaging and content for User Message and Signal Message refer to sections 4.2 and 4.3 respectively.

4.2 USER MESSAGE

The AS4 message structure provides a standard message header that addresses B2B requirements and offers a flexible packaging mechanism based on SOAP and MIME enveloping. The more specific eDelivery AS4 structure is illustrated below. Dashed lines style is used for optional message components.

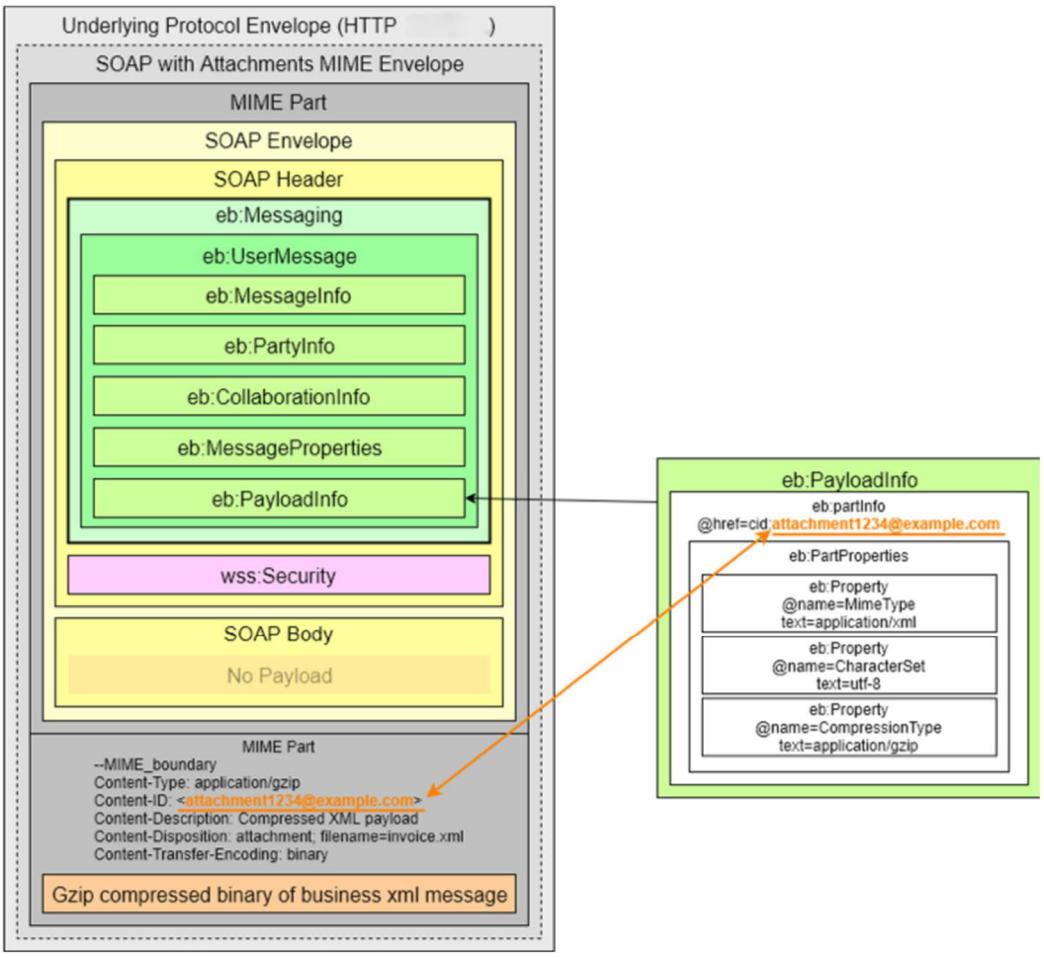

Figure 12: Detailed eb:UserMessage structure

This section identifies the different data elements present in the AS4 message header for which the business application will have to provide specific values for each individual message exchange.

In addition to these elements the AS4 message header contains other technical elements which are not to be provided by the business application but are derived from the P-Mode configuration or indirectly derived from other data elements specified (e.g. certificate of a party).

4.2.1 Eb:Messaging/eb:UserMessage/eb:MessageInfo

The eb:MessageInfo element has the following children:

- **eb:Timestamp (REQUIRED)** – A value representing the date at which the message header was created, and is conforming to a dateTime (see [R09]). It MUST be expressed as UTC. Indicating UTC in the Timestamp element by including the 'Z' identifier is optional;
- **eb:MessageId (REQUIRED)** – A value representing – for each message - a globally unique identifier conforming to the message identifier (msg-id) specification defined in section 3.6.4 of RFC 2822 [R10]. To ensure the global uniqueness of message identifiers, the value of eb:MessageId must be structured using a UUID on the left side and the fully qualified domain name of the sender's access point on the right side. The sender must ensure the UUID is unique across its access point domain;
- **eb:RefToMessageId (optional)** – when present, it must contain the eb:MessageId value of the message to which this message relates. The ICS2 message exchanges will make use of this field when a functional reply message can be traced back to a specific original AS4 message that triggered the reply. This feature is especially useful in the context of error handling, as described in section 4.5.

4.2.2 eb:Messaging/eb:UserMessage/eb:PartyInfo

The **eb:PartyInfo** provides the identification of the **Sender** and **the Receiver** of the message in two mandatory child elements **eb:From** and **eb:To**. For each of the parties (From and To) two mandatory child elements have to be provided. The first one is the **eb:PartyId** and allows for the actual identification of the party. The second one is the **eb:Role** element and defines the role the party has in the message exchange.

Note that the Sender and Receiver identified in the **eb:PartyInfo** refers to the party sending and receiving the AS4 message. These could be different from the actual Person filing when an intermediate **IT service provider** is involved in the message exchange with Customs. This aspect is further described in section 4.4.2.

4.2.2.1 eb:PartyId

The content of this element is a string value that provides an identification for the given party. The namespace for content values of this element is specified by the **eb:PartyId@type** attribute.

The ICS2 TI uses two complementary namespaces. One that allows the identification of an economic operator and a second one allows the identification of a Customs STI/NTI. The defined namespaces follow the convention for naming identifiers domains as defined in the e-SENS ebCore Party Id 1.3 specification ([R11]), and use 'unregistered' namespace domains.

This implies that the domain namespaces will have a structure as follows:

urn:oasis:names:tc:ebcore:partyid-type:unregistered:<**catalog-name**>:<**schema-name**>

where catalog-name will be '**eu-customs**' and schema-name will be one of the two values '**authority**' or '**EORI**'.

In the authority namespace **urn:oasis:names:tc:ebcore:partyid-type:unregistered:eu-customs:authority** each STI/NTI will be assigned an identifier providing it a PartyId. The partyId of the ICS2 STI is **sti-taxud**, the partyId of the NTI will be nti-<iso 3166-1 Alpha2 code>.

In the EORI namespace a structure is used where a given party (mandatory having an EORI[9] number) can have multiple partyId's defined. This allows for the party to have/use multiple AS4 message handlers (MSH) depending on the business domain or geographical region.

The structure of the partyId is <system_identifier>@<EORI>@<MS> where the first and third part are optionally to be used. So possible alternations are: <EORI>, <system_identifier>@<EORI>, <EORI>@<MS>, <system_identifier>@<EORI>@<MS>. The system identifier part is an alphanumerical string with a maximum length of 12 characters and is free to choose by the given party as long as uniqueness is ensured within the given party. The optional member State is an iso 3166-1 Alpha2 code indicating the Member State where the Certificate used in the message is registered in UUM&DS (in case this Member State is not the same as the one in which the EORI is registered).

Example values in the **urn:oasis:names:tc:ebcore:partyid-type:unregistered:eu-customs:EORI** schema are:

- BE1234567890
- system1@NL0987654321
- system2@NL0987654321
- system3@NL0987654321@FR

It should be noted that the initiator of message exchange (i.e. the Sender) must have a mapping at its disposal between the Receiver (To) PartyId and the physical address of the message handler

[9] The EORI to be used is that of the System Owner responsible of implementing and operating the Access Point.

to be addressed to reach this party to be able to initiate the exchange. Refer to section 4.4 on routing for details.

4.2.2.2 eb:Role

The Trader Interface defines two generic roles '**Trader**' and '**Customs**'.

4.2.3 eb:Messaging/eb:UserMessage/eb:CollaborationInfo

The eb:CollaborationInfo element contains the following child data elements:

- **eb:AgreementRef** (REQUIRED) – is a string that identifies the entity or artefact governing the exchange of messages between the parties;
- **eb:Service** (REQUIRED) – is a string identifying the service that acts on the message;
- **eb:Action** (REQUIRED) – is a string identifying an operation or an activity within a service that may support several of these;
- **eb:ConversationId** (REQUIRED) – is a string that allows for an identification of multiple messages exchanged in a conversation between Parties.

In the next subsection we describe the values of these elements for ICS2.

4.2.3.1 eb:AgreementRef

The eb:AgreementRef element is mandatory in ICS2 TI exchanges and serves the additional purpose of identifying a version of the Trader Interface common specifications. The first version is **EU-ICS2-TI-V1.0**.

As per ebMS 3 specification ([R07]), the eb: AgreementRef element will be qualified by a @type attribute with a value of **"" (empty string)**, to allow such values in the content of the data element.

As a result of ICS2 change management updates to the specifications can occur that have an impact on the HTI specifications. Whenever required, an updated value for the eb:AgreementRef element will be associated to this new version of the specifications. For a pre-defined transitional period, defined on a case by case basis at the moment of change, a TI shall potentially be required to support two concurrent versions.

4.2.3.2 eb:Service

As described in section 3.1.9, the following services are used for ICS2 information exchanges and allow identifying the direction of the information flow:

- **eu_ics2_t2c** – identifies the flow from trader to customs (i.e. from trader to TI);
- **eu_ics2_c2t** – identifies the flow from customs to trader ((i.e. from TI to trader).

As per ebMS 3 specification, the eb:Service element will be qualified by a @type attribute with a value of **eu-customs-service-type**, to allow such values in the content of the data element.

4.2.3.3 eb:Action

The ICS2 TI will use as action name the Message ID of the information exchange as defined in the common functional specification. **Annex 1** contains an inventory of supported messages[10].

