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

Operational FAQ

ICS2

Date:	16/05/2023
Status:	Submitted for acceptance (SfA)
Version:	3.50 EN
Author:	ITSM3-TES
Approved by:	DG TAXUD
Reference number:	DLV.3.2.3.7
Public:	DG TAXUD external
Confidentiality:	Publicly available (PA)

Document control information

Property	Value
Title	Operational FAQ
Subtitle	ICS2
Author	ITSM3-TES
Project owner	Head of Unit of DG TAXUD Unit B3
Solution provider	DG TAXUD Unit B3 Customs Systems
DG TAXUD Project Manager	Bartlomiej Bzdela
Version	3.50 EN
Confidentiality	Publicly available (PA)
Date	16/05/2023

Contract information

Property	Value
Framework Contract	DI/7811 (EUSS-SM Lot 2)
Specific Contract	DIGIT-EUSS

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
3.50	16/05/2023	Document submitted for acceptance (SfA)	I/R	All
3.40	05/05/2023	Document submitted for review (SfR).	I/R	Added sections: 3.2.1, 3.2.2, 3.2.3, 3.2.9, 3.2.30, 3.2.31. Modified section: 3.2.32
3.30	13/03/2023	Document submitted for acceptance (SfA)	I/R	All
3.20	03/03/2023	Document submitted for review (SfR).	I/R	Added section: 2.1.3
3.10	16/01/2023	Document submitted for acceptance (SfA)	I/R	All
3.00	05/01/2023	Document submitted for review (SfR).	I/R	Added sections: 3.2.5, 3.2.8, 3.2.15
2.90	15/11/2022	Document submitted for acceptance (SfA).	I/R	All
2.80	07/11/2022	Document submitted for review (SfR).	I/R	Added sections: 2.2.11, 3.2.4, 3.2.18
2.70	14/09/2022	Document submitted for acceptance (SfA).	I/R	All
2.60	05/09/2022	Document submitted for review (SfR).	I/R	Added sections: 3.1.5, 3.2.16, 3.2.17
2.50	13/07/2022	Document submitted for acceptance (SfA).	I/R	All

Version	Date	Description	Action[1]	Section
2.40	05/07/2022	Document submitted for review (SfR).	I/R	Modified sections 3.2.3 Added section 3.1.3, 3.2.15
2.30	20/05/2022	Document re-submitted for acceptance (re-SfA)	I/R	All
2.20	18/05/2022	Document submitted for acceptance (SfA).	I/R	All
2.10	04/05/2022	Document submitted for review (SfR). Document updated to accommodate Questions and Answers in scope of ICS2 operations and Conformance Testing irrespectively of a specific ICS2 Release.	I/R	Added sections: 2.2.10, 2.2.11, 2.2.12, 2.2.13, 2.3.6, 2.3.7, 2.3.8, 3.1.2, 3.1.3, 3.2.1, 3.2.2, 3.2.3, 3.2.5, 3.2.14 Modified Sections: 1.1, 1.2, 1.3, 1.4, 1.5, 2.2.2, 2.2.3, 3.2.6, 3.2.7, 3.2.10, 3.2.16, 3.2.19, 3.2.22
2.00	11/03/2022	Document submitted for acceptance (SfA).	I/R	All
1.90	03/03/2022	Document submitted for review (SfR).	I/R	Modified sections 2.3.5, 3.2.20
1.80	13/01/2022	Document submitted for acceptance (SfA).	I/R	All
1.70	05/01/2022	Document submitted for review (SfR).	I/R	Added section 3.2.18, 3.2.19, 3.2.20
1.60	15/11/2021	Document submitted for acceptance (SfA).	I/R	All
1.50	05/11/2021	Document submitted for review (SfR).	I/R	Added section 2.3.5
1.40	13/09/2021	Document submitted for acceptance (SfA).	I/R	All
1.30	03/09/2021	Document submitted for review (SfR) upon bi-monthly update.	I/R	Added sections 2.3.4, 3.2.15, 3.2.16, 3.2.17
1.20	13/07/2021	Document submitted for acceptance (SfA).	I/R	All
1.10	05/07/2021	Document submitted for review (SfR) upon bi-monthly update.	I/R	Added sections 2.1.9, 2.2.9, 3 Modified sections 1.1, 1.3
1.00	17/05/2021	Document submitted for acceptance (SfA).	I/R	All
0.10	05/05/2021	Document submitted for review (SfR).	I/R	All
0.01	01/04/2021	Initial draft	I/R	All

[1] Action: I=Insert R=Replace

Configuration management: document location

The latest accepted version of this controlled document is stored on: webgate.ec.europa.eu/pics

Table of contents

List of tables

List of figures

1 INTRODUCTION

1.1 DOCUMENT PURPOSE

This document incorporates the most common questions raised by MSs and EOs as well as the clarifications that have been provided by DG TAXUD and contractors of DG TAXUD who are involved in the support and monitoring activities of ICS2 operations and conformance testing. Moreover, this document incorporates questions about how to handle different types of incidents which have been detected during production of ICS2.

1.2 TARGET AUDIENCE

The target audience for this document includes any person from the National Administrations and the Economic Operators who are involved in the ICS2.

1.3 SCOPE

The scope of this document is to consolidate the knowledge from the most common questions raised by MSs and EOs as well as the clarifications that have been provided by DG TAXUD and contractors of DG TAXUD who are involved in the support and monitoring activities of ICS2 operations.

1.4 STRUCTURE

This document is organised as follows:

- **Chapter 1 – Introduction**: describes the scope and the objectives of the document;
- **Chapter 2 – Operational Frequently Asked Questions (FAQ)**: enlists the questions most frequently raised by DG TAXUD, contractors of DG TAXUD, MSs and EOs, along with the respective answers in relation to ICS2 Operational topics;
- **Chapter 3 – Conformance Testing Frequently Asked Questions (FAQ)**: enlists the questions most frequently raised by DG TAXUD, contractors of DG TAXUD, MSs and EOs, along with the respective answers in relation to Conformance Testing topics.

1.5 REFERENCE DOCUMENTS

The table below lists the documents that are referred to in the current document.

