OWNER:	ISSUE DATE:	VERSION:
DG TAXUD	27/07/2020	20.20

TAXATION AND CUSTOMS UNION DG

SUBJECT:

Design Document for Common Operations and Methods

Main Document

FRAMEWORK CONTRACT TAXUD/2013/CC/124

SPECIFIC CONTRACT 25

Document History[1]

Edition	Revision	Date	Description	Action[2]	Pages/Sections
DDNTA 8	00	23/03/2005	Implementing QA review comments. Implementing TC's comments based on TCE-MTM02-L1SA8-v0.20-EN (TCP-ECS Workshop, Athens, March 9th 2005). Submitted for Acceptance to Taxation and Customs Union DG.	I, R	As Required
DDNTA 8	10	15/04/2005	Implementing QA verification comments. Re-submitted for Acceptance to Taxation and Customs Union DG.	I/R	ECS & NCTS Appendices
0	10	05/03/2007	Restructure of DDNTA into DDNA with separate volumes for Common and specific Customs Domains.	I	All
0	20	23/03/2007	Implementing internal review comments. Submitted for review to Taxation and Customs Union DG.	I/R	As Required
1	00	09/05/2007	Implementing QA review comments. Submitted for acceptance to Taxation and Customs Union DG.	I/R	As Required
1	10	11/05/2007	Implementing verification comments. Re-submitted for acceptance to Taxation and Customs Union DG.	I/R	As Required
2	00	28/09/2007	Implement ECG Review comments. Submitted for acceptance to Taxation and Customs Union DG.	I/R	As Required
2	10	17/02/2008	DDCOM update for ICS domain Submitted for review to Taxation and Customs Union DG.	I/R	As Required
3	00	19/02/2008	Implementing review comments. Submitted for acceptance to Taxation and Customs Union DG.	I/R	As Required
3	10	09/06/2008	Incorporating RFA 816 functionality. Submitted for review to Taxation and Customs Union DG.	I/R	IV.2, VIII.2.17, VIII.4.12
4	00	25/06/2008	Implementing review comments. Submitted for acceptance to Taxation and Customs Union DG.	I/R	As Required
4	10	28/10/2008	Incorporating RFA 848 functionality for the incorporation of EOS in DDCOM. Implementing DDNA KEL v0.18. Implementing calls INC0807.109564 and INC0809.111672. Submitted for review to Taxation and Customs Union DG.	I/R	Section I.1.1, I.1.2, I.1.8, V.2, V.3.1, V.4, VII.5, VII.6.1, VII.6.2, VII.6.6, VII.6.7, VIII.2.6, VIII.2.17,

---

[1] This history shows for historical reasons the last two releases of the DDNTA before it was restructured into the DDNA. This version is the first version of the DDCOM submitted for review.

[2] Action: I = Insert; R = Replace

Edition	Revision	Date	Description	Action[2]	Pages/Sections
					VIII.4.10
5	00	18/11/2008	Implementing review comments. Submitted for acceptance to Taxation and Customs Union DG.	I/R	As Required
5	01	26/10/2009	Implementing DDNA KEL v0.21. Incorporating information regarding the IE12 message that is exchanged in the scope of the NCTS/TIR-RU pilot project. Submitted for internal review.	I/R	Sections: VI.2.2, VII.8, VIII.2.17, VIII.2.18, VIII.2.19, VIII.2.22, VIII.4.12
5	10	27/10/2009	Implementing internal review comments. Submitted for review to Taxation and Customs Union DG.	I/R	As required
6	00	05/11/2009	Implementing review comments. Submitted for acceptance to Taxation and Customs Union DG.	I/R	As Required
6	01	11/01/2010	Incorporating QTM 970 functionality for Customs Business Statistics. Implementing the following calls: • INC0909.135833 for the removal of the programmatic mode from CS/RD and the removal of IE031/IE032 attachments from CS/RD notifications; • INC0907.132635 for the support of printable ASCII characters only in non-language sensitive fields; • INC0908.133794 for the non-use of leading and trailing spaces within text fields; • INC0911.139015 for specifying that text fields shall be case sensitive; • INC0912.140662 for correcting the inconsistency between TR9181 in DDNA appendix Q2 and DDCOM section VII.5.7. Submitted for internal QC review.	I/R	Sections: I.1.8, II.2.3, II.3.1, II.3.2, II.3.3.3, II.3.3.4, II.4.1, V.2.1.1.2, V.2.1.2.1.2, VII.6.7, VIII.2.19, IX.1
6	10	12/01/2010	Implementing internal QC review comments. Submitted for review to Taxation and Customs Union DG.	R	As Required
7	00	01/02/2010	Implementing review comments. Submitted for acceptance to Taxation and Customs Union DG.	I,R	As Required
7	10	15/04/2010	Implementing ECG review comments. Submitted for review to Taxation and Customs Union DG.	I,R	As Required
8	00	20/04/2010	Implementing verification comments. Submitted for acceptance to Taxation and Customs Union DG.	I,R	As Required
9	00	28/02/2011	Project and contractual data is updated. Aligned with KEL 0.23 and review	I/R	Sections: VII.3, I.1.8, I.3,

Edition	Revision	Date	Description	Action[2]	Pages/Sections
			comments implemented. Submitted for review&acceptance to Taxation & Customs Union DG.		V.2.1.1.1, VII.6.1
9	10	01/02/2012	Project and contractual data updated. Aligned with KEL 0.24. Submitted for review to Taxation and Customs Union DG.	I/R	Sections: I.1.8.4, I.3.1.1, I.3.2, V.2.1.2.1.2, V.2.1.2.2
10	00	22/02/2012	The review comments are implemented. Submitted for acceptance to Taxation and Customs Union DG.	I/R	As Required
10	01	26/03/2012	Aligned with KEL 0.23a. Sent to the internal and language review.	I/R	Sections: I.1.8.5, V.2.1.2.1.1, V.2.1.2.2
10	10	30/03/2012	Comments from the internal and language review are implemented. Submitted for review to Taxation and Customs Union DG.	I/R	As Required
10	50	27/04/2012	Submitted for acceptance to Taxation and Customs Union DG.	I	6
10	60	24/07/2012	Project and contractual data updated. Aligned with KEL 0.25. **WARNING: This and the next version do NOT include the changes for KEL v0.24a.** Submitted for review to Taxation and Customs Union DG.	I/R	Sections: I.1.8.7, I.3.2, VII.1.2
11	00	20/08/2012	The review comments are implemented. Submitted for acceptance to Taxation and Customs Union DG.	I/R	Page 71
10	65	14/02/2013	Project and contractual data updated. Aligned with KEL 0.24a. **This and the next version were created in a side branch to address urgent business needs in DDNIA.** Submitted for review to Taxation and Customs Union DG.	I,R	Pages 20, 22, 29 and 32
10	70	27/02/2013	The review comments are implemented. Submitted for acceptance to Taxation and Customs Union DG.	I,R	Page 22
11	10	06/03/2013	Project and contractual data updated. Aligned with KEL 0.25a. **This and the next version include also the changes introduced within KEL v0.24a.** Submitted for review to Taxation and Customs Union DG.	I/R	Pages 22, 24, 31 and 34
11	50	08/04/2013	The review comments are implemented. Submitted for acceptance to Taxation and Customs Union DG	I/R	Page 23

Edition	Revision	Date	Description	Action[2]	Pages/Sections
11	51	07/08/2013	Aligned with KEL 0.26. KEL entries #326 and #332 are implemented. Sent to the internal review.	I/R	Pages 24, 28, 32-35, 79, 102-106
11	60	12/08/2013	The review comments are implemented. Submitted for review to Taxation and Customs Union DG.	I/R	Pages 32, 103-104
12	00	06/09/2013	The review comments are implemented. Submitted for acceptance to Taxation and Customs Union DG	I/R	Pages 19, 22, 25, 31, 32, 35, 41 and 56
12	01	08/01/2014	Project and contractual data updated. Aligned with KEL 0.27. No major changes implemented. Sent to the internal review.	I,R	Pages 28, 31, 32 and 35
12	10	14/01/2014	The review comments are implemented. Submitted for review to Taxation and Customs Union DG.	I,R	As required
13	00	19/02/2014	The review comments are implemented. Submitted for acceptance to Taxation and Customs Union DG.	I/R	As required
13	10	19/02/2015	Implementing QTM037 (RFC-List.28 Movements System RFC#353, #354, #355, #356, #357). Submitted for Review (SfR) to Taxation & Customs Union DG. Also for review by the National Administrations.	I/R	Sections: I.2.3, I.3.1.2, II.1.1, II.3, II.3.2.1.2, II.3.2.3, II.4.6.3.2, II.6.1.2, II.6.2.4, II.7.4, V.2.1.1.2, V.6.1, V.6.2, VIII 1.2
14	00	24/03/2015	Implementing DG TAXUD and NAs review comments. Submitted for Acceptance (SfA) to DG TAXUD.	I/R	As required
14	10	30/03/2015	Incorporating DG TAXUD verification comments. Re-Submitted for Acceptance (SfA2) to DG TAXUD. Content and layout fixed.	I/R	As required
14	20	09/02/2017	Implementing QTM142 (RFC-List.29 Movements System RFC#388) and RTC-19999 (RFC related to CSRD2). Submitted for Review (SfR) to DG TAXUD. Also for review by National Administrations.	I/R	Sections: I.1.8.12, I.3.1,I.3.2, II.3, II.4, IV.1.3, IV.2
15	00	16/03/2017	Implementing DG TAXUD and NPM review comments. Submitted for Acceptance (SfA) to DG TAXUD.	I/R	As required
15	10	03/10/2018	Implementing QTM291. Submitted for	I/R	See section

Edition	Revision	Date	Description	Action[2]	Pages/Sections
			Review (SfR) to DG TAXUD and to the Forerunners NAs (DE & PL).		I.1.8.13 Change history
16	00	20/12/2018	Implementing QTM291. Submitted for Acceptance (SfA) to DG TAXUD.	I/R	As required
16	10	04/04/2019	Implementing comments raised by DG TAXUD and the Forerunners NAs (DE & PL). SfA, for Review only, to DG TAXUD.	I/R	As required
17	00	26/06/2019	Implementing comments raised by DG TAXUD and QA4. Submitted for Acceptance (SfA) to DG TAXUD.	I/R	As required
17	10	24/07/2019	Implementing QTM291. Submitted for Review (SfR) to DG TAXUD and the Forerunners NAs (DE & PL).	I/R	As required
18	00	23/08/2019	Implementing comments raised by DG TAXUD and QA4. Submitted for Acceptance (SfA) to DG TAXUD.	I/R	As required
18	10	30/08/2019	Implementing QTM291. Submitted for Review (SfR) to DG TAXUD.	I/R	See section I.1.8.19 Change history
19	00	13/09/2019	Implementing DG TAXUD and QA4 review comments. SfA to DG TAXUD. SfR to National Administrations (via ECCG).	I/R	As required
19	10	06/12/2019	Implementing comments from National Administrations (via ECCG) and DG TAXUD. SfR to DG TAXUD & 'Sent for Acceptance by ECCG' (verification of comment implementation).	I/R	As required
20	00	19/12/2019	Implementing feedback received from National Administrations and DG TAXUD after verification of the version 'Sent for Acceptance by ECCG'. Submitted for Acceptance (SfA) to DG TAXUD.	I/R	As required
20	10	01/07/2020	Implementing RFC-List.31 SfR to DG TAXUD & ECCG for verification of RFC-List.31 implementation.	I/R	As required
20	20	27/07/2020	Implementing comments raised by DG TAXUD (incl. QA4) and ECCG. Submitted for Acceptance (SfA) to DG TAXUD and ECCG.	I/R	As required – See section I.1.8.24

Table of Contents

List of Figures

List of Tables

I General Introduction

I.1 Document Overview

I.1.1 Purpose of DDNA

The DDNA, the **Design Document for National Applications,** supersedes the Design Document for National Transit Applications for NCTS and ECS. It specifies the design requirements to which any Customs Movement Application needs to conform.

The DDNA is **applicable to every Transit, Export and Import Control Application** and must be considered as a mandatory document for all implementation and verification activities.

The DDNA is aligned with [R26], [R13], [R14], [R28] and [R29].

Document [R26] contains the specifications for the entire NCTS (encompassing all Phases and sub-Phases), foreseeing a number of electronic and other (paper) Information Exchanges.

Documents [R13] and [R14] contain the specifications for ECS and ICS respectively, foreseeing a number of electronic exchanges.

Documents [R28] and [R29] contain the L4 BPMs/FSS for AES-P1 and NCTS-P5 respectively, foreseeing a number of electronic exchanges.

The DDNA consists of four volumes. One volume exists for each system (Transit, Export and Import), defining the design requirements of the specific system, and there is one common volume, which defines common operations and methods for all systems. This volume is the Design Document for Common Operations and Methods (DDCOM) volume. For more information about DDCOM's purpose and structure, please refer to [I.1.3] and [0], respectively.

The document Design Document for Reference Data Application [R27] complements the DDNA for what concerns the management of reference data. It includes CS/RD related information extracted from DDCOM version 14.10 and defines all CS/RD2 interfaces available to National Administrations.

Information Exchanges are foreseen in the Common Domain (between National Administrations; between National Administrations and OLAF; and between National Administrations and Central Services), in the National Domain (local to a National Administration), and in the External Domain (between National Administration and Traders). Common Domain exchanges will always take place via the CCN/CSI communication platform or the Inter(Extra)net. The different formatting and transport mechanisms will, therefore, be defined, in detail, in the DDNA. Moreover, additional design constraints and additional details on error and exception handling will be stated.

Within the Customs systems, the Central Project Team (CPT) will produce a number of Centrally Developed Customs Application (CDCA) tools (e.g. STTA[3], TTA[3], CS/RD2, CS/MIS, TAXUD ieCA[4] and CTA[4]) in order to assist the NAs in implementing, verifying and operating their National Customs Application (NCA). All these CDCA tools must conform to this document, although their specification is not part of this document. In order to construct an NCA, the NA should therefore use this document, in order to decide which functionality remains to be implemented.

I.1.2   DDNA Structure

The DDNA consists of the following four volumes:

- Design Document for National Transit Application volume (DDNTA);

- Design Document for National Export Application volume (DDNXA);

- Design Document for National Import Application volume (DDNIA);

- Design Document for Common Operations and Methods volume (DDCOM).

I.1.3   Purpose of the DDCOM volume

This volume, which is the Design Document for Common Operations and Methods, defines the common features applicable to all Customs Applications.

In particular, this volume defines:

- How an NCA can exchange information with Central Services via a manual (web browser) mode;

- A number of principles for the NCAs that are common regardless of the transportation mechanism;

- The format of messages (EDIFACT and XML);

- How the messages need to be transported across the CCN/CSI.

    Note: the message exchange protocols between NCAs and CS/RD2 regarding the collection and dissemination of reference data can be found in [R27].

I.1.4   Scope of DDCOM volume

This volume is restricted to the electronic Information Exchanges within Customs systems.

This version of DDCOM is applicable to NCTS Phase 4, NCTS Phase 5, ECS Phase 2, AES Phase 1 and ICS Phase 1.

---

[3] Applicable to NCTS-P4, ECS-P2 and ICS-P1
[4] Applicable to NCTS-P5 and AES-P1

In addition, this version of DDCOM is also applicable to TAXUD ieCA specifications and implementation (e.g. exception handling, etc.).

I.1.5   *Intended audience*

The intended audience for this document includes:
- Any person responsible for the functional specifications of a Customs application;

- Any person responsible for the development of software in the context of a Customs application;

- Any person responsible for the definition of tests for a Customs application;

- Anyone within the affected service suppliers in the CCN/CSI projects responsible for the delivery of the required services to a Customs application;

- Any other authorised body affected by a Customs application, including EC/EFTA Joint Committee on Community/Common Transit, Electronic Customs Group, OLAF, and Traders Associations.

Readers are assumed to have a good understanding of the IT concepts and terminology used in this document. It is also assumed that readers are aware of the contents of the Functional Specifications of the various trans-European movement systems (including [R13], [R14] , [R24], [R26], [R28], [R29], [R32], [R33], [R34] and [R35]).

I.1.6 Structure of DDCOM Volume

This volume is structured in sections (further subdivided in chapters) that are applicable to all movement systems.

The different sections and chapter categories are distinguished by their heading naming convention.

This volume comprises the sections, chapters and lists of appendices summarised below:

SECTION I - GENERAL INTRODUCTION includes the following chapters:
- Chapter 1 describes the **purpose** and the **scope** of DDNA, the **intended audience**, the **internal structure** of the document, plus some document **service information**;
- Chapter 2 contains **definitions** used in this document (terminology, acronyms and abbreviations);
- Chapter 3 describes the relationship of this document with other Customs systems baseline documents. It defines dependencies with these documents and states the applicability of these documents. It also explains how this document, together with the other Customs systems documentation, should be used during the development and verification of the Customs applications being covered by the DDCOM;
- Chapter 4 describes the **symbolism and the conventions** used in the various models included in this document. It also discusses the technical naming conventions used for the data dictionary.

SECTION II - CENTRAL SERVICES deals with availability reporting and statistics. It is subdivided as follows:
- Chapter 1 defines the Messages involved in Central Services;
- Chapter 2 defines how statistics and availability data are exchanged;
- Chapter 3 defines the message protocols to be used for exchanges with the CS/MIS application via the Inter(Extra)net (for exchanges of statistics data and availability data);
- Chapter 4 defines the message protocols to be used for exchanges with the CS/MIS application via CCN/CSI.

SECTION III - SYSTEMS ADMINISTRATION deals with issues such as logging and tracing and any other administration function to be foreseen.

SECTION IV – TECHNICAL MESSAGE STRUCTURE defines the detailed technical structure of the Information Exchanges for movement systems. This section is further subdivided as follows:
- Chapter 1 introduces the key elements of a basic data dictionary. It defines a number of items that make up a message, such as Data Items, Data Groups, Code Lists (sets of discrete values). This chapter is accompanied by the corresponding DDNA Appendices Y, Z and C. Appendix C (for the domains where this applicable) with all the applicable code lists is directly generated by the application CS/RD2;
- Chapters 2, 3 and 4 presents the detailed Technical Message Structure (TMS) for the different Information Exchanges for the legacy and UCC compliant systems (during and post TP). The detailed TMS for all messages is included in each domain volume's Appendix Q2, possibly complemented by Appendices Q1 and/or Q3. This chapter will only explain how the Appendix Q2 needs to be interpreted and used;

- Chapters 5, 6, 7 are analysing various aspects that concern the design and definition of Rules, Conditions, TRTs, BRTs, Technical rules and Guidelines applicable to AES-P1 and NCTS-P5;
- Chapters 8 and 9 discusses the issue of **consistency** for the legacy and UCC compliant systems**.** It defines with which Customs documents this DDNA needs to be consistent (such as FTSS [R26] and SAM Mapping Specification [R12]) and it explains how this consistency has been achieved during the TMS definition.

