



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

Conformance Test Organisation Document for Economic Operators

ICS2 CTOD for EOs for Release 3

Date:	19/05/2023
Status:	Submitted for acceptance (SfA)
Version:	1.30 EN
Author:	ITSM3-TES
Approved by:	DG TAXUD
Reference number:	DLV.7.10.2
Public:	DG TAXUD external
Confidentiality:	Publicly available (PA)

Document control information

Property	Value
Title	Conformance Test Organisation Document for Economic Operators
Subtitle	ICS2 CTOD for EOs for Release 3
Author	ITSM3-TES
System Owner	DG TAXUD Unit A3 Risk Management and Security
Solution Provider	DG TAXUD Unit B3 Customs Systems
DG TAXUD Project Manager	DG TAXUD Unit B3 Customs Systems
Version	1.30 EN
Confidentiality	Publicly available (PA)
Date	19/05/2023

Contract information

Property	Value
Framework Contract	TAXUD/2021/DE/115
Specific Contract	SC10

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
1.30	19/05/2023	Implementing minor changes requested by DG TAXUD Document submitted for acceptance (SfA)	I/R	Added section 3.2.3 Modified 2.2, 3.3.1, 3.3.3
1.20	14/03/2023	Document submitted for acceptance (SfA)	I/R	All
1.10	24/02/2023	EOs Operations Checklist (v2): Annex B Inserted DG TAXUD certificate for signing the production messages: section 3.3.3 Submitted for Review (SfR) to DG TAXUD	I/R	3.3.3, ANNEX B
1.00	14/12/2022	Document submitted for acceptance (SfA)	I/R	All
0.10	28/11/2022	Document submitted for review (SfR)	I/R	All
0.01	15/11/2022	Document submitted for information (SfI)	I/R	All

¹ Action: I=Insert R=Replace

Configuration management: document location

Previous accepted version of this document is available on [Circabc](#).

Table of contents

1	INTRODUCTION	6
1.1	Document Purpose	6
1.2	Target audience	6
1.3	Scope	6
1.4	Structure	7
1.5	Reference Documents	7
1.6	Applicable Documents	8
1.7	Abbreviations & Acronyms.....	8
1.8	Definitions.....	9
2	TESTING ORGANISATION	13
2.1	Roles and Responsibilities.....	13
2.1.1	Economic Operator (EO) - Sender	13
2.1.2	IT Service Provider (ITSP).....	14
2.1.3	National Customs Authority / National ICS2 Project Team.....	14
2.1.4	DG TAXUD - European Commission.....	14
2.1.5	ITSM Contractors of DG TAXUD	14
2.1.6	National Service Desk (NSD).....	15
2.1.7	Central Service Desk (CSD).....	15
2.2	Planning and Milestones	16
2.3	Conformance Campaign Procedure.....	16
2.3.1	Prerequisites	16
2.3.2	Conformance Campaign Set up and Execution	17
2.4	Communications.....	18
2.5	Complementary Information	18
2.6	MON&BS as Supportive Tool (Only for MS Operators).....	19
2.7	STI-STP and Roles Requirements	19
2.8	EO Self-Conformance Test Execution	20
2.8.1	Set up a Conformance Campaign	20
2.8.2	Run the Conformance Campaign	24
2.8.3	Validate the Conformance Campaign Results	26
3	CONNECTION TO ICS2 CONFORMANCE TEST ENVIRONMENT	27
3.1	Registration of Certificates in UUM&DS	27
3.2	Communication Protocols	27
3.2.1	Establishment of Access Point(s)	28
3.2.2	Connectivity Verification	28
3.2.3	Connectivity URL information.....	29
3.3	Security	29
3.3.1	Certificate Requirements	29
3.3.2	Certificate Authorities	30
3.3.3	Certificates on Central Side.....	31
3.3.4	UUM&DS Business Profiles Requirements	31
4	CONFORMANCE TEST SPECIFICATION	33
4.1	Test Categories.....	33
4.2	Test Data	33
4.3	Test Validation	34

4.4	Test Incidents/Error/Problem Handling	34
4.5	Acceptance Criteria	35
5	RISK AND MITIGATION PLANNING.....	37
6	AFTER CT ACTIVITIES - OPERATIONS CHECKLIST	38
7	ICS2 TRANSITION STRATEGY FROM R2 TO R3.....	39
7.1	Deployment Window	39
7.1.1	Rail carriers deployment window when complete ENS is filed	39
7.1.2	Rail carriers deployment window when multiple ENS filings are filed	40
7.1.3	Road carrier deployment window.....	40
7.1.4	Maritime carrier and house filer deployment windows	40
7.1.5	Express operators deployment window for consignments on road.....	41
7.2	Principles.....	41
7.3	Impact of ICS2 Transition from Release 2 to Release 3	41
7.3.1	Impact on economic operators already part of ICS2 Release 2	41
7.3.2	Impact on operators that start filing Release 3 ENS filings.....	41
	ANNEXES	42
	Annex A: EO Project Plan Template	42
	Annex B: EO Operations Checklist for moving to Production	42
	Annex C: Incident Management Form.....	42
	Annex D: Guide to register certificate in UUM&DS	42
	Annex E: UUM&DS System Online Course	43
	Annex F: How to Access CIRCABC and Customs & Tax EU Learning Portal	43
	Annex G: EO Consolidated CT Report.....	45

List of tables

Table 1: Reference documents	7
Table 2: Applicable documents	8
Table 3: Abbreviations and acronyms	9
Table 4: Definitions	12
Table 5: List of prerequisites to be fulfilled	17
Table 6: List of actions to be performed during Conformance Campaign	17
Table 7: Business Profiles vs Corresponding STI-STP roles	32
Table 8: Priority calculation table	35
Table 9: NSD - Target and limit values for the incident management	35

List of figures

Figure 1: EO Conformance Testing	6
Figure 2: Communication channel among EO, NSD and CSD	15
Figure 3: Duration of EO Conformance testing	16
Figure 4: Manage Preferences	21
Figure 5: Register Self-Conformance Test Campaign	22
Figure 6: Register a Conformance Test Campaign - Business Role selection step	23
Figure 7: Register a Conformance Test Campaign – Business Scenario configuration step (no ENS Filing selection required)	24
Figure 8: Self-Conformance Test Campaign	25
Figure 9: Register a Conformance Test Campaign – ENS Filing selection step	26
Figure 10: TLS vs Message Security	30
Figure 11 Rail carriers deployment window when complete ENS is filed	39
Figure 12 Rail carriers deployment window when multiple ENS filings are filed	40
Figure 13 Road carrier deployment window	40
Figure 14 Maritime carrier and house filer deployment windows	40
Figure 15 Express operators deployment window for consignments on road	41
Figure 16: Create an account - EU Login	43
Figure 17: Complete registration in Customs & Tax EU Learning Portal	44
Figure 18: CIRCABC - Main Page	44

1 INTRODUCTION

1.1 DOCUMENT PURPOSE

This document defines the Conformance Testing procedure that needs to be applied by the Economic Operators (EOs) in order to perform the CT for their systems within the scope of ICS2 Conformance Testing (CT) for Release 3. The main purpose of this Conformance Test Organisation Document (CTOD) is to set out and explain the practical arrangements regarding the Self-Conformance Testing (CT) campaign, encompassing the necessary planning, preparation and execution activities. This document is complemented by the ICS2 Test Design Specifications for EO Conformance Testing [R03] [R04], which describe the business scenarios to be tested by the EOs.

1.2 TARGET AUDIENCE

The target audience for this document is any person or service in the Economic Operators Project Team, National Administrations Project Team and in the Central DG TAXUD Teams involved in:

- The development of the business scenarios, test scripts and test data for ICS2;
- The organisation and the coordination of the CT activities for ICS2;
- Preparing and implementing the EO CT campaign for ICS2;
- Executing the EO CT campaign for ICS2;
- The Quality Assurance for the ICS2 CT campaign.

It is assumed that the reader possesses the required knowledge of the ICS2 system, has studied the reference documents and where necessary the HTI Interface Control Document [R01].

1.3 SCOPE

The Conformance Test Organisation Document (CTOD) covers the organisation, preparation, execution and follow-up of the ICS2 EO Conformance Testing campaign. The CT campaign aims at Self-testing the compliance of the EO systems with the system-to-system (S2S) interface specifications of the Harmonised Trader Interface (HTI). This includes compliance with the AS4 interface profile, usage of Digital Certificates, semantic and syntactical validation of the messages sent by traders, testing the notifications that are dispatched towards traders and their responses to ICS2 requests. During the EO Self-Conformance Testing, the NES systems' input is simulated by mock-ups.

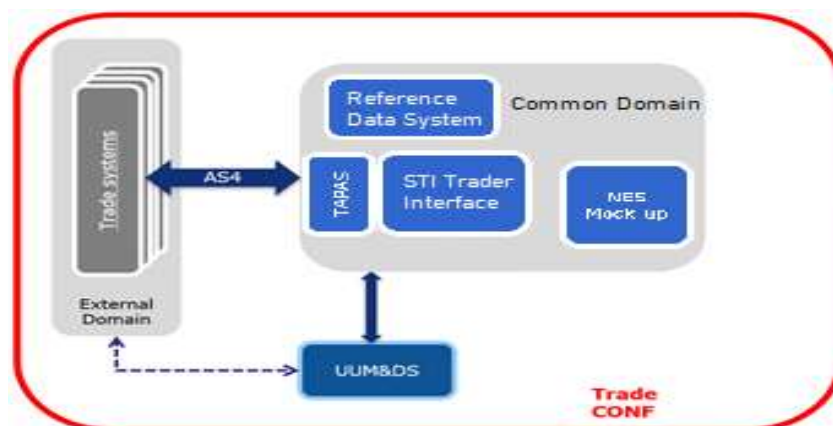


Figure 1: EO Conformance Testing

1.4 STRUCTURE

This document is organised as follows:

- **Chapter 1 – Introduction:** describes the scope and the objectives of the document;
- **Chapter 2 – Testing Organisation:** extensively presents the CT organisation;
- **Chapter 3 – Connection to ICS2 Conformance Test Environment:** presents the prerequisites that EOs need to connect to the ICS2 system;
- **Chapter 4 – Conformance Test Specification:** briefly summarises the test categories, test data, validation, error and problem handling, as well as acceptance criteria for closing the Conformance Testing;
- **Chapter 5 – Risk and Mitigation Planning:** presents the risk and mitigation planning;
- **Chapter 6 – After CT Activities - Operations Checklist:** briefly summarises the activities that should be accomplished after completion of the Conformance Test campaign;
- **Chapter 7 – ICS2 Transition Strategy from R2 to R3:** highlights the aspects of the transition which need to be further aligned and agreed among all involved parties – Member States, the Commission and the economic operators;
- **Annexes:** contain the various templates to be used during CT.