Ref.	Title	Originator	Version	Date
R01	ICS2 Design Document for National Applications	SOFT-DEV	4.40	29/07/2022
R02	MS Conformance Test Case Specifications Release 1	CUST-DEV3	3.40	05/03/2021
R033	EO Conformance Test Organisation Document (CTOD) for Release 1	ITSM3-TES	1.23	07/04/2021
R04	ICS2 HTI Interface Control Document	SOFT-DEV	3.30	02/03/2022
R05	MS Conformance Test Organisation Document (CTOD) for Release 1	ITSM3-TES	1.80	15/06/2021
R046	ICS2 Rules and Conditions	DG TAXUD ICS2 Project Team	1.24	19/03/2021
R057	MS Business Continuity Plan	DG TAXUD ICS2 Project Team	1.30	10/06/2022

Ref.	Title	Originator	Version	Date
R08	Test Design Specifications for Member States Conformance Test Scenarios for Release 2	SOFT-DEV	2.80	05/01/2023
R09	ICS2 Monitoring - Use Case Specifications	SOFT-DEV	5.90	24/01/2023
R10	CCN2-CFSS-R1.5 System Functional Specifications	CCN2-DEV	14.00	18/01/2022
R11	MS–TDS–Conformance Test Cases for Release 2	SOFT-DEV	2.50	09/01/2023
R12	ICS2 EOs Common Technical System Specifications package for ICS2 Release 2	DG TAXUD	N/A	19/09/2022
R13	Conformance Test Organisation Document (CTOD) for EO for Release 2	ITSM3-TES	1.40	09/08/2022
R14	Test Design Specifications for Economic Operator Conformance Test Scenarios for Release 2 & Release 3	SOFT-DEV	2.40	21/10/2022
R15	Test Design Specifications for Economic Operator Conformance Test Cases for Release 2 & Release 3	SOFT-DEV	2.00	27/12/2022
R16	Conformance Test Organisation Document (CTOD) for MS for Release 2	ITSM3-TES	1.20	02/02/2022
R17	ICS2 Harmonised Trader Interface Specifications	DG TAXUD	2.02	23/05/2022

Table 1: Reference documents

1.6 APPLICABLE DOCUMENTS

The table below lists the documents to which the current document must be compliant.

Ref.	Title	Originator	Version	Date
A01	TEMPO – Glossary of Terms	DG TAXUD	2.01-EN	07/04/2006
A02	Specific Contract DIGIT-EUSS	DG TAXUD	N/A	01/03/2023
A03	Framework Contract	DG TAXUD	N/A	26/09/2016

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
AS4	Applicability Statement 4
CA	Certificate Authority
CCN2ng	Common Communication Network 2 next generation
CEF	Connecting Europe Facility
CET	Central European Time
CL	Code List
CoA	Confirmation of Arrival
CoD	Confirm on Delivery
CoE	Confirmation of Exception

Abbreviation/Acronym	Definition
CR	Common Repository
CSD	Central Service Desk
CS/RD2	Common Service for Reference Data version 2
CT	Conformance Testing
CTC	Conformance Test Cases
DG TAXUD	Directorate General - Taxation and Customs Union
E2E	End-to-End
EIDAS	Electronic Identification, Authentication and trust Services
ENS	Entry Summary Declaration
EO	Economic Operator
EORI	Economic Operators Registration and Identification number
ESS	Employee Self Service (part of SYNERGIA SMT) (https://itsmtaxud.europa.eu/smt/ess.do)
FAQ	Frequently Asked Questions
GB	Great Britain
GMT	Greenwich Mean Time Zone
HTI	Harmonised Trader Interface
ICD	Interface Control Document
ICS2	Import Control System 2
ID	Identity Document
ITSM	IT Service Management
ITSP	IT Service Provider
LOTL	EU List of eIDAS Trusted Lists
LRN	Local Reference Number
MIME	Multipurpose Internet Mail Extensions
MPC	Message Partition Channels
MON	ICS2 Monitoring and Business Statistics Tool
MS	Member State
NES	National Entry System
NSD	National Service Desk
NPTL	National Project Team Leader
OIM	Oracle Identity Management
OMS	Other Member State
OPS	Operations
SaaS	Software as a Service
STI	Shared Trader Interface
STP	Specific Trader Portal
TAPAS	DG TAXUD Access Point for AS4 System
TES	Trans-European Systems
TI or ICS2 TI	ICS2 Trader Interface
UI	User Interface
UTC	Coordinated Universal Time
UUM&DS	Unified User Management and Digital Signatures
XI	United Kingdom (Northern Ireland)

Abbreviation/Acronym	Definition
WAYF	Where Are You From
WSDL	Web Services Description 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).
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.
Conformance Testing	This testing is done to obtain technical assurance that a National Administration or an Economic Operator is ready to enter the Trans-European System without risk of disturbing the parties already in operation in the system.
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	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.
ITSM Contractor	DG TAXUD contractor (ITSM3-OPS, ITSM3-TES) responsible for operating the central services and testing the centrally developed applications.

Table 4: Definitions

2 OPERATIONAL FREQUENTLY ASKED QUESTIONS (FAQ)

2.1 FAQ RELATED TO CENTRAL SIDE

2.1.1 What are the URLs for ICS2 CR User Interface?

Conformance:https://u2s.conf.ccn2.taxud/ics2-cr-web-ccn2/index.jsp
Production: https://u2s.prod.ccn2.taxud/ics2-cr-web-ccn2/index.jsp

2.1.2 What are the URLs for ICS2 Monitoring & Business Statistics tool?

Conformance: https://u2s.conf.ccn2.taxud/ics2-mon/index.html
Production: https://u2s.prod.ccn2.taxud/ics2-mon/index.html

2.1.3 What are the URLs for ICS2 STI-STP User Interface?

Conformance: https://conformance.customs.ec.europa.eu/euctp

Production: https://customs.ec.europa.eu/gtp/[1]

2.1.4 In case of question regarding the value of a timer in production, what is the proper communication channel for this to be addressed?

A Member State (MS) must address any request around value of timer in production directly to DG TAXUD via secure email. It is highlighted that such information must not be shared with EO.

2.1.5 What process should be followed for an MS to enter ICS2 Operations?

After the successful completion of the CT activities, a ticket should be registered in order the CL717 filter to be updated in CS/RD2 PROD. The CL717 - Country code (ICS2 MS) must include the country code of the MS who is going to enter ICS2 operations. Afterwards, a change should be implemented by ITSM3-OPS in order for the country code to be added from CS/RD2 in ICS2 Coherence Cache Memory in PROD. The actions described above need to have been completed at least one day before the planned GO live date for the NA.

2.1.6 Who is responsible for the registration of the national web services in the CCN2ng platform?

ITSM3-OPS is responsible to register the WSDL files for the national web services in the CCN2ng platform. However, the corresponding WSDL files have to be submitted to ITSM3-OPS by the respective MS. This is done by opening a Service request with CSD to SYNERGIA.

2.1.7 Which are the physical addresses of the NES partner endpoints that should be registered in the CCN2ng platform?

As per section 8.1 from the ICS2 Design Document [R01], the physical addresses of the NES partner endpoints to be registered in the CCN2ng platform should respect the following format:

https://{host_IP}:{port}/{serviceURL}

[1] For more information, the interested partied can take a look at the Europa site at EU Customs Trader Portal (europa.eu)

and should be supplied by each MS within separate WSDL file per NES service.

The **"https://{host_IP}:{port}"** will be common among one NES's endpoints, allowing the Central CCN2 Team to establish the connectivity between the CCN2ng platform and this NES.

However, an individual endpoint with unique **"serviceURL"** will be defined for each NES service:

- CCN2.Service.Customs.EU.ICS.NESControlBAS;
- CCN2.Service.Customs.EU.ICS.NESErrorNotificationBAS;
- CCN2.Service.Customs.EU.ICS.NESNotificationBAS;
- CCN2.Service.Customs.EU.ICS.NESReferralBAS;
- CCN2.Service.Customs.EU.ICS.NESRiskAnalysisBAS.