[10] When the value of this element is http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test, then the eb:Service element MUST have the value http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service. Such a value for the eb:Action element only indicates that the user message is sent for testing purposes and does not require any specific handling by the MSH.

4.2.3.4 eb:ConversationId

The Trader Interface exchanges do not make use of the eb:ConversationId in the context of ICS2 but according to standards , if none is provided, an MSH is expected to set the value “1”. For the trader interface, any value present in an incoming message will be ignored.

4.2.4 eb:Messaging/eb:UserMessage/eb:MessageProperties

This element has zero or more eb:Property child elements.

An eb:Property element is of xs:anySimpleType (e.g. string, URI) and has a required @name attribute and an optional @type. This allows expressing business context specific properties in the AS4 header allowing more efficient monitoring, correlating, dispatching and validating functions without requiring payload access.

The eDelivery AS4 profile used by ICS2 does not require the usage of message properties and this element will not appear in eb:UserMessage.

4.2.5 eb:Messaging/eb:UserMessage/eb:PayloadInfo

The eb:PayloadInfo element illustrated below identifies payload data associated with the message. Its purpose is:

- to make it easier to extract payload parts associated with this ebMS Message;
- to allow an application to determine whether it can process these payload parts, without having to parse them.

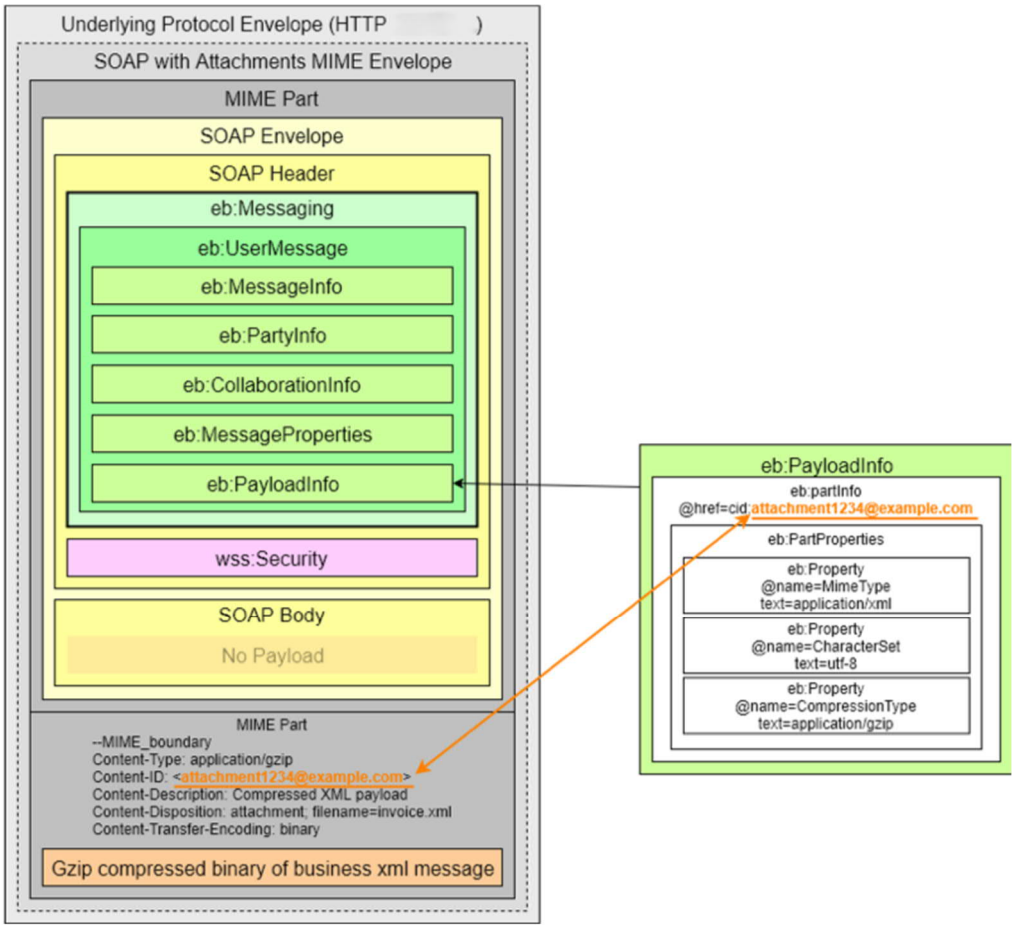

Figure 13: Payload info

In ICS2 messages the eb:PayloadInfo element will contain a single **eb:PartInfo** referencing the single business payload included as a MIME attachment, and optionally a number of **eb:PartInfo**

referencing the binary attachments (if there are binary attachments allowed in the business payload, please see section 3.1.10)

This **eb:PartInfo** has an @href attribute whose value is the [RFC2392] Content-ID URI of the payload object referenced. It also has one eb:PartProperties child element that contains zero or more **eb:Property** elements.

As per eDelivery AS4 specification the following applies to eb:PayloadInfo:

- Compliant eDelivery AS4 message always has an empty SOAP Body meaning that message payload must be exchanged in a separate payload Mime Part. This implies that the eb:PayloadInfo is mandatory;
- The ebMS3 mechanism of supporting "external" payloads via hyperlink references (as mentioned in section 5.2.2.12 of the ebMS3 Core Specification [R07]) must not be used;
- Payload parts must be compressed using gzip. Refer to [R07] for the handling of already compressed payloads.

Packaging requirements in the context of ICS2 for the single business payload eb:PayloadInfo:

- An eb:PartInfo/eb:PartProperties/eb:Property/@name="MimeType" value is required to identify the MIME type of the payload before compression was applied. Only “application/xml” is allowed;
- An eb:PartInfo/eb:PartProperties/eb:Property/@name="CharacterSet" value is recommended to identify the character set of the payload before compression was applied. Only “utf-8” is allowed. Even if the value is not set, the character set of the payload before compression must be UTF-8;
- An eb:PartInfo/eb:PartProperties/eb:Property/@name="CompressionType" with the value “application/gzip” is required;
- It must be possible for the producer to set the value of the @href attribute and this value must be passed on to the final consumer. It might be that in the context of ICS2 this can be generated by the sending MSH as it does not have a business meaning.

Packaging requirements in the context of ICS2 for the optional attachment eb:PayloadInfo elements:

- An eb:PartInfo/eb:PartProperties/eb:Property/@name="MimeType" value is required to identify the MIME type of the payload before compression was applied. It cannot be of MIME type application/xml. The allowed MIME types for attachments are application/pdf, image/jpeg;
- An eb:PartInfo/eb:PartProperties/eb:Property/@name="CompressionType" with the value “application/gzip” is required;
- It must be possible for the producer to set the value of the @href attribute and this value must be passed on to the final consumer. It might be that in the context of ICS2 this can be generated by the sending MSH as it does not have a business meaning.

4.2.6 Message Payload

The eDelivery AS4 communication used by the ICS2 Trader Interface is used to support the ENS filing related processes. The actual payload of each user message is one of the messages listed in the table in **Annex 1** and specifications can be found in the Technical Service Specifications [R06].

The specifics of how a message producer (i.e. trader’s business application) submits a business payload to the sending MSH depends on the interface(s) provided by the eDelivery AS4 conformant solution used and are out of the scope of this document.

However, the following requirements apply to ICS2 business message payloads:

- Each user message has one and only one business message payload, and optionally a number of binary attachment payloads;
- Each user message originates from a single Person filing;
- The business message is sent as payload MIME part and not in the soap body;
- The business message must be a schema valid xml message as per Technical Service Specifications [R06] and matching the AS4 service/action as per **Annex 1** and section 4.2.3;
- The business message maximal size recommended is 100MB uncompressed.

The following requirements apply to ICS2 attachment payloads:

- Due to limitations in other parts of the ICS2 system, the message maximal size recommended in the system is 20MB compressed, this is the sum of the compressed base64 encoded binary attachments and the compressed business message payload. To this end, large images and PDF documents will be resized in the TI or NES before dispatching to the Common Repository.

4.3 SIGNAL MESSAGE

The **ebMS Signal Message Unit** is represented by the XML infoset eb:Messaging/eb:SignalMessage. Its role is to activate a specific function in the Receiving MSH. **It is not intended to be delivered to a message Consumer**.

It has two child elements:

- eb:Messaging/eb:SignalMessage/eb:MessageInfo
  This REQUIRED element is similar to eb:MessageInfo as defined for user messages (see section 4.2.1);
- eb:Messaging/eb:SignalMessage/eb:[SignalName]
  This REQUIRED element defines the nature of the ebMS signal. There is only one eb:[SignalName] child element when [SignalName]=Receipt. There may be several children elements when [SignalName]=Error.

An ebMS signal does not require any SOAP Body: if the SOAP Body is not empty, it MUST be ignored by the MSH, as far as the interpretation of the signal is concerned.

A signal message has the following structure.