SECTION V – DESIGN PRINCIPLES explains how the system, defined in the previous sections, needs to be built. Basically, every Information Exchange needs to be formatted in one of two formats (EDIFACT and/or XML) and needs to be transmitted across one of two communications platforms (CCN/CSI or Inter(Extra)net). This section states a number of principles that are common, regardless of the message format and transportation mechanism:

- Chapter 1 discusses the overall **approach**;
- Chapter 2 discusses the usage of **character sets** and **Data Item conventions**;
- Chapter 3 defines **exception handling** (how Customs systems should prevent and handle failures, defects, errors or mistakes);
- Chapter 4 describes the use of **Functional error** data group in IE906 for ECS-P2, NCTS-P4 and ICS-P1;
- Chapter 5 describes the use of **Functional error** data group in IE906 for AES-P1 and NCTS-P5;
- Chapter 6 defines some constraints that are applicable to the Customs system, including performance and availability;
- Chapter 7 defines the **structure of Master Reference Number** and **Guarantee Reference Number**.

SECTION VI – EDIFACT MESSAGE FORMATTING defines in detail how messages need to be formatted in EDIFACT. This section is subdivided as follows:

- Chapter 1 introduces **EDIFACT conventions** in general;
- Chapter 2 defines **EDIFACT conventions** used in Customs systems;
- Chapter 3 provides an overview of **EDIFACT mapping** and points to the tables that list which Information Exchanges are mapped to each EDIFACT messages for each Customs domain (NCTSP4 or ECSP2);
- Chapter 4 describes the **Message Hierarchies**. Appendix Y accompanies this chapter;
- Chapter 5 explains the detailed low-level **mapping** of the Customs messages upon the UNSMs. Appendix H and Appendix I accompany this chapter;
- Chapter 6 describes the formatting of **Functional error in EDIFACT**;
- Chapter 7 describes the **EDIFACT CONTRL** message to be used in the EDIFACT exchanges.

SECTION VII – XML MESSAGE FORMATTING defines how messages need to be formatted in an XML format. This section is structured as follows:

- Chapter 1 defines **XML conventions** for Customs systems;
- Chapters 2 and 3 discusses the **XML formatting** of the Information Exchanges. Appendix R of DDNA accompanies this chapter;
- Chapter 4 discusses the **DTDs** of Customs messages where applicable. Appendix T accompanies this chapter;
- Chapter 5 describes the **XML CONTRL** message to be used in the XML exchanges;
- Chapter 6 describes the **Message Header** for the ICS-P1 exchanges.

- Chapter 7 describes the **Message Header** for the NCTS-P5 and AES-P1 exchanges.
- Chapters 8 and 9 describes **XSD** Conventions as well as the structure of the XSDs.

SECTION VIII – TRANSPORT OF MESSAGES VIA CCN/CSI defines how messages need to be transported across the CCN/CSI communication platform. This section is subdivided as follows:

- Chapter 1 defines **architectural assumptions** made for the transport of messages via CCN/CSI and details where references to CCN/CSI can be found.
- Chapter 2 presents the **mandatory CCN/CSI elements** that will ensure end-to-end communication between two CCN gateways.
- Chapter 3 presents the **recommended CCN/CSI elements** for sending and receiving messages.
- Chapter 4 defines the **configuration information** necessary for the CCN gateways;
- Chapter 5 defines the **CCN/CSI statistics services** provided by ITSM CONTRACTOR.

SECTION IX – TRANSPORT OF MESSAGES VIA INTER(EXTRA)NET defines how messages need to be transported across the Inter(Extra)net communication platform.

- Chapter 1 states common Internet principles;
- Chapter 2 discusses **security** aspects of Inter(Extra)net transport.

I.1.7   *Document service information*

The different parts that make up DDNA will each be submitted individually to configuration and version control. Individual components may be upgraded and delivered separately.

Maintenance will be provided for this document. The Taxation and Customs Union DG will define and schedule the different deliveries.

Comments can be submitted to this document, either via organised reviews or via calls to the Central Service Desk at ITSM (https://itsmtaxud.europa.eu/smt/ess).

Known errors to the DDCOM volume will be maintained in the format of the RFC-List published on CIRCABC.

Whenever a part of this document is referred to, reference will be given to an entire section or an entire chapter (within a section) or a paragraph (for any other subdivision).

This document will be submitted as a Word file with the following naming convention:
DDCOM-Main Document-v*y.zz*-SfR/SfA.doc, where *y* and *zz* are version and revision numbers.

I.1.8 *Change history[5]*

I.1.8.1 Changes in DDCOM versions 5.10 and 6.10

Version 5.10 of DDCOM incorporates the following changes:

- Implementation of DDNA KEL v0.21 (KEL entries #192, #201, #202 and #213);

- Incorporation of message exchange details (i.e., EDIFACT conventions, queue naming and addressing, national and Taxation and Customs Union DG gateways, configuration information) regarding the IE012 message that is exchanged in the scope of the NCTS/TIR-DATA pilot project.

Version 6.10 of DDCOM incorporates the following changes:

- Incorporation of new Customs Business Statistics functionality
  - *II.3.2.3*: Updated to:
    - o Introduce ECS and ICS business statistics;
    - o Specify that NAs will be able to send one IE411 message for multiple domains or multiple domain-specific IE411 messages;
    - o Indicate that CS/MIS will produce an IE412 message per domain as soon as an IE411 message is received;
    - o Define that, each time an IE412 is produced, CS/MIS will combine this IE412 with other IE412 messages created for other periods and generate a domain-specific XLS file, which will also be available for download on CS/MIS Web interface.
  - *II.7.1*: Updated to define that the IE411 message will have EDIFACT or XML format and will either be sent to the CS/MIS application across CCN/CSI or it will be uploaded on CS/MIS Web interface;
  - *II.6.1.2 and II.6.2.4*: Updated to include IE411.
- INC0909.135833
  - *II and IX*: Updated to remove of the programmatic mode from CS/RD and IE031/IE032 attachments from CS/RD notifications.
- INC0907.132635
  - *V.2.1.2.1.2*: Updated to specify the support of printable ASCII characters only in non-language sensitive fields.
- INC0908.133794
  - *V.2.1.1.2*: Updated to specify the non-use of leading and trailing spaces within text fields for both normal spaces and non-breaking spaces.
- INC0911.139015
  - *V.2.1.1.2*: Updated to specify that text fields shall be case sensitive.
- INC0912.140662

---

[5] This history shows for historical reasons the last release of the DDNTA before it was restructured into the DDNA.

- *VII.5.7:* Updated to correct the inconsistency between TR9181 in DDNA appendix Q2 and DDCOM section VII.5.7.

I.1.8.2 Changes from DDNTA version 8.10

DDCOM incorporates the following changes:
- The DDNA has been divided into four volumes – one each for Common, NCTS, ECS and ICS;
- Implementation of "FTSS – AES Addendum 1/2006";
- Implementation of DDNTA KEL v0.11.

I.1.8.3 Changes in DDCOM version 9.00

DDCOM incorporates the following changes:
- Implementation of DDNA KEL v0.23
- INC0908.134169 (DDNA KEL#224)
  The first and seventh paragraph of DDCOM section V.2.1.1.1 (Numerical fields) amended regarding the definition in the use of numerical value fields.
- INC0910.138415 (DDNA KEL#227)
  Section VII.3 (Document Type Definition) updated to exclude ICS.

I.1.8.4 Changes in DDCOM version 10.00

DDCOM incorporates the following changes:
- Implementation of DDNA KEL v0.24
  - IM15049 (DDNA KEL#300)
    Section V.2.1.2.1.2 "Non-language sensitive text fields" and second paragraph of section V.2.1.2.2 "Exchanges in XML format" amended regarding the clarification of ASCII characters usage.

I.1.8.5 Changes in DDCOM version 10.50

DDCOM incorporates the following changes:
- Implementation of DDNA KEL v0.23a
  - IM22001 (DDNA KEL#305)
    Section V.2.1.2.1.1 "Language-sensitive text fields" and second paragraph of section V.2.1.2.2 "Exchanges in XML format" amended regarding the usage of character set UNOK: Turkish, ISO 8859-9.

I.1.8.6 Changes in DDCOM version 10.70

No changes were implemented in the DDCOM version 10.70. In the scope of the DDNA Known Error List (KEL) 0.24a only changes in the DDNIA are implemented. **This version was created in a side branch to address urgent business needs in DDNIA.**

I.1.8.7 Changes in DDCOM version 11.00

DDCOM incorporates the following changes **(WARNING: This version does NOT include the changes for KEL24a)**:
- Implementation of DDNA KEL v0.25

- o IM23666 (DDNA KEL#313)
  The chapter 'VII.1.2 Character set support' amended - in order to avoid repeating of the supported character sets several times, the cross-reference to "V.2.1.2.1.1 Language-sensitive text fields" paragraph is added.

I.1.8.8 Changes in DDCOM version 11.50

No changes were implemented in the DDCOM version 11.50. In the scope of the DDNA Known Error List (KEL) 0.25a only changes in the DDNTA, DDNXA and DDNIA are implemented. **This version includes also the changes introduced within KEL v0.24a.**

I.1.8.9 Changes in DDCOM version 12.00

DDCOM incorporates the following changes:
- ▪ Implementation of DDNA KEL v0.26
  - o KE11054/IM15061 (DDNA KEL#326 'MRN and GRN structure (DDCOM update)')
    New sub-section V.6 'MRN and GRN structure' is added to the section V 'Design principles' in order to describe MRN and GRN structure.
  - o KE10029 (DDNA KEL#322 'Clarification of allowed value for 'MsgType' in IE411')
    The section 'II.7.1 Sending IE411 data to CS/MIS' is updated.

I.1.8.10 Changes in DDCOM version 13.00

No major changes were implemented in the DDCOM version 13.00. The changes included in the DDNA Known Error List (KEL) 0.27 do not affect DDCOM, but the DDNIA, DDNXA and DDNTA documents.

I.1.8.11 Changes in DDCOM version 14.10

DDCOM incorporates the following changes:
- ▪ Implementation of DDNA RFC-List.28:
  - o Multiple corrections in various sections of Chapter II, as defined in DDNA RFC #353 - (587) Removing IE413 and OTS-(related to KE11645/IM80519);
  - o Section II.3.2.5 is added and section II.7.4 is inserted , according to DDNA RFC #354 - (645) Error messages duplication to CS/MIS (related to IM92061);
  - o Section II.4.6.3.2 updated, as defined in DDNA RFC #355 - (575) Adding some flexibility in TR9200 (for ITSM Support) (related to KE/12049/KE12051/KE12052/IM36381);
  - o Sections V.6.1 and V.6.2 updated, as defined in DDNA RFC #356 - (574) DDCOM: MRN and GRN format (only capital letters) + incorrect MRN (related to KE12384/IM56447/IM67432);
  - o Section V.2.1.1.2 updated, as defined in DDNA RFC #357 - (643) DDCOM: management of XML escaping characters (related to IM80518).
  - o Section V.2.1.2.1.1 Language-sensitive text fields corrected for UNOG, as defined during the DDNA review cycle with NAs.

I.1.8.12   Changes in DDCOM version 15.00

DDCOM incorporates the following changes:
- Implementation of DDNA RFC-List.29:
  o Multiple corrections in section VIII, as defined in DDNA RFC #388 [(543) DDNTA: From 'NCTS/TIR-RU' to a more generic 'NCTS/TIR-DATA' description], to define the queues that will be used by the SPEED2 Platform;
- Implementation of RTC-19999:
  o Multiple updates in several sections with the general principle that:
    o For the backward compatibility of CS/RD2: DDCOM remains the reference point. The new Design Document for Reference Data Application (DDRDA) [R27] will point to it.
    o For the new functionalities of CS/RD2: the DDRDA [R27] is the new reference point. DDCOM only points to it.

I.1.8.13   Changes in DDCOM version 15.10

DDCOM incorporates the following changes:

- Changes in Section III with NCTS-P5 and AES-P1 requirements:

  o Section III.1 updated for information to be stored during the Transitional Period of NCTS-P5 and AES-P1 operations and when NCA[NCTS-P5/AES-P1] uses a convertor (TAXUD ieCA) or National Convertor (NCO) for downgrade or upgrade of messages for CD exchanges between NCA[NCTS-P5/AES-P1] and NCA [NCTS-P4/ECS-P2]

- Changes in Section IV with NCTS-P5 and AES-P1 requirements:

  o Section IV.2 title updated to clarify that concern only NCTS-P4, ECS-P2 and ICS-P1

  o Section IV.3 added for Technical message structure for NCTS-P5 and AES-P1. *Note: The definition of TRTs validity has changed compared to v15.10 to reflect the comment raised by NA-PL during the workshop on 14/12/2018.*

  o Section IV.4 added for Technical message structure for NCTS-P5 and AES-P1

  o Section IV.5 added for Numbering Convention for Rules/T/TRT and Conditions for NCTS-P5 and AES-P1

  o Section IV.6 added for Rules/T/TRT and Conditions definition and syntax for NCTS-P5 and AES-P1

  o Section IV.7 added for logic of Rules/T/TRT and Conditions validation sequence for NCTS-P5 and AES-P1

  o Section IV.8 title updated to clarify that concern only NCTS-P4, ECS-P2 and ICS-P1

  o Section IV.9 added to describe DDNA consistency for NCTS-P5 and AES-P1

- Changes in Section V with NCTS-P5 and AES-P1 requirements:

    o Section V.2.1.1.3 added to define Date/Time Fields (NCTS-P5 and AES-P1)

    o Section V.3.1 updated with minor/cosmetic corrections

    o Section V.3.2.1.1. updated to clarify Functional errors use for NCTS-P5 and AES-P1

    o Section V.3.2.1.4 added to specify exception handling after the Transitional Period (NCTS-P5 and AES-P1)

    o Section V.3.2.1.5 added to specify exception handling during the Transitional Period (NCTS-P5 and AES-P1)

    o Section V3.3. updated to clarify use of Functional error codes in IE906 (CD906C) for NCTS-P5 and AES-P1

    o Section V.4 updated to clarify use of Functional error in IE906 (CD906A)

    o Section V.5 added to specify the use of Functional error in IE906 (CD906C)

    o Section V.7.1 updated to clarify use of existing MRN structure for NCTS-P4, ECS-P2 and ICS-P1 and to define the XSD restriction for MRN data item in NCTS-P4, ECS-P2 and ICS-P1 (MRNType)

    o Section V.7.2 updated to define the XSD restriction for GRN data item in NCTS-P4 and NCTS-P5.

    o Section V.7.3 added to define the new MRN structure for NCTS-P5 and AES-P1 and to define the XSD restriction for MRN data item (MRNType) based on this structure.

- Changes in Section VII with NCTS-P5 and AES-P1 requirements:

    o Section VII.3 added to define XML mapping of Information Exchanges for AES-P1 and NCTS-P5

    o Section VII.5 updated to mention CD917C for NCTS-P5 and AES-P1 using the Message Header for NCTS-P5 and AES-P1

    o Section VII.6 title updated to clarify that concern only ICS-P1

    o Section VII.7 added to define the Message Header for NCTS-P5 and AES-P1

    o Section VII.8 title updated to clarify that concern only NCTS-P4, ECS-P2 and ICS-P1

    o Section VII.9 added to define the XSD principles and conventions for NCTS-P5 and AES-P1

- Minor change in Section IX removing CS/RD2 reference since such aspects of CS/RD2 are defined in DDRDA [R27].

I.1.8.14   Changes in DDCOM version 16.00

DDCOM incorporates the changes in v15.10 and minor changes introduced due to comments raised during the review cycle of the aforementioned version.

I.1.8.15   Changes in DDCOM version 16.10

The deliverables cover the following items:

- Implementation of comments marked as "Implementation delayed" for Iteration 2 during the review cycle of DDCOM v15.10 – **RTC id 35359**
- Example provided for C0810 in IV.5.1: example of a Condition which requires data from a different message than the one applicable, in order to be validated - **RTC id 34081**
- Mandatory CorrelID in UCC phases – **RTC id 35112**
- Completion of figures in VII.9 (XSD principles for new phases)
- Correction of XSD namespaces following comments raised by NA-DE - **RTC id 34299**
- Constraint was inserted in DDCOM about the maximum size of the XML message over CCN – **RTC id 34303**
- Code M was added in table 44 about *"Transit declaration and exit summary declaration and entry summary declaration"*. Also raised as a comment #447 - **RTC id 34657**
- GPS coordinates structure was defined in DDCOM – **RTC id 35157**
- Following comment #434 of Iteration 1 review cycle the queue naming for CTA and ieCA was revised and amended to reflect the new approach
- IE918/IE919 and corresponding references to CCN queues and functionality was removed entirely from DDCOM. Figure *"Figure 34: Normal Operations with CS/MIS"* was also updated. This was a comment raised during the review cycle of Iteration 1 that was not correctly implemented
- Definitions of R/C/G and BRTs/TRTs was revised to reflect the current/future status. DDCOM was updated to remove the distinction between Px.0/Px.1.**RTC id – 35110**

I.1.8.16   Changes in DDCOM version 17.00

DDCOM incorporates the changes in v16.10 and minor changes introduced due to comments raised during the review cycle of the aforementioned version.

I.1.8.17   Changes in DDCOM version 17.10

The deliverables cover the following items:

- Section II.1.1 updated to clarify that the identification of system phase will not be covered by the CS/MIS CDCA
- Section V.6.4.1 updated to reflect discussions with Forerunners MS and DG TAXUD about availability management i.e. to state that "Suspension of sending

messages must apply only in case of System Unavailability Type "N" as described in II.2.2.4)"

▪ Section V.9 added to define TIN XSD pattern applicable only for EORI TINs

▪ Section X added for the integration of SD-COM of NCTS-P4, ECS-P2 and ICS-P1 as DDCOM Annex

▪ Section XI added for the integration of SD-COM of NCTS-P5 and AES-P1 as DDCOM Annex:

    o Updated EBPs applicable to NCTS-P5 and AES-P1

    o Made reference to AO for NCTS-P5 and AES-P1 in regard to interfaces with Central Services

    o Made reference to ITSM2_LOT2-SC05-QTM-08-eCustoms TES Security Plan for security

    o Made reference to NCTS-P4 and ECS-P2 sections of Annex A about fallback procedures

I.1.8.18   Changes in DDCOM version 18.00

DDCOM incorporates the changes in v17.10 and minor changes introduced due to comments raised during the review cycle of the aforementioned version.

I.1.8.19   Changes in DDCOM version 18.10

The deliverables cover the following items:

▪ Section II.2.6 introduced to define in which Central Services the information about start of operations in the "To-Be" operational mode in the Common Domain and the information about the not implemented/supported functionality by NA "To-Be" should be declared by the NAs. The aforementioned information is important for the Transitional Period of NCTS-P5 and AES-P1.

▪ Section IV.5.1 updated by removing "Error reporting" from the template for rules & conditions.

▪ Section V.3.2 updated to be aligned with CD exchange patterns defined in DDNTA and DDNXA Section IV.

▪ Section V.3.3 updated to include the functional error codes list applicable for NCTS-P5 and AES-P1

▪ Section VII.7 updated by removing the "Priority" and "Test Indicator" data items from Message Header for NCTS-P5 and AES-P1.

▪ Section VIII.2.6 updated to state that for AES-P1 and NCTS-P5 all Information Exchanges shall be sent with Normal priority and therefore, appropriate CSI QoS priority parameter shall be used.

It should be noted that the following minor changes were implemented throughout the document for consistency reasons:

- "CS/ieCA" has been replaced "TAXUD ieCA".

- "N/ieCA" has been replaced "NCO" (National Convertor).