It is worth to clarify that although each web service holds its own physical address within the same NES, the Destination ID of the NES itself remains the same among all WSDL files and should respect the following naming convention:

CCN2.Partner.{Country Code}.Customs.TAXUD/ICS_NES.{ENV}

where the **{Country Code}** placeholder is the country code of the NES's country (i.e., two-letter country codes with capital letters as per ISO 3166-1 alpha-2) and the **{ENV}** placeholder depends on the environment with possible values:

- CONF: for the Conformance Testing environment;
- PROD: for the Production environment.

For example, the Destination ID of the Austrian (AT) NES in CONF environment is the "CCN2.Partner.AT.Customs.TAXUD/ICS_NES.CONF".

2.1.8 Which data elements should be used in XI and in GB?

The country code XI (Northern Ireland) is only to be used for the Addressed MS data element. In all other instances, GB should be used for any address or location referred to the United Kingdom, regardless of whether it refers to Northern Ireland or any other location in the UK. Even if the XI code is not used, in case of GB code, the ICS2 checks the postal codes and for those that Northern Ireland post code is detected, XI is identified as IMS. According to CLs that are used for each data element, in case of CL717 - Country code (ICS2 MS) applies, XI is used and in case of CL718 - Country code (ISO 3166) applies, GB is used.

2.1.9 Which country codes can be used under the code list CL718?

According to ICS2 DG TAXUD, the Country codes used in ICS2 are defined in ISO-3166 and COMMISSION IMPLEMENTING REGULATION (EU) 2020/1470. Country codes that are not subject of those two sources, cannot be added in CL718.

2.2 FAQ RELATED TO MS

2.2.1 How can an MS user access ICS2 Monitoring & Business Statistics tool?

In order to grant access in ICS2 Monitoring and Business statistics tool, there are required CCN2 roles that needs to be assigned to the users by National CCN2ng User Administrator.

More details about the CCN2 roles as well as general information regarding the ICS2 Monitoring & Business Statistics tool can be found under the following PICS URL:

https://webgate.ec.europa.eu/pics/group/20607/news/35502.

2.2.2 How may an MS register a planned unavailability?

As per section 3.10 of the Business Continuity Plan document [R057], also published on PICS:

https://webgate.ec.europa.eu/pics/filedepot/20607?fid=80683

MS shall use the ICS2 Business Statistics & Monitoring tool (https://u2s.prod.ccn2.taxud/ics2-mon/index.html) to register and notify each other about their planned unavailability.

2.2.3 How may an MS register an unplanned unavailability?

As per section 3.5 of the Business Continuity Plan document [R057], the NSD of the impacted MS records the unavailability in ICS2 Business Statistics & Monitoring tool: https://u2s.prod.ccn2.taxud/ics2-mon/screen/unavailability.

2.2.4 What is the required role for a user to register a new unavailability?

The required user role is the CCN2 role "Member State Service Support – Availability Manager". With this user role, a national CCN2 user can register unavailability.

2.2.5 Which time zone shall MSs use to declare their unavailability in ICS2 Monitoring & Business Statistics tool?

MS users shall register their planned unavailability in their local time zone. The MON & BS UI expects the date time of the planned unavailability always in the local time of the user. The notification e-mail that will follow the registration of the unavailability will convert the local time of the user into CET.

2.2.6 How may a user download a message from the ICS2 Monitoring & Business Statistics tool?

With the “Member State Service Support – Messages Operator” role a user should access ICS2 Monitoring & Business Statistics tool. The user should access the webpage dedicated to the search of messages and enter the intended search criteria. The list of retrieved messages is displayed, and the user can click on the message (text with blue characters) that would like to export. Then, a pop-up window will appear with more details about this specific message. At the bottom of this pop-up window, user may find an "Export" button. By clicking on this "Export" button, the related message will start to be downloaded.

2.2.7 What should an MS take into consideration regarding S2S user for NES in CCN2ng Oracle Identity Management?

While creating the S2S user for NES in the CCN2ng Oracle Identity Management (OIM) in production environment, the "User Login" and the "Common Name" fields should be identical and should be composed either of capital letters only or lower letters only, without any space character (e.g., “xxx.yyy” or “XXX.YYY”, but not something like “xXx YyY”).

2.2.8 What elements should an MS modify for the preparation of WSDL files to be uploaded on CCN2ng Platform in production environment?

In general, it is suggested to use the same WSDL files that were submitted in the scope of the conformance testing; however, MS should consider modifying the following elements:

- The name of the WSDL files should contain the term ‘’PROD’’ instead of ‘’CONF’’.

For example, the NES Control BAS WSDL file should be named after:
CCN2.Service.Customs.EU.ICS.NESControlBAS_1.0.0_CCN2.Partner.CC.Customs.TAXUD.ICS_NES.PROD_1.0.0.wsdl

- The address parameter should be updated with the details where NES and acknowledgement services will be exposed in the production environment, according to the below format:

http(s)://{Partner_Service_Host_IP}:{Partner_Service_Port}/{Partner_Service_url}

- The term ''CONF'' should be replaced by ''PROD'' in the Destination_ID parameter:

```
<wsa:Metadata>
   <ccn2:ServiceID>CCN2.Service.Customs.EU.ICS.NESControlBAS</ccn2:ServiceID>
      <ccn2:ServiceName>CCN2 Service Customs EU ICS NESControlBAS</ccn2:ServiceName>
      <ccn2:ServiceDescription>CCN2 Service Customs EU ICS NESControlBAS</ccn2:ServiceDescription>
      <ccn2:ServiceVersion>1.0</ccn2:ServiceVersion>
      <ccn2:DestinationID>CCN2.Partner.{Country Code}.Customs.TAXUD/ICS_NES.PROD</ccn2:DestinationID>
      <ccn2:XMLValidation>false</ccn2:XMLValidation>
</wsa:Metadata>
```

- In case that a MS will be using "https" communication, before the upload of the WSDL files, it is required to provide a certificate (signed by your internal or external Certificate Authority) for MS ICS2 application. In this certificate, the Subject Alternative Name (SAN) should contain the Mapped IP (MIP) address. The MIP will be communicated by the Central Network Team to MS through the related ticket and afterwards NA should share the certificate. The WSDL files will be uploaded only after the connectivity is set in place and the certificate is received from the MS.

2.2.9 Are there specific message types (IExxxx) where large messages from CR can be expected?

According to CCN2 Functional System Specifications [R10] the maximum size of a message that is sent through CCN2ng is 20MB. If a message exceeds this size, CCN2 will return an error message of type CCN2-VAL-1005. As observed in the message exchange process, the average byte size of the IE4Q02, IE4Q01 and IE4N05 messages is 20KB or less except of the IE4R02 message. As a general rule, a NES should be able to receive messages up to the defined maximum size of 20MB, since this is the specified size limit. Additional information on the physical attachment, which is stored in CR, is provided in 2.2.12.