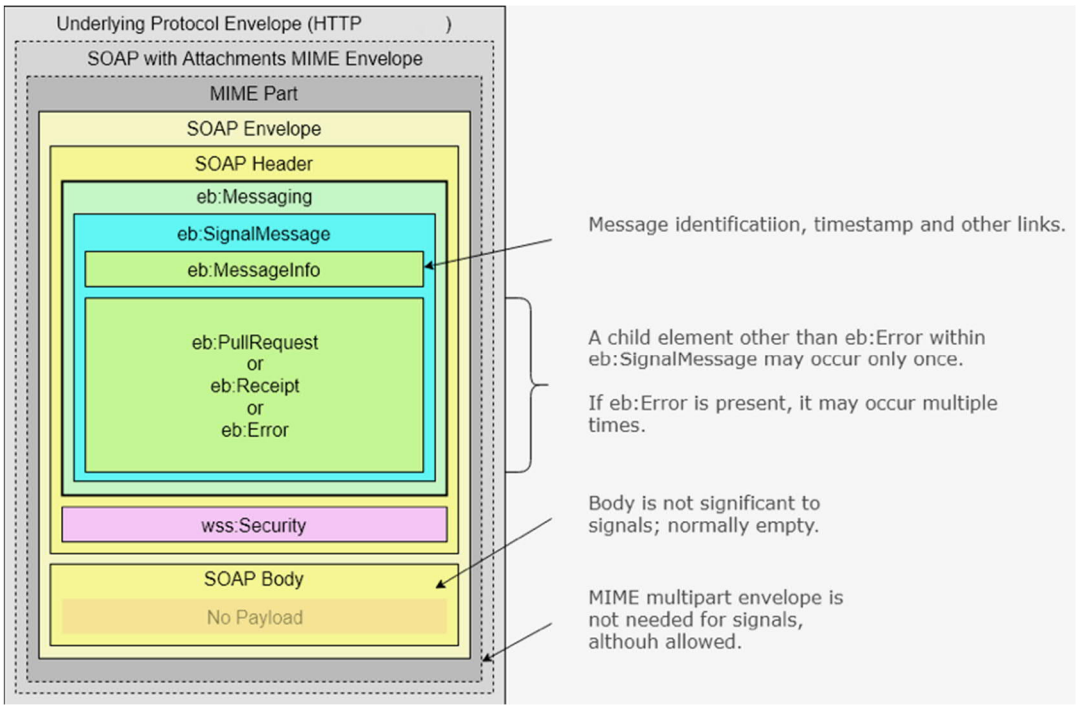

Figure 14: Signal message

4.3.1 eb:Messaging/eb:SignalMessage/eb:Receipt

A receipt signal message is the acknowledgment that the receiving MSH successfully processed the AS4 message, i.e. it was able to apply the expected P-Mode and is able to deliver the message to the consumer. The value of eb:MessageInfo/eb:RefToMessageId MUST refer to the message for which this signal is a receipt.

4.3.2 eb:Messaging/eb:SignalMessage/eb:Error

Error generation and error reporting are orthogonal concepts in ebMS V3. While the generation of errors is a matter of conformance, the reporting of errors may be subject to an agreement. Consequently, the way errors are to be reported is specified in the P-Mode (P-Mode.ErrorHandling feature) that results from such an agreement. The eDelivery profile specifies that errors must be reported and transmitted synchronously (using the HTTP Response) to the Sender and should be reported (Notify operation in the messaging model) to the Consumer and Producer.

An ebMS Error is represented by an eb:Error XML infoset, regardless of the way it is reported. The ICS2 TI makes use of the following properties:

- **origin** (optional attribute);
- **category** (optional attribute);
- **errorCode** (required attribute);
- **severity** (required attribute);
- **refToMessageInError** (required if error(s) related to a particular ebMS message);
- **shortDescription** (optional attribute);
- **Description** (optional element);
- **ErrorDetail** (optional element).

In **Annex 4** a list of ebMS error codes is defined.

It is important to note that only technical errors related to the communication over AS4 are sent in this way. Business validation failures are sent back to the sender using the already mentioned information exchange message IE3N01 and IE3N99 using a user message, in the context of One-Way/Push or Two-Way/Push-and-Push Message Exchange Pattern.

4.3.3 eb:Messaging/eb:SignalMessage/eb:PullRequest

When the trader system is using the One-Way/Pull MEP, the messages will be delivered after sending of a PullRequest signal by its MSH, as explained in section 4.1.3.3 One-way/Pull MEP. The PullRequest signal specifies the MPC from which to pull messages. For this purpose, the eb:PullRequest element has a single attribute specified @mpc and this attribute has to have a specific value:

> @mpc=urn:fdc:ec.europa.eu:2019:eu_ics2_c2t/EORI/<PartyId> where partyId is defined as in section 4.2.2.1.

4.4 MESSAGE ROUTING

The eDelivery AS4 specification covers message exchanges with the abstract concepts of sending and receiving MSH where each actor in the exchange can take the receiving and sending roles alternatively.

To be able to address the correct MSH when sending an ICS2 message to an EO, the Trader Interface needs a way to match functional information to the P-Mode configuration and URI of the corresponding access point.

4.4.1 Destination resolution

The eDelivery access point of an EO needs to be configured to address predetermined and established Trader Interface access points (Shared TI, National TI) while a Trader Interface acts as a central node and must be able to send messages to many parties. To be able to participate in ICS2 exchanges an Economic Operator's Access point must enroll and pass conformance testing as described in section 5.1. This allows AS4 P-Mode parameters, such as sealing (AS4 signature) certificates and endpoint URIs of this access point to be configured on the TI side.

Section 3.3.2.3 details the rules that determine the endpoint and channel used for functional replies.

For ENS Filings or Arrival Notifications received by a TI the functional reply will be sent to the AS4 access point from which the initial filing was sent. Other functional messages, referring to a previously assigned MRN, will be sent to the access point of the person filing who sent the message that this MRN was assigned to.

This means the Trader Interface must keep track of the eb:From/eb:PartyId in the AS4 header information in relation to the unique functional identifier of the message (LRN or MRN) in the functional message payload (see FunctionalReferenceID in section **3.1.9**). This allows it to match a functional reply to the eb:To/eb:PartyId of the destination when it takes the sending role.

In some notification scenarios, the Trader Interface needs to notify an EO other than the Person filing in which case the access point and PartyId to be used are different ones. In this case the TI access point will use the preferences provided by the target EO at enrolment time (see section 5.1) to determine the default eb:To/eb:PartyId and AS4 access point for the outgoing message.

4.4.2 IT Service Provider

There may be cases where a Person filing is using an **IT service provider** that constructs the technical compliant message and subsequently delivers this message to a Customs authority by addressing the appropriate STI/NTI.

Exactly as in the case of an EO, to be able to send ICS2 messages, an IT Service Provider must enroll the Access Point with customs authorities and provide the configuration of the access point in the same way as described above (and in chapter 5.1) for an Economic Operator. The Trader Interface AS4 access point will then perform the same security validation checks as for any other registered system.

4.5 ERROR HANDLING

Technical errors that occur during the AS4 protocol (connection problems, incorrect AS4 headers, etc.) are handled using the appropriate AS4 mechanism and the error signal message. The mechanism of signal messages is explained in section 4.3 oben and the types of errors are listed in Annex 4 unterhalb.

Nevertheless, as the ICS2 interactions with traders are asynchronous, validation of an incoming message can result in functional errors being detected after the reception. In that case a functional error message is asynchronously sent to the sender. This message is defined as IE3N99 for a general validation error, and as IE3N01 in case of a lifecycle validation error.

The message structure of the IE3N99 is defined as pictured below. The IE3N01 has a similar structure.

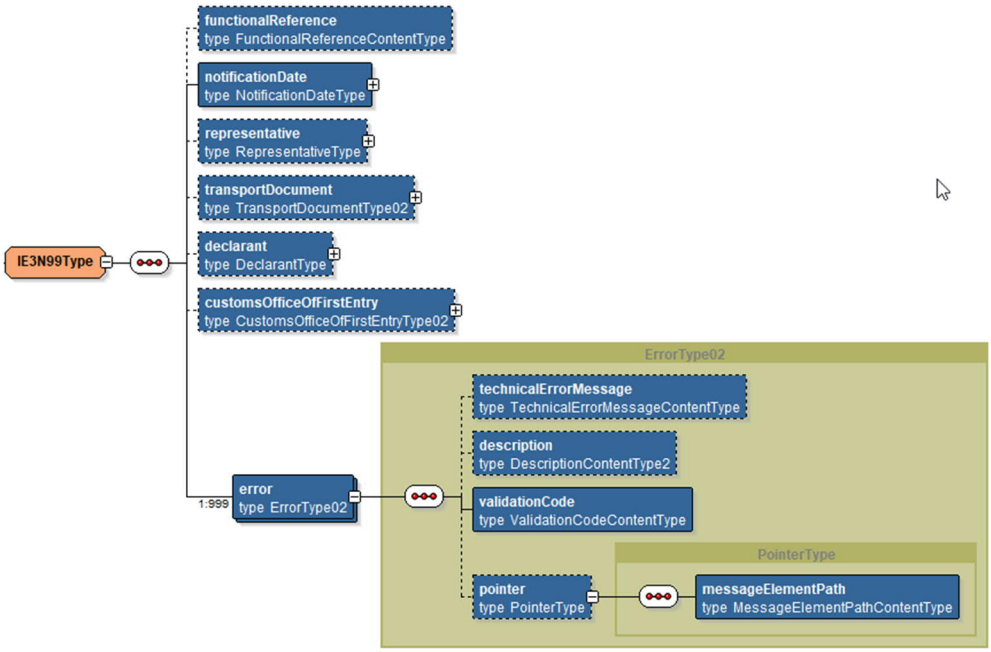

Figure 15: IE3N99 message structure

The following list explains this message:

- **FunctionalReferenceID** is used to correlate the error message to the original message on a business (or functional) level. As the error messages are asynchronous, it is important that the EO system can correlate the error to the original message. The functional reference of the original message will be used here, as follows:

Message type	Message description	Reference element
IE3Fxx	ENS Filing	LRN
IE3Axx	ENS Filing Amendment	MRN
IE3Q04	Invalidation Request	MRN
IE3Q05	ENS Consultation	MRN

IE3N06	Arrival Notification	LRN
IE3R02	Additional Information Response	MRN
IE3R03	High Risk Cargo & Mail screening response	MRN

Table 8: Functional reference

Nevertheless the AS4 message header element will also contain a technical correlation id referring to the AS4 messageId of the original message. This is useful in the case the original message was unparsable or the functional reference id is not unique (for example in case of consultations);

- **NotificationDate:** is the timestamp of the validation of the message;
- **Representative**: the legal representative as indicated in the original message will be used if available;
- **TransportDocument**: the document number of the original message will be used if available;
- **Declarant**: the declarant as identified in the original message will be used if available;
- **CustomsOfficeOfFirstEntry**: the location as identified the original message will be used if available;
- **Error:** The cardinality of the errors is 1 up to 999. If the message is syntactically correct, the error message will list all possible semantical errors found in a message, and not stop at the first error;
    - **The technical error message** gives more info about the error if relevant. In the case of syntactical errors, the more detailed parser exception (such as "missing element Identification Number") will be found in the description. This description is not translated, only English will be used;
    - **The description** gives a human readable description of the error in English only;
    - **The ValidationCode** is defined by a code list defined in ICS2 Information Exchange Message Specifications [R04] containing the code and the description;
    - **The pointer** of the error contains the location of the error defined by an XPath location in the XML document.