I.1.8.20 Changes in DDCOM version 19.00

DDCOM incorporates:

- The changes covered in v18.10.

- Minor changes introduced due to comments raised during the review cycle of the aforementioned version.

- The update of section II.1.1 and section II.3.1 to specify that the information related to the start date of operations in the "To-Be" operational mode in Common Domain for NCTS-P5 and AES-P1 will be managed by CS/MIS CDCA.

I.1.8.21 Changes in DDCOM version 19.10

DDCOM incorporates:

- Changes introduced due to comments raised by National Administrations (via ECCG) and DG TAXUD during the review cycle of version 19.00.

- The addition of a table summarizing the expected validation of TMS for NCTS-P5 and AES-P1 at the end of section IV.3.

- VIII.2.26 updated to indicate that the maximum size of a message handled by the CSI stacks (NJCSI, C CSI) is 20MB per compressed message.

I.1.8.22 Changes in DDCOM version 20.00

DDCOM incorporates:

- Changes introduced during the implementation verification of the comments raised by National Administrations (via ECCG) and DG TAXUD on version 19.10.

- Correction in V.8, the term 'GNSS' is used instead of 'GPS'(single occurence).

- Table 39 in Section V.5 updated (for the examples).

- The term 'CSE' replaced by 'Specs Manager' as needed (new name of the DG TAXUD application that manages the specifications).

- The Documentation of <xs:simpleType name="TimeType"> was improved (to clarify the usage of UTC time).

- Text clarified in section V.4 (In case a specific C_DES_CON or C_EXT_RES building rule is violated, the particular error reason code 'TRxxxx' is used).

- The layout of Table 18 was optimised (for BRT numbering).

- The sequential numbers are starting from '00' (and no more from '01') for BRT and TRT.

- The update of "Table 47: Codes to be used in MRN field 4 Procedure identifier for NCTS-P5" with the new corresponding columns related to DA-Annex B.

- In Table 48, the check digit field type changed to "Numeric 1".

- Section VII.7.2 (Message Type) corrected by removing types A and B.

- Section VIII.2.26 Maximum Message size clarified.

- The obsolete message types IE030, IEx31, IEx32 are removed from section X.2.4 Restriction on the Central Services and other sections in Chapter X.

I.1.8.23   Changes in DDCOM version 20.10

DDCOM incorporates:

- MRN acronym corrected in Sections I.1.6, I.2.3, V.7.1.

- Section V.3.2.1 enhanced with the existing practice for Exception Handling to avoid looping of error messages.

- Tables 47 corrected by removing the reference to the columns F10, F11, F20, F30, F31, F40, F41, F42, F43, F44, F45, F50 or F51 of Annex B of UCC DA.

- Table 46 enhanced with code E.

- Structure of the XMLs in section V.7.2 updated.

- Section IV.3 enhanced with sub-sections according semantic validation for NCTS-P5 and AES-P1.

- Section II restructured and updated according to the new CS/MIS2 specifications in general, as well as the upgraded functionality of IE411D, the addition of IE903D, IE974C/IE975C, IE078C/IE578C and the removal of IE912C .

- Section V.3.2.1.5.1 has been updated to illustrate what happens if ieCA convertor detects an error in a converted message. Figure 11 has been added to illustrate it.

- Changes in Tables 19, 20, 21, 22.

I.1.8.24   Changes in DDCOM version 20.20

DDCOM incorporates:

- The corrections in the section *I.3 Applicable and reference documents*, and the addition of the referenc to the important document **ieCA Uses Cases** that complements this DDCOM for the NAs using the ieCA for the conversion of NCTS and/or ECS/AES messages;

- The removal of messages incorrectly added in section *II.3 Message exchanges with CS/MIS across the Web*;

- Clarifications in the section *II.4.5 Exchanging the proactive monitoring messages*;

- Updated figures in section *II.4.6 Sending the IE078 and IE578 for linked MRNs*;

- Additional details and corrections provided in section *IV.5.1 Definition of Rule, T, TRT, BRT or Condition*;

- Information on the Gateways and CCN queues added or corrected in section *VIII.2.17 Queue naming and addressing* (new group of queues for 'Availability' and 'Link'), in sections *VIII.2.18 National Gateways*, *VIII.2.19 Taxation and Customs Union DG Gateways* and *VIII.2.20 European Anti-fraud Office Gateway*;

- Minor cosmetic corrections.

I.2 Definitions

I.2.1 Definitions

Definitions of many of the terms used in this document may be found in the "Glossary of Terms" [R1]. Definitions of the business terms relating to Transit may also be found in [R2].

I.2.2 Terminology

A number of terms are used with a very specific meaning in this document:

Name	Description
Code List	A set of discrete values. Some Data Items can only contain a set of discrete values, in which case they will have an associated Code List. Note: the term entity is also used in CS/RD2, where those are maintained.
Conversion	It is the conversion of one or more messages from the Transitional UCC phase to the legacy phase and vice versa
Customs or Customs Domain	A Customs regime e.g. Import, Export and Transit.
Customs Office List	A collection of data related to Customs Offices. This set of data is maintained by National teams in the CS/RD2 application.
Customs System	Any of the Customs IT systems, e.g. NCTS.
Data Group	A Data Group is a part of the Technical Message Structure; it groups Data Items related to the same subject and it is denoted by a Data Group name.
Data Item	A Data Item is an elementary (atomic) piece of information; part of a Data Group.
Functional Message Structure (FMS)	Logical data structure of an Information Exchange, as defined in FTSS [R26], FSS - AES [R13] ,FSS - AIS [R14], AES L4 BPMs [R28] and NCTS-P5 L4 BPMs [R29] .
Information Exchange	A logical exchange of information between two locations. An Information Exchange is the conceptual exchange of information between two organisations, independent of its physical means.
Inter(Extra)net	The Internet (World Wide Web) or an Extranet operated on the CCN communications platform.
Inter(Extra)net message	An additional message, introduced to support Information Exchanges via the Internet or an Extranet, according to the HTTP protocol.
Location	A location is the place where the Customs operation is performed.
Message formatting	Representation (of a Technical Message Structure) in or mapping to exchange syntax (e.g. XML or EDIFACT).
Message transport	The sending (and reception) of a formatted message across a communications platform (such as CCN/CSI, the Inter(Extra)net).

Name	Description
Organisation	An organisation is a number of individuals acting in a concerted way towards a common business purpose with allocated roles and responsibilities. An organisation can have one or more roles of a specific type.
Reference Data	Data which defines the set of permissible values to be used by other data fields. RD is widely re-used and widely referenced and is often defined by external or internal standards/norms. RD normally changes slowly and reflects changes in the modes of operation of the business, rather than change in the normal course of business. With respect to CS/RD2, RD covers business and technical Code Lists. RD consists of Common RD and National RD [R27].
Technical Message Structure (TMS)	The data structure of the Information Exchange as it needs to be implemented. A TMS is a structure (and hierarchy) of Data Groups.
Time Sequence Diagram	Graphical representation of the message flow between locations over time for a particular Customs operation.

Table 1: Definitions

Name	Description	Applicability
Rule	A text that specifies (from a Functional perspective) how a Data Group or a Data Item must be filled in. It places a constraint on the content. It is also used to specify when the information must be provided at HEADER level or at GOODS ITEM level.	NCTS-P4, ECS-P2 and ICS-P1
Rule	An instruction that specifies (from a Functional and Technical perspective) how a Data Group or a Data Item must be filled in. It places a constraint on the content. It may be computable and testable.	NCTS-P5, AES-P1
Condition	A text that specifies (from a Functional perspective) whether a Data Group or a Data Item is mandatory or optional or it cannot be used. It constrains when the data shall be filled in and not its content.	NCTS-P4, ECS-P2 and ICS-P1
Condition	An instruction that specifies (from a Functional and Technical perspective) whether a Data Group or a Data Item is mandatory or optional or it cannot be used. It constrains when the data shall be filled in and not its content. It is always computable and can be executed and tested.	NCTS-P5, AES-P1
Technical Rule	An additional instruction needed from the IT technical point of view, complementing or clarifying functional rules	All

Name	Description	Applicability
	(mainly) and conditions.	
Business Rule for Transition (Bxxxx)	The BRTs ensure the conversion of a pre-UCC movement during the Transitional Period (TP) and enable all the UCC features after the Transition Date. • A BRT-1 enforces a relaxed validation of R/C before the end of TP and is applicable for the whole lifecycle of any movement opened during the Transitional Period. A BRT-1 is applicable (validated) only when the Decisive date (e.g. <Declaration acceptance date>) is before or equal to <End of TP>; • A BRT-2 applies some UCC data requirements, defining the final structure for movements accepted after the end of the Transitional Period. A BRT Category 2 is applicable (validated) when the Decisive date (e.g. <Declaration acceptance date>) is after <End of TP>.	NCTS-P5, AES-P1
Sequencing Rule	A text that defines in which order the Condition(s), Technical Rule(s) for Transition, Technical Rule(s) and Rule(s) must be validated. It can only be applied only in cases where the generic rules for the validation order (specified in the DDCOM) are not sufficient.	NCTS-P5, AES-P1
Guideline	An instruction on how to fill in a Data Group or a Data Item. It is not subject to automated testing.	NCTS-P5, AES-P1
Technical Rule for Transition	A restriction that enforces a stricter message structure before the end of the TP. Their purpose is to ensure message compatibility with pre-UCC NCAs during TP.	NCTS-P5, AES-P1

Table 2: Rules, Conditions and Guidelines Definitions

I.2.3 Acronyms and Abbreviations

The following acronyms are used in this document:

Acronym	Description
AAR	Anticipated Arrival Record
ACK	Acknowledgement
AEO	Authorised Economic Operator
AER	Anticipated Export Record
AES	Automated Export System
AIS	Automated Import System
API	Application Programming Interface
ATR	Anticipated Transit Record
BANSTA	BANking STAtus message
BGM	Beginning of Message. This is the name of a segment of an EDIFACT-message
BPM	Business Process Models
BRT	Business Rules for Transition
CAoDep	Competent Authority of Country of Departure
CASO	Central Application Security Officer
CCN	Common Communication Network
CD	Common Domain
CDCA	Centrally Developed Customs Application
CDIA	ITSM CONTRACTOR Directory Administrator
CoA	Confirm on Arrival
CoD	Confirm on Delivery
COL	Customs Office List
CONTRL	Syntax and service report message (CONTRL) EDIFACT message
CPT	Central Project Team
CS	Central Services
CS/MIS	Central Services Management Information System
CS/MIS2	Central Services Management Information System 2
CS/RD2	Central Services Reference Data 2
CSE	Consolidated Specifications Environment
CSI	Common Systems Interface
CSIDD	CCN/CSI Data Descriptor
CSO	ITSM CONTRACTOR Central Security Officer

Acronym	Description
CSS	Central Services Specification
CUSCAR	CUStoms CArgo Report EDIFACT message (UNSM)
CUSDEC	CUStoms DEClaration EDIFACT message (UNSM)
CUSRES	CUStoms RESponse EDIFACT message (UNSM)
DDCOM	Design Document for Common Operations and Methods
DDNA	Design Document for National Applications
DDNIA	Design Document for National Import Applications
DDNTA	Design Document for National Transit Applications
DDNXA	Design Document for National Export Applications
DDRDA	Design Document for Reference Data Applications
DG TAXUD	TAXation and Customs Union Directorate General
DMR	Data Maintenance Request (EDIFACT)
DROOLS	Dave's Recycled Object-Oriented Language
DTD	Document Type Definition
DTI	Direct Trader Input
EBP	Elementary Business Process
EC	European Community
ECG	Electronic Customs Group
ECS	Export Control System
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EFTA	European Free Trade Association
EORI	Economic Operator Registration & Identification
EOS	Economic Operators' Systems
EXC	Exception Report
EXP	Expiration Report
EXS	Exit Summary Declaration
FMS	Functional Message Structure
FSS	Functional System Specification
FTSS	Functional Transit System Specification
FTX	Free TeXt. This is the name of a segment of an EDIFACT-message
GENRAL	GENeRAL purpose message
GESMES	GEneric Statistical MESsage EDIFACT (UNSM)
GNSS	Global Navigation Satellite System

Acronym	Description
GRN	Guarantee Reference Number
GSS	Generic Security Services
GUI	Graphical User Interface
HS6	Harmonised System 6
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over SSL
ICR	Issue Control Report
ICS	Import Control System
IDL	Interface Definition Language
IE	Information Exchange
ieCA	IE Conversion Application
IFL	Implementation of Functional Languages
ISO	International Standards Organisation
IT	Information Technology
ITSM	IT Service Management
KEL	Known Error List (now replaced by RFC-List.xx)
LAA	Local Application Administrator
LAD	Local Application Designer
LRN	Local Reference Number
LSO	Local Security Officer
LSYA	Local System Administrator
MDS	Message Duplication Service
MIME	Multipurpose Internet Mail Extensions
MRN	Master Reference Number
MS	Member State
NA	National Administration
NACK	Negative ACKnowledgement
NCA	National Customs Application
NCF	Notification of Crossing Frontier
NCO	National Convertor
NCTA	National Customs Test Application
NCTS	New Computerised Transit System
ND	National Domain

Acronym	Description
NDCA	Nationally Developed Customs Application
NECA	National Export Control Application
NTA	National Transit Application
OLAF	Office européen de Lutte Anti-Fraude / European Anti-fraud Office
OoDep	(Customs) Office of Departure
OoDes	(Customs) Office of Destination
OoExp	(Customs) Office of Export
OoExt	(Customs) Office of Exit
OoGua	(Customs) Office of Guarantee
OoLdg	(Customs) Office of Lodgement
PARTIN	Party Information EDIFACT message (UNSM)
PARTTC	Party Transit Computerisation EDIFACT message (PARTIN + DMRs)
QoS	Quality of Service
RD	Reference Data
RFC	Request For Change
SA	System Administration
SAD	Single Administrative Document
SAD	*ieCA* System Architecture Document
SAM	Single Administrative Message
SC	Specific Contract
SGML	Standard Generalised Markup Language
SMTP	Simple Message Transfer Protocol
SPEED2	Single Portal for Entry or Exit of Data 2
SPEED-ECN	Single Portal for Entry or Exit of Data – EDI/CSI Node
SR	Strongly Recommended
SSL	Secure Socket Layer
STTA	Standard Transit Test Application
TC	Technical Centre
TMS	Technical Message Structure
TRP	Test Reference Package
TRT	Technical Rule for Transition
TSD	Time Sequence Diagram
TTA	Transit Test Application
UDP	Upload/Download Parsing

Acronym	Description
UML	Unified Modelling Language
UN	United Nations
UNB, UNH, UNT, UNZ, UCD, UCI, UCM, UCS	These are not abbreviations but names of (service) segments of an EDIFACT-message
UNSM	United Nations Standard Message (e.g. CUSDEC)
URI	Universal Resource Identifier
UTF	UCS Transformation Format
WGS84	World Geodetic System
WWW	World Wide Web
XML	eXtensible Markup Language
XSD	XML Schema Definition
XSDL	XML Schema Definition Language
XSLT	XML (Extensible Markup Language) Stylesheet Language for Transformations.

Table 3: Acronyms

I.3 Applicable and reference documents

I.3.1 Applicable documents and standards

I.3.1.1 Documents

The following documents are applicable to this document:

Ref.	Reference	Title	Release
A1	CCN/CSI-PRG-AP/C-01-MARB	CCN/CSI Application Programming Guide (C language)	11
A2	CCN/CSI-PRG-HL/Cob/BS1000-01-MARB	HL Programming Guide (COBOL Language for BS1000)	Ed01
A3	CCN/CSI-PRG-HL/CICS-01-MARB	HL Programming Guide (COBOL Language for IBM CICS environment)	prg-hl-cob_XXX-00
A4	CCN/CSI-REF-HL/C-01-MARB	CCN/CSI HL Reference Manual	16.00
A5	CCN/CSI-REF-GSS/C-01-BING	CCN/CSI GSS Reference Manual	05
A6	CCN/CSI-REF-ComD/C-01-MARB	CCN/CSI Common Definitions Reference Manual (C language)	15
A7	CCN/CSI-REF-ERR-01-MARB	CCN/CSI Error Reason Codes Reference Manual	08
A8	CD3-FQP-Framework Quality Plan	Project Quality Plan	1.10
A9	CUSTDEV3-SC21-CQP	SC21 Contract Quality Plan	1.00
A10	TAXUD/2013/CC/124	Framework Contract	1.00
A11	SC21	Specific Contract 21 under the Framework Contract TAXUD/2013/CC/124	Dated 24/07/2013
A12	31992R2913	Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code	Consolidated version 01/01/2014
A13	31993R2454	Commission Regulation (EEC) No 2454/93 of 2 July 1993 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code	Consolidated version 08/12/2015
A14	-	-	-
A15	-	-	-
A16	ToC-eCUST-TES	Terms of Collaboration for the Customs Trans-European Systems	5.20 (Revision 2020)

Ref.	Reference	Title	Release
A17	UCC	Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code	Consolidated version 01/01/2020
A18	UCC IA	Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code	Consolidated version 01/01/2020
A19	UCC DA	Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code	Consolidated version 25/07/2019
A20	UCC TDA	Commission Delegated Regulation (EU) 2016/341 of 17 December 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards transitional rules for certain provisions of the Union Customs Code where the relevant electronic systems are not yet operational and amending Delegated Regulation (EU) 2015/2446	Consolidated version 01/05/2016
A21	UCC WP	Commission Implementing Decision (EU) 2019/2151 of 13 December 2019 establishing the work programme relating to the development and deployment of the electronic systems provided for in the Union Customs Code	16/12/2019
A22	Revised UCC Data ANNEX B	Annex B of the UCC-DA and Annex B of the UCC-IA	10.0 3.3
A23	CD3-FQP	Framework Quality Plan	1.30 14/05/2020
A24	TAXUD/2019/DE/141 SC25	Specific Contract 25 under the Framework Contract TAXUD/2013/CC/124	18/09/2019

Table 4: Applicable Documents

Note that all documents listed above are applicable to the present volume (and are input to this volume). Any change in any of the documents above is likely to have direct and immediate consequences for this document:

- The series of documents, [A1] to [A7], define the interfaces of the CCN/CSI communications platform and therefore they are used for the description of CCN/CSI information in the DDCOM volume;

- Document [A8] is the Project Quality Plan and therefore it is applicable to DDCOM;

- Documents from [A9] to [A11] are contractual documents of the specific Quoted Time and Means Action.

The Central Project Team will implement configuration management on all documents and CDCA software versions in order to assure coherence.