2.2.10 What are the technical differences between the .xml versions of the messages for Release 1 & Release 2?

Release 1 and Release 2 messages are distinguished based on XML namespaces and WSDL end-points.

- For Release 1:

The business payload (e.g. IE3F32, …) is in the xml namespace "urn:wco:datamodel:WCO:CIS:1".

The EO will set the eb:AgreementRef at AS4 level to “EU-ICS2-TI-V1.0”.

The webservice end points for the interactions between CR-NES all refer to ‘V1’ versions (e.g., xmlns=http://xmlns.ec.eu/BusinessActivityService/ICS/IRiskAnalysisOrchestratio...V1).

- For Release 2:

The business payload (e.g. IE3F32, …) is in the xml namespace " urn:wco:datamodel:eu:ics2:2".

The EO will set the eb:AgreementRef at AS4 level to “EU-ICS2-TI-V2.0”.

The webservice end points for the interactions between CR-NES all refer to ‘V2’ versions (e.g., xmlns=http://xmlns.ec.eu/BusinessActivityService/ICS/IRiskAnalysisOrchestratio...V2).

The R1 and R2 flows are totally separated, both from a content perspective (business payload in different namespace), as well from a technical end-point perspective. R1 and R2 have different WSDL endpoints.

2.2.11 How can an actor distinguish F30/F32 reply messages in ICS2 Release 2?

In the IE3R01 (acknowledgment) message, the "Specific Circumstance Indicator" attribute is added. The value for this attribute indicates whether it concerns a reply to a F30 or a F32 filing. This attribute is added in the latest iteration of the specifications. The IE3N03 (assessment complete) message does not contain the "Specific Circumstance Indicator" attribute. It declares the assessment complete for a given MRN.

2.2.12 In Release 2, in the messages sent from CR (such as IE4R02/IE4R03), is the hyperlink field URI a link to an external website or to a physical attachment located within the ICS2 CR?

The URI is a link to a CR UI page. The received physical attachment is stored within the CR database, and when the MS recipient wants to retrieve it via a URI, then the CR system generates a URI and populates it in the outgoing message.

The URI generated by the CR system has the following indicative format: “/screen/ensdata/binaryattachment?uuid={UUID}”.

The member state is responsible to add the CR UI context path. With a final result like: “https://ics2domain/ics2-cr-web-ccn2/#/screen/binaryattachment?attachment?uuid={UUID}”.

Indicative example would be: “https://ics2domain/ics2-cr-web-ccn2/#/screen/ensdata/binaryattachment?uuid=HRCM-e35003266956-4091-82d9-0f5a7c7fa9b0”.

When the user visits this URI in the CR UI and has the access rights, they will automatically download the attachment.

2.2.13 Which roles does the user need to have to download the attachment from CR UI?

Related to the Security Protection, the logged in user allowed to download the attachment are, according to Security Plan:

- Member State – Customer Risk Analyst;
- Member State – Customs Risk Management Official;
- Member State – Customs Control and Clearance Officer;
- Member State – Customs Control and Clearance Manager;
- Member State – Business Process Analyst.

More specifically, every user with any of the above roles is able to download the attachment in case the respective NES of the national user has received this URI.

2.2.14 In ICS2 Release 2 a new 'URI' field has been added. The filename field is still mandatory. For an attachment this would be the file name, for a URI, would this be the file path?

The filename field will remain the same in both cases, as it is populated from the incoming message that contains the attachment.

As the CR application is currently implemented, it expects in the incoming messages (e.g., IExxx) to include inside the Binary attachment at least the FileName, the BinaryObject and the MIME type.

In case the incoming message contains a URI, this will be ignored, since only the CR application generates the URI for the outgoing message (e.g., IE4Q02).

2.3 FAQ RELATED TO EO

2.3.1 What does the condition Cxxx for the optionality of data element 'Commodity code' in an IE3F32 message mean?

In the data element 'Commodity code' of an IE3F32 message no condition is applied as referred Cxxx does not exist in ICS2-CFSS-R&C-v1.12[R046R046]. Considering that cardinality for 'Commodity code' is 0..1, the 'Commodity code' is Optional in ICS2 Release 1.

Nevertheless, in ICS2 Release 2, Cxxx is replaced with C3025 in IE3F43 messages and data element 'Commodity code' is Conditional. With respect to IE3F32 message, Cxxx is removed and data element 'Commodity code' is Optional.

2.3.2 What is the process in case an EO would like to add further good items within an existing ENS filling?

It is not possible for new good items to be added to an existing ENS filling. The EO must invalidate the initial ENS filling and to lodge a new one including the new good items.

2.3.3 In case an EO (sender) asks for a message with specific LRN, what is the process for detecting such message at central side?

- The EO should raise this request to its respective NSD for further investigation. If needed, the NSD will raise this issue to the CSD;
- ITSM3-TES will search on ICS2 Monitoring & Business Statistics tool. In case the message cannot be detected, TES will extend the search to Kibana;
- In case no message detected, ITSM3-TES will address the LRN to ITSM3-OPS TAPAS Team in order to check at TAPAS level;
- If no message has been identified after above actions, the LRN will be addressed to ITSM3-OPS Network Team to search on F5 logs.

2.3.4 How are the phone numbers included in the ENS Filings (sent by the EOs) validated from STI? Please also include some examples.

In the STI, when the communication type is “TE”, it is validated against rule R3006.

The pattern, which the rule is checking is the following one:
ITU_E123_PATTERN = "^\\+(?:[0-9] ?){6,14}[0-9]$”

The pattern ^\+(?:[[0-9]] ?){6,14}[[0-9]]$ can be explained as three parts:

1. A string is required in which the first character must be '+' (pattern part: \+);
2. Then, a digit from 0-9 followed by a space character can be repeated minimum 6 times and maximum 14 times (pattern part: (?:[[0-9]] ?){6,14}).

Note that space character after a digit is not mandatory and can appear only one time;

3. After that, a digit from 0-9 is required (pattern part: [[0-9]]).

Please find below some valid and invalid examples:
+3067493493 valid
+30 67493493 valid
+3 0 5 6 7 8 3 valid
+ 30 67493493 invalid (space character after '+')
+30 6743 invalid (digits after '+' are 5 and not 6, space is counted as one repetition with digit 0)
+30 1234567891011123 invalid (characters after '+' are 17, maximum length exceeded)
General note: Regardless the pattern, a valid international phone has the following format: +XX NNN XXXXXXX where XX = country code, NNN = city code, XXXXXXX = number.

2.3.5 Is there any alert triggered before the expiration of the registered certificates in the UUM&DS system?

The user can subscribe to the notifications via ADMIN-EXT, in “Dashboard” section, select “My Notifications” and then select “Expiring user certificate”.

The user should check in due time that the certificate is active, also the user is responsible to renew it before its expiration date. This will ensure that there will be no interruption in operations due to certificate expiration.