The above message will be sent over AS4 following that protocol. To allow the sender to correlate the error message to the original message, the AS4 correlation mechanism is used. That means that the eb:RefToMessageId is used and will always contain in this case the AS4 message id of the original message.

4.6 SECURITY

The security requirements of the ICS2 Trader Interface include confidentiality, integrity, authentication and authorisation. These are catered for at different levels of the communication layers (network, transport or message layer) as described in Table 9.

Confidentiality is ensured by applying transport level encryption. Message level encryption is considered redundant[11], deviating from the eDelivery specifications on this.

[11] In the context of the STI Project Group it was concluded that double encryption was an unnecessary and redundant measure adding a burden to the performance of the system and that it would be enough to rely on encryption at Transport level only.

To ensure integrity and authentication, the TI makes use of the mechanisms and standards specified in the eDelivery AS4 profile applicable to the message layer. These rely on the use of electronic certificates to seal the messages and from which it can be guaranteed that the message was not modified during its transport and provides proof of the identity of the person delivering the message.

The above security measures cover the so called non-repudiation capability which is a major benefit of the use of AS4 protocol. This means that both sender and receiver have the full guarantee and proof of message being delivered by an identified party with integrity and in full confidentiality.

To ensure only registered and authorised parties can deliver and receive messages to and from the TIs, the TI uses a registration and authorisation mechanism based on UUM&DS. This happens at the functional level. These are represented in figure 16 and further described below.

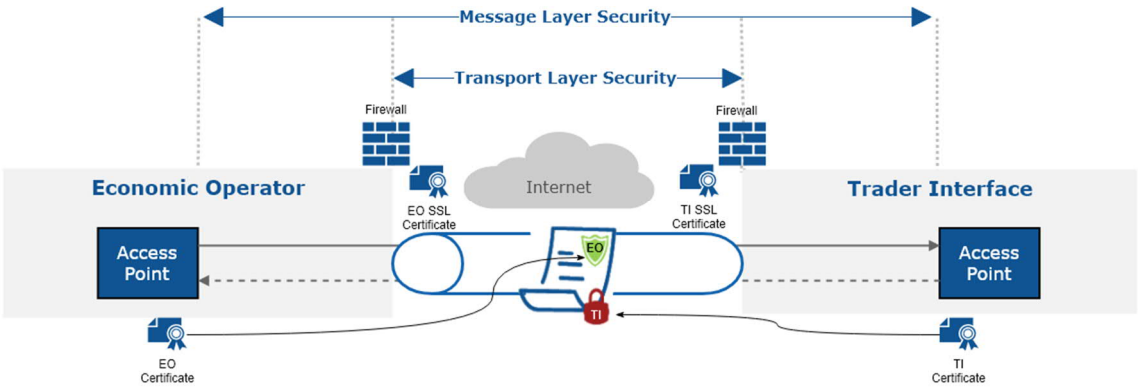

Figure 16: TLS vs Message security

An additional measure was assessed in order to provide via the UUM&DS system the opportunity for the EOs to give explicit permission to one or more IT Service Providers to deliver and receive ICS2 related messages on their behalf[12]. The extent of this measure was analysed and considered too burdensome both to trade and to the MS forcing the EOs into an additional registration procedure and the MS to establish the administrative procedure for this objective.

Having the party exchanging the ENS messages explicitly identified, registered and authorised ensures that any responsibility for misuse of the system can be clearly located and traced; also the introduction of the cited measure does not add to the prevention of the potential misuse of the system. For this reason this measure is currently not planned to be implemented[13].

The following table summarises the modes of implementation, prerequisites and types of certificates required for the different Communication Requirements:

Requirement	Layer	Protocol Specifications	Implementation	Certificate CA

[12] In the context of the STI Project Group (STIPG) it was observed that this measure is implemented in the current ICS systems by a minority of the STIPG participating MS; and some of those currently implementing it agree on not including it for ICS2. The remaining MS however expressed concerns on the lack of direct technical authorisation to the system by the Person filing.

[13] Nevertheless the measure is technically feasible and could be introduced if there is common agreement by the MS on this necessity. The main impact to the system would be the addition of a field in our use of the AS4 protocol (OriginalSender) and the implementation of extra functionalities and interfaces in UUM&DS; these on top of potential administrative procedures to be stablished by MS for trade.

Communication	Network	TCP/IP	Open Internet	N/A
Encryption	Transport	2 Way TLS (SSL)	Network Infrastructure	Trusted CA
Message Integrity (seal)	Message	AS4	Trader interface AS4 Access Point	
Identification (seal)				
Authorisation (register)	Functional	UUM&DS		N/A

Table 9: Communication Layer Requirements

4.6.1 Transport Layer Security

Within the ICS2 project the usage of **2-Way Transport Layer Security** (TLS) is mandatory to provide message confidentiality and authentication. The 2-way TLS covers on the one hand the Server authentication: using a server certificate, allows the client to make sure the HTTPS connection is set up with the right server; and on the other hand the Client Authentication: using a client certificate, allows the server to make sure the HTTPS connection is set up with a non-anonymous client.

The TLS should be implemented according to recent security standards. If TLS is not handled by the AS4 message handler itself, but by another component (such as a firewall, proxy server or router), these requirements are to be addressed by that component.

The eDelivery AS4 specifications ([R01] section 3.8.1. Transport Layer Security) define the following minimal requirements:

- Products compliant with this profile must support TLS 1.2 [RFC5246];
- It must be possible to configure accepted TLS cipher suites in the AS4 message handler. Products must support cipher suites included in the subset considered future-proof (see [R13], section 5.1.2). Vendors must add support for newer, safer cipher suites, as and when such suites are published by IANA/IETF;
- Support for SSL 3.0 and for cipher suites that are not currently considered secure should be disabled by default;
- Perfect Forward Secrecy, which is required in [BSITLS], is supported by the TLS_ECDHE_* and TLS_DHE_* cipher suites, which are therefore preferred and should be supported.

Transport Layer client authentication authenticates the Sender (when used with the Push MEP binding) and the Receiver (when used with Pull). Since this profile uses WS-Security for message authentication, the use of client authentication at the Transport Layer can be considered redundant. However, the Trader Interface will use **2-Way TLS Authentication** as it blocks anonymous access to the system already at the transport layer.

For this purpose, a certificate will be required to be provided by a Certificate Authority included in a list of trusted CAs[14] that will include any CA accepted by the Customs Authority of the Member States as recognised for this purpose. If the certificate is valid according to a trusted CA access is granted at transport layer.

[14] A Trusted CA in the ICS2 context is any CA trusted by the Customs Authorities of any Member State. The verification if a certificate was issues by a trusted CA will be done by UUM&DS at the moment of registration of the certificate in Customs.

4.6.2 Message Layer Security

The ICS2 Trader Interface relies on the message layer security features provided by the eDelivery AS4 specifications. In particular it uses the X.509 Certificate Token Profile to support the sealing of all AS4 messages. As illustrated in Figure 16 above, the private key of the sending MSH certificate is used to seal the message. The receiving MSH uses the public key of the sender's certificate to verify the origin (identity) and integrity of the message.

For AS4 message implementation, a certificate will be required to be provided by a Certificate Authority included in a list of trusted CAs that will include any CA accepted by the Customs Authority of the Member States as recognised for this purpose.

Only certificates delivered by a CA approved by a Member State or included in the Europa List of Trusted Lists[15] will be accepted. The UUM&DS system will facilitate the identification of MS approved CAs and verification of a given certificate being delivered by an approved Certificate Authority.

This sealing is based on the W3C XML Signature recommendation and must use the precise configuration parameters defined by eDelivery AS4 for the usage of these standards (specific digest and signature algorithms) based on identifiers defined in this recommendation (see **P-Mode parameters** [**Annex 1**]).

To avoid the additional burden to Economic Operators of double registering MSH certificates also in the DG TAXUD environment, the Dynamic Receiver profile enhancement will be used as detailed in section 4.3 of the eDelivery AS4 profile [R01]. This means that AS4 messages sent by traders will have to contain the certificate chain used to seal the messages in a BinarySecurityToken element[16]. For interoperability and efficiency the full certificate path must be included with the signature, rather than just the leaf certificate. This means that the Sending MSH MUST use the X509PKIPathv1 Token Type option. In this option the wsse:BinarySecurityToken includes an ordered list of X.509 certificates packaged in a PKIPath. Use of this token type MUST be indicated as indicated in Table 10.

Location	Element	Attribute	Value
Trader AS4 message	wsse:BinarySecurityToken	ValueType	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1
Trader AS4 security policy file	sp:X509Token	sp:IncludeToken	http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/IncludeToken/AlwaysToRecipient

Table 10. Dynamic Receiver profile enhancement

The X509v3 Token Type and PKCS7 Token Type SHOULD NOT be used. A BinarySecurityToken token reference MUST be used to reference the signing token.

[15] The Europa List of Trusted Lists is described at https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/List+of+Trusted+Lists

[16] The required configuration for this purpose is product specific but all products conformant to eDelivery should support it.

Refer to **Annex 5** for a detailed description of how and at which stages of the communication flow the security controls are applied.

4.6.3 Authorisation security controls

To ensure that the Sender access point delivering AS4 messages containing ENS filings has the authorisation to do so, the ICS2 trader Interface requires the registration and validation of the Sender delivering messages to the TI. This is to be implemented via an authorisation mechanism that relies on the UUM&DS system.

The Sender parties to be authorised for exchanging messages with the TI need to register their identification number (EORI) and the certificate that will be used for sealing the AS4 messages.

The parameters taken into account for these security controls are:

- The eb:From/eb:PartyId of the sender of the AS4 message;
- The certificate used for sealing the AS4 message (sealing certificate of the sending access point, matching parameter PMode[1].Security.X509.Signature.Certificate);
- The list of parties as registered in UUM&DS (incl. EORI and associated certificates) for exchanging messages with the TI in ICS2 (there may be more than one certificate for one economic operator).

The trader interface (TI) access point will implement validation of the certificate used for message sealing by the sender against information available through UUM&DS:

- Sender's certificate is checked for validity against accepted Certificate Authorities;
- Sender's PartyId is checked via UUM&DS to verify it has the authorisation to send messages to ICS2. To do so, the association between the sender's PartyId (EORI) and the certificate used for sealing will be validated versus the registered ones by the Customs Authorities.