I.3.1.2   Standards

The following standards are applicable to this document:

Ref.	Reference	Title	Release
S1	ISO 9735	ISO 9735 - Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules	
S2	UNTDID, D96B	United Nations Trade Data Interchange Directory D.96B (United Nations)	
S3	UN/ECE TRADE /WP.4/R.1186/Rev.1	Syntax and Service Report Message (CONTRL)	1
S4	Extensible Markup Language (XML) 1.0 (Fifth Edition) http://www.w3.org/TR/2008/REC-xml-20081126/	XML standard	
S5	Unicode 1999-05-17 (Revision 2)	Unicode standard	
S6	ISO 8859-1 ISO 8859-2 ISO 8859-3 ISO 8859-4 ISO 8859-5 ISO 8859-7 ISO 8859-9	Character set standards	
S7	RFC-1630	Universal Resource Identifiers in WWW: A Unifying Syntax for the Expression of Names and Addresses of Objects on the Network as used in the World-Wide Web.	
S8	RFC-1867	Form-based File Upload in HTML	
S9	RFC-1950	ZLIB Compressed Data Format Specification version 3.3	
S10	RFC-1951	DEFLATE Compressed Data Format Specification version 1.3	
S11	RFC-1952	GZIP file format specification version 4.3	
S12	RFC-2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Inter(Extra)net message Bodies	
S13	RFC-2046	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	
S14	RFC-2047	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text	

Ref.	Reference	Title	Release
S15	RFC-2048	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures	
S16	RFC-2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples	
S17	RFC-2068	Hypertext Transfer Protocol—HTTP/1.1	
S18	XML Schema 1.0	http://www.w3.org/TR/xmlschema-0/	
S19	XML Schema 1.1	https://www.w3.org/TR/xmlschema11-1/ https://www.w3.org/TR/xmlschema11-2/	
S20	ISO 8601	https://www.iso.org/iso-8601-date-and-time-format.html	

Table 5: Applicable Standards

The following standards are referenced in this document but are not applicable:

Ref.	Reference	Title	Release
S21	RFC-2069	An Extension to HTTP: Digest Access Authentication	
S22	ISO 6346	International standard covering the coding, identification and marking of intermodal (shipping) containers	

Table 6: Reference Standards

[S1] and [S2] are mandatory EDIFACT standards. For EDIFACT formatting, most Transit Information Exchanges will be mapped upon EDIFACT messages (UNSMs) defined in the EDIFACT directory [S2]. Some Information Exchanges require however, mapping upon an EDIFACT message that is not part of this message directory; this EDIFACT message (CONTRL) is defined in [S3].

Additional standards to be taken into account are the XML ([S4]) standard and a number of character set standards ([S5] and [S6]).

[S7] to [S17] are specific RFC standards, applicable to Central Services only and [S20] is a reference document for Central Services.

I.3.2 Reference documents

The following documents are also of interest to the Customs application designer:

Ref.	Reference	Title	Release
R1	TMP-GDL-GLSRY	Glossary of Terms	3.11
R2	TSS-CSA-UNS	User Needs Specification	2.04-EN
R3	ITSM2_LOT2-SC05-QTM-08-eCustoms TES Security Plan	eCustoms TES Security Plan	1.30-EN
R4	CCN/CSI-OVW-GEN-01-MARB	CCN/CSI System Overview	17.00
R5	CCN/CSI-AD-GEN-01-MARB	CCN/CSI Architecture Design	10.00
R6	CCN/CSI-TRA-CSI-01	CCN/CSI Course Notes (mod1)	16.00
R7	CCN/CSI-TRA-CSI-01	CCN/CSI Course Notes (mod2)	20.00
R8	CCN/CSI-TRA-CSI-01	CCN/CSI Course Notes (mod3)	17.00
R9	CCN/CSI-ACG-GEN-01-MARB	CCN/CSI Application Configuration Guide	09
R10	CCN/CSI-SIG-SRA-01	Software Installation Guide – Statistics Receiver Application	Ed00
R11	DDNA_RFC-List	DDNA RFC-List	RFC-List.31
R12	EDIWG/0100-10	Single Administrative Message - Mapping Specification	1.00-EN
R13	FSS – AES	FSS – AES Addendum: ECS	Corrigendum 1/2013
R14	FSS – AIS	FTSS – AIS Addendum: ICS	Corrigendum 1/2017
R15	ECS P2-SD	Scope of AES-ECS Phase 2	11.00
R16	DDNXA	Design Document for National Export Application	11.00[6]
R17	DDNTA	Design Document for National Transit Application	20.00[7]
R18	DDNIA	Design Document for National Import Application	13.00
R19	CD3-ieCA-SAD-System Architecture Document	ieCA System Architecture Document (ieCA-SAD)	2.30 26/03/2020

---

[6] Applicable to ECS-P2

[7] Applicable to NCTS-P4

Ref.	Reference	Title	Release
R20	NCTS P4-SD	Scope of NCTS Phase 4	20.00
R21	ICS P1-SD	The Business Scope of ICS Phase 1	13.00
R22	TTA-SRD-System Requirements Definition	System Requirements Definition for TTA	6.20
R23	EOS – DDNA	EORI-AEO Design Document for National Applications	21.00
R24	EORI – SPM-REQ	EORI-AEO System process model and requirements	20.00
R25	DGXXI/627/97 Rev. 3	PROPOSAL FOR STRUCTURE OF REFERENCE NUMBERS IN NCTS	N/A
R26	TSS-FSF-REL4	FTSS 4.00	Corrigendum *1/2017*
R27	DDRDA	Design Document for Reference Data Application	2.40
R28	AES L4 BPMs	EU Customs Functional Requirements BPM Report for Automated Export System (AES)	8.00
R29	NCTS-P5 L4 BPMs	EU Customs Functional Requirements BPM Report for New Computerised Transit System (NCTS)	6.00
R30	SLA-eCUST-TES-ACM	Service Level Agreement for Availability and Continuity of Customs Trans-European Systems between National Administrations and DG TAXUD	2.80 03/11/2017
R31	DIH-18-002	DIH-18-002 Governance of Reference Data in CSRD2	1.00
R32	Transition Strategy for ECS-P2 to AES	Transition Strategy from ECS P2 to AES	2.00
R33	Transition Strategy for NCTS-P4 to NCTS-P5	Transition Strategy from NCTS Phase4 to Phase5	1.10
R34	UCC AES Vision	UCC Automated Export System (AES) - Vision	1.40
R35	UCC NCTS-P5 Vision	UCC New Computerised Transit System (NCTS Phase 5) - Vision	1.10
R36	FSS-AES	Functional System Specification – AES Document	2.20
R37	FSS-UCC NCTS-P5	Functional Transit System Specification (FTSS) – NCTS Addendum	4.20
R38	NCTS-P5_AES_AO	NCTS P5/AES Architecture Overview	3.00
R39	FSS-Business Statistics for UCC AES-NCTS	Business Statistics for Transit and Export - Functional System Requirements	2.00

Ref.	Reference	Title	Release
R40	DDNXA	Design Document for National Export Application	5.13 (July 2020)
R41	DDNTA	Design Document for National Transit Application for NCTS-P5	5.13 (July 2020)
R42	ieCA-UC	ieCA Use Cases	1.10 (July 2020)

Table 7: Reference Documents

- The first document, [R1], contains the glossary applicable to NCTS and/or ECS (terminology, acronyms and abbreviations used in only NCTS and ECS);

- [R2] is accompanied by the User Needs Specification, [R2], defining a number of desirable end-user requirements for NCTS;

- The seven documents, from [R4] to [R10], contain additional documentation on CCN/CSI;

- [R11] is the archive which contains all accepted RFCs for the RFC-List.29 (published on CIRCABC);

- The SAM Mapping Specification, [R12], is a document describing the Interchange Exchange format;

- The two documents [R13] and [R14] present various business process threads of the Export Core business [R13] and the Import Core business [R14] for ECS-P2 and ICS-P1 respectively;

- Document [R15] is the Scope of AES-ECS Phase;

- The next three documents are the domain specific DDNA volumes [R16], [R17] and [R18] for ECS-P2, NCTS-P4 and ICS-P1;

- [R19] describes the system architecture of TAXUD ieCA and NCO;

- The next document, [R20], defines the scope of NCTS;

- Document [R21] is the Scope of AIS-ICS Phase 1;

- The next document, [R23], is the EOS DDNA;

- Functional specifications for EOS are contained in [R24];

- [R25] is the document which defines structure of the reference numbers used in NCTS (MRN and GRN);

- FTSS [R26] is the Functional Transit System Specification. It defines the business processes that are supported by DDCOM for NCTS-P4;

- DDRDA [R27] defines all the interfaces available to the National Administrations to upload to and to download data from CS/RD2;

- AES L4 BPMs [R28] is the Functional AES System Specification;

- NCTS-P5 L4 BPMs [R29] is the Functional NCTS System Specification;

- FSS-AES [R36] present various business process threads of the Export Core business for AES-P1;

- FSS-UCC NCTS [R37] present various business process threads of the Transit Core business regarding NCTS-P5;

- NCTS P5_AES_AO [R38] defines the overall NCTS P5 and AES TES architecture, which shall be implemented by different logical components/applications;

- FSS-Business Statistics for UCC AES-NCTS [R39] specifies the functional requirements for business statistics for NCTS-P5 and AES-P1;

- DDNXA [R40] is the specific DDNA volume for AES-P1;

- DDNTA [R41] is the specific DDNA volume for NCTS-P5.

I.4 Symbolism and Conventions Used
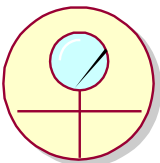
This chapter presents the symbolism used in this document. An explanation of symbolism used in the appendices can be found at the beginning of the relevant Appendix.

I.4.1 Time Sequence Diagrams

The Information Exchange sequences are presented using Time Sequence Diagrams. Time Sequence Diagrams visualise the Information Exchange sequence between all locations involved in a particular scenario for a Customs movement. Examples of scenarios are, using Transit movements, the core flow for simplified procedure and the core flow including diversion.

As each Time Sequence Diagram can only be used to show one possible flow of Information Exchanges, a large number of Time Sequence Diagrams is required to specify all allowed Information Exchange sequences.

The business modelling elements used are the following:

Name	Notion	Icon (Example)	UML Stereotype
Business Worker	A business worker is an abstraction of software or even a system that is a composite of these and represents a role performed within business scenarios. A business worker collaborates with other business workers, is notified of business events and performs responsibilities. In the context manipulates business entities of the present document, a business	OoDep	<<business worker>>

Name	Notion	Icon (Example)	UML Stereotype
	worker is an NCA, which has active participation in the realisation of processes as these are defined in FTSS. Each business worker (NCA) collaborates with other business workers (NCA) through the Common Domain and manipulates business entities such as data, messages in order to perform some activities (its responsibilities) as these are defined in FTSS.		
Business Actor	A business actor represents a role played in relation to the business by someone or something (application) in the business environment. In the context of this document, this is used for the traders, who play a significant role in the business.	: Trader Principal	<<business actor>>

Table 8: UML business modelling elements

The **roles** that can be taken by organisations are defined in each domain specific DDNA volumes ([R16], [R17] and [R18]).

Customs Offices of a NA and the infrastructure used by a NA are not specified in DDNA.

Each Time Sequence Diagram can only depict one possible sequence of Information Exchanges that is used to record one particular operation. Each different operation might lead to another Time Sequence Diagram.

All the components of a Time Sequence Diagram are shown in the following figure:
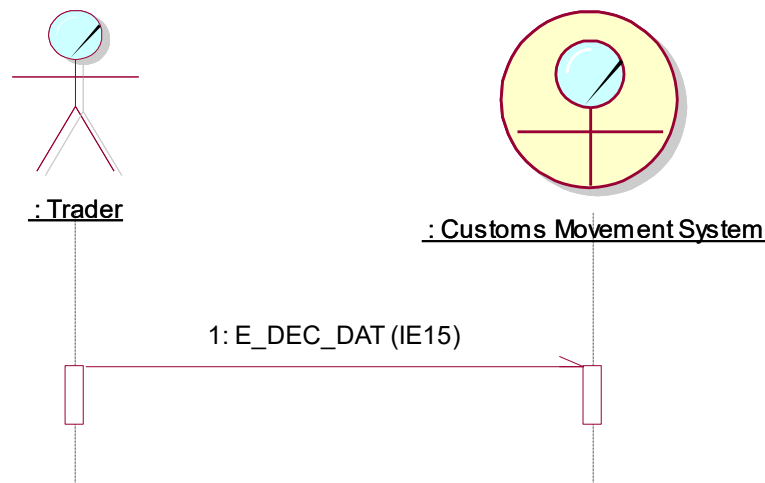
Figure 1: Time Sequence Diagram

In a TSD, each role is represented by an icon (see Table 8) with the name of the role and a vertical line, called the "lifeline". The name "lifeline" comes from the UML-concept that an object's life can be ended. This does not apply here.

An arrow between the lifelines represents each Information Exchange (message) between two roles, where the arrow shows the direction of the Information Exchange. Attached to the arrow, a label gives the sequence number of this Information Exchange in the scenario and the coded name and number of Information Exchange.

The above figure (Figure 1) illustrates that the "Trader" submits a message to the Customs Office application. The name of the IE that is sent to Customs Office application is indicated above the Information Exchange.

The narrow rectangles on the lifelines are called 'focus of control'. It represents the relative time that the control of the flow is focused in that role, thus the time that the role is directing messages. When more than one message starts from (or ends in) the same focus of control, this means that these messages are sent (or received) shortly after each other. The arrows will appear close to each other in that case as well. Please note that in this case the sequence of sending the messages is not important. Therefore, the sequence used to represent them in the TSDs is only indicative. When for two messages exchanged the sequence is important, they are presented to start from a different 'focus of control'.

The Time Sequence Diagrams conform to the Unified Modelling Language, which is an industry standard for Object Oriented modelling.

The UML business modelling element (Table 8), which will be used for each Role Type in the TSDs is shown in each domain specific DDNA volume ([R16], [R17] and [R18]).

Not all possible combinations are given in this DDNA; only the most relevant ones have been included.

TSDs are developed using ARIS tool but are not integrated with the L4 BPMs.

I.4.2 State Transition Diagrams

State Transition Diagrams consist of states and transitions between those states. Each state represents the condition of a Customs movement for a particular Customs Office Role. Each transition starts at a given state and goes to another state. A transition is allowed to reach its original state. Each transition is triggered by the exchange of a message between two organisations. Events that are causing a state transition are decisions taken, timer start/expiration or message exchanges. State Transition Diagrams show transitions that are triggered by the exchange of a message or by timer expiration.

Every State Transition Diagram in this document is related to one particular role only. For that role, it will define how state transitions take place according to events (such as the reception of a message from another role).

States will be shown as a box and an arrow will show transitions.
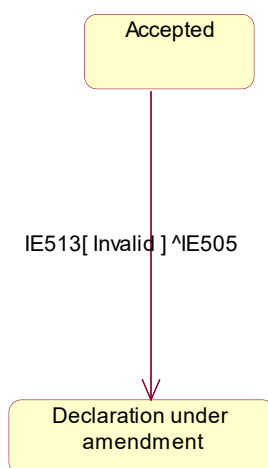
Figure 2: Example of State Transition Diagram

State transitions have the following format A[]^B or [C]^B. The transition is caused by the receipt of message A and if the condition inside the square brackets is satisfied, the state transition is performed and the message B is sent. Please note that only the IE numbers shall be used in the state transitions.

In the example above (which is part of the State Transition Diagram for the Office of Export up to the release of movement), the transition from "Accepted" to "Declaration under amendment" is triggered by the reception of a Declaration Amendment (IE513) message and if the Declaration Amendment is "invalid". As a result, an Amendment Rejection IE505 message is sent back from Office of Export to the Trader.

When multiple messages are sent as a consequence of an event, a dot sign will separate these multiple messages ("."). This dot sign needs to be understood as a logical AND.

I.4.3 Data Dictionary

The data dictionary, contained within this DDNA, defines:
  ▪ Data Items;

- Data Groups;
- Code lists (sets of discrete values).

A number of naming and spelling conventions and rules have been maintained for these throughout this DDNA.

I.4.3.1 Data Items

Every name shall start with a capital (uppercase) letter.

Every name can contain letters, digits, and a number of additional characters: the space character, the brackets "(" and ")", the ampersand character "&", the underscore "_", and the slash character "/". No other characters are allowed.

Within the name, lowercase letters should preferably be used (except for the first character and except for abbreviations that will always be in uppercase).

I.4.3.2 Data Groups

Every name shall start with a letter.

Every name can contain letters, digits, and a number of additional characters: the space character, the brackets "(" and ")", the ampersand character "&", the underscore "_", and the slash "/". No other characters are allowed.

Only uppercase letters are allowed.

I.4.3.3 Code lists

For information on Codelists please refer to DDRDA [R27].

II Central Services

II.1 Messages involved

II.1.1 Messages involved in Customs Applications

In the business area 'Central Services', the Information Exchanges can be distinguished in three categories:

Those exchanged between CS/RD2 and any other application operating in the Common Domain, as defined in DDRDA [R27].

The National CS/RD2 teams are invited to create subscriptions that will extract the needed information on regular basis for NCTS-P5 and AES-P1. During the elaboration phase, the information will be available to the National Project Teams via CSRD2 CONF.

In addition, the codelists that are of interest for the traders (related to the ED messages) will be published on DDS2 europa.eu website.

Those exchanged between CS/MIS and NCTS-P4, ECS-P2, ICS-P1 in the Common Domain:

- Notification of System Unavailability to Common Domain C_UNA_COM (IE070);
- Notification of System Unavailability to National Domain C_UNA_NAT (IE071);
- Full Unavailability Schedule C_UNA_DAT (IE971);
- Sending of Statistics Data C_STA_SND (IE411);
- Statistics Generated Sent to National Domain C_STA_GEN (IE412).

For NCTS-P5, AES-P1, CS/MIS2[8] functionality has inherited the majority of the above exchanges and has been extended with the following IEs:

- Notification of System Unavailability to Common Domain C_UNA_COM (IE070);
- Notification of System Unavailability to National Domain C_UNA_NAT (IE071);
- Full Unavailability Schedule C_UNA_DAT (IE971);
- Sending of Statistics Data C_STA_SND (IE411);
- NCA Availability Request C_AVA_RES (IE974);
- NCA Availability Response C_AVA_REQ (IE975);
- Inter-Domain Linking C_MRN_LNK (IE078/IE578).

---

[8] CS/MIS2 is backward compatible with CS/MIS. This implies keeping the existing CS/MIS interfaces, exchange protocols and application behaviours and extending them with new interfaces unique to CS/MIS2. Any reference to CS/MIS2 is focused on the additional functionality of the new system.

Those exchanged between TAXUD ieCA and any other application operating in the Common Domain, as defined in ieCA SAD [R19].

In addition to this, although not strictly an Information Exchange, the technical CCN/CSI statistics and audit files also need to be considered.

The following messages from the Core Business area are also used for the CCN/CSI based exchanges:

- Internal CCN/CSI messages [CCN/CSI Confirm on Delivery Acknowledgement C_COD_ACK (IE908), CCN/CSI Confirm on Arrival Acknowledgement C_COA_ACK (IE909), CCN/CSI Expiration Notification C_EXP_NOT (IE910), and CCN/CSI Exception Notification C_EXC_NOT (IE911)]. These messages are related to the internal usage of CCN/CSI and, when correctly used, are transparent to the user. Details concerning the technical CCN/CSI messages are included in Transport of messages via CCN/CSI;

- Messages for error reporting [Functional NACK C_FUN_NCK (IE906), EDIFACT NACK C_EDI_NCK (IE907), XML NACK C_XML_NCK (IE917)]:

    o EDIFACT NACK C_EDI_NCK (IE907) is used for reporting EDIFACT formatting errors when the message is exchanged in EDIFACT format;

    o XML NACK C_XML_NCK (IE917) is used for reporting XML formatting errors when the message is exchanged in XML format;

    o Functional NACK C_FUN_NCK (IE906) is used for reporting Functional errors (e.g. violation of Information Exchange building rules).