1.5 REFERENCE DOCUMENTS

Ref.	Title	Originator	Version	Date
R01	HTI Interface Control Document	DG TAXUD	3.30	02/03/2022
R02	ICS2 HTI-Definitions	DG TAXUD	1.11	16/03/2020
R03	Test Design Specifications for Economic Operator Conformance Test Scenarios for Release 2 & Release 3	SOFT-DEV	2.40	21/10/2022
R04	Test Design Specifications for Economic Operator Conformance Test Cases for Release 2 & Release 3	SOFT-DEV	2.00	27/12/2022
R05	eDelivery AS4 Profile	https://ec.europa.eu/cef-digital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.15	1.15	11/11/2020
R06	ICS2 Monitoring Use Case Specifications	SOFT-DEV	5.70	19/09/2022
R07	UUM&DS – User Guide	DG DIGIT	3.70	09/02/2021
R08	ICS2 Harmonised Trader Interface Specifications	DG TAXUD	2.02	22/05/2022
R09	ICS2 EOs Common Technical System Specifications for ICS2 Release 2 & Release 3	DG TAXUD	N/A	Sept 2022
R10	ICS2 Transition from R2 to R3 strategy	DG TAXUD	0.30	15/09/2022

Table 1: Reference documents

1.6 APPLICABLE DOCUMENTS

Ref.	Title	Originator	Version	Date
AD01	TEMPO – Glossary of Terms	DG TAXUD	3.11	23/08/2013
AD02	Specific Contract 10	DG TAXUD	N/A	01/06/2022

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
AS4	Applicability Statement 4
CA	Certificate Authority
CCN2	Common Communications Network 2 (middleware)
CONF	Conformance Environment
CPT	Central Project Team
CRS	Customs Reference System
CS/RD2	Common Service for Reference Data version 2
CSD	Central Service Desk
CT	Conformance Testing
CTAS	Conformance Test Automated Scripts
CTOD	Conformance Test Organisation Document
DDS2	Data Dissemination System 2
DG TAXUD	Directorate General - Taxation and Customs Union
E2E	End-to-End
EC	European Commission
ECICS	European Customs Inventory of Chemical Substances
ENS	Entry Summary Declaration
EO	Economic Operator
EORI	Economic Operators Registration and Identification number
EO-DECL	Economic Operator Declarant
EO-REP	Economic Operator Representative
EO-CONF	Economic Operator Configurator
EUCTP	EU Customs Trader Portal
HTI	Harmonised Trader Interface
HTTPS	Hypertext Transfer Protocol Secure
ICD	Interface Control Document
ICS2	Import Control System 2
ITSM	IT Service Management
ITSP	IT Service Provider
LOTL	EU List of eIDAS Trusted Lists
MEP	Message Exchange Pattern
MRN	Movement Reference Number

Abbreviation/Acronym	Definition
MS	Member State
MON&BS	ICS2 Monitoring and Business Statistics tool
NSD	National Service Desk
OPS	Operations
PROD	Production Environment
S2S	System-to-System
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
STI	Shared Trader Interface
STP	Shared Trader Portal
TAPAS	DG TAXUD AS4 Access Point
TARIC	Tarif Intégré de la Communauté
TES	Trans-European system
TI	Trader Interface
TLS	Transport Layer Security
UCC	Union Customs Code
URL	Uniform Resource Locator
UUM&DS	Unified User Management and Digital Signatures

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.

A complete list of the ICS2 terminology can also be found in the ICS2 Definitions document [R02].

Term	Definition
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 Shared Trader Interface (STI) or an access point used by an Economic Operator (EO).
Business Role	A business role is defined as the responsibility for performing specific behaviour, to which an actor can be assigned. The business role is determined according to the interaction that an EO's system has with ICS2. Business roles consist of the following types: <ul style="list-style-type: none"> • Carrier; • Express Operator; • House Filer; • Notify Party; • Person Notifying the Arrival; • Postal Operator.
Business Scenario	A Business Scenario is a simulation of business processes in operations expressed in a number of steps to cover a specific functionality of the system for testing purposes. The Business Scenarios are pre-configured at the application level and considered as pre-conditions for the user Interface Use Cases.
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,

Term	Definition
	<p>(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;</p> <p>(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.</p>
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 an Economic Operator is ready to enter the trans-European system without the risk of disturbing the parties already in operation in the system.
Conformance Test Organisation Document	The Conformance Test Organisation Document covers the organisation, performance and follow-up of the ICS2 Conformance Testing. It describes the activities to be performed during the CT as well as the roles and responsibilities of the CPT (Including ITSM contractor) and the MS.
Delegate/ Representative	The person who is assigned the authorisation(s) by the delegator.
Delegation	The delegation is the action of a person (legal or natural) to assign to another natural or legal person to act on his behalf by delegating one or more of his authorisations defined as business profiles. The scope of the delegated business profiles (scoped by application) can be the same or a subset of one of the original business profiles.
Delegator	The person who owns the authorisations and decides to assign -all or part of- them to another natural or legal person (delegate).
EO Self-Conformance Testing	As of Release 2, EOs will be given the possibility of Self-Conformance testing. EO Self-Conformance Testing will be the new approach used for EO CTAS as of Release 2 and it is a different approach compared to the standard EO CTAS that was followed for Release 1. The approach to verify the conformance of the EO systems will be based on test scenarios and business scenarios. Those will be triggered from the ICS2 STI STP conformance campaign screen(s), dedicated solely for the purpose of an EO user to configure and execute the conformance test campaigns.
House Filer	House filer is an entity authorised to carry out operations related to the shipment of consignments or a person having at its disposal all the necessary data elements to lodge ENS filing, e.g., freight forwarder, ground handling agent, importer (more relevant for ICS2 R3).
ITSM	The DG TAXUD contractor responsible for the central operation in ICS2.
ITSM3-OPS	Private consortium in charge of the operations of the DG TAXUD infrastructure and datacentre facilities; subcontractors of the DG TAXUD.
ITSM3-TES	Private consortium in charge of IT service management; subcontractors of the DG TAXUD.
IT Service Provider	An IT Service Provider (ITSP) is a legal person that offers services involving the development of system for the delivery and reception of messages to and from ICS2 TL.

Term	Definition
	<p>An IT Service Provider must be identified and registered by Customs to be authorised to exchange messages with TI.</p> <p>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 sent by the ITSP to Customs.</p>
Notify Party	<p>A Notify Party is an entity who has an agreement with and represents an air carrier who is acting as declarant or person presenting the goods, e.g., freight forwarder, ground handling agent etc.</p>
Person Filing	<p>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 bill of lading or air waybill in any form and can be either carrier, NVOCC, 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.</p>
Person Notifying the Arrival	<p>A Person notifying the arrival is a carrier that actually operates means of transport and submits Arrival notification.</p>
QA	<p>Quality Assurance also used to describe DG TAXUD's contractor responsible for Quality Assurance.</p>
Sender	<p>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.</p>
Shared Trader Interface (STI)	<p>The STI represents the IT system that will be used by Economic Operators to communicate with customs authorities in the context of ICS2. The STI will be developed, hosted and operated by DG TAXUD.</p>
Test Case	<p>A test case is a set of steps applied to transit the system from a known initial state to an expected final state. It is characterised by:</p> <ul style="list-style-type: none"> • An identifier that uniquely identifies the test case; • A short description of its purpose; • One or several actors performing the actions on the system; • A set of prerequisites describing the initial state of the system; • A set of steps defining the actions performed by the actors and their expected results. Steps may describe input values and expected output values if applicable for the tested feature; • A set of post-conditions describing the state in which the system is expected to be after the execution of the steps; • A set of pass criteria defining the conditions under which the test can be considered as passed. <p>A test scenario is realised by one or several test cases without an explicit mapping between the test cases and the test scenario guidelines.</p>
Test Scenario	<p>A test scenario is a set of guidelines enabling to assess the testing coverage of a feature against its specifications. It is characterised by:</p> <ul style="list-style-type: none"> • An identifier that uniquely identifies the test scenario; • A description of the covered feature.

Term	Definition
	A set of guidelines (e.g. a high-level action performed on an abstract set of data) that can be ordered if the tested feature requires it.
UUM&DS	Unified User Management and Digital Signature System (UUM&DS) implements identity federation between the Commission and all 27 Member States' identity and access management systems for the purposes of providing secure authorised access to the EU Customs electronic systems for EU Economic operators and persons other than the economic operators.

Table 4: Definitions

2 TESTING ORGANISATION

The organisation of the Conformance Testing campaign for Economic Operators follows the agreed approach for the overall operational strategy organisation agreed with the Member States.

The main principle being that Member States or National Customs Authorities are responsible for the coordination of Economic Operators (EO) CT activities and for the training of EOs regarding the EO Self-Conformance Testing campaign.

For the initiation of a test campaign, the EO must first contact the National Authorities and provide their EORI number¹, their plan for CT execution, and their plan for moving to ICS2 Operations. During the test campaign, National Authorities will coordinate directly with the EO keeping DG TAXUD informed of the progress status.

2.1 ROLES AND RESPONSIBILITIES

The current section presents the roles and responsibilities of the stakeholders involved in the ICS2 Conformance Testing for Release 3.

2.1.1 Economic Operator (EO) - Sender

The Economic Operator is any person who has been identified by the legal provisions obliged to submit ENS filing to the customs authorities via the Shared Trader Interface (STI) using a system (EO system) (see [legal framework](#) which is contained in the Union Customs Code (UCC) and its Implementing Provisions). For the Conformance Testing activities, the role of Sender is defined, which corresponds to the EO or IT Service Provider (ITSP)² who implements the technical interface to be tested and used for sending the technical messages to the STI. Specifically, the concrete responsibilities of the Sender related to Conformance Testing are the following:

- Read and understand in depth the relevant documentation that is published (see section 2.5);
- Define an EO SPOC as a focal point in the coordination with the National Customs Authority;
- Obtain the required digital certificates (i.e., for TLS and for sealing);
- Implement the AS4 access point (according to the HTI – Interface Control Document [R01]);
- Obtain an EORI by a responsible MS and registers the digital sealing certificate in [UUM&DS](#) in CONF environment (see section 4.2.2.1 of the HTI – Interface Control Document [R01]);
- Request to NSD the creation of users and roles in UUM&DS in CONF environment for accessing the EUCTP, and consequently the STI-STP (see Annex EAnnex E);
- Provide to responsible MS a plan for EO Self-Conformance Testing;
- Make sure that EO CT prerequisites (i.e., certificate registration, AS4 Access Point configuration, connection is in place) are fulfilled before CT campaign commences (see 2.3.1);
- Self-execute successfully through STI-STP, all conformance test business scenarios relevant to its business role and the ENS filing types that the EO is obliged to submit;
- EO SPOC to follow up tickets (in case of errors regarding CT) that were registered by NSD;
- Contact National Service Desk (NSD) and request for support in case errors are detected or information is needed by using a template (see Annex C).

¹ EORI number must exist in the EOS system in CONF and consequently in CRS.

² Please note that despite using the Service Provider services, EOs (Postal Operators) established in the European Union remain "declarant" and are legally obliged to comply with timely, accurate and complete entry summary declaration lodgement and all related procedural requirements, as per Union Customs Code and its implementing provisions.

2.1.2 IT Service Provider (ITSP)

An IT Service Provider (see definition in 1.8) is a legal person contracted by a Person filing for services involving the delivery and reception of messages to and from ICS2 TI. ITSP can provide business services to multiple EOs. During Self-conformance testing, the ITSP must register a conformance test campaign for each business role that intends to perform and to run the campaign by testing all the pre-defined business scenarios successfully. If the selected role is Carrier or House filer, ITSP should select out of a list with ENS filing types that are available for testing. Upon selection of the type, a set of business scenarios corresponding to those ENS filings will be proposed for execution.

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.