The particulars of enrolling for the exchange of messages with ICS2 and registering the EORI and the certificates required for sealing and for TLS are detailed in the operational section below.

It must be noted that the certificate to be used for sealing the messages is that of the Sender. This is the legal person responsible for operating the Access Point. In many cases this is the Person filing itself; however in case of use of ITSP services it is the certificate of the IT Service Provider that is used. This implies also the fact that authorisation mechanisms explained above apply to the ITSP also.

5 OPERATIONAL

5.1 ENROLMENT AND OPERATION

This chapter presents the prerequisites and procedures the different actors need to fulfil to be able to deliver/receive an ENS Filing (or other relevant) message via the STI/NTI.

5.1.1 Establishing an Access Point by Trade

An Access Point is a technical gateway used for the exchange of messages with an ICS2 Trader Interface (TI).

In order to be able to establish an Access Point to exchange messages with a TI the EO or IT Service Provider[17] should:

- Implement the Access Point according to HTI specifications and the use of the specified eDelivery AS4 profile (both described in this document);
- Obtain a TLS certificate from a trusted CA to be used at the transport layer (https) for identifying itself following the 2-way TLS security mechanisms. A Trusted CA in the TLS context can be a commercial CA trusted by DG TAXUD. The CA used need to be notified to DG TAXUD, but the certificate does not require registration;
- Obtain a certificate from a trusted CA to be used for sealing at message layer (according to the AS4 specifications). A Trusted CA in the context of message sealing is any CA trusted by the Customs Authorities of any Member State. Any certificate in the LOTL lists[18] can be used. Exceptionally, additional certificate authorities might be accepted for registration on certain MS;
- Register with the Customs Authorities as a system actor of ICS2, as documented in the UUM&DS registration guidelines ([R15]) for centrally. For non-centrally managed identities, the National Customs Helpdesk should be contacted. The process includes the upload of the public key of the certificate that will be used for message sealing (to be later accessed for authorisation purposes) and the need of conformance test environment certificates;
- Inform the TES helpdesk on the intention to implement a given access point to exchange ENS messages with the STI and each NTI and specify the physical address (URL), the partyID (including the EORI), the CA to be used for TLS encryption certificate and the desired mode of communication (Pull or Push). In a later release this will be implemented as a self- registration mechanism in the STI/NTI preferences section. To perform this step the trader is authenticated using UUM&DS;
- Pass the connectivity and conformance test of the Access Point for compliance with the HTI specifications. The specific steps are provided in the conformance test documentation [R14].

Any given economic operator can implement and use as many Access Points as necessary. It is allowed to have multiple partyID's defined. This allows for the party to have/use multiple AS4 Access Points depending on the business domain or geographical region.

[17] In the case of IT Service Providers, the registration in Customs imply also obtaining an EORI number. Although ITSPs are not EOs obliged to obtain an EORI number, the use of this code for system authorisation purposes was considered the most pragmatic and simple solution (as was confirmed in the context of the STI project Group).

[18] List of trusted lists as can be found here: https://webgate.ec.europa.eu/tl-browser/#/

5.1.2 Preparing and sending a Message by Trade

Having determined the Access Point through which the message will be sent,

- The ENS filing (or other) functional message is formed according to ICS2 message specifications ([R06]);
- This functional message is then embedded as a payload in the AS4 message which on its own complies with the ICS2 HTI Technical Specifications as described in section 4;
- The AS4 message is then sealed at the message layer using the appropriate certificate[19];
- Subsequently, this sealed and encrypted AS4 message is sent to the TI via https using the 2-way TLS (at transport layer).

5.2 SELECTING AN ICS2 TRADER INTERFACE

Each Member State has a Trader interface (TI). This can be a national operated National Trader Interface (NTI) or the Shared Trader Interface (STI). When sending an ICS2 message, a trader must select the correct MSH protocol address (URL) of the TI of the addressed Member State according to the IT technical rules defined in section 3.3.2.4.

The list of MSH protocol addresses per ICS2 trader interfaces (STI and NTIs) and their public keys of the certificate that will be used for message sealing will be defined here in a later version of this document.

5.3 PREFERENCES FOR NOTIFICATIONS

Optionally a trader can register his notification preferences by contacting the TES helpdesk.[20] The types of preferences are:

- The PartyId of the default access point (see section 4.4 on routing);
- The request to receive some type of notifications (see the ICS2 Business Process Description [R02] for more information), for instance a Person filing can request to receive 'ENS not complete' notification messages IE3N02.

5.4 REFERENCE DATA

The code lists needed to create the ICS2 messages, as well as the customs office codes, together with other reference data used for semantic validation, will be published on the Europa web pages. The following are the different reference data domains for which publications are provided.

1.8.1.1.1 CS/RD2 IT application

Non-confidential ICS2 code lists to be used by the traders will be published on the Europa website (DDS2).

1.8.1.1.2 CRS IT application

The EORI data used by the ICS2 system is published on the DDS2 EORI module. It is accessible to traders both

- using a web UI: http://ec.europa.eu/taxation_customs/dds2/eos/eori_validation.jsp;

[19] Pull requests must also be sealed to ensure the party authorization to request the messages pull.

[20] In a later release the trader will be able to manage its notification preferences by a web user interface (STI/NTI UI).

- using a web interface for S2S interaction: Its WSDL file can be obtained here: http://ec.europa.eu/taxation_customs/dds2/eos/validation/services/validation?wsdl.

1.8.1.1.3 TARIC3 IT application

The TARIC data used by the ICS2 system is published on the DDS2 TARIC UI module. It is accessible to traders both:

- using a web UI: http://ec.europa.eu/taxation_customs/dds2/taric/taric_consultation.jsp;
- downloading monthly updates in Excel format on the CIRCABC website. Traders can subscribe ad hoc to changes by a mail to TAXUD-dds-TARIC@ec.europa.eu.

1.8.1.1.4 ECICS2 IT application

The CUS data used by the ICS2 system is published on the DDS2 ECICS UI module. It is accessible to traders:

- using a web UI: http://ec.europa.eu/taxation_customs/dds2/ecics/chemicalsubstance_consultation.jsp

5.5 TESTING

In a later version of this document this section will contain information about the organisation of trader conformance testing.

5.6 OPERATIONAL SERVICE LEVEL

The ICS2 TI will be available 24 hours per day, 365 days per year (24x365). In case of a system failure a fall-back procedure will need to be defined according to Art. 6 (3) (b) UCC. This fall-back procedure will be specified in the ICS2 business continuity plan which will provide the different measures to be taken for business continuity for the ICS2 overall system and for the ICS2 TI in particular.

Downtime due to maintenance activities and the deployment of a new application version will be avoided to the maximal extent possible by following the zero-downtime principle. Any other maintenance activity where this principle cannot be achieved will take place in an allocated service window of maximum 1 hour per week and will be planned and announced sufficiently in advance.

Outside the maintenance window, the target availability of the ICS2 TI will be of 99,25% for STI Release 1 and 99.45% from STI Release 2 onwards.

TES helpdesk support information will be provided in TES helpdesk related documentation.

5.7 CHANGE MANAGEMENT

In a later version of this document this section will contain information about the change management process to be defined by DG TAXUD.

The ICS2 TI will be able to support two versions of an ENS filing and of ENS notifications, the most recent and a previous version. A reporting party may only use one version. The ability to support two versions of a declaration is needed to ensure a smooth transition by a change in a declaration.

The version of the messages used is defined in the eb:AgreementRef. The first version is **EU-ICS2-TI-V1.0** implementing the corresponding message specifications as defined in [R04] and [R06].

Annex 1. SERVICE OPERATIONS

In the following table, the reader can find the description of ICS2 TI services, the operations (or actions) of those services and the user messages payload of those operations. The payload is the part of transmitted data that is the actual intended message. The actions of the services map to the message ID as given in ICS2 Information Exchange Specifications document [R04]. Each action has a corresponding message payload which corresponds to the relevant information exchange message name in that same document.

Service Name	Action	Message Id	Short Description	Payload Description
eu_ics2_t2c	*Mode of transport: Sea and inland waterways*			*An ENS Filing Message is submitted by the EO system and is received by the ICS2 TI Application. An ENS Filing means either partial or full ENS data set required by the legislation per specific mode of transport or business model.* *In case the reader wishes to find detailed information regarding the content (payload) of each message, they can refer to the ICS2 Information Exchange Specifications document [R04] and look-up the relevant message ID.*
	IE3F10	*IE3F10*	*Complete dataset – Straight bill of lading containing the necessary information from consignee*	
	IE3F11	*IE3F11*	*Complete dataset – Master bill of lading with underlying house bill(s) of lading containing the necessary information from consignee at the level of the lowest house bill of lading*	
	IE3F12	*IE3F12*	*Partial dataset – Master bill of lading only*	
	IE3F13	*IE3F13*	*Partial dataset – Straight bill of lading only*	
	IE3F14	*IE3F14*	*Partial dataset – House bill of lading only*	
	IE3F15	*IE3F15*	*Partial dataset – House bill of lading with the necessary information from consignee*	
	IE3F16	*IE3F16*	*Partial dataset – Necessary information required to be provided by consignee at the lowest level of transport contract (the lowest house bill of lading)*	
	IE3F17	*IE3F17*	*Partial dataset – Necessary information required to be provided by consignee at the lowest level of transport contract (straight bill)*	
	Mode of transport: Air cargo (general)			
	IE3F20	*IE3F20*	*Complete dataset lodged pre-loading*	
	IE3F21	*IE3F21*	*Partial dataset – Master air waybill lodged pre-arrival*	