2.3.6 Will there be a possibility for EOs with few movements to lodge ENS via a GUI, as it will not be feasible for these EOs to develop a full-fledged ICS2 system-to-system application?

It will be feasible for the EOs to lodge the ENS using EU Customs Trader Portal ICS2 Shared Trader Portal (STI-STP): EO needs to have EORI number, EO needs to successfully log into EUCTP (STI-STP) via UUM&DS authentication and identification. The EO needs to fill all data required for ICS2 ENS filings as per Common Functional Technical Specification.

Using STI-STP EO can also verify the status of their submission, make amendments to submitted ENSs, configure preferences related to notifications and check notifications.

2.3.7 Are there any actions an Airline Company needs to perform in order to announce an ITSP being the technical connection?

There is no need to register the IT service supplier. The ITSP acts as Sender who is delivering the messages to STI on behalf of its clients.

The relation between the Economic Operator (Airline) and IT Service Provider does not need to be registered in anywhere.

On the other hand, in case of any legal dispute, IT Service Provider needs to prove to Customs Authorities that such relation was established during the period when messages were sent to ICS2.

2.3.8 What should be the business content of messages if the user of the services of an ITSP is a GHA (Ground Handling Agent) that represents multiple Airline Companies?

The business content of messages will have to include both the Airline EORI number and GHA (Ground Handling Agent) EORI number in respective ENS messages attributes, in this case:

- Airline Company - would be declarant;
- Ground Handling Agent – would be representative;
- ITSP would be technical sender only in AS4 message.

3 CONFORMANCE TESTING FREQUENTLY ASKED QUESTIONS (FAQ)

3.1 FAQ RELATED TO MS

3.1.1 What is the use of Synergia and how can a user obtain a Synergia account?

For the purposes of CT campaign and later for the operations in production, the official platform to be used is the Synergia ESS. All the service requests, requests for information, notifications and incidents that might occur as well as investigations and resolutions for the issues or the problems, will be registered and handled via this ticketing system.

As per MS – CTOD [R16], in order to obtain a Synergia account, the user shall navigate to ITSM Portal (https://itsmtaxud.europa.eu/sites/itsm-portal/home.html) and choose "Not registered yet?" and provide the filled-in and signed by NPTL form to ITSM Service Desk (support@itsmtaxud.europa.eu).

3.1.2 What is the usage of MON&BS as supportive tool to the EO-Self Conformance Campaign?

MS operators shall access ICS2 Monitoring and Business Statistics tool in CONF environment to consult the registered EO Self-Conformance Test campaigns and to follow up the execution of the related business scenarios. The aim is for MSs to provide meaningful assistance to EO during Self-conformance test campaign. The MS might also help EO to configure its access point or communication paths in case the EO has any temporary issue accessing STI-STP. With the Member State Service Support – Monitoring Operator role a user is involved in the following use cases:

- Management of Trader Preference:
  - Consult the trader preferences;
  - Modify a trader preference;
  - Create a new trader with his/her respective preferences;
  - Manage a trader preference.

- EO Self-Conformance Test Campaign:
  - Consult the EO Self-Conformance Test campaigns (consult the business scenarios of each test campaign and consult the messages of each business scenario[2]);
  - Consult successful EO Self-Conformance Testing;
  - Upload successful EO Self-Conformance Testing;
  - Search EO messages not compliant with a successful Self-Conformance testing.

It is important to highlight that the use of ICS2 MON&BS tool is available only to the MS and EC users. The EO can manage ICS2 related preferences and Self-register a conformance test campaign through the STI-STP. In this case, the execution of the Campaign will be tracked by STI.

3.1.3 Can an MS user access STI-STP in Conformance Environment?

An MS user can access STI-STP by using a using a dummy – EORI/certificate. The use of "fake" EORI will allow to access to STP interface only. Sending the messages to STI-STP will require development of AS4 gateway and the compliance to ICD specification [R04]. The primary tool to support EOs during Self Conformance Campaign is ICS2 MON&BS tool which provide all views for NA teams.

[2] This feature is available only in the CONF environment.

3.1.4 Who is involved in the IsAlive (connectivity verification)?

Prior to the start of CT activities, an MS should verify the connectivity of the NES with ICS2. To do so, the MS has to send an isAlive request towards the Risk Analysis Orchestration Business Application Service of the ICS2 Common Repository as defined in section 6.1 of the [R11]. This activity will take place in the ticket that will be registered with the submission of the WSDL files. On the same ticket, the Central Operations Team will send isAlive request from central side towards the NES services to confirm that these are up and running. IsAlive tests must take place at least one (1) week before the CT starting date. ITSM3-TES should highlight this activity during the Coordination call. Only when isAlive tests from both central and NES sides are successful, an MS can proceed with CT execution (functional testing).

3.1.5 How can an MS verify that they have sent a successful isAlive test in Conformance Environment of ICS2 R2?

The MSs can submit an isAlive request towards the Risk Analysis Orchestration Business Application Service (CCN2.Service.Customs.EU.ICS.RiskAnalysisOrchestrationBAS) at any time when CONF environment is up. This isAlive request can be sent by using the template available in MS – CTOD, Annex J [R16R16R16] ensuring that the correct address is also being used https://s2s.conf.ccn2.taxud:8441/CCN2.Service.Customs.EU.ICS.RiskAnalysisOrchestrationBASV2 and **that the soap requests are updated with V2**.

<adr:To>partner:CCN2.Partner.EU.Customs.TAXUD/ICS_CR_**V2**.CONF</adr:To>

<adr:From>

<adr:Address>partner:CCN2.Partner.XX.Customs.TAXUD/ICS_NES_**V2**.CONF</adr:Address>

</adr:From>

<adr:ReplyTo>

<adr:Address>partner:CCN2.Partner.XX.Customs.TAXUD/ICS_NES_**V2**.CONF</adr:Address>

</adr:ReplyTo>

<adr:FaultTo>

<adr:Address>partner:CCN2.Partner.XX.Customs.TAXUD/ICS_NES_**V2**.CONF</adr:Address>

</adr:FaultTo>

Also, in this template, each MS should adjust the <From>, <ReplyTo>, <FaultTo>, <Username> and <Password> fields accordingly.

Upon implementation of the above action, NES must receive back a HTTP 202 status response, validating that the service is available.

3.2 FAQ RELATED TO EO

3.2.1 Who is considered a Sender in the context of the ICS2 system?

ICS2 introduced the role of Sender, which consists of the system actor that technically constructs and exchanges the messages with the STI in accordance with the ICS2 message specifications. To guarantee integrity, and the non-repudiation of origin and receipt, the party acting as a Sender must register a digital certificate used to seal the exchanged messages in the UUM&DS system under its EORI.

The Sender can be the declarant/representative itself or it can be an IT Service Provider (ITSP) contracted by the declarant/representative. To be noted is that in such case, the declarant/representative remains declarant/representative. The ITSP is a technical actor that is also identified by an EORI as used in the technical AS4 message header.