2.1.3 National Customs Authority / National ICS2 Project Team

The role of National Customs Authority (or dedicated National ICS2 Project Team) is to be the SPOC for CT requests by the Sender. Specifically, the National Customs Authority is responsible for the following activities:

- Ensures the communication, the coordination and the schedule with the EO;
- Provides the EO CT Project Plan (Annex A) to DG TAXUDs;
- Verifies and validates the sealing certificate registration by the EO;
- Organises and delivers trainings to EOs;
- Registers Economic Operators. This shall be provided by Member States using other systems: EOS (Economic Operator Systems) and UUM&DS;
- Manages processes related to the registration, identification and maintenance of the identities of the Economic Operators and their representatives, in their Identity & Access Management (IAM) systems, connected to the UUM&DS;
- Provides to EOs the UUM&DS user-roles in CONF environment needed to access EUCTP, and consequently the STI-STP (see section 3.3.4);
- Checks the business and technical readiness of Traders before they start to send ENS to the STI;
- Maintains the EO Consolidated Report (Annex G) to monitor the EO Self-Conformance Testing progress of the EOs that pertain under their responsibility;
- Provides the service desk support to EOs for CT related incidents;
- Acts as an escalation point along with DG TAXUD.

2.1.4 DG TAXUD - European Commission

DG TAXUD has the overall responsibility for the conformance testing. In particular, DG TAXUD is responsible for the following activities:

- Provides the central Access Point and STI services for the Conformance Testing;
- Manages the ITSM Contractors;
- Delivers the training and relevant training material to MS;
- Produces and publishes on [Europa](#) page ([CIRCABC groups ICS2 release 3](#)) ICS2 Common Functional and Common Technical System Specifications;
- Provides support to ITSM contractors when is needed;
- Acts as an escalation point in the context of the daily operation of the NSD.

2.1.5 ITSM Contractors of DG TAXUD

The role of ITSM is to provide support during EO conformance testing campaign. The support may include some of the following activities:

- Based on the configuration provided by Sender through STI-STP, implement configurations at TAPAS and STI level for the establishment of the connectivity between TAPAS and EO System AS4 Access Point(s); [OPS]
- Configures and maintains the conformance environment; [OPS]
- Handles issues in DG TAXUD ticketing system (ITSM SYNERGIA ESS) dispatched by NSD, which need further investigation by the development team or/and DG TAXUD; [OPS and TES]
- Consolidates weekly the EO CT plan provided by MS in order to ensure sufficient system capacity; [TES]
- Provides training session to MS, when defined by DG TAXUD, regarding EO Self-Conformance Testing execution; [TES]
- Registers incidents regarding technical or business-related defects related to central components for further investigation by the development team or/and DG TAXUD; [TES]
- Provides report on the EO CT progress based on data extracted from ICS2 MON&BS; [TES]
- Performs risk analysis and escalates, if necessary, to DG TAXUD the issues or blocking points identified during the EO Self-Conformance Testing. [TES]

2.1.6 National Service Desk (NSD)

The role of National Service Desk is to provide meaningful support to the EOs in the activities that concern the EO Self-Conformance Testing. The NSD is responsible for the following activities:

- Provides assistance in the upload and registration of the sealing certificate in UUM&DS CONF;
- Supports the establishment of EO's AS4 Access Point(s);
- Follows-up and provides assistance to EOs through ICS2 MON&BS during Self-conformance test campaign;
- Logs any issues/incidents found during EO Self-Conformance Test campaign that need to be investigated by National Service Helpdesk or Central Service Desk;
- Resolves any issue/incident occurred during the EO Self-Conformance Test campaign or dispatching them to Central Service Desk in case this is related to ICS2 central components;
- Follows-up the CT incidents and shares the provided feedback to relevant EOs;
- Represents the EO in the information exchange flow from NSD towards CSD and vice versa.



Figure 2: Communication channel among EO, NSD and CSD

2.1.7 Central Service Desk (CSD)

The EO Self-Conformance Test campaign issues that are related to ICS2 central components, will be assigned to DG TAXUD Central Helpdesk, who will dispatch to the appropriate central support teams. Central Service Desk is responsible to provide support to NSD in case of EO CT related issues that cannot be resolved at NSD level.

2.2 PLANNING AND MILESTONES

Before the start of each Conformance Testing, the EO SPOC should share the planning of CT activities (see Annex A) to their responsible³ National Customs Authority.


Q2 2023			Q3 2023			Q4 2023			Q1 2024		
April	May	June	July	August	September	October	November	December	January	February	March
			ICS2 R3 EO Self-Conformance Test Campaign								
			EO Connectivity Establishment				EO Self-Conformance Testing ICS2 R3				
						End-to-End					

Figure 3: Duration of EO Conformance testing

EOs can start the connectivity establishment through STI-STP UI (as this is described in section 3.2.1, 3.2.2) from the beginning of July 2023. Functional testing can start as of mid-November 2023.

It is strongly recommended for EOs to start the CT campaign at the first half of the CT timeline⁴ that has been defined and as far as possible from the end, in order to ensure that there will be sufficient time for software corrections and re-testing before entering the ICS2 operations on 01/03/2024. In order to ensure enough support availability at NSD level, the plan for the Conformance Testing must be sent to the MSs by the Sender before the testing date and also, any changes in the initial plan should be communicated in a timely manner.

2.3 CONFORMANCE CAMPAIGN PROCEDURE

This section provides an overview of the EO Conformance Test procedure to be followed.

2.3.1 Prerequisites

Table 5 summarises the prerequisites that should be fulfilled by each entity in order EO to be ready for starting the Self-Conformance Testing. For each action there is a reference of the current or external document where audience can consult for more details.

Action	EO	MS	ITSM3-OPS	Reference
1. Set up the necessary infrastructure to perform the tests	√			R01
2. Communicate EO plan for Self-conformance execution to MS	√			Annex A
3. Communicate EO plan for Self-conformance execution to DG TAXUD		√		2.1.3
4. Obtain EORI from National Customs Authority	√	Support		2.1.1
5. Obtain the required digital certificates (i.e., for TLS and for sealing)	√			3.3.1

³ As 'responsible' is considered the National Customs Authority from which a Sender has obtained its EORI number.

⁴ The timeline that is depicted in Figure 3 regarding E2E campaign is indicative and may change. More details regarding E2E campaign will be described in E2E CTOD.

Action	EO	MS	ITSM3-OPS	Reference
6. Develop and validate EO Access Point(s) according to HTI – ICD	√	Support		R01
7. Create UUM&DS user and roles in CONF environment for accessing EUCTP and STI-STP	√	Support		2.7
8. Connect to ICS2 Conformance Environment				
8.1 Upload and register the sealing certificate in UUM&DS in CONF environment	√	Support		3.1
8.2 Establishment of EO's AS4 Access Point(s) through STI-STP in CONF environment	√			3.2.1
8.3 Configure EO's AS4 Access Point(s) at TAPAS and STI level CONF environment			√	3.2.1
8.4 Verify proper establishment of the connectivity	√			3.2.2

Table 5: List of prerequisites to be fulfilled

2.3.2 Conformance Campaign Set up and Execution

Table 6 summarises the actions that should be accomplished to set up and execute EO Self-Conformance Campaign. For each action there is a reference of the current or external document where audience can consult for more details.

Action	EO	MS	ITSM3-OPS	Reference
1. Set up Conformance Test campaign in STI-STP	√			2.8.1
2. Run Conformance Test campaign in STI-STP				
2.1 Perform Self-conformance testing in STI-STP	√			2.8.2 4
2.2 Follow up and support EO Self-CT through ICS2 MON&BS		Support		2.6
3. Conformance Test campaign Validation				
3.1 Test results are validated on STI				4.3
3.2 Consult EO Self-CT campaign status via ICS2 MON&BS UI		√		2.6
3.3 Upload in PROD environment via MON&BS UI a file with the success EO Self-Conformance Test Campaigns that have been previously downloaded from CONF environment		√		R06
4. Implement activities after Conformance Test campaign				
4.1 Establishment of EO's AS4 Access Point(s) through STI-STP in PROD environment	√			6
4.2 Configure EO's AS4 Access Point(s) at TAPAS and STI level in PROD environment			√	6
4.3 Complete activities defined in the Operational Checklist	√			Annex B

Table 6: List of actions to be performed during Conformance Campaign

2.4 COMMUNICATIONS

Continuous communication and synchronisation between all the involved parties are essential during the Conformance Testing activities.

As mentioned before, the EO SPOC is responsible for sending its request relevant to EO Self-Conformance Testing to the National Customs Authority. Then, the National Customs Authority should inform the National Service Desk for providing the necessary feedback. In case a request cannot be solved by NSD, then, NSD dispatch the initial request to Central Service Desk by registering a ticket in DG TAXUD ticketing system (ITSM SYNERGIA ESS). National Customs Authority should ensure that any feedback that will be provided through the registered ticket will reach the EO SPOC who initially raised the request.

DG TAXUD ticketing system will be used during the CT activities by ITSM for issues that need to be further investigated or escalated to the National Service Desk or/and DG TAXUD. For this reason, ITSM is also responsible to send an email to the National Customs Authority when registering a ticket for traceability purposes.

2.5 COMPLEMENTARY INFORMATION

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 [R08];
- ICS2 EOs Common Technical System Specifications package for ICS2 Release 2 & Release 3 [R09].

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

- Conformance Test Organisation Document (CTOD) for EO for Release 3 [current document];
- Test Design Specifications for EO Conformance Test Cases (TDS-CTC) for Release 3 [R04];
- Test Design Specifications for EO Conformance Test Scenarios (TDS-CTS) for Release 2 and Release 3 [R03];
- Trainings that will be provided by National Administrations to EOs:
 - ICS2 EO Self-Conformance Test (R3-NA-EO-CT);
 - Digital certificates and registration of certificates – national component (R3-NA-EO-UUMDS);
 - NA services and support to EOs.
- Material which will be made publicly available in [Europa](#) webpage:
 - Self-Conformance Test (R3-EO-CT);
 - UUM&DS system: Your passport to EO applications (EO-UUM&DS);
 - Business Continuity Plan (R3-EO-BCP);
 - Use of STP for ENS registration (R3-EO-STP);
 - ICS2 End-To-End test for EO (R3-EO BCP).

In general, the latest accepted version of the EO Self-Conformance Testing related documentation is stored on:

https://circabc.europa.eu/ui/group/617eb8f3-5946-4fe5-a01f-42974a83b29c/library/f94a672b-0790-4a68-a09a-a8d5382ccaca?p=1&n=10&sort=modified_DESC .

2.6 MON&BS AS SUPPORTIVE TOOL (ONLY FOR MS OPERATORS)

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 MS to provide meaningful assistance to EO during Self-conformance test campaign. 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 scenario⁵);
 - Consult successful EO Self-Conformance Campaigns;
 - Upload successful EO Self-Conformance Campaigns;
 - Search EO messages not compliant with a successful Self-Conformance testing;
 - Manage EO Compliance Monitoring Mailing List.

It is important to highlight that the use of ICS2 MON&BS tool is available only to MS and EC users. The EO can manage ICS2 related preferences and Self-register a conformance test campaign through the STI-STP⁶. In this case, the execution of the Campaign will be tracked by STI.

Further information relevant to the use of ICS2 MON&BS in the EO Self-Conformance Testing is described in section 2.1.6, 3.7 and 3.8 of ICS2 Monitoring Use Case Specifications [R06]⁷.