Service Name	Action	Message Id	Short Description	Payload Description
	IE3F22	*IE3F22*	*Partial dataset – House air waybill lodged pre-arrival*	
	IE3F23	*IE3F23*	*Partial dataset — Minimum dataset lodged pre- loading in accordance with Article 106(1) second subparagraph of Delegated Regulation (EU) 2015/2446 without master air waybill reference number*	
	IE3F24	*IE3F24*	*Partial dataset — Minimum dataset lodged pre- loading in accordance with Article 106(1) second subparagraph of Delegated Regulation (EU) 2015/2446 with master air waybill reference number*	
	IE3F25	*IE3F25*	*Partial dataset — Master air waybill reference number lodged pre-loading in accordance with Article 106(1) second subparagraph of Delegated Regulation (EU) 2015/2446*	
	IE3F26	*IE3F26*	*Partial dataset — Minimum dataset lodged pre- loading in accordance with Article 106(1) second subparagraph of Delegated Regulation (EU) 2015/2446 and containing additional house air waybill information*	
	IE3F27	*IE3F27*	*Complete dataset lodged pre-arrival*	
	IE3F28	*IE3F28*	*Complete dataset lodged pre-loading – Direct air waybill*	
	IE3F29	*IE3F29*	*Complete dataset lodged pre-arrival – Direct air waybill*	
	Mode of transport: Express consignments			
	IE3F30	*IE3F30*	*Complete dataset lodged pre-arrival*	
	IE3F32	*IE3F32*	*Partial dataset — Minimum dataset lodged pre-loading in accordance with Article 106(1) second subparagraph of Delegated Regulation (EU) 2015/2446*	
	Mode of transport: Postal consignments			
	IE3F42	*IE3F42*	*Partial dataset - Master air waybill containing necessary postal air waybill information lodged in accordance with the time-limits applicable for the mode of transport concerned*	

Service Name	Action	Message Id	Short Description	Payload Description
	IE3F43	*IE3F43*	*Partial dataset — Minimum dataset lodged pre- loading in accordance with Article 106(1) second subparagraph of Delegated Regulation (EU) 2015/2446*	
	IE3F44	*IE3F44*	*Partial dataset — Receptacle identification number lodged pre-loading in accordance with Article 106(1) second subparagraph of Delegated Regulation (EU) 2015/2446*	
	Mode of transport: Road			
	IE3F50	*IE3F50*	*Road mode of transport*	
	Mode of transport: Rail			
	IE3F51	*IE3F51*	*Rail mode of transport*	
	IE3A10 *IE3A11* *IE3A12* *IE3A13* *IE3A14* *IE3A15* *IE3A16* *IE3A17* *IE3A20* *IE3A21* *IE3A22* *IE3A23* *IE3A24* *IE3A26* *IE3A27* *IE3A28* *IE3A29* *IE3A30* *IE3A32* *IE3A42*	*IE3A10* *IE3A11* *IE3A12* *IE3A13* *IE3A14* *IE3A15* *IE3A16* *IE3A17* *IE3A20* *IE3A21* *IE3A22* *IE3A23* *IE3A24* *IE3A26* *IE3A27* *IE3A28* *IE3A29* *IE3A30* *IE3A32* *IE3A42*	*Amend ENS*	*An ENS Amendment Message is submitted by the Sender access point and is received by the ICS2 TI Application. An ENS Amendment Message with name E_ENS_xxx_AMD amends the movement declaration filed through the corresponding message with name E_ENS_xxx_DEC.* *In case the reader wishes to find detailed information regarding the content (payload) of each message, they can refer to the ICS2 Information Exchange Specifications document [R04] and look-up the relevant message ID.*

Service Name	Action	Message Id	Short Description	Payload Description
	IE3A43 *IE3A44* *IE3A50* *IE3A51*	*IE3A43* *IE3A44* *IE3A50* *IE3A51*		
	IE3Q04	*IE3Q04*	*Invalidation Request*	*An Invalidation Request is submitted by the Sender access point and is received by the ICS2 TI Application. An Invalidation Request is the request for invalidation of an already registered ENS filing.*
	IE3N06	*IE3N06*	*Arrival Notification*	*An Arrival Notification is submitted by the Sender access point and is received by the ICS2 TI Application. An arrival notification identifies the Member State of Actual First Entry and triggers controls on goods which were identified being a risk requiring a control at the first point of entry in the EU.*
	IE3R02	*IE3R02*	*Additional Information Response*	*An Additional Information Response is submitted by the Sender access point and is received by the ICS2 TI Application. Through an Additional Information Response, the Economic Operator will respond with the additional information that was requested. This can be through text and/or attached images or documents.*
	IE3R03	*IE3R03*	*High Risk Cargo & Mail screening response*	*An HRCM screening response is submitted by the Sender access point and is received by the ICS2 TI Application. Through an HRCM screening response, the Economic Operator will respond to the request for high risk cargo screening with the results of the screening that the Economic Operator performed.*
eu_ics2_c2t	*IE3R01*	*IE3R01*	*ENS Registration Response*	*The ICS2 TI receives an ENS filing, performs validation on received ENS filing, registers ENS*

Service Name	Action	Message Id	Short Description	Payload Description
				filing and assigns MRN to ENS filing. The ICS2 TI notifies successful registration and MRN to the Person filing. This notification may be also communicated to the Carrier when it has requested to be informed and is different from the Person filing.
	IE3N10	*IE3N10*	*Amendment notification*	*ENS lifecycle validation is performed on an amendment of an ENS filing and succeeds. The ENS filing is now amended. The ICS2 TI creates an Amendment notification and sends it to the Person filing.*
	IE3R07	*IE3R07*	*Invalidation Acceptance Response*	*ENS lifecycle validation is performed on an invalidation request for an ENS filing and succeeds. The ENS filing is now invalidated. The ICS2 TI creates an Invalidation Acceptance Response and sends it to the Person filing.*
	IE3R04	*IE3R04*	*Arrival Registration Response*	*The ICS2 TI receives an Arrival Notification of the means of transport, performs validation on received Arrival Notification, registers Arrival Notification and assigns MRN to Arrival Notification. The ICS2 TI notifies successful arrival notification registration and MRN to the Person filing.*
	IE3Q02	*IE3Q02*	*Additional Information request*	*The Responsible Member State makes a request for Information. The ICS2 TI creates an Additional Information Request and sends it to the Person filing. The message will contain an indication on whether:* *- the additional information is to be provided through a response to this message; or* *- through an amendment to the EO's original filing.*

Service Name	Action	Message Id	Short Description	Payload Description
	IE3Q03	*IE3Q03*	*High Risk Cargo & Mail screening request*	*Decision to request HRCM screening was made. The ICS2 TI creates an HRCM Screening Request and sends it to the Person filing.*
	IE3Q01	*IE3Q01*	*Do Not Load Request*	*The risk assessment of an ENS filing is complete. The Economic Operator will be requested to not load a part of his initially declared consignment. The ICS2 TI sends the Do Not Load Request to the Person filing. This notification must be also communicated to the Carrier when the Carrier is different from the Person filing. The specific parts that are not to be loaded will be indicated through the message.*
	IE3N04	*IE3N04*	*Additional Information Request notification*	*The Responsible Member State makes a request for Information. The ICS2 TI creates an Additional Information Request notification and sends it to the Carrier when it has requested to be informed and is different from the Person filing.*
	IE3N05	*IE3N05*	*High Risk Cargo & Mail screening request notification*	*Decision to request HRCM screening was made. The ICS2 TI creates an HRCM screening request notification and sends it to the Carrier. The Carrier is notified that the Person filing was requested to perform high risk cargo screening and provide his results.*
	IE3N03	*IE3N03*	*Assessment Complete notification*	*The risk assessment of an ENS filing is complete. The ICS2 TI sends the Assessment Complete Notification to the Person filing. This notification may be also communicated to the Carrier when it has requested to be informed and is different from the Person filing.*

Service Name	Action	Message Id	Short Description	Payload Description
	IE3N08	*IE3N08*	*Control notification*	*A control recommendation was received. e-Screening was performed and it was decided that a control is to be performed at the first port or airport of arrival. The ICS2 TI creates a Control Notification to the Person filing (carrier) who submitted the arrival notification.*
	IE3N09	*IE3N09*	*AEO Control notification*	*The Authorised Economic Operator will be notified about the controls that will be performed on the goods that are under his responsibility. The ICS2 TI sends an (AEOS) Control Notification to the Person filing. This notification may be also communicated to the Carrier whenever applicable.*
	IE3N02	*IE3N02*	*ENS Not complete notification*	*An ENS is marked as not complete after:* *- the timer for ENS completion has expired; and* *- completeness did not derive from the "Relate ENS filings" sub process.* *The ICS2 TI sends the ENS Not Complete Notification to the Person filing. This notification may be also communicated to the Carrier whenever applicable. This notification shall also be communicated to all persons that have not yet filed that are connected to the TI.*
	IE3N07	*IE3N07*	*ENS In Incorrect State notification*	*The state of an ENS filing is checked upon arrival. The ENS is not in a correct state to announce its arrival. The ICS2 TI creates an Incorrect State Notification and sends it to the Person filing (carrier) who submitted the arrival notification.*
	IE3N01	*IE3N01*	*ENS lifecycle validation error notification*	*ENS lifecycle validation is performed on a stored ENS filing and fails. The ICS2 TI creates an ENS Lifecycle Validation Error Notification and sends it*

Service Name	Action	Message Id	Short Description	Payload Description
				to the Person filing. The produced error will be about: *- one or more key data element(s) being not unique; and/or* *- the incorrect state of any of the concerned ENS(s).*
	IE3N99	*IE3N99*	*Notify Error*	*When an syntactical or semantic validation error is found while the Person filing is using the ICS2 TI, the ICS2 TI creates a Validation Error Notification, logs a security event and sends it to the Person filing. The error notification includes the error description and the error code.*
	IE3N11	*IE3N11*	*ENS Pending Notification*	*The Person not yet filed is informed that he is obliged to file an ENS filing. The ICS2 TI sends the ENS Pending Notification with ID IE3N11 to the Person not yet filed.*

Table 11: Description of ICS2 TI User Messages payload

Annex 2. P-MODES SUMMARY

The following table lists the processing mode parameters defined by the eDelivery AS4 specifications and specifies where the TI specifications further constrain the processing mode.

It also describes whether the parameter is not part of eDelivery (**not profiled**) or whether it is not applicable in the TI use case (**unused**). Unprofiled parameters may be part of the AS4 profile and may allow a sending MSH to choose a value, which would then be used by the receiving MSH to handle the reception and the response. The MSH ignores unused parameters.

The names of the P-Mode parameter in the table follow the notation described in Annex D 2.1 of [R07].