    The usage of Functional NACK C_FUN_NCK (IE906), XML NACK C_XML_NCK (IE917) and EDIFACT NACK C_EDI_NCK (IE907) is further explained in Design principles, chapter V.3.

In addition, a number of HTTP messages have been defined (for enabling Information Exchange with standard Web technologies). These are (the prefix IM_ denotes an HTTP message):

- IM_REGISTER: for subscription notifications;

- IM_RESULT: for returning the result of another HTTP message (ok/failure or URI[9] where information can be found);

- IM_NOTIFICATION: for notification of new information or presence of upload results;

- IM_INITIATE_DOWNL: for initiation of a download operation;

- IM_GET_FILE: for starting the sending of a file.

---

[9] URI stands for Uniform Resource Identifier, and is equal to the name of the Web page where some information can be retrieved. It should be considered as the address where information is available.

These HTTP messages are all in an Internet specific format. Their meaning is explained in Central Services (II.3.3), their format in IX Transport of messages via the Inter(extra)net.

Appendix A in each domain specific volume ([R16], [R17] and [R18]) shows all messages relevant to the message protocols for Central Services.

Central Services can be split into six functionally different components:

- The exchange of common reference data;

- The exchange of Customs Office List;

- The exchange of conversion request/responses;

- The exchange of availability data (IE070, IE071 and IE971);

- The exchange of business statistics data (IE411 and IE412[10]);

- Monitoring of messages and movements (CCN/CSI audit files) and statistics on the messages (CCN/CSI technical statistics) and on the error messages that are generated to reject erroneous messages.

The first two items (Reference Data and Customs Office List) are covered centrally by the CS/RD2 CDCA tool. For more information, please refer to [R27].

Conversion request and responses are defined in ieCA SAD [R19].

Availability data, statistics (business & technical) and monitoring of movements are applicable only for the movement systems and are covered by the CS/MIS CDCA. In addition, the information about start date of operations in the "To-Be" operational mode in Common Domain for NCTS-P5 and AES-P1 will be managed by CS/MIS CDCA.

II.2 The different sections of the CS/MIS tool

Statistics and availability management for the movement systems are supported by a centrally developed Customs application (CDCA) called CS/MIS (Central Services/Management Information System). This system collects the statistics and availability data from the various NAs via two physical media (the Web and CCN/CSI) and distributes the information to the NAs after centralised consolidation[11].

This section deals with the following Information Exchanges:

Common IEs:

- Statistics: Technical CCN/CSI statistics;

- MRN nursing: CCN/CSI Audit files;

---

[10] IE412 is not applicable for NCTS-P5 and AES-P1

[11] The EO statistics are out of the CS/MIS and CS/RD2 scopes and are provided by the EOS CDCO.

- Availability data: IE070, IE071 and IE971;
- Business Statistics: IE411 and IE412[10].

The role of the CS/MIS tool

CS/MIS is a system in the Common Domain, located at the ITSM site. Its role is threefold:

- Keep track of system unavailability;
- Manage and distribute statistics on system, business and resources regarding the Customs systems;
- Monitor of Customs movements (MRN nursing).

CS/MIS web site is integrated into the ITSM Portal site.

II.2.1 CCN/CSI technical statistics

Separate CCN/CSI technical statistics will be generated for the CCN/CSI network resources and the use of the Common Domain for each Customs system. Technical CCN/CSI statistics provide information collected on the CCN gateways used by Customs Applications. The reports generated here inform the user about utilisation of the CCN/CSI network resources (e.g. number of messages).

Technical statistics report on the use of the Common Domain (CD) by a Customs application. CCN message transport information is collected daily on each NA CCN gateway. It is forwarded daily to the ITSM CONTRACTOR and from there further on to the CCN gateway accessed by ITSM. There, the statistics data is captured by CS/MIS and stored on disk.

Note that the generation of technical statistics data and the collection and forwarding of this data will be performed by the ITSM CONTRACTOR. Therefore, this process is transparent to the NA and no specific implementation from the NA side is required. However, NAs will be able to view and download the statistics from CS/MIS web site.

Technical statistics will be sent across the CCN/CSI platform as a flat file. A separate queue will be created in the Taxation and Customs Union DG gateway for the collection of the Technical statistics for each Customs system (see section VIII paragraph VIII.2.19).

II.2.2 Movement Monitoring

CCN/CSI audit files from all the Customs Systems' gateways will be collected by ITSM CONTRACTOR and sent to Taxation and Customs Union DG gateway at ITSM. Separate queues will be created in the Taxation and Customs Union DG gateway for the collection of the CCN/CSI audit files from all the CCN gateways for each Customs system (see section VIII paragraph VIII.2.19).

CS/MIS will then consolidate these audit files daily.

A user will be able to perform "MRN Tracking" in one of two ways to get all the data available about a particular MRN:

- The user can directly enter the MRN into a web form;

- The user can make a query (using a web form) to get a list of the MRNs matching the query and then select a particular MRN from that screen.

In the above cases the result will be a screen displaying all the messages and reports related to that MRN or query. The user shall also be able to request downloading a file in HTML, Excel or XML format that incorporates the results of the submitted query.

In addition to the "MRN Tracking" functionality, the system also presents the "Message Tracking" functionality. Message Tracking gives the user the ability to retrieve a list of messages matching the criteria selected in the Messages query web form and then select a particular message from that screen.

The Messages query results are displayed in a list of entries displaying the type of the message(s), the related CORREL ID(s) and reports.

The CS/MIS application will incorporate the "Movement Query" functionality, which will enable the user to retrieve information about the number of movements (number of distinct MRN) exchanged per country pair, according to the selection criteria of the Movement query web form.

The user will be able to view the data-using HTML or download them in an Excel format.

CCN/CSI audit files from all the Customs Systems' gateways will be collected by ITSM CONTRACTOR and sent to Taxation and Customs Union DG gateway at ITSM.

CS/MIS will then consolidate these audit files daily.

II.2.2.1 Information about inter-linked movement (NCTS-P5/AES and AES/EMCS)

National administrations will collect information about linked movements and submit this information to CS/MIS2 via

- an IE078 (NCTS-P5) linking an NCTS MRN to one or more AES MRNs;

- and IE578 (AES-P1) linking an AES MRN to one or more EMCS ARCs.

The activities to be performed by CS/MIS2 upon the arrival of the linking message (IE078/IE578) are the following:

- Extract the linking information from the message;

- Locate the linked movements in CS/MIS2, set a flag indicating the fact that they are linked and set a reference for locating the linked information;

- Store the linking information.

Error handling:

- In case the received IE078 or IE578 is invalid, CS/MIS2 will respond to the NA with an IE917 (for formatting errors) or IE906 (for business rule violation). .

II.2.3   Business statistics

Business statistics serve to provide information to the user on Customs operations from the business perspective.

NCTS, ECS and ICS business statistics are collected on a monthly basis in the National Domain under automatic procedures by the NCA. Business statistics are sent to the CS/MIS application across CCN/CSI or uploaded on CS/MIS Web interface by means of the Sending of Statistics Data C_STA_SND (IE411). NAs may send IE411 statistical messages that include data for multiple domains (NCTS and/or ECS and/or ICS) and/or IE411 messages that include data for one customs domain. If an NA sends more than one IE411 message concerning a given month and customs domain, the latest information will overwrite any previously communicated data (i.e. if in the first message IE411 for a statistic type a value has been transmitted and the second message IE411 does not contain this certain statistic type, the first value remains valid; if a statistic type value is transmitted in both messages, the second value is used to update the message IE412[10]);

Each time an IE411 message is received by CS/MIS, a Statistics Generated Sent to National Domain C_STA_GEN (IE412[10]) message is automatically produced per Customs Domain impacted. The produced IE412[10] messages are available for download via the CS/MIS Web interface in any of the following formats: XML, XLS, HTML or TXT.

In addition, each time an IE412[10] message is produced, CS/MIS combines this IE412[10] message with other IE412[10] messages created for other periods and generates a domain-specific XLS file, which is also available for download on CS/MIS Web interface.

II.2.4   Availability monitoring & alerting

Monitoring of Customs Systems informs the NAs about the unavailability of any NA, so that they can take measures to prevent the transmission of messages to the disabled NA.

Three different types of unavailability may be communicated:
1. The NA may plan a scheduled unavailability in advance. This information is entered into CS/MIS, using a Notification of System Unavailability to Common Domain C_UNA_COM (IE070) with System Unavailability Type "S", kept in a central database and distributed as Notification of System Unavailability to National Domain C_UNA_NAT (IE071) to the other countries (in case the information was entered into CS/MIS via IE070).
2. Unscheduled unavailability may be communicated by any non-system means to the Central Help Desk. It is then entered into CS/MIS and monitored by the Central Help Desk. It can also be communicated through a web form on CS/MIS web site or by uploading a Notification of System Unavailability to Common Domain C_UNA_COM (IE070) with System Unavailability Type "U". All NAs receive an e-mail notification.
3. Apart from this, the NA should inform the CS/MIS application about the non-implementation of a particular business service, in order to advise the other NAs not to send messages related to this business service to the specific NA. In order

to achieve this, the NA will upload a Notification of System Unavailability to Common Domain C_UNA_COM (IE070) with System Unavailability Type "N" for the particular business service. This information will be distributed to the other countries via the Notification of System Unavailability to National Domain C_UNA_NAT (IE071).

Every NA prepares its own unavailability schedule that is distributed to all other NAs in order to prepare the other NAs for the disruption of service. FTSS [R26], FSS-AES [R13] and FSS-AIS [R14] foresees a mechanism for this purpose: the NA sends its unavailability schedule to the CS/MIS, which stores the information and distributes the unavailability to all other countries.

Four messages will be used for this:

- An IE070 message contains an update from a NA to its currently known schedule;

- An IE071/IE971 message is sent by CS/MIS as an e-mail attachment to all countries to update their local unavailability information about the other NAs; [12]

- An IE971 is sent in XML format containing the complete schedule of unavailability.

CS/MIS web site will provide the functionality to manually upload the IE070 message. A separate instance of this message will be used for each Customs system. The format to be used will be XML and the file can be uncompressed, zip compressed or gzip compressed.

There can be many causes of unscheduled interruptions to the services. Therefore, any means of non-system communication (telephone, fax, e-mail) as well as an IE070 having of Type "U" (Unscheduled) may be used to advise the CS/MIS operator about this kind of event. The modifications to the unavailability are broadcast to all NAs by means of an IE071 in XML format attached to e-mail. Unavailability information is also notified to the Central Help Desk.

Statistics on unscheduled unavailability are reported by CS/MIS.

Users will also be able to request from the CS/MIS web site an IE971 in XML format containing the complete schedule of unavailability. They will also be able to see live on the CS/MIS web site which countries are currently unavailable.

II.2.4.1   Availability monitoring & alerting for NCTS-P5/AES-P1

In CS/MIS2 the monitoring and alerting functionality is extended for NCTS-P5/AES-P1. The Operational Status of an NA can be detected as: 'Available', 'Suspicious' and 'Unavailable'.

- The NA is considered 'Available' when it shows '*normal*' activity over the Common Domain and no other source (Central Monitoring Service) has raised an issue.

---

[12] The IE071 is also sent to the country from which the IE070 originated.

- The NA is considered 'Suspicious' when there is no message sent over the Common Domain for the configured interval (e.g. 30 minutes) though there are requests sent to this NA, with response pending, or messages cumulating in the queue.

- The NA is considered 'Unavailable' when it is in the "Suspicious" state and the IE974/IE975 request/response ping mechanism has confirmed the unavailability or some other source (Central Monitoring Service) has raised an unavailability issue.

The IE974/IE975 request/response ping mechanism is used by CS/MIS2 for confirming a detected potential unavailability. It is triggered by the detection of a potential unavailability of a NA. This process enables the system to detect performance decrease or potential undeclared unavailability of National Applications based on the analysis of movement monitoring data (i.e. their activity over the Common Domain sensed by the events recorded by the audit records). A decision for an alert is taken considering contextual information (e.g. declared unavailability, activity patterns, National holidays, strikes, pandemics), the information provided by existing central monitoring services and the IE974/IE975 ping mechanism. In case of absence of message IE975C, during a period that is configurable per country and per system in CS/MIS2, an alert is sent via e-mail (at least) by CS/MIS2 to a distribution list that includes the NHD of the country where the unavailability is detected, and the Central Project Team (ITSM Business Monitoring team).

II.2.5 Duplication of the error messages

The messages IE906, IE907 and IE917 exchanged between National Applications or National Application and TAXUD ieCA will be automatically duplicated at CCN level, in a transparent manner for the National project teams, for possible analysis for the CS/MIS users, and in particular for the ITSM Business Monitoring team who will be able to determine the error reasons. This process does not require any change of the configuration or developments by the National teams.

The duplication of the messages (IE906, IE907 and IE917) will be activated by ITSM CONTRACTOR by using the CCN MDS component. A copy of all error messages will be generated and dispatched to the specific CCN queues of CS/MIS.

CS/MIS must be capable of storing and processing the data elements of the error messages that are relevant for the business monitoring. Those elements will be automatically deleted from CS/MIS after a configurable period of time (e.g. 12 months).

For each CS/MIS domain, it will be possible to query the error messages, and to export into an MS-Excel file the result of the query, for further manual processing and analysis.

The information that will be available in CS/MIS will include:

For IE906A and IE906B:
- o MRN
- o Error type
- o Error pointer
- o Error reason *
- o Original attribute value *

For IE907A:
- o EDIFACT errors (INTERCHANGE, MESSAGE -> SEGMENT-> DATA ELEMENT)

For IE917B:
- o MRN
- o Entry key
- o Error Location *
- o Error Line Number
- o Error Column Number
- o Error Reason
- o Original attribute value *
- o Error Code

For IE906C:
- o MRN
- o Error pointer
- o Error code
- o Error reason
- o Original attribute value *

For IE917C:
- o MRN
- o Error line number
- o Error column number
- o Error pointer
- o Error code
- o Error text
- o Original attribute value *

Optional fields

II.2.6 *Information for the identification of Recipient NA operational mode during the Transitional Period of NCTS-P5 and AES-P1*

Section IV [R41] and [R40] defines how the Recipient NA operational mode shall be identified by the Sender in "To Be" and what shall checks must be performed prior submission of IE to Common Domain.

This requires the following information:

1. Information about start date of operations in the "To-Be" operational mode in Common Domain for NCTS-P5 and AES-P1

2. Information about Not implemented/supported functionality

The following sub-sections define where this information should be defined.

II.2.6.1 **Information about start date of operations in the "To-Be" operational mode in Common Domain for NCTS-P5 and AES-P1**

Each NA shall declare and maintain (when necessary) the start date of operations in the "To-Be" operational mode in Common Domain. This information is critical for the operations during the Transitional Period of NCTS-P5 and AES-P1.

This information will be declared by each NA and by updating the respective information in CS/MIS. The information about start date of operations in the "To-Be" operational mode in Common Domain for NCTS-P5 and AES-P1will be disseminated to NAs via an interface with similar protocol to CS/RD2.

Finally, an interface will also be established between CS/MIS and CS/RD2.

II.2.6.2 **Information about Not implemented/supported functionality by NA "To-Be"**

Each NA running in the "To Be" NA operational mode in Common Domain must also declare any functionality not implemented/operated via the "Availability Management" in CS/MIS.

In particular, the *Business service not implemented (System Unavailability Type "N")* shall be used for "specific" functionalities (if any) not implemented yet by pertinent NA in the scope of "To Be" phase. These functionalities cannot be any of functionalities/scenarios of the "To Be" phase guarantying the business continuity as defined in Section IV of [R41] and [R40].

Finally, this unavailability must be declared in CS/MIS before the start of operations. Please refer to section II.2.4 for availability management in CS/MIS.

II.3 Message exchanges with CS/MIS across the Web

Introduction

This chapter describes the mechanism for exchanging the following messages with CS/MIS:

II.3.1   IEs for Availability

- Availability: IE070, IE071, IE971.

CS/MIS offers separate data capture screens for some of the above messages. Dedicated instances of these messages will be exchanged for each separate Customs system. The user can supply the information to CS/MIS via a form provided in one of these screens. This is the case for IE070 (notification of unavailability). The following table shows the possibilities and in which direction each message is sent (Upload = from NCA to CS/MIS, Download = from CS/MIS to NCA).

IE	Upload/ Download	Data capture on screen of CS/MIS	Manual operation via browser
IE070	Up	X	X
IE071	Down	-	X
IE971	Down	-	X

Table 9: CS/MIS interfaces across the Web

No error reporting is foreseen via dedicated error message exchanges but only basic transfer.

The messages sent to the CS/MIS application will be generated by the HTML GUI according to the data entered by the user.

II.3.2   IEs for statistics

Information exchanges IE411 and IE412[10] are used for the exchange of Business Statistics data.

CS/MIS allows the manual upload of IE411 messages on the Web Interface. Either dedicated instances of these messages will be uploaded for each separate Customs system or one instance including data for all Customs systems. The user can simply supply the information to CS/MIS via a form provided in a screen.

The following table shows the possibilities and in which direction each message is sent (Upload = from NCA to CS/MIS, Download = from CS/MIS to NCA).

IE	Upload/ Download	Data capture on screen of CS/MIS	Manual operation via browser
IE411	Up		X
IE412[10]	Down		X

Table 10: Additional CS/MIS interfaces across the Web

No error reporting is foreseen via dedicated error message exchanges but only basic transfer.

II.3.3   CS/MIS HTTP exchanges protocols

II.3.3.1   Subscription

In order to subscribe a user for e-mail or CCN/CSI notifications, a web-based administration module accessed via a dedicated URI only is used.

II.3.3.2   Notification
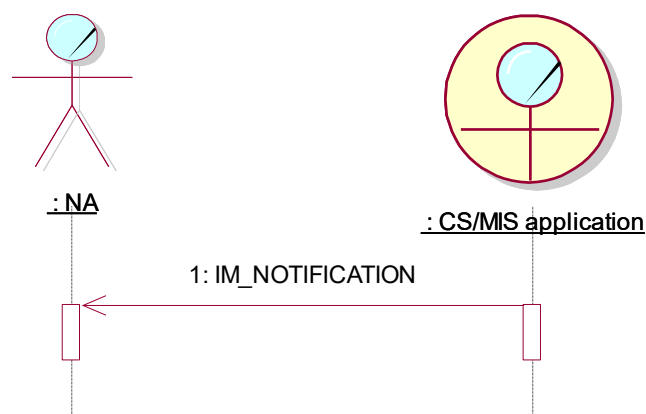
Figure 3: Notification from CS/MIS

Notifications are sent to the registered user by means of e-mail (IM_NOTIFICATION) to the e-mail address defined at registration, informing the user when new information is available. Distinct notifications will be sent to each Customs system subscriber.

II.3.3.3 Downloading from CS/MIS

In order to download an Information Exchange from CS/MIS a user first needs to request the download through the GUI, which will generate an IM_INITIATE_DOWNL message. This message contains details of the actual information requested.

The CS/MIS application replies by means of an IM_RESULT message. This message contains the URI where the requested information can be downloaded. The download then needs to be initiated by means of an IM_GET_FILE message. This triggers a "get" from the URI defined beforehand.