2.7 STI-STP AND ROLES REQUIREMENTS

The approach to verify the conformance of the EO systems is based on business scenarios that combine certain test cases. Those will be triggered from the ICS2 STI-STP conformance campaign screen(s), dedicated solely for the purpose of an EO user to configure and execute the conformance test campaigns.

The EO can access STI-STP by accessing first the EU Customs Trader Portal (EUCTP) via the internet using the following [link](#) or the website of their responsible National Customs Authority. Access to the EUCTP Portal is validated and managed through the UUM&DS.

The following roles alongside with their key functionalities are required for an EO to perform EO Self-Conformance Testing through STI-STP:

- Economic Operator Declarant (EO-DECL):
 - Search/View Submission following EUCTP rules;
 - STI-STP Search Messages (View ENS Filing with Declarant/Representative EORI);
 - Manage Preferences (read-only access);
 - Consult CONF Test Campaign (only in CONF environment).

- Economic Operator Representative (EO-REP):
 - Search/View Submission following EUCTP rules;
 - STI-STP Search Messages (View ENS Filing with Declarant/Representative EORI);

⁵ This feature is available only in the CONF environment.

⁶ Self-registration of conformance test campaign is implemented through STI-STP in the CONF environment.

⁷ The reference document is accessible only by MSs and it is published [here](#).

- Manage Preferences (read-only access);
- Consult CONF Test Campaign (only in CONF environment).
- Economic Operator Configurator (EO-CONF):
 - Manage Preferences-Access Point Configuration (write access);
 - Register / Consult CONF Test Campaign (only in CONF environment).
- Person Notifying Arrival (EO-PNA):
 - Search/View Submission following EUCTP rules;
 - STI-STP Search Messages (View ENS Filing with Declarant/Representative EORI);
 - Consult CONF Test Campaign (only in CONF environment).
- Notify Party (EO-NOP):
 - STI-STP Search Messages (View ENS Filing with Declarant/Representative EORI);
 - Consult CONF Test Campaign (only in CONF environment).

2.8 EO SELF-CONFORMANCE TEST EXECUTION

This section provides a top-level description of the steps that should be performed by EO to run conformance testing through STI-STP. The process consists of 3 main steps:

- Set up a conformance campaign;
- Run the conformance campaign;
- Validate the conformance campaign results.

2.8.1 Set up a Conformance Campaign

An EO Self-Conformance campaign requires:

1. Pre-Conditions:

- 1.1 UUM&DS access has been granted, and certificate is uploaded and registered in the CONF environment, successfully;
- 1.2 The EO user is successfully logged into [EUCTP](#) via UUM&DS authentication and identification, in the Conformance environment;
- 1.3 The AS4 connectivity between the EO system and ICS2 is in place (EO System certificate is properly registered in UUM&DS).

2. Manage Preferences:

- 2.1 AS4 configuration has been implemented or can be updated as per section 3.2.1.

Manage Preferences (first option)

The screenshot shows the 'Manage Preferences' interface in the EU Trader Portal. The page is titled 'Manage Preferences' and is for a user identified as 'CO declarant/representative acting also as a sender'. There are two tabs: 'As Person Filing' (selected) and 'As Carrier'. The 'Optional Notifications' section lists various notification types with toggle switches. The 'Default communication path' section shows a table with columns for 'Address', 'Party ID', and 'Action'. The 'Access Point Configuration' section shows a table with columns for 'Party ID', 'Supported STP service version', 'Message format', 'Access URL', 'P.O. Client Identifier', 'Technical contact name', 'Technical contact email address', 'Phone', and 'Action'. Annotations include: 'Click on Finish to save the changes', 'Warning: back to the previous page to select a different type of preferences. If there are changes on this page not saved, confirmation dialogues warns that user saved losing the changes', 'Use STP which complies with the requirements: Appropriately to Person Filing and Carrier', 'The system information: Party ID format is defined in ICS; Supported STP service version is determined. Defined in ICS; Parties are monitored for the status of a single party from an EOPN (Trader), except the required (mandatory) long name parts, and the 'Access point' field explains. A single EOPN (Trader) can setup multiple parties.', and 'Details not available for the Party ID. It also do default communication path'.

Figure 4: Manage Preferences

3. Register a Self-Conformance Test campaign:

3.1 The EO selects “Conformance Tests” from the STI-STP main menu;

3.2 The EO selects the "Finish Configuration” button once all the configuration fields are filled;

CONF - Conformance Tests

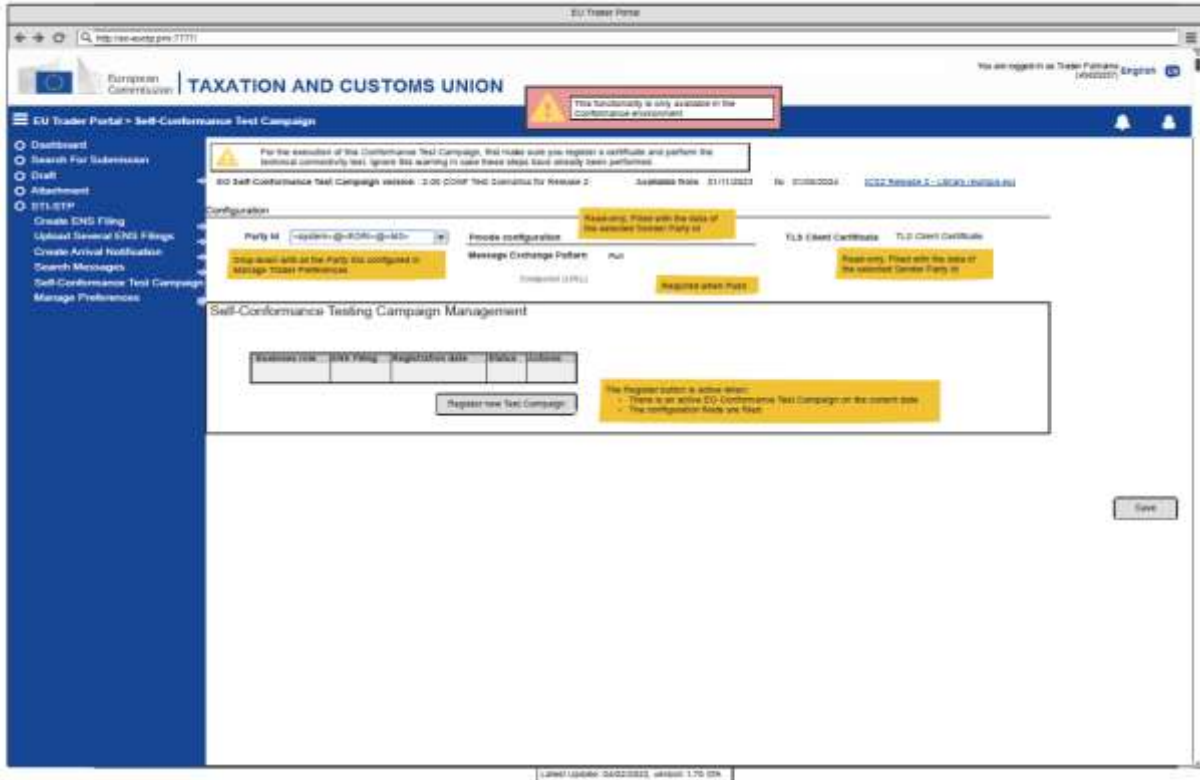


Figure 5: Register Self-Conformance Test Campaign

3.3 The EO selects a business role. Depending on the role selection, a pre-defined set of business scenarios will be available for execution;

CONF - Business Role Selection - Carrier

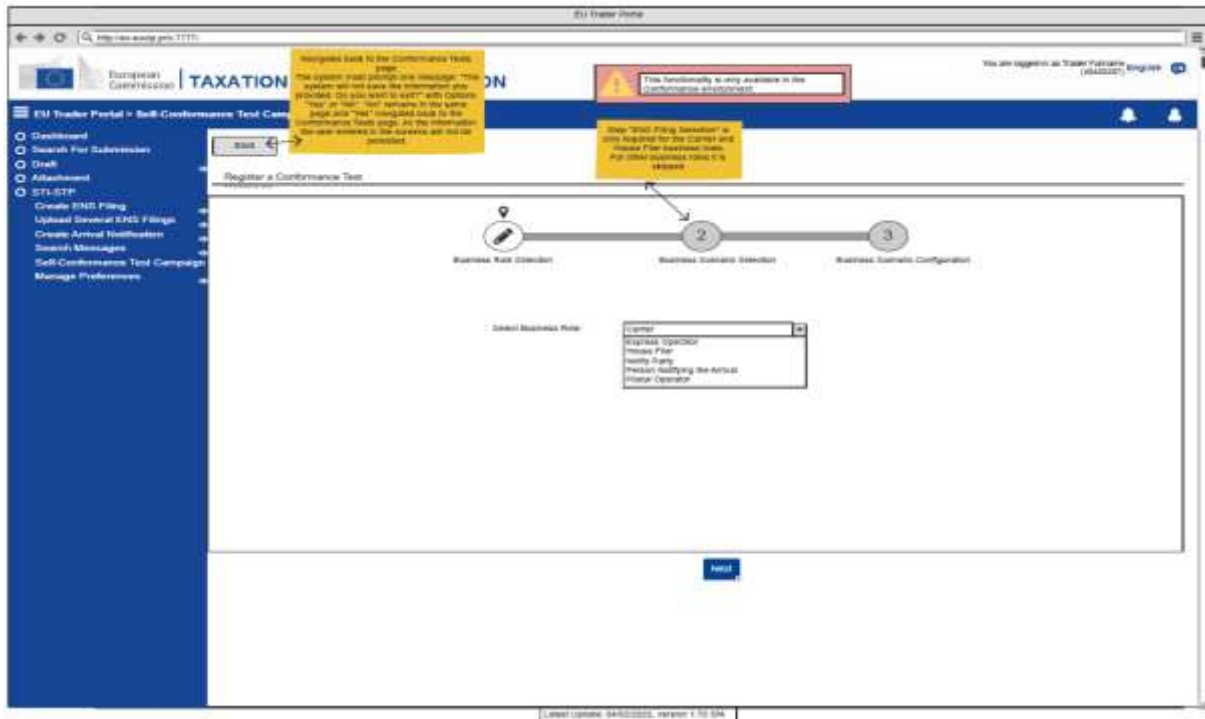


Figure 6: Register a Conformance Test Campaign - Business Role selection step

3.4 The EO fills in Identifiers (the LRN's of all ENS filings part of a business scenario) and user saves the configuration. Then, configuration will be stored in ICS2 STI of the CONF environment.