1. GENERAL P-MODE PARAMETERS

P-Mode Parameter	Value in the TI profile (eDelivery AS4 default)	Notes
PMode.ID	**Unused**	
PMode.Agreement	EU-ICS2-TI-V1.0	See 4.2.3
PMode.MEP	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay	See 4.1.3
PMode.MEPBinding	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push	See 4.1.3
PMode.Initiator.Party	Initiating MSH specific value	See 4.2.2.1
PMode.Initiator.Role	Initiating MSH specific value: '**Trader**' or '**Customs**'	See 4.2.2.2
PMode.Initiator.Authorization.username	**Unused**	
PMode.Initiator.Authorization.password	**Unused**	
PMode.Responder.Party	Responding MSH specific value	See 4.2.2.1
PMode.Responder.Role	Responding MSH specific value: '**Trader**' or '**Customs**'	See 4.2.2.2
PMode.Responder.Authorization.username	**Unused**	
PMode.Responder.Authorization.password	**Unused**	

Table 12. General P-Mode Parameters

2. PROTOCOL

P-Mode Parameter	Value in the TI profile (eDelivery AS4 default)	Notes
PMode[1].Protocol.Address: **required**	(Required, https URL of the receiver)	
PMode[1].Protocol.SOAPVersion	(1.2)	

Table 13. Protocol

3. BUSINESSINFO

P-Mode Parameter	Value in the TI profile (eDelivery AS4 default)	Notes
PMode[1].BusinessInfo.Service	Message specific value: **eu_ics2_t2c** or **eu_ics2_c2t**	See 4.2.3.2
PMode[1].BusinessInfo.Action	Message specific value as per functional specifications	See 4.2.3.3
PMode[1].BusinessInfo.Properties	**Unused**	See 4.2.4
PMode[1].BusinessInfo.MPC	**Unused**	
PMode[1].BusinessInfo.subMPCext	**Unused**	
PMode[1].BusinessInfo.PayloadProfile	**Unused**	

Table 14. BusinessInfo

4. ERRORHANDLING

P-Mode Parameter	Value in the TI profile (eDelivery AS4 default)	Notes
PMode[1].ErrorHandling.Report.SenderErrorsTo	**Unused**	
PMode[1].ErrorHandling.Report.ReceiverErrorsTo	**Unused**	
PMode[1].ErrorHandling.Report.AsResponse	(True)	
PMode[1].ErrorHandling.Report.ProcessErrorNotifyConsumer	(True)	

PMode[1].ErrorHandling.Report.DeliveryFailuresNotifyProducer	(True)	

Table 15. ErrorHandling

5. RELIABILITY

The reliability P-Mode parameters refer to an older protocol and are unused in AS4 eDelivery. eDelivery relies on receipts and errors in this regard.

6. SECURITY

P-Mode Parameter	Value in the TI profile (eDelivery AS4 default)	Notes
PMode[1].Security.WSSversion	(1.1.1)	
PMode[1].Security.X509.Sign	(True)[21]	.
PMode[1].Security.X509.Signature.Certificate	(Signing Certificate of the Sender)	
PMode[1].Security.X509.Signature.HashFunction	(http://www.w3.org/2001/04/xmlenc#sha256)	
PMode[1].Security.X509.Signature.Algorithm	(http://www.w3.org/2001/04/xmldsig-more#rsa-sha256)	
PMode[1].Security.X509.Encryption.Encrypt	False	
PMode[1].Security.X509.Encryption.Certificate	(Encryption Certificate of the Receiver)	
PMode[1].Security.X509.Encryption.Algorithm	(http://www.w3.org/2009/xmlenc11#aes128-gcm)	
PMode[1].Security.X509.Encryption.MinimumStrength	(128)	
PMode[1].Security.UsernameToken.username	**Unused**	
PMode[1].Security.UsernameToken.password	**Unused**	
PMode[1].Security.UsernameToken.Digest	**Unused**	
PMode[1].Security.UsernameToken.Nonce	**Unused**	
PMode[1].Security.UsernameToken.Created	**Unused**	
PMode[1].Security.PModeAuthorize	(False)	

[21] In addition to setting this value to true, a product specific configuration has to be performed in order to ensure that the complete certificate chain used for signature is embedded in the messages (see section 4.6.2 for further details).

P-Mode Parameter	Value in the TI profile (eDelivery AS4 default)	Notes
PMode[1].Security.SendReceipt	(True)	
PMode[1].Security.SendReceipt.NonRepudiation	(True)	
PMode[1].Security.SendReceipt.ReplyPattern	(Response)	

Table 16. Security

7. PAYLOADSERVICE COMPRESSIONTYPE

P-Mode Parameter	P-Mode Parameter	Notes
PMode[1].PayloadService.CompressionType	(application/gzip)	

Table 17. Payload Service Compression Type

8. RECEPTIONAWARENESS

P-Mode Parameter	P-Mode Parameter	Notes
PMode[1].ReceptionAwareness	(True)	
PMode[1].ReceptionAwareness.Retry	(True)	
PMode[1].ReceptionAwareness.Retry.Parameters	**not profiled**	Implementation specific[22]
PMode[1].ReceptionAwareness.DuplicateDetection	(True)	
PMode[1].ReceptionAwareness.DetectDuplicates.Parameters	**not profiled**	Implementation specific[22]

Table 18. Reception Awareness

[22] The way this parameter is specified (format) is product specific. In a later version of this document, guidelines will be given about the number of retries and the interval between retries.

Annex 3. SAMPLE MESSAGE SCENARIO

The following sequence diagram provides an overview of an ENS Filing message by an Economic Operator (EO) and its reply by a Trader Interface from an AS4 perspective.

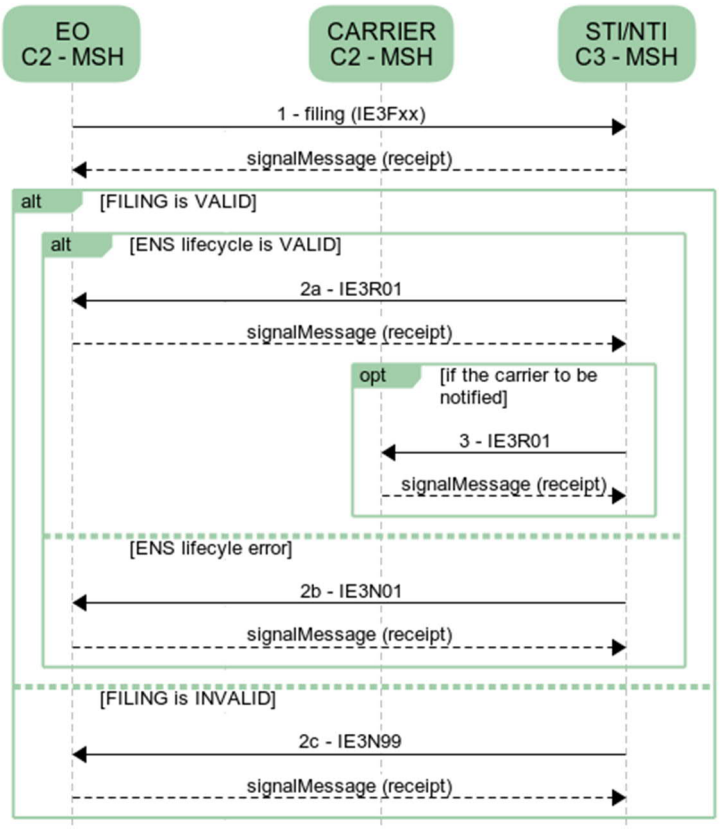

Figure 17: ENS Filing message scenario.

The sequence diagram depicts the following scenario:

(1) IE3Fxx - ENS Filing. An Economic Operator (EO) submits an ENS Filing (IE3Fxx) using an AS4 message handler (C2-MSH) to an STI/NTI AS4 message handler (C3-MSH):

- This message has as **eb:MessageId** a unique value '1'[23];
- The eb:From/eb:PartyId identifies the EO and has an eb:From/eb:Role of 'Trader';
- The eb:To/eb:PartyId identifies the addressed STI/NTI and has an eb:To/eb:Role of 'Customs';
- The addressed **eb:Service** is 'eu_ics2_t2c' with an **eb:Action** of 'IE3Fxx';
- In the eb:PayloadInfo a single eb:PartInfo that specifies in its eb:Property's as Mime type 'application/xml', as Characterset 'utf-8' and as CompressionType 'application/gzip' (see section 4.2.5);
- The message contains one additional Mime part (as specified in the eb:PayloadInfo) containing the **functional payload**, i.e. a functional message IE3Fxx as specified in the common functional specification and encoded in the XML format as specified by the applicable XSD. The functional message contains an **LRN** specified by the EO.

[23] In this document, simple values like '1','2' are used for readability of the document. However in a real implementation, the sender must guarantee uniqueness of these message id's and typically would consists out of an UUID or equivalent id generating system.

The **SignalMessage** depicted in the sequence diagram for each of UserMessages is a synchronous http response and contains the AS4 receipt of the UserMessage by the receiving MSH. It contains the seal of the receiving MSH in relation with the submitted UserMessage (see section 4.3.1).

The UserMessage IE3Fxx is received by the C3-MSH of the STI/NTI addressed and further processed by this system. This processing will result in a **single reply message** with regards to this ENS filing. This message can be an ENS registration response, an Error notification or an ENS lifecycle validation error notification. Independent of the message type, the following AS4 properties apply:

- The message has as eb:MessageId a unique value of '2';
- The **eb:ReftoMessageId** is specified and has a value of '1' referring to the eb:MessageId of the initial ENS filing;
- The eb:From and eb:To Parties are inversed;
- The addressed eb:Service is 'eu_ics2_c2t'. However, the eb:Action property depends on the **specific message type** returned;
- In the eb:PayloadInfo a single eb:PartInfo is specified with in its eb:Property's as Mime type 'application/xml', as Characterset 'utf-8' and CompressionType 'application/gzip';
- The message contains one additional Mime part (as specified in the eb:PayloadInfo) containing the specific functional message as specified in the eb:Action property as specified in the common functional specification and encoded in the XML format as specified by the applicable XSD.