3.2.2 Who is considered an IT Service Provider (ITSP) in the context of the ICS2 system?

An ITSP is any party that delivers IT Services to a declarant/representative by operating an AS4 access point as a Sender. An ITSP must be identified (EORI & digital certificate) and registered in UUM&DS to be authorized to exchange messages with the Shared Trader Interface (STI).

Therefore, a party that provides a Software as a Service (SaaS) platform to an ITSP, or to a declarant/representative, is not an ITSP. It only provides technical components that require additional specific operational configuration to properly function as a Sender. This configuration occurs under the responsibility of the ITSP or declarant/representative that procured the SaaS services. ICS2 requirements for this configuration are documented in ICS2 Interface Control document [R04].

3.2.3 Is a declarant/representative that uses an IT Service Provider (ITSP) to lodge an ENS in the ICS2 system obliged to register a digital certificate in UUM&DS?

No. Only parties that operate an AS4 access point as a technical 'Sender' of ENS filings must register a digital certificate in UUM&DS. A Sender is understood as a system actor in the context of the ICS2 system and is authenticated and authorized from the system security point of view to exchange messages with the STI. The declarant/representative that uses an IT Service Provider (ITSP) doesn't need a digital certificate registered in UUM&DS. Only the declarant/representative EORI included in the business payload of the messages needs it.

3.2.4 Which documents should an EO or ITSP Provider consult for their preparation prior to conformance testing?

Trade association representatives can find the published versions of the EO Self-Conformance Testing related documentation on CIRCABC. All EOs can find the publicly accessible EO self-conformance Testing related documentation on the public CIRCABC and the EO Self-Conformance Testing related training materials in Customs & Tax EU Learning Portal (europa.eu).

For the smooth preparation prior to CT activities, EOs should read and comprehend all the relevant documentation that has been provided to EOs:

- ICS2 Harmonised Trader Interface Specifications[R04];
- ICS2 EOs Common Technical System Specifications package for ICS2 Release 2 [R12**Chyba! Nenašiel sa žiaden zdroj odkazov.Chyba! Nenašiel sa žiaden zdroj odkazov.**].

Particularly, the consultation of the below documents is considered essential during the CT execution:

- Conformance Test Organisation Document (CTOD) for EO for Release 2 [R13];
- Test Design Specifications for EO Conformance Test Cases for Release 2 R15 [R15R15R15**Chyba! Nenašiel sa žiaden zdroj odkazov.Chyba! Nenašiel sa žiaden zdroj odkazov.Chyba! Nenašiel sa žiaden zdroj odkazov.Chyba! Nenašiel sa žiaden zdroj odkazov.Chyba! Nenašiel sa žiaden zdroj odkazov.**];
- Test Design Specifications for EO Conformance Test Scenarios for Release 2 [R14];
- Trainings that will be provided by National Administrations to EOs:
    - ICS2 Conformance Test;
    - Digital certificates and registration of certificates;
    - NA services and support to EOs.
- Material which will be made publicly available in Europa webpage:
    - Self-Conformance Test (EO-CT);
    - UUM&DS system: Your passport to EO applications (EO-UUM&DS);
    - Business Continuity Plan (EO-BCP);
    - Use of STP for ENS registration (EO-STP).

In general, the latest accepted version of the EO Self-Conformance Testing related documentation is stored on:
https://circabc.europa.eu/ui/group/ea5f882b-9153-4fc1-9394-54ac8fe9149a/library/3a95f619-b6f0-4286-9673-466190f8fb88?p=1&n=10&sort=modified_DESC.

3.2.5 Which steps should be followed by an Economic Operator (or an ITSP) to establish the AS4 connectivity prior to the conformance testing?

- Deploy one or more Access Point(s) according to HTI Interface Control Document specifications [R04];
- Obtain a TLS certificate to be used at the transport layer (https) for identifying itself following the 2-way TLS security mechanisms;
- Obtain a sealing certificate to be used for sealing at message layer (see section 4.6.2 of the HTI Interface Control Document [R04];
- Sender must be registered by Customs Authorities following the agreed national procedure. This includes the upload of the sealing certificate;
- Configure their own AS4 Access Point(s) in STI-STP:
    - Log in on EUCTP and access STI-STP via UUM&DS authentication and identification;
    - Select "Manage Preferences"[3] from STI-STP menu;
    - Add information on “Party Id definition”:
        - Provide the Party ID (The Party ID format is defined in section 4.2.2.1 of the HTI Interface Control Document [R04]);
        - Define Message Exchange Pattern (“push” or “pull”);
        - Provide the Endpoint (i.e., URL) (Available if the MEP is “push”);
        - Provide the Certificate Authority that issues the TLS certificate;
        - Insert Technical details (Name, Email address, Phone).
    - Add information on “Default communication path”:
        - Select Business domain (Postal, Maritime, Air, Rail, Road, Express);
        - Select Communication path (UI, S2S);
        - Party Id (Mandatory in case the communication path is S2S).

[3] User manual is provided as part of the STP application and supported by training material (to be delivered).

3.2.6 How can an EO ensure that a request for the Access Point configuration has been sent to ITSM?

In "Manage Trader Preferences" section of STI-STP, the EOs will need to choose the "Add Party ID" and fill in the requested information of their Access Point. In order to send the request for the Access Point configuration to ITSM, they should press "Save & Notify" and afterwards "Save Trader Preferences". Then the system will display to the user the below messages:

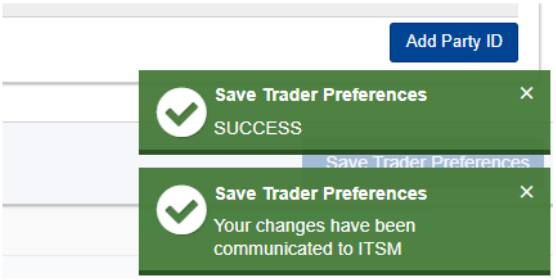

Figure 1: Save Trader Preferences

3.2.7 How can an EO delete a configured access point through STI-STP?

The EO should first delete the respective communication path of this access point and then she/he will be able to delete the access point.

3.2.8 How many certificates should be used by the EOs?

Each EO should obtain:

- A TLS (Transport Layer Security) certificate from a trusted Certificate Authority 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;
- A digital certificate to be used for sealing at message layer, which should be registered in the National UUM&DS Application or in the Central UUM&DS Application (see section 0). In case that an EO uses the services of an ITSP, then this EO does not need to register this certificate since it will be done by its ITSP.

3.2.9 How can an EO verify that the TLS (Transport Layer Security) certificate they have obtained is from a trusted Certificate Authority?

A trusted Certificate Authority in the TLS context can be a commercial CA trusted by DG TAXUD. An Economic Operator can consult the list of trusted Certificate Authorities on CIRCABC and check if their TLS is included in the list.

3.2.10 From which Certificate Authorities (CAs) can an EO issue its certificate for ICS2 message sealing (signing)?

The digital certificate for message sealing must be issued by a Certificate Authority (CA) that is on the official EU wide LOTL[4] or on the National Customs alternate list of the Member State to whom National UUM&DS would like to register this certificate.