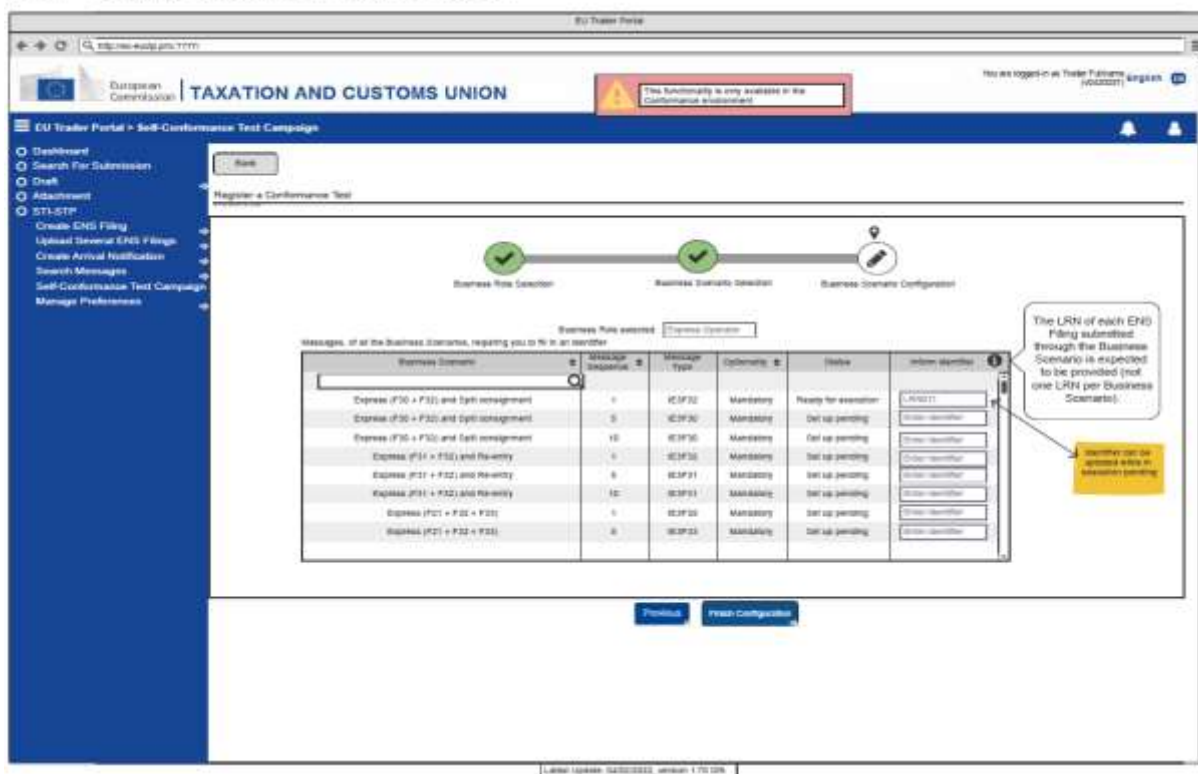


Figure 7: Register a Conformance Test Campaign – Business Scenario configuration step (no ENS Filing selection required)

Further details about the business scenarios are provided in the respective Test Design Specifications for Economic Operators [R03] [R04].

2.8.2 Run the Conformance Campaign

In order for an EO to start running Self-conformance testing, the configuration of the environment from ITSM contractor (OPS) must first be completed (see section 3.2.1). This activity may require up to 10 days.

Then, EO is required to:

1. Provide configurations fields in ICS2 STI-STP conformance test configuration screen:
 - 1.1 Provide the sender Party ID;
 - 1.2 Select MEP (“push” or “pull”);
 - 1.3 Provide the Endpoint (i.e., URL) (Mandatory if the MEP is “push”);
 - 1.4 Provide the Certificate Authority that issues the TLS certificate.

CONF- View registered Test Campaign - Carrier and Express Operator

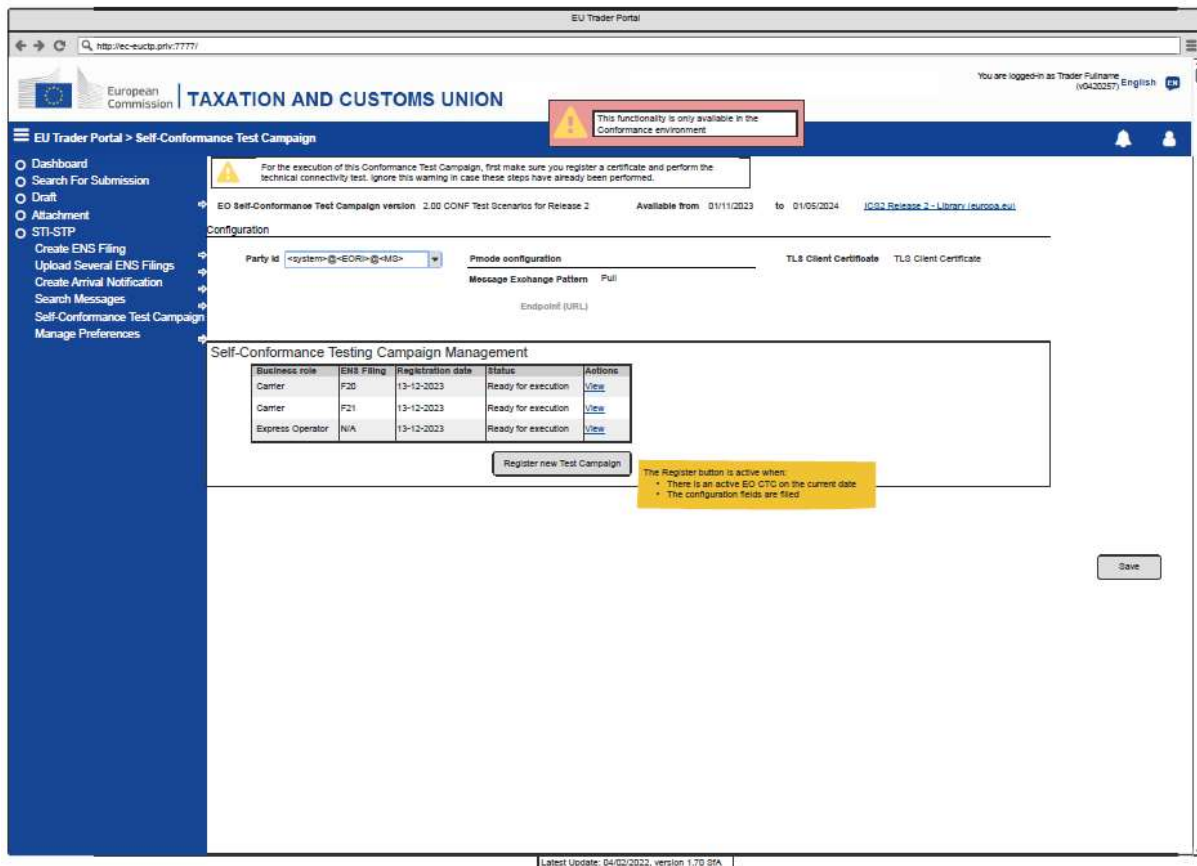


Figure 8: Self-Conformance Test Campaign

2. Select role according the EO type as per Figure 6 (e.g., Postal Operators, Express Operators; Notify Party, Person Notifying the arrival, Carriers, House Filers).

Select the drop-down value of the ENS Filing of the campaign. Available values depend on the Business Role selected and are the ENS Filings included in the ongoing Campaign.

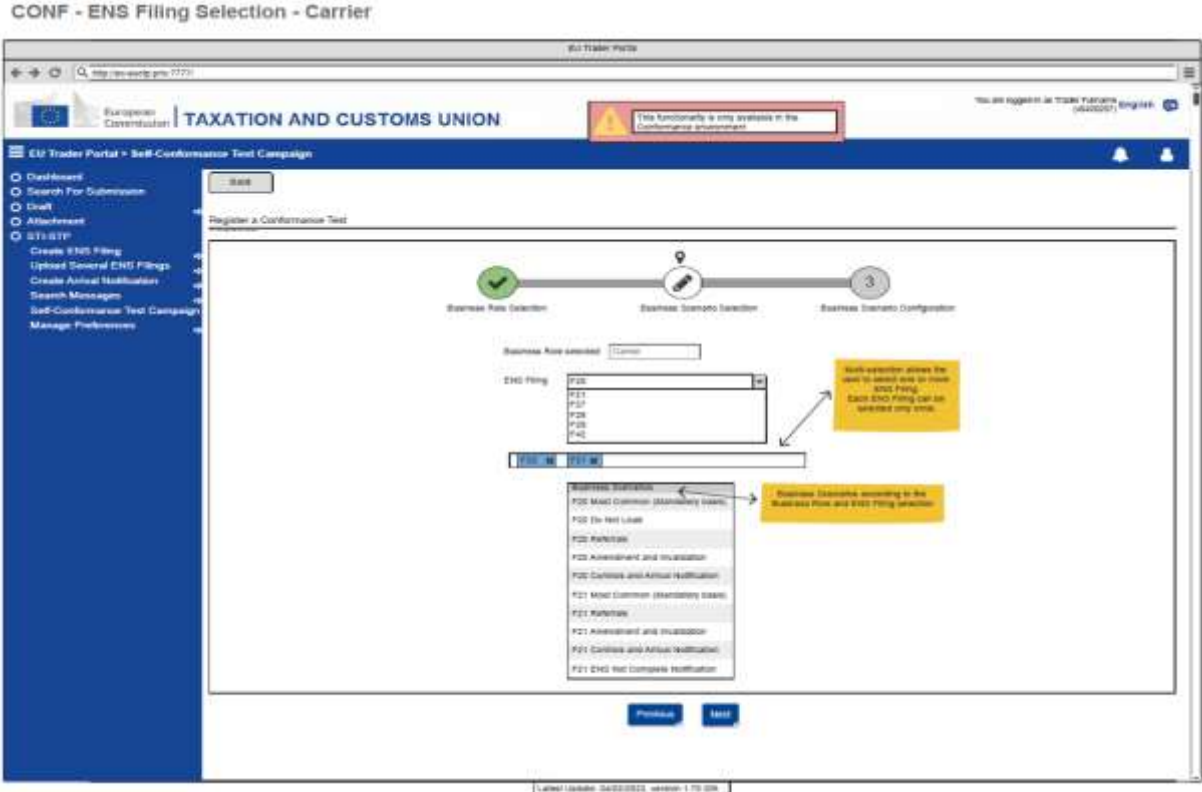


Figure 9: Register a Conformance Test Campaign – ENS Filing selection step

A set of business scenarios corresponding to those ENS Filings will be proposed for execution. Once the business scenario is triggered by the EO, an automated script is used to simulate other EO business roles (if any in the scenario), to simulate NES messages and validate the successful completion of the business scenario. Only once all business scenarios are completed, the campaign can be considered successful.

As described also in section 2.1, MS and NSD are responsible for following up and supporting EO through ICS2 MON&BS during Self-conformance testing.

2.8.3 Validate the Conformance Campaign Results

The conformance campaign results are validated automatically. Member States support the validation process, while they assist EOs by troubleshooting in case of errors detected during EO Self-Conformance Testing. For more details on the test validation please consult section 4.3.

3 CONNECTION TO ICS2 CONFORMANCE TEST ENVIRONMENT

The following sections present the necessary elements of the Conformance Environment infrastructure that the sender (EO or their IT Service Provider) should take into consideration in order to connect to ICS2 Conformance Environment. The prerequisites that the sender needs to fulfil in order for its system to send and receive ICS2 messages from and to the STI are the following:

- Registration of a certificate in Unified User Management and Digital Signatures (UUM&DS) and the association between this certificate and their EORI;
- Establishment of the Access Point.