Depending on the STI/NTI processing **one of the following** reply messages applies:

(2a) IE3R01 – ENS Registration response. The message confirms the registration of the ENS Filing and the attribution of an MRN to this filing. In addition to the common properties the following AS4 properties apply:

- The eb:Action is set to the value 'IE3R01';
- The additional Mime part contains a functional message of type IE3R01. This message contains the **LRN** provided in the functional payload of the initial ENS filing and the corresponding **MRN** attributed by the STI/NTI.

(2b) IE3N01 – ENS lifecycle validation error notification. The message indicates that the ENS to which this filing is related is in a state that does not allow a filing. In addition to the common properties the following AS4 properties apply:

- The eb:Action is set to the value 'IE3N01';
- The additional Mime part contains a functional message of type IE3N01. This message contains the **LRN** provided in the functional payload of the initial ENS filing. It also provides an indication of the actual reason(s) for the life cycle validation error.

(2c) IE3N99 – Error notification. The message indicates that there are syntax and/or semantical errors found in the initial ENS filing. In addition to the common properties the following AS4 properties apply:

- The eb:Action is set to the value 'IE3N99';
- The additional Mime part contains a functional message of type IE3N99. This message contains the **LRN** provided in the functional payload of the initial ENS filing if it could be extracted from the initial ENS filing. It also provides an indication of the actual error(s). In the case no LRN can be provided, the only way to associate this reply message with the initial ENS filing is the eb:RefToMessageId property.

(3) IE3R01 – ENS Registration response to Carrier. In case of the registration of the ENS filing (2a), the ENS registration response message is optionally also sent to the carrier identified

in the initial ENS filing if the carrier has expressed the preference to receive such messages[24]. In addition to the common properties the following AS4 properties apply:

- The eb:Action is set to the value 'IE3R01';
- The additional Mime part contains a functional message of type IE3R01. This message contains the **LRN** provided in the functional payload of the initial ENS filing and the corresponding **MRN** attributed by the STI/NTI.

[24] Note that this means that the Carrier must be registered in this TI.

Annex 4. EBMS ERRORS

The following sections describe ebMS errors according to the stage they are likely to occur. It also includes a table for UUM&DS extensions.

1. EBMS PROCESSING ERRORS

The table below describes the Errors that may occur within the ebMS Module itself (ebMS Errors that are not Escalated Errors), i.e. with @origin="ebms". These errors MUST be supported by an MSH, meaning generated appropriately, or understood by an MSH when reported to it.

Error Code	Short Description	Severity	Category Value	Description or Semantics
EBMS:0001	ValueNotRecognized	failure	Content	Although the message document is well formed and schema valid, some element/attribute contains a value that could not be recognized and therefore could not be used by the MSH.
EBMS:0002	FeatureNotSupported	warning	Content	Although the message document is well formed and schema valid, some element/attribute value cannot be processed as expected because the related feature is not supported by the MSH.
EBMS:0003	ValueInconsistent	failure	Content	Although the message document is well formed and schema valid, some element/attribute value is inconsistent either with the content of other element/attribute, or with the processing mode of the MSH, or with the normative requirements of the ebMS specification.
EBMS:0004	Other	failure	Content	
EBMS:0005	ConnectionFailure	failure	Communication	The MSH is experiencing temporary or permanent failure in trying to open a transport connection with a remote MSH.
EBMS:0006	EmptyMessagePartitionChannel	warning	Communication	There is no message available for pulling from this MPC at this moment.
EBMS:0007	MimeInconsistency	failure	Unpackaging	The use of MIME is not consistent with the required usage in this specification.

Error Code	Short Description	Severity	Category Value	Description or Semantics
EBMS:0008	FeatureNotSupported	failure	Unpackaging	Although the message document is well formed and schema valid, the presence or absence of some element/ attribute is not consistent with the capability of the MSH, with respect to supported features.
EBMS:0009	InvalidHeader	failure	Unpackaging	The ebMS header is either not well formed as an XML document, or does not conform to the ebMS packaging rules.
EBMS:0010	ProcessingModeMismatch	failure	Processing	The ebMS header or another header (e.g. reliability, security) expected by the MSH is not compatible with the expected content, based on the associated P-Mode.
EBMS:0011	ExternalPayloadError	failure	Content	The MSH is unable to resolve an external payload reference (i.e. a Part that is not contained within the ebMS Message, as identified by a PartInfo/href URI).

Table 19. ebMS Processing Errors

2. SECURITY PROCESSING ERRORS

The table below describes the Errors that originate within the Security Module, i.e. with @origin="security". These errors MUST be escalated by an MSH, meaning generated appropriately, or understood by an MSH when reported to it.

Error Code	Short Description	Severity	Category Value	Description or Semantics
EBMS:0101	FailedAuthentication	failure	Processing	The signature in the Security header intended for the "ebms" SOAP actor, could not be validated by the Security module.
EBMS:0102	FailedDecryption	failure	Processing	The encrypted data reference the Security header intended for the "ebms" SOAP actor could not be decrypted by the Security Module.
EBMS:0103	PolicyNoncompliance	failure	Processing	The processor determined that the message's security methods, parameters, scope or other security policy-level requirements or agreements were not satisfied.

Table 20. Security processing errors

3. RELIABLE MESSAGING ERRORS

The table below describes the Errors that originate within the Reliable Messaging Module, i.e. with @origin="reliability". These errors MUST be escalated by an MSH, meaning generated appropriately, or understood by an MSH when reported to it.

Error Code	Short Description	Severity	Category Value	Description or Semantics
EBMS:0201	DysfunctionalReliability	failure	Processing	Some reliability function as implemented by the Reliability module, is not operational, or the reliability state associated with this message sequence is not valid.
EBMS:0202	DeliveryFailure	failure	Communication	Although the message was sent under Guaranteed delivery requirement, the Reliability module could not get assurance that the message was properly delivered, in spite of resending efforts.

Table 21. Reliable message errors

4. AS4 FEATURE ERRORS

The following error codes are extending the set of ebMS V3 error codes to support the AS4 additional features. They are to be generated and/or processed by an AS4 MSH depending on which feature is supported (i.e. depending on the conformance profile):

Error Code	Short Description	Severity	Category Value	Description or Semantics
EBMS:0301	MissingReceipt	failure	Communication	A Receipt has not been received for a message that was previously sent by the MSH generating this error.
EBMS:0302	InvalidReceipt	failure	Communication	A Receipt has been received for a message that was previously sent by the MSH generating this error, but the content does not match the message content (e.g. some part has not been acknowledged, or the digest associated does not match the signature digest, for NRR).
EBMS:0303	Decompression-Failure	failure	Communication	An error occurred during the decompression.

Table 22. AS4 feature errors

5. UUM&DS FEATURE ERRORS

UUM&DS validation errors returned by the Trader Interface AS4 access point is described here. The ebMS error EBMS:0004 will be returned, with the sub-code as defined in the table unterhalb.

EBMS Error Code	Subcode	Meaning
EBMS:0004	A001	UUM&DS rejected the authorization and the incoming message is rejected.

EBMS:0004	A002	Technical user trying to connect to the rest API is rejected.
EBMS:0004	A003	Internal UUM&DS error, or UUM&DS is down

Table 23. UUM&DS errors

Annex 5. MESSAGE LAYER SECURITY CONTROLS

The next paragraphs provide a detailed description of the security controls of an eDelivery AS4 implementation, as well as the communication flow between Access Points as depicted in the figure below.

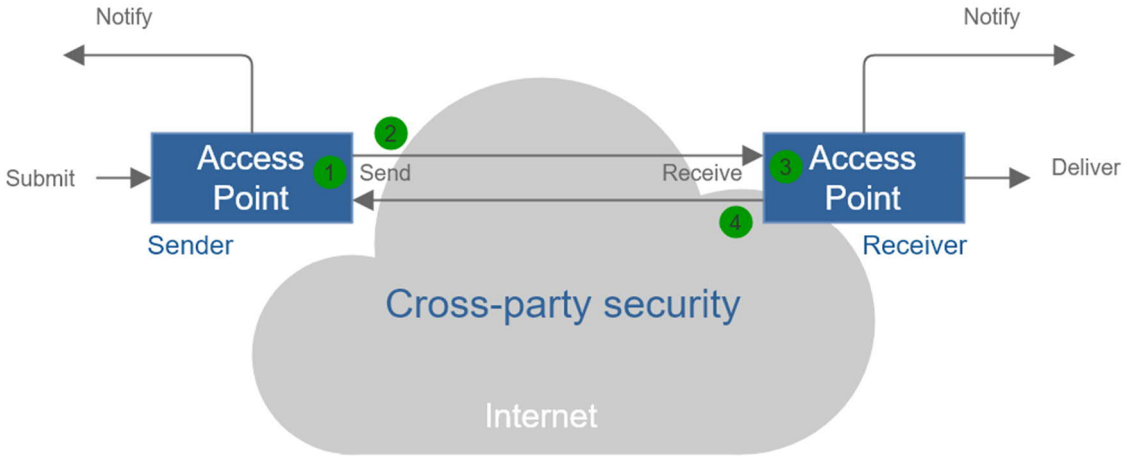

Figure 18: Security controls of eDelivery AS4 implementation

1. The sender Access Point creates an AS4 message composed of a **SOAP header, an empty SOAP body and one payload** (or more if attachments are handled as separate payloads) with the receiver as a recipient. The unencrypted and electronic sealed content is included in an attachment. The electronic seal is performed using a recommended cipher suite with the private key of the sender. In addition, the header containing the message metadata details, such as message ID is also sealed by the sender. The electronic seal digest of the header and of the content payload are included in the WS-Security header, whereas the SOAP body is sent empty as described in the eDelivery AS4 profile;
2. The message is sent through a TLS connection, providing message confidentiality and authenticity at the transport layer. The TLS cipher suites should follow the ENISA guidelines as described in the eDelivery AS 4 specifications;
3. The receiver verifies the integrity and authenticity of the message according to the digital certificate (public key) of the sender. This assures the receiver that the sender was the sender of the message, and that the message was not tampered with during communication;
4. Upon reception and verification, the receiver generates an evidence receipt based on the message information received, electronically seals it using its digital certificate and sends it to the sender as proof of receipt. The electronic seal provides integrity and authenticity of the evidence as the sender can verify that the message has been received by the receiver.

*** *End of document* ***