The CS/MIS application then sends the requested information. In the example below an IE971 is sent back. Different URIs will be available at CS/MIS for initiating download of IE071, and IE412[10]. In addition, different URIs will be also available for downloads related to each Customs system.
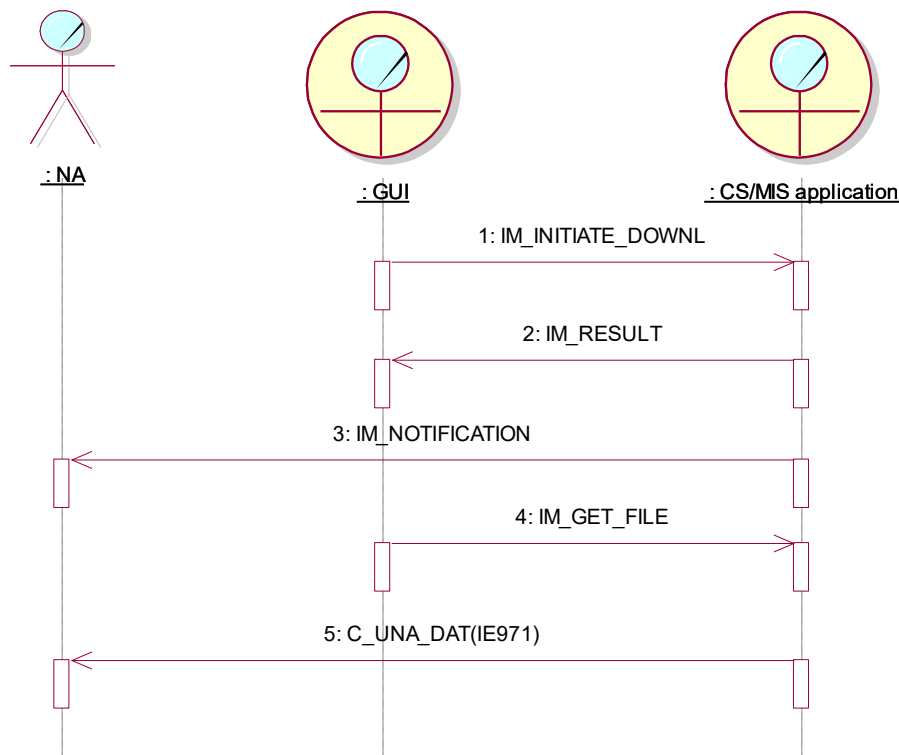
Figure 4: Downloading from CS/MIS

II.3.3.4 Uploading to CS/MIS

In order to perform an upload, the user sends the data to the CS/MIS application (IE070 in the example below). The (NA local) file to be uploaded is chosen through the GUI.

Different URIs will be available at CS/MIS for upload of IE070 and IE411.

In addition, different URIs will be also available for uploads related to each Customs system.

: NA

: CS/MIS application

1: C_UNA_COM(IE70)
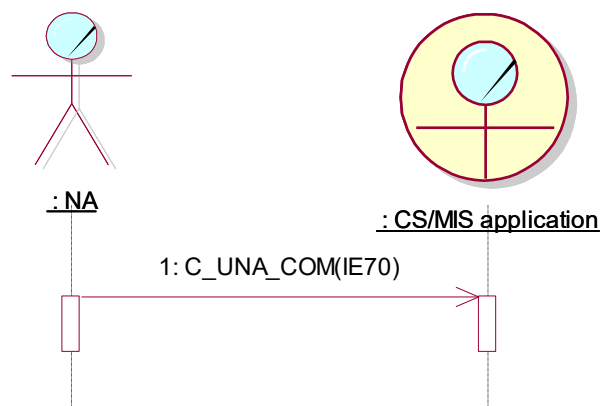
Figure 5: Uploading an IE070

II.3.4 CS/MIS manual mode of operation

A browser interface enables the download of an IE071 and an IE412[10] over internet. Distinct download links will be available for each Customs system.

II.4 Message exchanges with CS/MIS via CCN/CSI

This section deals with the IE411, the CCN/CSI technical statistics, the CCN/CSI audit files and the exchange of MRN Follow up queries and responses.

II.4.1 Sending IE411 data to CS/MIS

II.4.1.1 For NCTS-P4, ECS-P2, ICS-P1

The IE411 message has EDIFACT (CD411B) or XML (CD411C) as its format and is either sent to the CS/MIS application across CCN/CSI or it is manually uploaded on CS/MIS Web interface.

CS/MIS has a dedicated address on the CCN/CSI network and a dedicated queue for capturing the business statistics.

If the IE411 message is sent to the CS/MIS application across CCN/CSI, in the message descriptor the value 'CSIMQMT_DATAGRAM' must be used for the data element 'MsgType'.

If CS/MIS has problems with parsing IE411, an IE906, IE907 or IE917 message is returned to the originator.

Note: The replacement of CS/MIS by CS/MIS2 will not impact the configuration of the National Applications sending the CD411B or CD411C.

II.4.1.2   For NCTS-P5 and AES-P1

The CD411D message must have only XML format. It must be sent to the CS/MIS2 application across CCN/CSI or it is manually uploaded on CS/MIS2 Web interface.

CS/MIS2 has a dedicated address on the CCN/CSI network and a dedicated queue for capturing the business statistics.

If the CD411D message is sent to the CS/MIS2 application across CCN/CSI, in the message descriptor the value 'CSIMQMT_DATAGRAM' must be used for the data element 'MsgType'.

If the CS/MIS2 application detects an XML error when parsing the CD411D, it replies by sending a message CD917C (XML error) or CD906C (functional error) to the originator.

II.4.1.2.1 *Partial submission of business statistics via multiple submissions of CD411D*

The entire set of the mandatory Statistics Types that are specified in the CS/RD2 codelist CL057 (*StatisticsType*) for a specific period can be provided in more than one submission of the CD411D. However, <u>all</u> the 'Series Elements' of a Statistics Type are expected to be provided in the instance of the CD411D that provides the pertinent data for this specific Statistics Type and reporting period.

In CS/MIS2, the '*Reporting completion date*' defines the time interval for providing the entire set of Statistics Types for a specific period.

In case of partial submissions, the relevant warnings will be reported back to the sending NA (please see II.4.1.2.3) when the allotted time elapses. It is noted that warnings may be also sent before the end of the allotted time, in case that the entire set of the Statistics Types are provided before the '*Reporting completion date*'.

II.4.1.2.2 *Update of already provided Statistics Types related data*

An instance of CD411D can be also sent by an NA to update (i.e. replace) already submitted data (received by CS/MIS2 via a previous submission of an CD411D) for a specific reporting period, before or after the expiration of the '*Reporting completion date*'.

An operator at the 'STATISTICAL CHARACTERISTICS' level denotes if the provided data for a specific Statistics Type in a submission of an CD411D is intended for new registration or for update (i.e. replacement) of already submitted data (which was forwarded by a previous submission of an CD411D for the same period).

It is emphasised that in case of update, the entire set of 'SERIES ELEMENTS' for a specific Statistics Type must be provided; any previously registered values will be <u>replaced</u> by the

new ones. It is noted that the update will be also used in case that an NA wants to 'de-support' data for previously submitted Statistics Type.

Erroneous use of the operator will lead to rejections of the CD411D. Indicatively, such cases could be the submission of more than one "new" registrations for the same Statistics Type for a specific period as well as the submission of update of data that have not been previously submitted or received.

II.4.1.2.3 *Validations performed by CS/MIS2 on a received CD411D*

If the message is correct (no CD906C nor CD917C exchanged), the CS/MIS2 Central Application shall immediately validate the content of the Business Statistics messages (CD411D) submitted by the NA, in terms of data quality. The first step of the validation is to verify that the Business Statistics message contains all the mandatory Statistics Types applicable (as defined in CS/RD2 code list CL057). The second validation will perform predefined *Consistency Checks* on the actual submitted values. In case of findings, CS/MIS2 will send to the originator of the CD411D the warning message (IE903) that includes the relevant Consistency Check code(s) (as defined in CS/RD2 code list CL903).

II.4.2 *Sending the Technical Statistics*

Generation of technical statistics is performed under the supervision of the ITSM CONTRACTOR. The ITSM CONTRACTOR therefore installs and configures the necessary software on the CCN gateways. The only thing that is required from the NA is support during the configuration of the CCN gateway. Technical statistics are sent to CS/MIS at ITSM in a dedicated statistics queue created for each Customs system. They will be sent as a flat text file.

II.4.3 *Sending the CCN audit files*

Generation of CCN audit files is performed under the supervision of the ITSM CONTRACTOR. The ITSM CONTRACTOR therefore installs and configures the necessary software on the CCN gateways. The only thing that is required from the NA is support during the configuration of the CCN gateway. Audit files are sent to CS/MIS in the dedicated audit files queue created for each Customs system. They will be sent as a flat text file.

II.4.4 *Duplicating the Error Messages*

Duplication of error messages is performed under the supervision of the ITSM CONTRACTOR. The ITSM CONTRACTOR therefore installs and configures the necessary software on the CCN gateways. The only thing that is required from the NA is support during the configuration of the CCN gateway. Duplicated messages are sent to CS/MIS in dedicated queues created for each domain.

II.4.5 *Exchanging the proactive monitoring messages*

As described in section II.2.4.1, the IE974/IE975 request/response ping mechanism is used by CS/MIS2 for confirming a detected potential unavailability of the NCTS-P5 and AES National Applications. It is triggered by the detection of an inactivity period of a NTA or

NECA. CS/MIS2 shall constantly monitor Gateways and Applications of the NAs and shall use the ping mechanism of the IE974/IE975 to verify the availability.

The IE974C is sent to an NCA when it is considered 'Suspicious' for unavailability, since there is no activity over the common domain based on the analysis of movement monitoring data (i.e. their activity over the Common Domain sensed by the events recorded by the audit records). The ping mechanism (i.e. exchange of the IE974/IE975 messages) confirms the unavailability, when the NCA does not reply with the IE975C within a specific timeframe (i.e. configurable per NA). As a result, the CS/MIS2 dispatches alert notifications with the relevant information to the National Admistination where the unavailability is detected and to the Central Project Team (i.e. ITSM Business Monitoring team).

In the following Figure 6, we see NCA_1 receives the IEx02 message[13] from NCA_2, but NCA_1 does not respond (neither with IEx03 message nor with IE906/IE917). Additionally, there is no specific activity from the NCA_1 for quite some time in the Common Domain (i.e. no message sent by NCA_1). In that case, the CS/MIS2 shall send the CD974C. As no CD975C is received from NCA_1, CS/MIS2 shall record that NCA_1 is unavailable and alert notifications are sent (e.g. via e-mail).
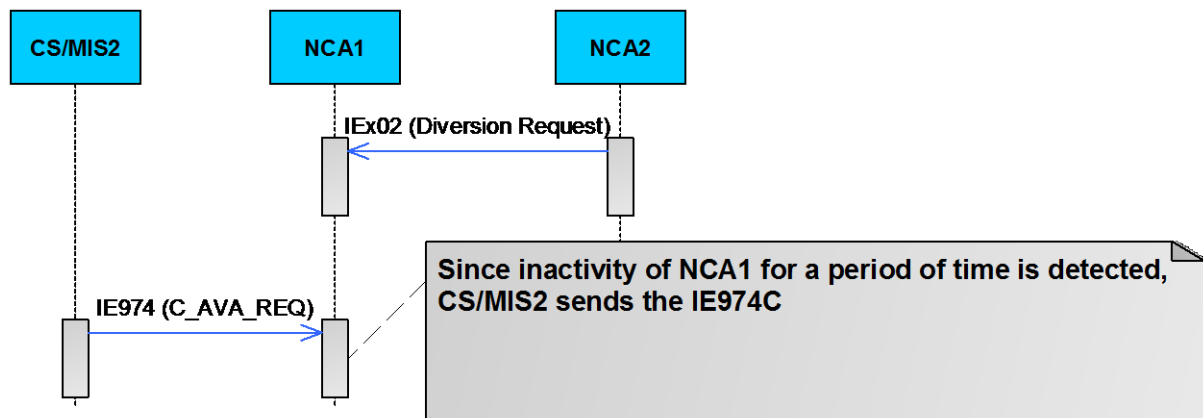
Figure 6: Dispatch of the IE974 from CS/MIS2 for a detected unavailability

---

[13] This ping mechanism is applicable for NCTS-P5 and AES.

In the following Figure 7, we see that CS/MIS2 sends the IE974 at specific intervals to check the availability status of the NCA_1. Indeed, when NCA_1 is available again, it responds to NCA_2 with IEx03 and with the IE975 to CS/MIS2[14].
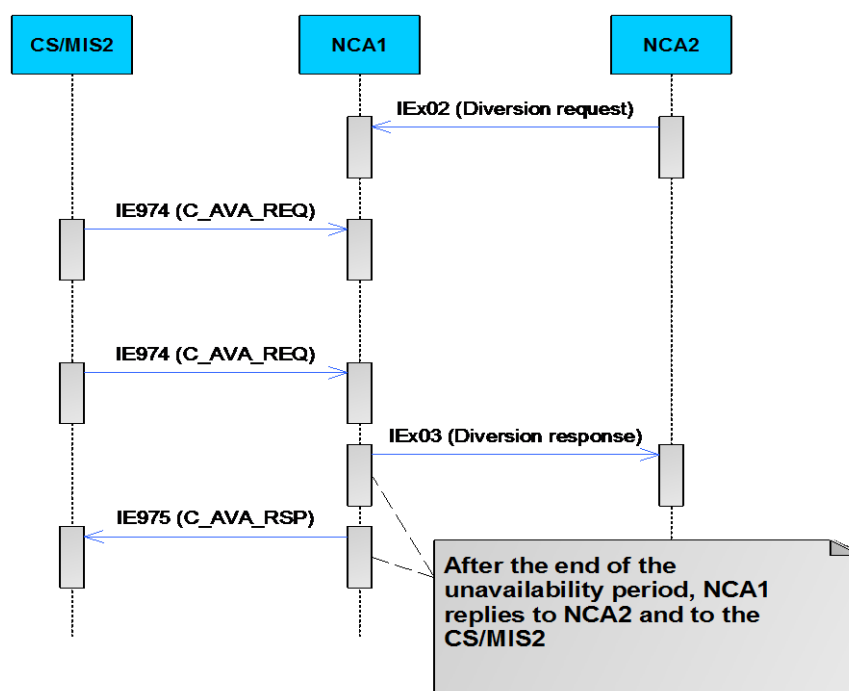
Figure 7: Dispatch of the IE975 to CS/MIS2 when NCA_1 becomes available

II.4.6   *Sending the IE078 and IE578 for linked MRNs*

II.4.6.1   **Sending the IE078 for linked MRNs (NCTS-P5/AES-P1)**

When a transit movement is released for transit and includes one or more AES movement(s) as previous procedures (i.e. Export MRN(s) declared as 'PREVIOUS DOCUMENT'), then together with the dispatch of CD001C (for international transit) or the dispatch of CD003C (for international diversion of national transit, with no CD001C exchanged on the Common Domain) to the Office of Destination, the message CD078C is also sent by the NTA (i.e. the Office of Departure) to CS/MIS2. The CS/MIS2 application will process this message and use this inter-domain linking information to update the *MRN Follow up* section. This will enable the CS/MIS2 users (i.e. NCTS users and AES users) to easily monitor the status of their transit movement(s) that follow the export movement(s). Please refer to section III.II.7 of the DDNTA Main Document [R41] for more details.

---

[14] One (1) IE975C is sent as a reply to each IE974C when NCA_1 is available again.
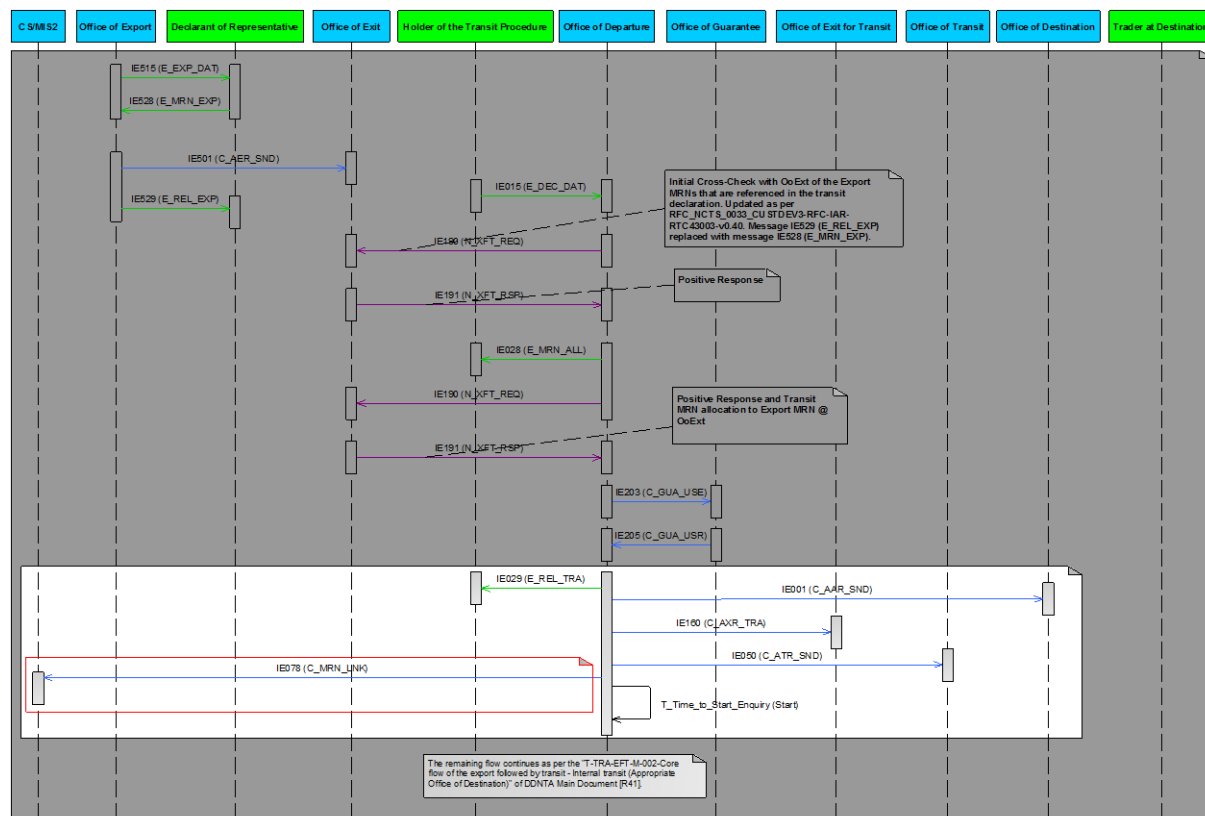
Figure 8: Dispatch of the Inter-Domain Linking message (IE078) in case of Export followed by Transit

II.4.6.2 Sending the IE578 for linked e-ADs (AES-P1/EMCS)

When an export movement is released for export and includes one or more EMCS movement(s) as previous procedures (i.e. EMCS e-AD(s) declared under Goods Item/Previous Document), then together with the dispatch of CD501C (or CD503C in case of direct export becoming indirect export) to the Office of Exit, the message CD578C is also sent by the NECA (i.e. the Office of Export) to CS/MIS2, which will process this message and use this inter-domain linking information to update the *MRN Follow up* section[15]. This will enable the CS/MIS2 users (i.e. AES users) to easily monitor the status of their export movement(s) that include goods under excise duty suspension arrangement. Please refer to section III.4.1.6 of the DDNXA Main Document [R40] for more details.