3.1 REGISTRATION OF CERTIFICATES IN UUM&DS

Unified User Management and Digital Signatures (UUM&DS) will be used to verify that the sender has the authorisation to send and receive messages to and from the STI. In specific, for the S2S, the authorisation of the senders will be performed through the use of a certificate. The senders that will be authorised for exchanging messages with the STI need to register their identification number (EORI) and the certificate that will be used for sealing the AS4 messages.

The DG TAXUD AS4 access point will interact with UUM&DS to validate the association between the EORI number and the certificate embedded in the message. Only certificates issued by a Certificate Authority that is trusted by UUM&DS can be registered.

The certificates that will be used must be registered in CONF environment, either on National UUM&DS at MS level or on UUM&DS at central level. In the first case, the MS is responsible for registering sender as new entity in National UUM&DS, while in the other case, the certificates can be registered centrally. It should be noted here that a sender should have the profile “BP_MANAGE” to access the UUM&DS Admin application to register a certificate.

Customs & Tax EU Learning Portal offers a course (see Annex E) including specific information on the use of UUM&DS. It is strongly recommended all EOs and their Customs representatives to attend this online 30-minute course prior to any interaction with UUM&DS. The expected outcomes of the course are: attendee to be able to confidently work with the UUM&DS, to carry out certificate registration and apply delegation and roles assignments authorisation tasks within the UUM&DS.

For more information regarding the registration of certificates, the format of the certificates and the roles/profiles that the sender needs to have, please refer to Annex D. Information on how to verify the successful registration of EO System digital certificate is described in section 5.1.1 of the HTI – Interface Control Document [R01].

3.2 COMMUNICATION PROTOCOLS

EOs are responsible for sending and receiving ICS2 messages from and to the STI. This communication between the EO and STI (S2S interaction) is performed over a secure HTTPS connection on the public internet by using AS4 as a business message exchange protocol which ensures the security and reliability requirements (see section 4 of ICS2 HTI – ICD [R01]).

For this communication, a mandatory component is the AS4 access point software [R05], which should be implemented by the senders (EO itself or by the IT Service Provider) in order to communicate with the DG TAXUD 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.

3.2.1 Establishment of Access Point(s)

For the CT activities, EO or ITSP should establish one or more Access Point(s) for exchanging messages with the ICS2 STI via TAPAS. The establishment of the Access Point(s) can be performed by:

- Deploy one or more Access Point(s) according to HTI Interface Control Document specifications [R01];
- 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 [R01] and 3.2.3 from current document);
- Sender must be registered by Customs Authorities following the agreed national procedure. This includes the upload of the sealing certificate (see section 3.1);
- 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"⁸ 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 [R01]);
 - 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 ID (Mandatory in case the communication path is S2S).

By providing the above information, an email will be launched to ITSM contractor with a request to create a ticket in Synergia SMT asking ITSM3-OPS to configure this new access point. Then, change activities must take place on central side (at TAPAS and STI level) for the registration of the EO. Once the change activities have been completed on central side the ticket will be assigned to the National Service Desk of their responsible MS via Synergia SMT to inform the EO to proceed with the connectivity verification activities (as those are described in section 3.2.2). By default, the required configuration changes are implemented within 5 days from request. Therefore, EO should start testing 5 days after providing Access Point configuration in Shared Trader Portal. This should start without any communication from NSD. NSD should be contacted only in case of issues.

Note: EO must configure AS4 access point to seal the AS4 messages with the sealing 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 [R01]. 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.

3.2.2 Connectivity Verification

Upon implementation of the configurations activities (as those are described in previous section 3.2.1), the establishment of the connectivity between TAPAS and EO System AS4 Access Point(s) must be verified towards both directions.

⁸ User manual is provided as part of the STP application and supported by training material (to be delivered).

In order to do so, the EO System should send a test message to TAPAS as described in section 4 of ICS2 Test Design Specifications for EO Conformance Test Cases [R04]). The TAPAS system verifies the digital signature using UUM&DS and automatically replies with an AS4 signal message allowing the EO system to verify the correct connection. Additionally, it will validate that the EORI embedded in the message is associated with the message in the embedded certificate using the information registered in UUM&DS.

The signal message will give an indication whether the UUM&DS configuration is correct. If the initial test message fails due to UUM&DS issues, it will generate an authorisation AS4 error message. Only when successful connectivity is verified, EO is ready for Self-Conformance Testing execution.

3.2.3 Connectivity URL information

On ICS2 central side, the TAPAS conformance service is available at: <https://conformance.customs.ec.europa.eu:8445/domibus/services/msh>.

For TAPAS production service is available at: <https://customs.ec.europa.eu:8445/domibus/services/msh>

For conformance environment the Public (source) IP that the TAPAS central side is using for sending messages (from TAPAS to EO) is: 147.67.18.4. Traffic from this IP needs to be allowed through the EO firewalls to be able to receive messages from TAPAS Central side.

The only network ports that are 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.

3.3 SECURITY

The security is an important aspect of the communication between the sender and STI. Confidentiality, integrity, authentication and authorisation are the security requirements of the STI.

Confidentiality is ensured by applying Transport Layer Security (TLS), while integrity is ensured by message signature or sealing according to section 4.6 of HTI Interface Control Document [R01]. Finally, as mentioned above, UUM&DS will be used for authorisation and authentication purposes.

3.3.1 Certificate Requirements

To ensure that 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 (see section 4.6 of ICS2 HTI – ICD [R01]).

as long as the CA is present on the “National Customs Alternate List”¹⁰. Certificates issued by such CA can only be used to perform the registration at National Customs Authority.

3.3.3 Certificates on Central Side

Regarding the 2-way SSL that is implemented, the GlobalSign CA chain is used with conformance.customs.ec.europa.eu:8445 service. Below are the locations that can be downloaded:

- <https://secure.globalsign.net/cacert/Root-R3.crt>
- <https://secure.globalsign.com/cacert/gsrsovsslca2018.crt>

Regarding the sealing/signing certificate, there is a DG TAXUD certificate for signing the conformance messages. Below is the relevant certificate information:

- Owner: CN=TAPAS_gw, OU=SPEED2ng TL, O=SPEED2ng, L=Brussels, C=BE;
- Issuer: CN=SPEED2.CONF.CA, OU=SPEED2, O=DG TAXUD, L=TAXUD DC, C=BE¹¹.



TAPAS_CONF.zip

Regarding the sealing/signing certificate, there is a DG TAXUD certificate for signing the production messages. Below is the relevant certificate information:

- Owner: CN= European Commission - STI TAXUD, OU=DG TAXUD, O=European Commission, L=Brussels, C=BE;
- Issuer: CN=Advanced eIDAS Class2 e-Szigno CA 2016, O=Microsec Ltd., L=Budapest C=HU.



European Commission - STI TAXUD_seal.zip

3.3.4 UUM&DS Business Profiles Requirements

To access UUM&DS web services, an Economic Operator or a Customs Representative must be registered in UUM&DS. A UUM&DS user must have at least one Business Profile to access an application protected by a UUM&DS Policy (see section 6.5.4 and 6.5.6 of UUM&DS User Guide [R07]).

Registering a certificate can be done either centrally or locally, depending on the MS implementation. For central registration, an EO needs to have ‘BP_MANAGE’ business profile (see Annex D), whereas in local registration they should contact the National Service Desk of their responsible MS.

Moreover, 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 (see section 2.7).

UUMDS type of actor	Delegated from	UUM&DS business profile configured as available	STI-STP role
		EXECUTIVE	EO-DECL

¹⁰ MSs are responsible for managing the National Customs alternate list.

¹¹ Certificate Attributes: CN: Common Name, OU: Organisational Unit, O: Organisation, L: Locality, C: Country Name.

Economic Operator (Trader and ITSP)		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

Table 7: Business Profiles vs Corresponding STI-STP roles

*An EO or Customs Representative (delegator) can delegate all or a subset of their business profiles to any employee (delegate). Details on the concept of delegation are presented in section 5.4.1 of UUM&DS User Guide [R07] and in the UUM&DS online course in Annex E of the current document.

4 CONFORMANCE TEST SPECIFICATION

4.1 TEST CATEGORIES

The tests are subsumed in two main categories:

The Connectivity Test category, which consists of one test scenario verifying the prerequisites (see section 3.2.2) that the sender (the EO or their ITSP) needs to fulfil in order for EO system to connect to ICS2 Conformance Environment and be able to exchange ICS2 messages with STI.

The Functional Test category, which consists of business scenarios (a pre-defined sequence of test scenarios) verifying that the sender (the EO or their ITSP) properly exchanges ICS2 messages with STI. It is worth mentioning that the message exchanges during the tests of this category depend on the role of each sender. A sender can have one of the following roles:

1. Postal Operator;
2. Express Operators;
3. Notify Party;
4. Person Notifying the arrival;
5. Carriers;
6. House Filers.

Details about the tests included in the above categories are provided in the respective Test Design Specifications for Economic Operators [R03] [R04].

4.2 TEST DATA

The EO Self-Conformance Testing consists of the execution of pre-defined Business Scenarios that combine a set of steps to cover a specific functionality of the system. The steps of each business scenario are linked to relevant test cases (see section 6 of ICS2 Test Design Specifications for EO Conformance Test Cases [R04]). The aim of each business scenario is to facilitate the CT sample data construction and to depict the correspondence of the ENS lodged data with the responses that STI generates.

The flow of information and the mapping of the data elements across the sequence of exchanged messages is described for each business scenario in section 5 of ICS2 Test Design Specifications for EO Conformance Test Cases [R04]. In the same section, for each business scenario, there is a separate Microsoft Excel file attached that depicts the correlation and the identifiers of the exchanged messages, as well as reference values.

The data to be used for the Self-conformance testing must be customised by EOs¹² similarly to their data to be used in production (e.g., “Declarant”, “Addressed Member State”, “LRN”, etc.). STI-STP UI will provide instructions for any data dependency per business scenario.

The sequence of the test case to be executed is defined by the provided business scenarios and it is depicted in steps. The execution sequence must follow the steps as depicted in the relevant table of each business scenario. One test case can be included in different business scenarios; thus, it can be executed multiple times. It is possible that the expected response messages sent from STI towards the EO system (such as Assessment complete and RfI/RfS requests) are not generated immediately after the incoming EO message towards the STI. This occurs due to the fact that there are some applicable timers on the simulated NES messages. In case there is a validation error (IE3N99) from STI to EO, then this is generated almost immediately.

¹² An EO can see only their own data. Therefore, in the case that an EO uses an ITSP (or other EO) as Sender, EO can either use the same data as their Sender or to have UUM&DS rights for both themselves and the Sender.

In case the execution of a test case failed, then, this test case should be re-triggered. However, the test resumes only from the failed test case, and it is not required to re-test any preceding test case that was executed successfully.

Moreover, in order to create the ICS2 messages during test case execution, the sender will use the reference data from the following reference data systems:

- CS/RD2 (reference data published in [CIRCABC](#));
- TARIC3 (reference data published in dedicated [European Commission website](#));
- CRS (reference data published in dedicated [European Commission website](#));
- ECICS2 (reference data published in dedicated [European Commission website](#));
- EOS (reference data published in dedicated [European Commission website](#)), because during CT each EO should provide its valid EORI number.

The times and frequency of the updates of the reference data used by the ICS2 system to validate messages will be aligned with the times and frequency of the publications enlisted above, in order to ensure alignment of the reference data available to EOs and that used by the ICS2 system.