The Certificate Authorities (CAs) on the LOTL can be divided into two categories:

1. CAs that issue qualified certificates;
2. CAs on the LOTL that issue non-qualified certificate for e-signature/sealing.

CAs for both categories are published in https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home.

A certificate issued by the CAs on the LOTL can be used to perform registration at a National Customs Authority of any EU Customs authority. Alternatively, an EO can use a certificate issued by other CAs as long as the CA is present on the "National Customs Alternate List"[5]. Certificates issued by such CA can only be used to perform the registration at National Customs Authority.

3.2.11 If a company is on the LOTL does this mean that all certificates issued by this company fulfill the requirements of ICS2?

The requirement for ICS2 is that the CA (meaning the root certificate) that issued the 'advanced seal certificate' is on the LOTL. It is not the company that must be on the list, but the actual CA root certificate that directly or indirectly issued the certificate. Most companies issue all kind of certificates using different CA root certificates depending on the trust level required. Hereby some of the CA root certificates of a company are on the list and others are not.

3.2.12 Who is responsible for managing the National UUM&DS alternate list?

An MS is responsible for managing the National Customs alternate list.

3.2.13 Who is responsible for managing the LOTL?

The actual content of LOTL is managed and published by each MS.

3.2.14 How does an EO communicate its sealing certificate?

Each EO should register its sealing certificate in the National UUM&DS Application of its Member State. In case there is no National UUM&DS application, the Member State should decide if Central UUM&DS application should be used. The process for the latter case is described in the UUM&DS Central Certificate Registration Manual for EOs, which is published in PICS:

https://webgate.ec.europa.eu/pics/filedepot/24416?fid=62623

3.2.15 How can a user verify the successful registration of EO System digital certificate?

Considering that the registration of each EO System certificate is done in the corresponding National UUM&DS application, where neither DG TAXUD nor the contractors provide any access, the successful certificate registration may only be verified by the EO itself.

Nevertheless, the successful certificate registration is a precondition for the execution of all EO functional test cases. This means that, in case that the certificate was not correctly registered, TAPAS will return the EBMS:0004 exception with subcode: A001 to the EO and will not allow any further EO message exchange.

3.2.16 Can an EO register the same sealing certificate in CONF and PROD?

An EO can use the same sealing certificate that has been used for CONF as long as it is registered in UUM&DS, but it has to be registered also in UUM&DS in PROD.

3.2.17 What is usage of sealing certificate in AS4 message exchanges with ICS2?

The EO has to configure AS4 access point to sign (seal) the AS4 messages with the given certificate and should embed the full certificate path inside the AS4 message. This is established by configuring set-up to embed a wsse:BinarySecurityToken with a valueType attribute of type X509PKIPathv1 as per section 4.6.2 of ICS2 HTI – ICD [R04]. A certificate path is the chain of certificates from the Root Certificate of the CA - intermediate certificate issued by the CA/n - EO leaf certificate as issued by the CA. This is a critical aspect.

3.2.18 Can an EO use the same certificates as ICS2 Release 1 for ICS2 Release 2?

An EO can also reuse the certificates already in use by the first access point in Release 1. This way nothing must be procured and no new registrations have to occur in UUM&DS.

In that scenario the EO will simply have to register a second partyID for their EORI number:

Existing access point: partyId = GR0777555666 (= simply their eori number);

New access point: partyId = accesspoint2@GR0777555666 (= in line with HTI-ICD section 4.2.2.1).

3.2.19 How can a user register a sealing certificate depending on if the EO is the holder of the key or not?

Certificate registration can be performed in one of the following ways:

1. Holder of the Key:

    a. Log in as an EO (in the WAYF) and access Admin-Ext (in case of Central Certificate Management) or the relevant MS site (in case of Local Certificate Management);

    b. EO registers the certificate using the certificate's private key.

2. Not Holder of the Key: (process valid ONLY for Central Certificate Management)

    a. EO creates a delegation to one of the employee;

    b. EO shares public key with the employee;

    c. Employee registers his own certificate (as Holder of the Key);

    d. Employee logs in using the delegation from the EO;

e. Employee registers the EO's certificate (using the public key) and signs the registration with his own private key (from the certificate he has already registered).

3.2.20 How can an EO use UUM&DS system?

The following URL redirects to an online course that provides EO with specific information about how to use the UUM&DS. Upon completion of the course, an EO will be able to confidently work with the UUM&DS and carry out delegation, certificate registration and authentication processes within the UUM&DS process flow.

Attend course by accessing the following URL:

https://customs-taxation.learning.europa.eu/course/view.php?id=494&section=1

3.2.21 Which UUM&DS Business Profiles should an EO have in the scope of Self-Conformance Test Campaign?

In the scope of Conformance Testing Campaign, an EO or a Customs Representative should have 'STISTP_EXECUTIVE' and/or 'STISTP_CONFIGURATOR' business profiles to grant the access rights of the required STI-STP roles.

UUM&DS Business Roles vs Corresponding STI-STP roles

UUMDS type of actor	Delegated from	UUMDS business profile configured as available	STI-STP role
Economic Operator (Trader and ITSP)		EXECUTIVE	EO-DECL
		CONFIGURATOR	EO-CONF
		EXECUTIVE_LIMITED	EO-PNA
		CONSULTATIVE	EO-NOP
Employee*	Economic operator	EXECUTIVE	EO-DECL
		CONFIGURATOR	EO-CONF
		EXECUTIVE_LIMITED	EO-PNA
		CONSULTATIVE	EO-NOP
Customs Representative		EXECUTIVE	EO-REP
		CONFIGURATOR	EO-CONF
Employee*	Customs Representative	EXECUTIVE	EO-REP
		CONFIGURATOR	EO-CONF

Figure 2: UUM&DS & STI-STP roles

3.2.22 How can type D countries who do not have access to UUM&DS CONF and PROD delegate UUM&DS Business Profiles?

Type D countries have their own Subdomain Administrator who is managing the national user accounts. A Member State needs to contact their national Subdomain Administrators.

3.2.23 Can an IT Service Provider perform the CT activities using the EORI number of its customers (airline companies) instead of using its own?

The messages sent to STI need to be sealed with ITSP digital certificate registered in UUM&DS (no need to use Airlines certificates or UUM&DS delegation function).

In case that an EO (Airline company customer of ITSP) is not a Sender and the EO uses the services of an IT Service Provider, then this EO does not need to register this certificate since it will be done by its ITSP.

The EORI number of EOs (Airline companies) is to be used only in the business payload of the messages.

In case ITSP is providing the services to a few parties, he may use many EORIs in the business message payload, each time the EORI of the party (Declarant) on whose behalf messages are sent.

When an ITSP offers its services to several EOs of the same business role, then, during Self-conformance testing, it is required to perform only one campaign, not a separate campaign for each EO.