---

[15] It covers both international and national EMCS movements.

At this stage, EMCS movements (ARC Follow up) are visible in CS/MISE and not in CS/MIS2. In case of national EMCS movements, where MSA of Dispatch = MSA of Export, the national domain exchanges between MSA of Dispatch and MSA of Export may not be visible via CS/MISE (if loopback mode not implemented yet).
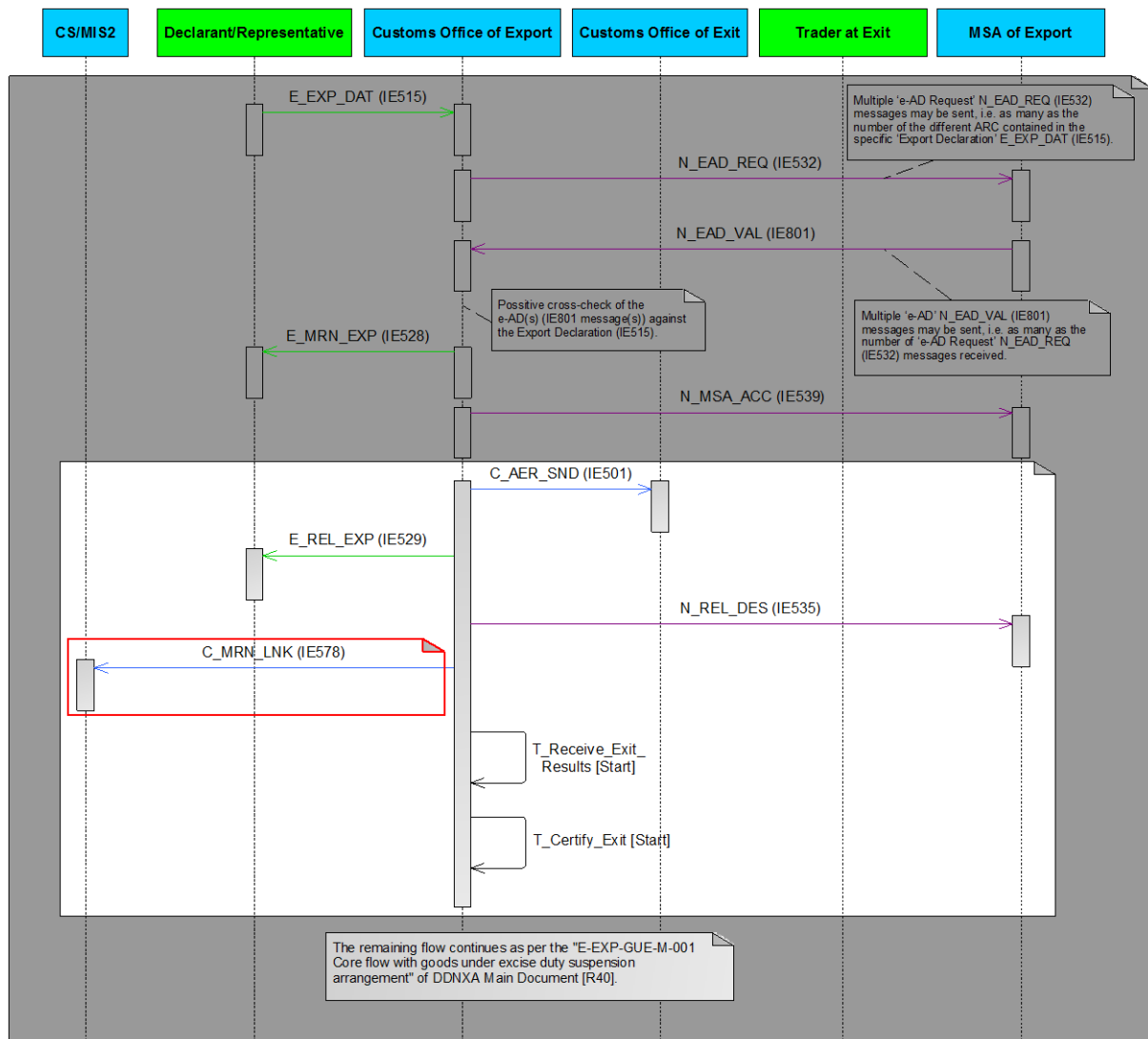
Figure 9: Dispatch of the Inter-Domain Linking message (IE578) in case of Export of Goods under Excise Duty Suspension Arrangement

III Systems Administration

III.1 Introduction

For all Customs systems the procedures and tools (i.e. archiving procedures, configuration management, version control, data management, fallback procedures, problem tracking, and audit trail) used for system administration are a national matter and consequently do not concern other National Administrations. All NCAs need to keep a log of exchanged information, for relating an error to the information that has been exchanged and to solve any disputes regarding exchanged information. This log needs to contain:

- The content of the messages that have been exchanged (either sent or received), thus including all steering information specified by the Data Group MESSAGE (see Design principles), e.g. interchange reference, interchange addresses, message reference, MRN, and functional message type;

- A timestamp showing at which date and time the Information Exchange (IE) has been prepared for sending or has been received;

- For NCTSP4 and ECSP2 exchanges the result of conversion of received EDIFACT interchanges (if the exchange is in EDIFACT format) and a related timestamp including all detected errors;

- All messages before those are sent over CCN, in the format used and with the related timestamp;

- The result of application processing of the message, including all detected errors and any state change triggered by the message. If any error has been detected, the message will be viewed as not being processed by a National Application (NCA);

- A timestamp showing the date and time at which the Information Exchange (IE) has been exchanged through CCN. At reception, the timestamp is the date and time of receiving the Information Exchange (IE). At sending, it is the date and time of delivering the message to the CCN Gateway of the sending National Application;

- The CSI header for the particular message. The structure of the CSI header is given in the CCN/CSI Common Definitions Reference Manual (C language or jCSI), see VIII

- The status of the exchange of the message across CCN (e.g. reception of a Confirm on Delivery and its related timestamp);

- The name of the queue to which the message has been submitted.

During the Transitional Period of NCTS-P5 and AES-P1 operations and when NCA[NCTS-P5 and AES-P1] uses a convertor (TAXUD ieCA or NCO) for downgrade or upgrade of messages for CD exchanges between NCA[NCTS-P5 and AES-P1] and NCA [NCTS-P4/ECS-P2] the NCA[NCTS-P5 and AES-P1] must store:

- the content of the original messages that are sent for conversion (for Upgrade conversion is the message received from Common Domain and to be converted, for Downgrade conversion is the message produced by NCA and to be converted) along with the result of conversion in EDIFACT or XML format (for Upgrade conversion is the converted message processed by the NCA[NCTS-P5 and AES-P1], for Downgrade

conversion is the converted message submitted by NCA[NCTS-P5 and AES-P1] in Common Domain) .

- in case of functional (IE906) or CONTRL (IE917 or IE907) errors submitted/received for a submitted message, the originally submitted/received functional (IE906) or CONTRL (IE917 or IE907) along with the "converted" functional (IE906) or CONTRL (IE917 or IE907) with **generic error reporting**. Please refer to V.3.2.1.5.3.

As there is a one to one correspondence between a CSI message, an EDIFACT/XML interchange, and an EDIFACT/XML message, this log does not need any further detail and can consist of one table. Note that the data needs not to be logged in application format since those formats will be different per Application.

IV Technical Message Structure

IV.1 Data dictionary

Whenever there is a reference to an Appendix of DDNA, please note that there is a separate set of Appendices for each domain, which accompanies each domain specific DDNA volume.

IV.1.1 Data Items

The different Data Items that are part of each movement system are listed in Appendix Z of the corresponding set of DDNA Appendices and in the CSE database.

Every Data Item is identified by a unique name provided in Appendix Z. The naming conventions are listed in section I.4.3.1 of this document. Note that every name will contain, in principle, some lowercase characters, except for the following:

- Those that are consisted by a single acronym (e.g. MRN);

- NAD LNG (not used in AES-P1 and NCTS-P5).

Every Data Item has an associated type (which can be numeric, alphanumeric, decimal, time, date and datetime) and, in some cases, a Data Item can have only discrete values. In this case, the Data Item is said to have an associated Code List.

Note that there are two categories of free text fields:

- Fields with an associated language code (LNG field). This LNG field may contain the code of the language in which the text was originally written;

- Fields without such language code.

For AES-P1 and NCTS-P5 there is no language associated to any of the fields, since the data are encoded in UTF-8.

IV.1.2 Data Groups

The different Data Groups being part of each movement system are listed in Appendix Y of the corresponding DDNA volumes.

Every Data Group consists of a number of Data Items in a particular order. Every message is composed of a certain number of Data Groups in a particular hierarchy. Every Data Group is identified by a name. Note that group names are not unique. It may thus very well happen that the same group name is found in different messages. Moreover, groups with the same name may hold only a subset of the available set of data items and sub-data groups that the data group can hold.

Note that some Data Groups may not always have the same Data Item sequence in different messages.

IV.1.3 Code lists

Code list is a synonym of RD Entity, originating from CS/RD. For the RD Entity definition (and other CS/RD2 related definitions) please refer to DDRA [R27].

A name and a number identify code lists. Code Lists are maintained by the central reference application (CS/RD2), see [R27] and [R31]. DDRDA [R27] also describes the methods that can be used for the synchronisation of National Customs Applications with CS/RD2 content. Furthermore, Traders can also access Codelists from DDS2 on europa.eu site.

IV.2 Technical message structure for NCTS-P4, ECS-P2 and ICS-P1

The structure and format of the different Information Exchanges for movement systems is included in the corresponding Appendix Q. These appendices contain a message format description for every Information Exchange that is part of the specific system.

The technical message description is supplied in two parts.

The first part is the message description. This description contains the overall layout of the messages. It defines the different Data Groups that are part of the message, the sequence of the groups, the level of hierarchy of the Data Groups, the optionality of the Data Group, the possible repeat count, and associated rules and conditions. Concerning the optionality, it should be noted that the following rules apply:

- If a Data Group is always required, it is marked as "R" for movement systems;

- If there are some rules and conditions related to the presence of the Data Group, it is marked as 'D';

- If there are no rules and conditions related to the presence of a particular Data Group, it is marked as 'O'. However, if information is available it should be included in the message despite the fact that this Data Group is characterised as optional. It should be noted that when data in one message is derived from another message the rules and conditions are carried forward.

In order to go down one level in the hierarchy the Data Group at the higher level in the hierarchy needs to be present.

The second part of the TMS contains the description of the different Data Items. This description includes the sequence of the data elements in the group, the optionality, and the associated rules and conditions.

Concerning the optionality of the Data Items, the following rules apply:

- If a Data Item is always required, it is marked as "R";

- If there are some rules and conditions related to the presence of the Data Item, it is marked as 'D';

- If there are no rules and conditions related to the presence of a particular Data Item, it is marked as 'O'. However, if information is available it should be included in the message despite the fact that this Data Item is characterised as optional. Moreover,

when data is derived from another message the rules and conditions are implicitly carried forward.

Concerning the rules and conditions, the rules and conditions from [R26], [R13] and [R14] have been copied. These are marked as 'Rule xxx' and 'Cond yyy' as specified in the appropriate FSS version. Additional technical rules have also been added. These have been marked as 'TR xxxx'.

Note that not all rules and conditions of [R26], [R13] and [R14] have been copied. The reasons for this are discussed in chapter IV.7.

Additional explanation on the message format for the movement systems is included in Appendix Q.

The message description part of this document consists of message hierarchies, correlation tables to map the Information Exchanges to these hierarchies, and mappings to the different used EDI-formats (EDIFACT, XML).

The status codes used for Data Groups and Data Items for FMS in the FSS ([R26], [R13], [R14]) is related to the status codes used in DDNA volumes as follows:

Status description	FSS status code	DDNA status code	EDIFACT status code
Required/mandatory	R	R	M
Optional	O	O	C
Dependent/Conditional	C	D	C

Table 11: Use of status codes

The abbreviations stand for Required, Mandatory, Optional, Conditional and Dependent.

The DDNA status codes are used in the Correlation tables in the corresponding Appendix J and the TMS in Appendix Q.

The EDIFACT status codes appear in the corresponding Appendix H in the left-hand columns of the mapping tables.

IV.3 Technical Message Structure for NCTS-P5 and AES-P1

Following analysis of conversion needs, a single technical message structure will be delivered in DDNA system specific volumes (NCTS-P5 and AES-P1):

Structure	Description	Intended Usage & Implementation
Technical Message Structure	A single Technical Message Structure (e.g. IE501C) containing TRTs and BRTs. TRTs and BRTs are structured in such a manner (their validity is date-dependent) in order to be phased out without the need of a software change of the UCC NCAs.	Shall be implemented by NCA in **NCTS-P5** and **AES-P1**

Table 12: Technical Message Structures for NCTS-P5 and AES-P1

The **Transitional Structural Constraints** are implemented in DDNA system specific volumes for NCTS-P5 and AES-P1 with the form of TRTs (Technical Rules for Transition).

The TRTs will have limited validity period. They must be applied in validation process of a message in case following condition is true:

IF [Current Date] *is*

- *less than or equal to* **Common Transitional Period End Date**

THEN TRT is active

ELSE TRT is inactive

with Current Date = Date of Message Validation

The **Business Structural Changes/Constraints** are implemented in DDNA system specific volumes for NCTS-P5 and AES-P1 with the form of BRTs (Business Rules for Transition). Two (2) different categories of BRTs are defined:

- BRT-1 that relaxes validations of R/C and is applicable for messages having a Decisive date (e.g. <Declaration acceptance date>) before the end of the Transitional Period;

- BRT-2 that enforces a stricter message structure and is applicable for messages having a Decisive date (e.g. <Declaration acceptance date>) after the end of the Transitional Period.

The values of Decisive date (potentially different per type of message) is defined in the DDNA specific volumes.

The structure and format of the different Information Exchanges for movement systems is included in the corresponding Appendix Q2. These appendices contain a message format description for every Information Exchange that is part of the specific system.

The technical message description is supplied in two parts.

The first part is the message description. This description contains the overall layout of the messages. It defines the different Data Groups that are part of the message, the sequence of the groups, the level of hierarchy of the Data Groups, the optionality of the Data Group, the possible repeat count, and associated Rules and Conditions. Concerning the optionality, it should be noted that the following rules apply:

- If a Data Group is always required, it is marked as "**R**" for movement systems;

- If there are Conditions related to the presence of the Data Group, it is marked as '**D**';

- If there are no Rules and Conditions related to the presence of a particular Data Group, it is marked as '**O**'. However, if information is available it should be included in the message despite the fact that this Data Group is characterised as optional.

In order to go down one level in the hierarchy the Data Group at the higher level in the hierarchy needs to be present.

The second part of the TMS contains the description of the different Data Items. This description includes the sequence of the data elements in the group, the optionality, and the associated Rules and Conditions.

The following codes apply for the optionality of the Data Items:

- **Required ('R')**: a Data Item is marked as 'R'if it is always required;

- **Dependent ('D')**: a Data Item is marked as 'D' if there are some Conditions related to the presence of the Data Item;

- **Optional ('O'):** a Data Item is marked as 'O' if there are no Conditions related to the presence of a particular Data Item. However, if information is available it should be included in the message despite the fact that this Data Item is characterised as optional.

The DDNA optionality codes are used in the Correlation tables of Appendix J and in the TMS of Appendix Q2.

Definitions for Rules, Conditions, Ss, Ts, TRTs, BRTs and Guidelines are provided in Table 2.

The Rules and Conditions from [R28], [R29] are the baseline. It is worth noting that not all Rules and Conditions of [R28], [R29] have been copied in DDNA. The reasons for this are discussed in chapter IV.8.

Section IV.4 defines the numbering convention for Rules, Conditions, Technical Rules (T) Technical Rules for Transition (TRT) and Business Rules for Transition (BRT).

Further information about the syntax of Rules, Conditions and Technical Rules can be found in section IV.5.

The logic for the validation of multiples Rules & Conditions using the correct sequence is defined in section IV.6 (for NCTS-P5 and AES-P1).

The following table summarizes the expected validation of TMS for NCTS-P5 and AES-P1:

Validation Level	Validation element	Sender of IE	Recipient of IE
Syntax/Structural Validation	XSD (incl. technical codelists)	Mandatory	Mandatory
Semantic Validation	Business Codelists	Mandatory	Mandatory
	Rules and Conditions • Sequencing Rules (Sxxxx) • BRTs (B1xxx) / BRTs (B2xxx) • TRTs (Exxxx) • Conditions (Cxxxx) • Rules (Rxxxx) • Technical Rules (Txxxx)	Mandatory	Conditional – Only If specific Rule/Condition is applicable for Recipient validation

Table 13: Expected validation of TMS for NCTS-P5 and AES-P1

IV.3.1   Semantic Validation for NCTS-P5 and AES-P1

IV.3.1.1   Rules/Conditions Validation Principles for External Domain IEs

The Rules/Conditions validation will be differentiated for External Domain (ED) messages compared to Common Domain (CD) and National Domain (ND) messages. A basic principle is that the ED IEs CCx15C and CC170C are messages acting as declarations with 'legal' consequences for the declarant. The Traders' legal responsibility must not be transferred to the recipient National Customs Applications (NCA) that performs the declaration data validation.

The validation levels are the following:

a. The legislation (that imposes physical and documentary controls);

b. The *checkable* R/Cs at the NTA/NECA side in the declaration IEs;

c. The *non-checkable* R/Cs at the NTA/NECA side (cannot be checked by NTA/NECA because relevant data are not available at NTA/NECA).

Both **Sender** and **Recipient** in ED must check all R/Cs considering the above levels. However, their validation will be defined at national level.

An NA is authorised to add additional or modify R/Cs or to define stricter regular expressions to enforce maximum consistency. It shall avoid 'relaxed' R/C validation that would lead to less quality of data. The content of some codelists can be extended with National values (for national usage only), while the content of other codelists could be restricted if one or more values are not applicable).

Any justified deviation on the codelists applied on ED message that would also impact the Common Domain messages needs to be documented as a National Deviation for acceptance by the Central Project Team, with decision taken before the Conformance Testing activity starts.

IV.3.1.2   Rules/Conditions Validation Principles for Common Domain IEs

The following principles are applicable:

1. Any *Validation Definition* indicated in the DDNxA Appendice K concerns only the Common Domain IEs and not the External Domain nor National Domain IEs;

2. The CD IEs that are based on the declaration IEs shall conform to the CD Technical Specifications irrespectively if an NA has defined a national variant of the declaration (e.g. CCx15C.xsd different from the one published by DG TAXUD);

3. The **Sender** must ensure the quality of data, meaning that <u>all</u> R/C <u>must</u> be validated, except those (defined in the DDNxA Appendice) that can be validated only after the exchange of supplementary IEs or that demand physical/documentary control;

4. It is <u>Required</u> for the **Recipient** to validate what is received in terms of validation against XSD.

5. It is <u>Strongly Recommended</u> for the **Recipient** to validate what is received (in terms of validation against the codelists defined in CS/RD2, the validation of R/Cs, the validation against interfaced applications (e.g. EOS, TARIC) as defined in the rules or recommended in the guidelines.