4.3 TEST VALIDATION

As described in previous section, the Member States meaningfully support the validation process of EO Self-Conformance Testing. The validation is implemented through ICS2 MON&BS with the use case 'Consult successful EO Self-Conformance Campaign' as described in section 3.8.2 of ICS2 MON-UCS [R06].

The conformance campaign results are validated automatically. The exchanged messages per business scenario will be stored in ICS2 STI in the conformance environment. A business flow is considered as successfully executed only if all inbound and outbound messages of that particular business flow are found.

In case there are some dependencies in the sample data and particular data values are expected, this is indicated in the steps of the business scenario. No assertions on the content of the sample data will take place, however, message structure will be validated in order to comply with ICS2 Common Functional and Technical Specifications:

- No mandatory fields are missing from the exchanged messages;
- No business rules and conditions are violated;
- No code lists are violated.

Results of the successful Self-Conformance campaign will be imported in the production system to allow verification of the incoming messages. In case an EO lodges ENS filings for which they have not performed EO Self-Conformance, the impacted MSs will contact them.

4.4 TEST INCIDENTS/ERROR/PROBLEM HANDLING

During the execution of a business scenario, in case the test output differs from the expected one, the specific test case that was executed is considered as “failed”. EO should investigate the reason of the failure and if the issue is at their side (e.g., incorrect configuration), actions should be taken to resolve the issue.

Otherwise, if the issue cannot be solved at their side, the EO SPOC should inform directly the responsible MS. Then, an expert analysis must be performed by the MS on the failure to establish a diagnosis. Through ICS2 MON&BS, MS supports EO Self-Conformance Test campaign by carrying out the use cases that are described in section 2.6 of the current document. The proper correction procedure shall then be initiated at the National side depending on the results of the diagnosis.

In case the diagnosis from MS reveal that an unexpected Central Application error is encountered, MS should further address this issue to Central side. Then, MS via NSD should register a ticket that will be assigned to CSD with a priority rating (see **Table 8**) upon its registration in Synergia SMT. Analysis and troubleshooting for such error will take place on Central side by ITSM contactors. If needed, ITSM can escalate the ticket to Central Development Team or DG TAXUD.

Once solution is provided through the relevant ticket in Synergia, CSD will assign back the ticket to NSD. Then, MS should inform directly the EO SPOC about the outcome of their initial request.

The following table calculates the priority of an incident based on urgency and impact parameters:

Urgency	Impact	Low	Medium	High
Low		Low	Medium	High
Medium		Medium	High	Critical
High		High	Critical	Critical

Table 8: Priority calculation table

The following table calculates the target and limit time values of NSD for incident management:

Incident Management Time		
Priority	Target Time	Limit Time
4 – Critical	2 Hours	5 Hours
3 – High	10 Hours	1 Business Day
2 – Medium	2 Business Days	3 Business Days
1 – Low	4 Business Days	5 Business Days

Table 9: NSD - Target and limit values for the incident management

4.5 ACCEPTANCE CRITERIA

As described in previous section (see section 2.8.2), the business scenarios to be executed by an EO for passing the conformance test campaign, depend on the role that EO’s system plays in the interaction with ICS2. EO Self-Conformance Test campaign is considered as completed once all the pre-defined business scenarios have been executed successfully.

MS with actor 'Member State Service Support - Monitoring Operator' can consult the successful EO Self-Conformance Campaigns that have been loaded in the system. The system displays a grid with the list of the successful EO Self-Conformance Campaigns currently loaded, with the columns:

- Sender PartyID;
- Business role;
- ENS Filing type;
- Registration date;
- Status.

By identifying the PartyID (EORI) of a specific Sender, MS verifies that this Sender has successfully completed CT campaign. Consequently, MS shall confirm that a Sender is able to offer services to other EOs.

5 RISK AND MITIGATION PLANNING

During the Conformance Testing, potential risks related to the planning, the testing environment or the specifications can be identified. Indicative risks are presented below:

1. Inaccurate/erroneous common system specifications;
2. Business scenarios do not cover the main ICS2 functionalities that should be tested;
3. Unavailability or failure of the testing environment (e.g., DG TAXUD Access Point, STI-STP);
4. Dependent Systems (e.g., UUM&DS) not available for testing;
5. Insufficient level of knowledge regarding the Self-conformance testing campaign procedures;
6. Insufficient access in relevant documentation;
7. Delay in obtaining the required certificates by the Certificate Authorities;
8. Deployment of EO system is not yet completed for CT execution;
9. Delay or problem impacting the EO Plan;
10. Insufficient support during EO CT campaign by NSD and MS.

The following mitigation actions should be taken in order to reduce any of the above risks during the CT Campaign:

1. Detailed review of the relevant documentation (e.g., Test Design Specifications) by National and DG TAXUD;
2. Test execution regarding the availability and configuration of the testing environment before the ICS2 Conformance Testing;
3. Validation of the infrastructure requirements for the testing environment;
4. DG TAXUD to set up a Training Strategy including trainings by MS and training material;
5. EOs need to have established good level of knowledge for the Self-conformance testing through the training material given by the MSs and have established channels for support in case of eventual issues during the CT;
6. All stakeholders need to ensure in advance access in relevant documentation;
7. EOs need to obtain and register the required certificates in advance and certainly before the CT campaign commences;
8. EOs need to communicate to MS the correct status of their systems in advance and certainly before the CT campaign commences. In case of status discrepancies, these should be communicated well in advance;
9. Execution of tests by EOs at the beginning of the CT timeline in order to ensure that there will be sufficient time to resolve any identified issues and to re-test;
10. Support meetings with MS and Trade Associations organised by TES when is considered necessary;
11. MS must ensure enough service availability of the NSD for supporting EO CT campaign as well as for handling the requests/issues raised by EOs during EO CT.

6 AFTER CT ACTIVITIES - OPERATIONS CHECKLIST

Upon successful completion of the conformance testing activities, there is a set of activities that must be accomplished by EOs in production environment before they move to ICS2 Operations.

The Operations Checklist incorporates the tasks that have been defined by the Common Specifications before the deployment of an EO system in production environment. The purpose of this checklist is to depict the actual status of the EO system transition from the conformance environment to the production.

Like the preparation prior to CT activities, the EO must connect their system to the production environment as well. This implies registration of the sealing certificate in National or Central UUM&DS in production environment and establishment of the AS4 access point(s) in production environment.

The Operations Checklist template for ICS2 Release 3 is attached in Annex B. The template might be subject to change in the future. Any updates in the Operations Checklist will be disseminated to the MSs via email communication.

7 ICS2 TRANSITION STRATEGY FROM R2 TO R3

The purpose of ICS2 transition from R2 to R3 strategy is to highlight the aspects of the transition which need to be further aligned and agreed among all involved parties – Member States, the Commission and the economic operators.

7.1 DEPLOYMENT WINDOW

With reference to ICS2-Transition from R2 to R3 strategy document [R10] a deployment window is a period (several months) which can be granted to the economic operators in order for them to connect to the system and to become operationally ready avoiding a big bang. The deployment window can be granted to the EOs, which are already connected to ICS2 R2 system but have to implement additional functionalities (for example, the case of the express operators lodging F34 as of R3), and also to those, which are connecting to the system for the first time.

The deployment window allowed by the legislation for each release is not applicable by default – it needs to be granted by the Member States in close coordination with the Commission. In order to facilitate trade operations, the agreed deployment window needs to be aligned across all Member States per mode of transport and business model filing ENS and the sequence of the connection of the different parties. **For example, all maritime carriers operating across ICS2 countries need to have the same deployment window irrespective in which country they file an ENS filing.**

The maximum deployment window possible to be granted to the EOs for new functionalities from ICS2 R2 to R3 is from **01/03/2024** until **31/03/2025**.

In the following sections the different deployment windows are depicted per carrier. Explanatory details can be found on section 3.2 of ICS2-Transition from R2 to R3 strategy document [R10].