Relevant information can also be found in the following link https://taxation-customs.ec.europa.eu/business/customs-procedures-import-and-export/customs-procedures/economic-operators-registration-and-identification-number-eori_en.

3.2.24 Can an EO use two separate IT Service Providers to comply with ICS2 Release 2 requirements? If yes, can the two IT Service Providers perform their Conformance Testing separately?

An EO can use two separate IT Service Providers to comply with ICS2 Release 2 requirements. For example, one for mail and another for cargo transportation. An EO has the ability to perform the Conformance Testing at any time within the timeframe of execution and as many times needed, even separately and with the IT Service Providers of its choice.

3.2.25 Do EOs need an EORI if they are not established in the customs territory of the Union?

Persons not established in the customs territory of the Community should request the assignment of the EORI number to the customs authorities of the EU country responsible for the place where they first lodge a declaration or apply for a decision. It is irrelevant if the economic operator is a company (legal person) or a natural person.

If an IT Service Provider will act on behalf of multiple airline companies (EOs), the ITSP who is the actual party sending the messages to Shared Trader Interface (Sender), needs to have the EORI number and digital certificate from the LOTL registered in one of the European UUM&DS.

3.2.26 Which EORI number should an EO use?

- In case that an EO implements its own access point, then the EO holds both Sender and Declarant roles and should use its unique EORI number, in order to register its certificate and also use it in the functional payload (ENS filing);
- In case that an EO uses ITSP services, then the IT Service Provider holds the Sender role and should register a certificate with its own EORI number. However, the EO still holds the Declarant role and should use its own EORI number for the ENS filing.

3.2.27 How can an EO request the addition of an EORI in EOS/CRS Conformance Environment?

If an EO needs to use for their Conformance Campaign an EORI that does not exist in EOS/CRS then they should contact their Responsible MS. The MS is able to create the EORIs in EOS, which will be replicated to CRS. In both environments, Conformance and Production, EOS/CRS and ICS2 systems

are integrated. Conformance and Production thought are separated environments, if an EORI is needed for CT, the EORI should be logged in Conformance. If it is needed in Production, then the encoding should happen in Production. In the eventual scenario that the MS don't manage to encode the EORIs on their side for any reason (e.g. access rights or any temporary issue), they could eventually log a ticket to Central Service Desk.

3.2.28 How should an EO configure P-Mode?

An EO should follow Annex II P-MODES SUMMARY from ICS2 HTI – ICD [R04] also published on PICS:

https://webgate.ec.europa.eu/pics/filedepot/20607?cid=19248&fid=79935

Specifically, Annex II includes all the required P-Mode configuration parameters. In addition, an EO should consult section 4.6.3 of the same documentation, which describes a particular configuration on the handling of the TLS certificates that cannot be expressed as a P-Mode parameter but is nevertheless an AS4 configuration element.

3.2.29 In the response messages an EO receives from TAPAS, what is a globally unique identifier for a specific multipart/related MIME part?

Such unique identifier is the eb:MessageId + the Content-Id of the part (In AS4 terms: eb:MessageId element value + eb:PartInfo@href attribute value of the given part).

3.2.30 What should be the "MPC" use attribute in an incoming user message?

According to ICS2 HTI – ICD [R04] section 4.1.3.3, for an incoming user message the @mpc attribute should not be specified, thus, this results in the usage of the default MPC.

3.2.31 Which is the IP address for sending messages from TAPAS to EOs?

The TAPAS central side is using the IP address 147.67.18.4 for sending messages from TAPAS to EO side. Traffic from this IP needs to be allowed through the EO firewalls to be able to RECEIVE messages from TAPAS Central side.

3.2.32 What network ports are allowed to be used on EOs side for traffic through central firewall?

For security reasons, the only network ports allowed are 80, 443, 9443, 9444, 9445, 8443, 4443, 8445, 9081, 9082 and 9003.

If other ports are to be used by EOs then Central Service Desk should be notified to implement a change to allow traffic on that port through central firewall.

3.2.33 Which are the most common issues identified during the ICS2 connectivity setup trials with EOs/ITSPs?

- In the messages sent to TAPAS, most EOs/ITSPs erroneously include the leaf certificate instead of the full certificate chain, (please check section 4.6.2 from the ICS2 HTI – ICD [R04]);
- The receipt messages sent from an EO to TAPAS, it is observed to be wrongly signed (the empty SOAP body is not part of the signature). The receipt message occurs when an EO receives a user message from TAPAS. Then, the EO responds back with a receipt message indicating that it has successfully received the user message from TAPAS. The SOAP Body of this receipt

message should be signed, otherwise TAPAS fails to validate the receipt messages received back and finally considers that the initial user message was never sent to EO;

- The Economic Operator obtained a digital certificate and registered it in UUM&DS, however the selected security parameters are wrong, either hash function/signing algorithm or AgreementRef ("AgreementRef" is the parameter which defines which version of messages is used, for Release 1/ Release 2). ICS2 Interface Control Document [R04] requires the use of the following hash function sha256 and signing algorithm rsa-sha256. See ICS2 HTI – ICD [R04] section Annex 2 Section 6. Concerning "AgreementRef", "EU-ICS2-TI-V2" is used for ICS2 Release 2 messages and "EU-ICS2-TI-V1.0" is used for Release 1 messages.

3.2.34 Which elements should contain unique values in the ENS fillings?

The Technical Message header ID number should be unique per declarant for each message sent by an EO. The LRN number should be unique too, otherwise the message will be rejected with an IE3N99. There is a requirement for Transport document (master level) to be unique for at least 1 year. For Transport document (house level) it is advised to be unique, but it is not mandatory. Within the same house level ENS filing there should not be repetitive Transport document (house level) number. In F32 messages combination of Transport document (house level) and Reference number/UCR should be unique for at least one year.

3.2.35 What is the meaning of the N99 error codes?

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. The validation code will indicate the precise error, which is referring to CL723 (Functional Error Codes), listed in ICS2-HTI-CL-(2022-05-2023)-v2.01 [R17].

3.2.36 Which is the correct expression for the time values inside fillings?

For all elements that contain timestamps, the values should be expressed in UTC format. This expression is the GMT zone followed by letter "z". No local time zones or central European time should be used in that expression. An alternative way could be to use the local time followed by an offset (which points out the difference of that local time from the GMT). For more information, please refer to section of 4.2.1 of ICS2 HTI – ICD [R04].

3.2.37 How should an EO raise an issue to Service Desk?

Structural issues with the system of the EO should be addressed to the National Service Desk where the EO has registered its EORI number.

The issues that are related with the certificates of an EO should be addressed in the National Service Desk where the certificates were registered. This will be in the majority of cases, the National Administration where the EORI number was registered but can differ from that sometimes, in particular when an ITSP for operating an ICS2 access point is used for the submission of messages by the EO.

The National Service Desk is responsible for resolving any issue/incident that occurred or dispatch them to Central Service Desk. The responsible National Administration will share the information of the relevant tickets (that are registered in SYNERGIA ESS) with the EO.