7.1.1 Rail carriers deployment window when complete ENS is filed

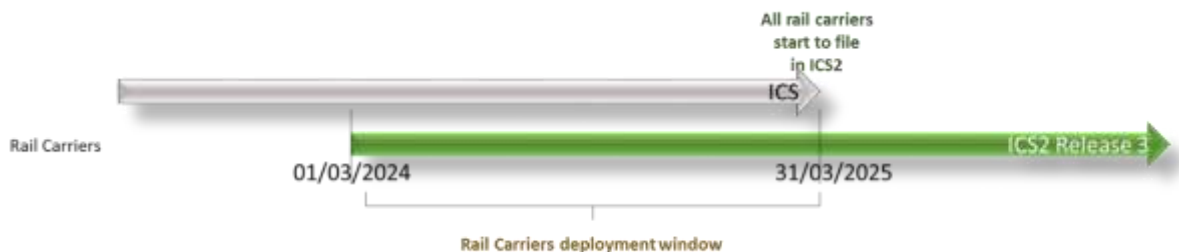


Figure 11 Rail carriers deployment window when complete ENS is filed

7.1.2 Rail carriers deployment window when multiple ENS filings are filed

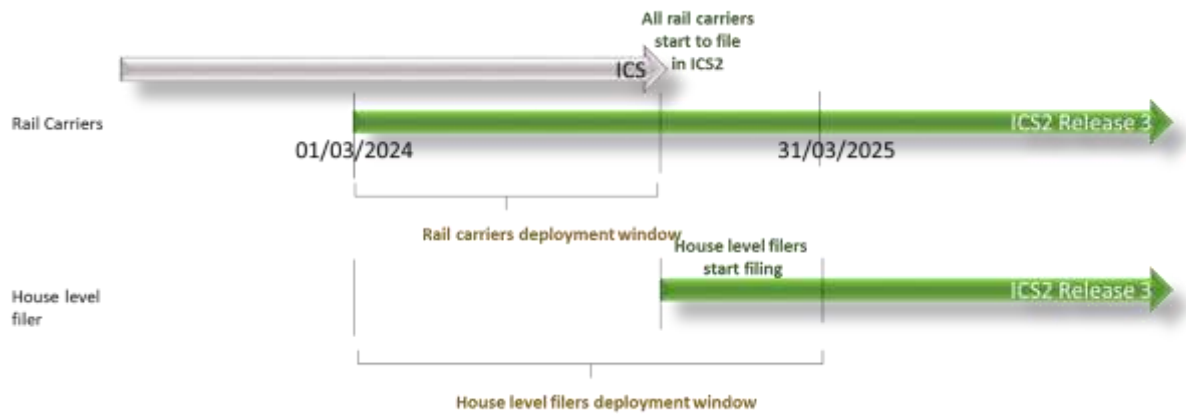


Figure 12 Rail carriers deployment window when multiple ENS filings are filed

7.1.3 Road carrier deployment window

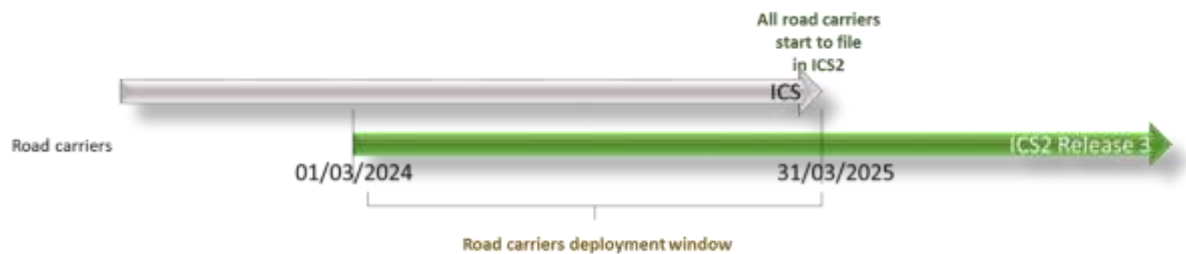
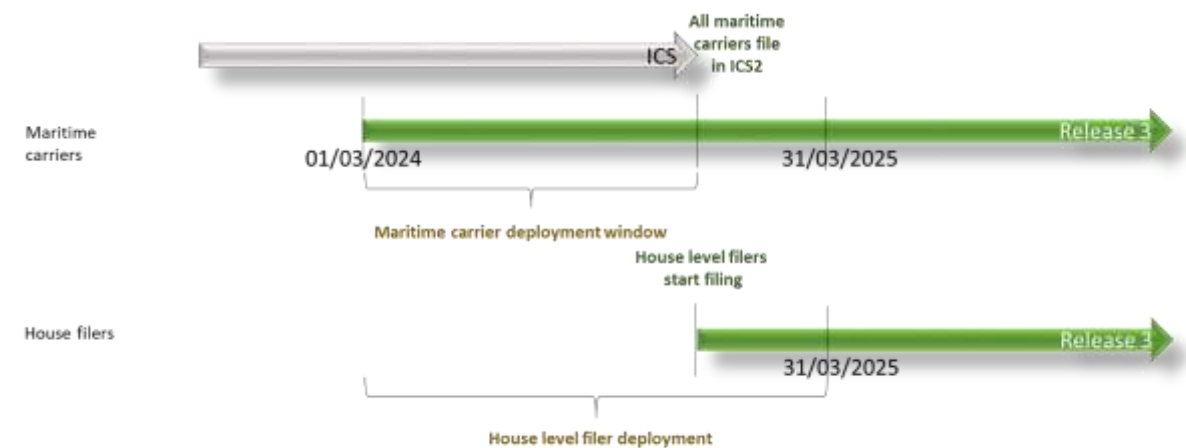


Figure 13 Road carrier deployment window

7.1.4 Maritime carrier and house filer deployment windows



*House level filer = freight forwarder, consolidator, importer, etc.

Figure 14 Maritime carrier and house filer deployment windows

7.1.5 Express operators deployment window for consignments on road

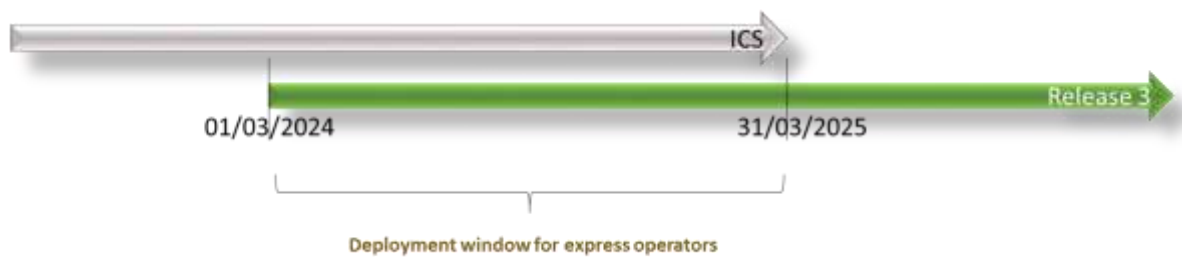


Figure 15 Express operators deployment window for consignments on road

7.2 PRINCIPLES

The ICS2 Transition Strategy from R2 to R3 principles are listed in ICS2-Transition from R2 to R3 strategy document [R10], however EOs should take into consideration the following points in the context of preparation for the Start of Operations:

- ICS2 R3 functionality extends ICS2 R2 functionality from the perspective of new economic operators (new ENS filing types are added) with a common database behind. Consequently, there is no data migration envisaged between the two releases. There are no new business processes added;
- Deployment windows are primarily concerned with the operational readiness and, in addition, with the technical connectivity constraints;
- No customized technical solutions will be implemented in ICS2 R2/R3 architecture, processes or information exchanges to facilitate ICS2 Transition from R2 to R3;
- Entry formalities for the ENSs, which were lodged in ICS, will be finalised in ICS, irrespective of when the goods arrive at the Customs Office of First Entry;
- ICS is envisaged to be available for 200 days after the end of the ICS2 R3 deployment window. However, the Member States can take a decision to decommission their national ICS application earlier in case there are no active ENS(s) available.

7.3 IMPACT OF ICS2 TRANSITION FROM RELEASE 2 TO RELEASE 3

7.3.1 Impact on economic operators already part of ICS2 Release 2

The economic operators already connected to ICS2 R2 are not impacted by the transition to R3 since there are no changes to the messages or any other functionalities.

7.3.2 Impact on operators that start filing Release 3 ENS filings

All cargo transported by maritime, rail and road mode of transport is currently covered by an ENS filed in ICS. Until the economic operators, transporting this cargo, connect to ICS2, they need to continue filing their ENSs to ICS.

ANNEXES

ANNEX A: EO PROJECT PLAN TEMPLATE



Project Plan for EO
CT R3_[EO Name]

ANNEX B: EO OPERATIONS CHECKLIST FOR MOVING TO PRODUCTION

Operations Checklist depicts the activities that must be implemented by EOs to be considered as ready to enter in ICS2 Operations.



ICS2_R3_Operation
s Checklist_EO-v2.xls

ANNEX C: INCIDENT MANAGEMENT FORM



Incident
Management Form.c

ANNEX D: GUIDE TO REGISTER CERTIFICATE IN UUM&DS

In order to register its certificate in UUM&DS Admin application, the sender should provide the “BP_MANAGE” business profile and follow the below steps:

1. The sender authenticates in UUM&DS and accesses the UUM&DS Admin application;
2. The sender goes to the screen where its identity is displayed, and selects the "Certificates" tab;
3. The sender clicks on the + icon to add a new certificate;
4. The sender specifies that he wants to register a certificate for signing, for which he is able to sign the registration document with the private key related to this certificate;
5. The sender fills in the form by providing a name, a description; the purpose is automatically set to "SIGNING";
6. UUM&DS generates a PDF file containing the information about the sender with a text indicating his intention of registering the certificate being part of the signature of this registration, and seals it as a proof of creation;
7. The sender downloads the sealed PDF registration and needs to sign it with the private key corresponding to the certificate that has been uploaded;
8. The sender uploads the signed registration;
9. UUM&DS validates the signature of the registration:
 - a. The signature must be valid (cryptographic verification);
 - b. The document signed should have not been altered except the addition of a new signature;
 - c. The signing certificate should be trusted by UUM&DS;
 - d. The signing certificate should not be already registered for another identity.

10. UUM&DS establishes the level of the certificate registration: Qualified or Non-Qualified. The level is the lowest value of the certificate and the signature of the certificate registration;
11. UUM&DS provides the information of the registration: information about the certificate, purpose and computed level (Non-Qualified, Qualified);
12. The certificate becomes active for UUM&DS digital signatures operations.

ANNEX E: UUM&DS SYSTEM ONLINE COURSE

Attend course by accessing the following URL:

[Course: UUM&DS system: Your passport to EU applications, Topic: en \(europa.eu\)](#)

ANNEX F: HOW TO ACCESS CIRCABC AND CUSTOMS & TAX EU LEARNING PORTAL

To log in to Customs and Tax EU Learning Portal, a user needs to be registered in EU Login. In order to do so, the new user shall navigate to the main official page (<https://customs-taxation.learning.europa.eu>) and choose "Login" in the right section of the page. Then, the user shall press the "Create an account" link which will redirect him to a new page where user should insert their personal details.

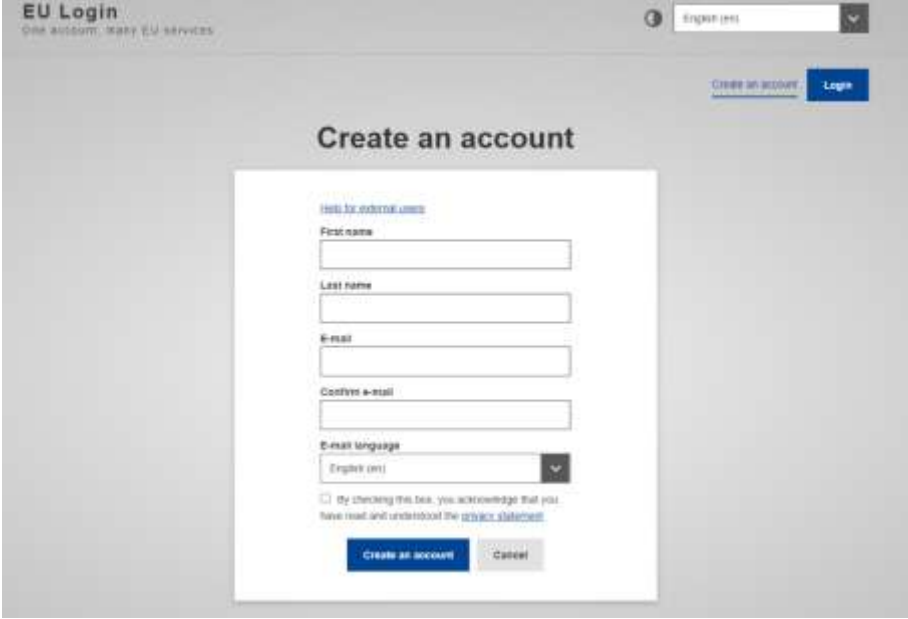
The image shows a screenshot of the 'EU Login' website's 'Create an account' page. The page has a light grey background. At the top left, it says 'EU Login' and 'One account. Many EU services'. At the top right, there is a language dropdown menu set to 'English (en)'. Below this, there are two buttons: 'Create an account' (in blue text) and 'Login' (in a blue box). The main heading is 'Create an account'. Below this, there is a white box containing the registration form. The form includes a link for external users, fields for 'First name', 'Last name', 'E-mail', and 'Confirm e-mail', a dropdown for 'E-mail language' (set to 'English (en)'), and a checkbox for terms and conditions. At the bottom of the form are two buttons: 'Create an account' (in a blue box) and 'Cancel' (in a grey box).

Figure 16: Create an account - EU Login

After providing the requested details, the user should press the "Create an account" button and an e-mail will be sent to the e-mail address that was provided. Then, by clicking on the link provided via the e-mail, the user should generate a personal password and as a result access will be granted.

Afterwards, by redirecting to the main page, the user should edit their profile and complete the registration by adding further details (e.g., Location, Institution, etc.)

Figure 17: Complete registration in Customs & Tax EU Learning Portal

Click on ‘Save’ button and proceed with the acknowledgment and accepting of all the policies.

To access CIRCABC, user shall navigate to CIRCABC main page (<https://circabc.europa.eu/ui/welcome>) by using the “EU Login” in case user is already registered in EU Login. Otherwise, user shall click on the “Create EU Login account” button.



Figure 18: CIRCABC - Main Page

By clicking on “Create EU Login account” button, the process to be followed is the same as described above.

Note: For accessing any publicly available folders in CIRCABC, no user account creation is required.

ANNEX G: EO CONSOLIDATED CT REPORT



EO Consolidated
Report for EO CT R3.