6. It is <u>Required</u> for the **Recipient** to validate some specific R/Cs that are *non-checkable* by the **Sender**, or is crucial to trigger or not an important process (e.g. to assess if the Safety & Security Data are all available and valid (or not), to enforce a request (or not) of a separate EXS).

7. The **Recipient** <u>shall not</u> validate some specific R/Cs, because it is considered that only the **Sender** can verify the accuracy of the information included in the message exchanged. Consequently, the **Recipient** shall not reject an incoming IE based on the validation result of these specific R/Cs.

IV.3.1.2.1 Validation values

Based on the above principles, Rules/Conditions validation definition for Sender and Recipient will be based on the below allowed set of validation values for the Common Domain IEs:

*   "R" (Required validation by all countries),

*   "SR" ('Strongly recommended'),

*   "N" (Not allowed/applicable validation),

- "-" (Not defined, for the External Domain & National Domain).

Any R/C will have a *global validation value* for both "Validation by Sender" and "Validation by Recipient" attributes, taken from the values of the above list.

In some cases, the *global validation value* must be overwritten by an *exceptional validation value*. Indeed, some R/C need to be validated differently for one or more specific IE(s). In that case, the globally assigned value for the "Validation by Sender" and "Validation by Recipient" attributes is replaced by *exceptional validation value* that will be declared specifically for this (these) IE(s).

IV.3.1.2.2 Validation general categories

1. No validation value will be declared to all **Guidelines** and **Sequencing Rules**;

2. For **TRT**s the validation value for the **Sender** will be "R" and for the **Recipient** will be "SR";

3. **BRT-1**s that disable R/C and define optionality must be validated by both **Sender** and **Recipient** (Validation value: "R");

4. **BRT-1**s that operate like Rules must be validated by the **Sender** and for the **Recipient** the validation value will be applied on a case-by-case basis.

5. **BRT-2**s that disable R/C and define optionality must be validated by both **Sender** ("R") and **Recipient** ("R");

6. **BRT-2**s that apply format restriction must by validated by the **Sender** ("R"). Validation by **Recipient** is Strongly Recommended ("SR");

IV.4 Numbering Convention for Rules & Conditions (R/C/T/TRT/BRT/S/G) for NCTS-P5 and AES-P1

The following numbering conventions will be followed per case:

Item	Naming Convention	Example
Rule	R[0-9]{4}	R0918
Condition	C[0-9]{4}	C0004
Technical Rule	T[0-9]{4}	T0005
Technical Rule for Transition (TRT)*	E[1]{1}[0-9]{1}[0-9]{2}	E1101
Business Rule for Transition (BRT)**	B[1-2]{1}[0-9]{1}[0-9]{2}	B1002
Sequencing Rule	S[0-9]{4}	S0001
Guideline	G[0-9]{4}	G0001

Table 14: R/C/T/TRT/BRT/S/G Numbering Convention

* Particularly for TRT, second, third and fourth/fifth positions shall be filled in as follows:

- **Second position [1]{1}**: can have only the following value

Value	Description
1	Denotes a Condition-like structure

Table 15: Value for second position of TRT number

- **Third position [0-9]{1}**: can have one of the following values:

Value	Description
1	Formatting Restrictions
2	Patterns Restrictions
3	Optionality Restrictions
4	DG Repetitions Restrictions

Table 16: Values for third position of TRT number

- **Fourth and Fifth position [0-9]{2}**:

A sequential number starting from '00' shall be filled in for each TRT.

** Particularly for BRT, second and third to fifth positions shall be filled in as follows:

- **Second position [1-2]{1}**: the category of the BRT. It can have one of the following values:

Value	Description
1	BRTs that must be validated for movements accepted before the end of TP (e.g. for movements accepted during TP but still open after TP)
2	BRTs that must be validated if acceptance date of declaration is after TP for applying some UCC data requirements in post transition phase in structures (XSDs) which are common during TP and after TP

Table 17: Values for second position of BRT number

- **Third position [0-9]{1} – Category**: For each BRT category, a number of sub-categories are defined:

Category	Sub-category	Description
1	5	Codelists value mismatch: values between previous and new phase do not match
1	8	Rules & Conditions issues
2	1	Formatting Restrictions
2	2	Patterns Restrictions
2	3	Optionality Restrictions
2	4	DG Repetitions Restrictions

Table 18: Values for third position of BRT number

It is noted that the Category types can be combined only with certain values from Table 17 as depicted in the above table.

- **Fourth and Fifth position [0-9]{2}**:

A sequential number starting from '00' shall be filled in for each BRT.

IV.5 Rules/T/TRT/BRT, Conditions and Guidelines definition and syntax for NCTS-P5 and AES-P1

IV.5.1 Definition of Rule, T, TRT, BRT or Condition

This section defines the various classes of rules and conditions that are used in the Technical Message Structures. It defines the various attributes of the rules and conditions and some of the principles of their definitions. Some examples are provided for a good comprehension of the provided information.

The 'Rules and Conditions' (generic term) are defined in Specs Manager and exported per system in the pertinent Appendix Q2, Q2 R/C and K of the system specific DDNA volume.

Each Condition, Rule, Technical Rule, TRT, BRT, Guideline and Sequencing Rule shall be defined as follows:

Functional Description →See Appendices Q2 and Q2 R/C	• textual description • defines the Condition, Rule, Technical Rule and Guideline from business/functional point of view, • use pointers based on business name of data group/item.
Technical Description →See Appendices Q2 and Q2 R/C	• textual description • defines the Condition, Rule, Technical Rule, TRT, BRT and Sequencing Rule from technical point of view, • uses XPath pointers.
Validated by Sender →See Appendix K	• enum value ('R', 'SR', 'N', '-'), • indicates whether the particular Rule, Technical Rule, TRT, BRT or Condition shall be validated by the Sender of the message (prior submission).
Validated by Recipient →See Appendix K	• enum value ('R', 'SR', 'N' , '-'), • indicates whether the particular Rule, Technical Rule, TRT, BRT or Condition shall be validated by the Recipient of the message (upon reception).
DROOLS implementation flag →See Appendix Q2 R/C	• flag (Yes/No), • indicates whether DROOLS implementation exists for the particular Rule, Technical Rule, TRT, BRT or Condition.

Table 19: Definition of Rule, T, TRT, BRT or Condition

The "Validation by Sender"/"Validation by Recipient" attributes of each R/C are defined per message mapping and listed in Appendix K of the specific DDNA volume. This means that, based on the business need, each IE has been evaluated and assigned a specific "Validation by Sender"/"Validation by Recipient" value for all R/C applied to it.

An example follows for C0105:

Functional Description	IF <CUSTOMS OFFICE OF EXIT FOR TRANSIT (DECLARED)> is PRESENT THEN <CUSTOMS OFFICE OF TRANSIT (DECLARED)> = "R" ELSE <CUSTOMS OFFICE OF TRANSIT (DECLARED)> = "O"
Technical Description	IF /*/CustomsOfficeOfExitForTransitDeclared is PRESENT THEN /*/CustomsOfficeOfTransitDeclared = "R" ELSE /*/CustomsOfficeOfTransitDeclared = "O"
Validated by Recipient	SR
Validated by Sender	R
DROOLS implementation flag	Yes

Table 20: Definition of a Condition: example of C0105 (applicable to NCTS-P5)

An example follows for R0222:

Functional Description	IF the zero value is recorded for a specific goods item for <GOODS SHIPMENT-GOODS ITEM-PACKAGING.Number of packages> THEN <GOODS SHIPMENT-GOODS ITEM-COMMODITY-GOODS MEASURE.Gross mass> is EQUAL to '0' (zero value)
Technical Description	IF the zero value is recorded for a specific goods item for /*/GoodsShipment/GoodsItem/Packaging/numberOfPackages THEN /*/GoodsShipment/GoodsItem/Commodity/GoodsMeasure/grossMass> is EQUAL to '0' (zero value);
Validated by Recipient	SR
Validated by Sender	R
DROOLS implementation flag	Yes

Table 21: Definition of a Rule: example of R0222 (applicable to AES-P1)

An example follows for C0810, a Condition applied on one Data Group or Data Item of message **A** which requires data from a message **B** in order to validate the message **A**:

Functional Description	IF <CD001C-CONSIGNMENT -TRANSPORT EQUIPMENT.Number of seals is GREATER than '0'
	OR <CD003C-CONSIGNMENT-TRANSPORT EQUIPMENT.Number of seals is GREATER than '0'
	OR <CD003C-CONSIGNMENT-INCIDENT-TRANSPORT EQUIPMENT.Number of seals is GREATER than '0'
	THEN <CD018C-CONTROL RESULT.State of seals> = "R"
	ELSE <CD018C-CONTROL RESULT.State of seals> = "O"
Technical Description	IF /CD001C/Consignment/TransportEquipment/numberOfSeals is GREATER than '0'
	OR /CD003C/Consignment/TransportEquipment/numberOfSeals is GREATER than '0'
	OR /CD003C/Consignment/Incident/TransportEquipment/numberOfSeals is GREATER than '0'
	THEN /CD018C/ControlResult/stateOfSeals = "R"
	ELSE /CD018C/ControlResult/stateOfSeals = "O"
Validated by Recipient	SR
Validated by Sender	R
DROOLS implementation flag	Yes

Table 22: Definition of a Condition: example of C0810 (applicable to AES-P1/NCTS-P5, NCTS-P5 version is used)

IV.5.1.1   Conditions

Conditions are defined in Table 2. All Conditions should be formulated with the IF THEN ELSE syntax. Typically, the antecedent part of a condition (IF-part) evaluates one of the following:

- the exact value of a data group/data item

- if the value of a data item is in a SET of values (e.g. CL009 or {0, 1, 2, 4, 9}

- if a data group/data item is present (has value)

The consequent part of a condition (THEN-part) defines the optionality of the data group(s)/data item(s). The following symbols will be used to indicate optionality:

- "R" indicating that the pertinent data group/data item is Required;

- "O" indicating that the pertinent data group/data item is Optional;

- "N" indicating that the pertinent data group/data item cannot be used.

Pointers to data groups/items in Functional Description of Conditions shall be in the form of **full path** in angle brackets.

Example: *<MESSAGE-OFFICE OF DESTINATION.Reference number>*

When a condition indicates that a dependent data group/item 'cannot be used' in a specified case, then the specific data group/item must not be present at all in the message structure and therefore shall not include them either with a 'NULL' value, empty value or even spaces.

IV.5.1.2   Rules, Technical Rules and Guidelines

Rules, Technical Rules and Guidelines are defined in Table 2.

In case Rules and Technical Rules evaluates one of the following:

1. the exact value of a data group/data item

2. if the value of a data item is in a SET of values (e.g. CL009 or {0, 1, 2, 4, 9})

3. if a data group/data item is present (has value)

then must be formulated with the IF THEN ELSE syntax.

Rules and Technical Rules *Functional Description* can include:

A. **<Full path>** pointers to data groups/items.

   Example: <MESSAGE-HEADER.Declaration type >

B. **<Context specific>** pointers to data groups/items where the context is the Rule/T/TRT-Rule applicability in the IE under validation.
   Example: <Applied Element>

If a Rule or Technical Rule checks that the value of a data group/item is member of set of values (if there are multiple values) or requires the allowed value of a data group/item to be

member of a set of values (if there are multiple values), then a reference to **Codelist** shall be provided within the Functional Description instead of specific distinct values.

*Example: the value of the **<Applied Element>** must be in **SET** CL999 (Codelist name)*

Guidelines consist usually of a simple textual description but can be formulated with the IF THEN ELSE syntax if this is considered necessary.

IV.5.1.3 Technical Rules for Transition and Business Rules for Transition

TRTs and BRTs are defined in Table 2. All TRTs and BRTs should be formulated with the IF THEN syntax. The antecedent part (IF-part) evaluates:

- the decisive date as defined in the corresponding DDNA volumes for BRTs

- the current date for TRTs

against the date of the end of the Transitional Period.

The consequent part of (THEN-part) defines the XPath where the BRT/TRT is applicable and the corresponding rule that must be enforced (applied by sender and validated by the recipient), regarding the format, optionality, multiplicity and R/C applicability.

Pointers to data groups/items in Functional Description of BRTs/TRTs shall be in the form of **XPath**.

Example:
//Consignment/HouseConsignment/ConsignmentItem/Commodity/descriptionOfGoods*

IV.6 Logic of Rules/T/TRT/BRT and Conditions validation sequence for NCTS-P5 and AES-P1

In some cases, specific sequence of R/C/T/TRTs/BRTs validation for a specific Data Item/Data Group is necessary to avoid conflicts. In such cases, a Sequencing Rule ('S') is defined and assigned to the specific Data Item/Data Group specifying the sequence of R/C/T/TRT/BRT validation execution. **Only one Sequencing Rule is allowed per Data Item or per Data Group.**

An example of a Sequencing Rule is the following: *S1018: The validation of particular Data Group/Item shall be performed in the following sequence: C0215 > C0315*

In case a Sequencing Rule is not applied and the validation concerns a message with a Message Submission Date within the Transitional Period, by default the BRT and subsequently TRT validation shall be performed first and then the validation of any other Conditions, Rules and Technical Rules shall take place (if the sequence has no impact on the validation).

The recommended sequence of validation for any validation that does not involve an 'S' and regardless the period that this is performed is the following: Format Validation (XSD) → Codelist Validation → BRTs/TRTs Validation → Conditions Validation → Rules Validation → Technical Rules Validation.

If a Sequencing Rule exists, then the textual description of the Sxxxx must contain only the conflicting R/C/T/TRT/BRT applicable to the specific DI/DG to unambitiously define the sequence of validation.

The above logic is reflected in Figure 10.

Validation should be performed, reporting at least the first error found and as many errors as possible that can be reported as well.
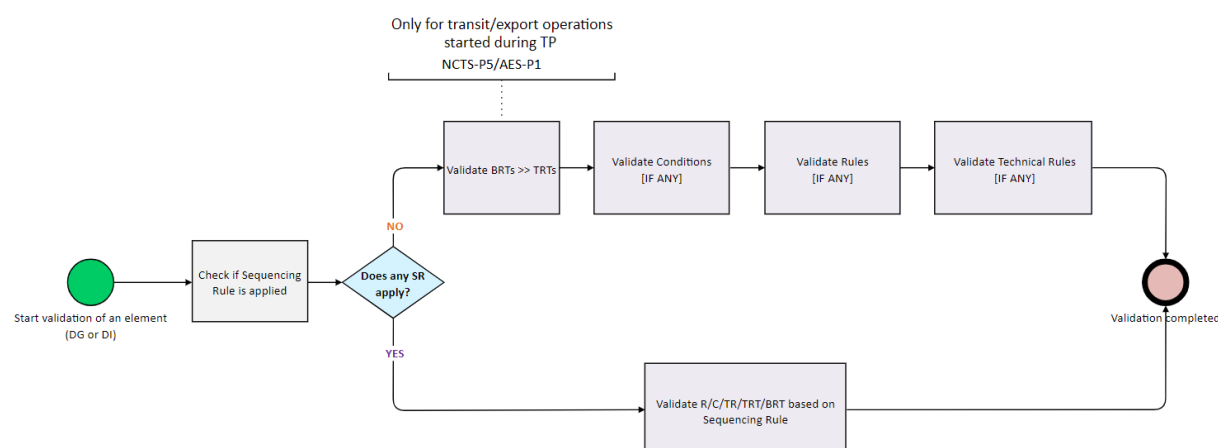
Figure 10: Logic of validations sequence in NCTS-P5 and AES-P1

IV.7 DDNA consistency for NCTS-P4, ECS-P2 and ICS-P1

The Information Exchanges for the movement systems are aligned with the Single Administrative Message (SAM) Mapping Guide. As the SAM Mapping Guide covers import and export, and needs to cover each Customs system, changes have been made to Information Exchanges in some cases where more detail needed to be added.

The details of all changes between the DDNA TMS and the SAM and/or [R26], [R13] and [R14] are included in the corresponding Appendix Q.

Since these appendices define the detailed list of the Technical Message Structures, they start by first explaining the deviations from the FSS ([R26], [R13] and [R14]) and the SAM Mapping Guide.

As a general overview the major changes between DDNA TMS and FSS FMS and SAM are:

- Changes in the naming conventions – some names have been changed between DDNA and FSS ([R26], [R13] and [R14]);

- Expansion of Information Exchanges inside other Information Exchanges – FSS ([R26], [R13] and [R14]) presents some messages inside messages. In DDNA, the content of the sub-messages has been put in the master-message;

- Message group – this data-group is added in every message;

- Implementation of FMS conditions and rules;

- Technical Rules and Conditions.

IV.8 DDNA consistency for NCTS-P5 and AES-P1

The Information Exchanges for the movement systems are aligned with the UCC Data Annex B and EUCDM. Any deviations will be justified. The details of all changes between the DDNA TMS and [R28], [R29] are included in the corresponding Appendix Q.

Since these appendices define the detailed list of the Technical Message Structures, they start by first explaining the deviations from the FSS ([R28], [R29]).

As a general overview the major changes between DDNA TMS and FSS FMS are:

- Changes in the naming conventions – some names have been changed between DDNA and FSS ([R28], [R29]);

- Message group – this data-group is added in every message;

- Technical Rules and Conditions;

- **Technical Rules for Transition** and **Business Rules for Transition** will be added as structural changes to enable the conversion process and ensure backwards compatibility of the CC movements created before the end of the TP. Please refer to section IV.4.

V Design principles

V.1 Approach

Every Information Exchange needs to be in a structure that conforms to this document (TMS). The TMS needs to be formatted in either EDIFACT or XML format, as specified within this document in EDIFACT message formatting (VI) and XML message formatting (VII).

The formatted message needs to be transported across CCN/CSI or across the Inter(Extra)net according to the rules laid out in Transport of messages via CCN/CSI and Transport of messages via the Inter(extra)net.

This applies only to the mandatory exchanges. For the (strongly) recommended exchanges, it is highly advised to use similar conventions and rules.

Because Information Exchanges are used to update data of Customs operations held by different applications the data needs to be uniquely identifiable. Not all data is uniquely identifiable. Therefore, the following rules are applied to updates of operation data:

- Key fields:
  - o The MRN is a key to the Customs operation. It is unique and refers to a specific Customs system movement. Each goods item is uniquely identified by its goods item number within an MRN:
    - If information regarding an MRN needs to be changed, the MRN identifies the operation;
    - If information regarding a particular goods item needs to be changed, the goods item number of that particular goods item is exchanged, together with the changed information;
  - o The GRN is a key to uniquely identify the Guarantee Information in Transit;

- Non-key fields: That information that is not uniquely identifiable (e.g. with an MRN or goods item number) is completely exchanged and replaces the information that has already been exchanged. For instance, if a new goods item needs to replace an existing goods item, the existing goods item number with the new information replaces the previously exchanged information of that goods item.

V.2 Character Sets and Data Item conventions

Every NA may maintain locally different character set(s) and Data Item conventions. These have usually been selected in order to best fit the NA's business needs. Customs systems do not impose any standards concerning national usage of character sets or Data Item conventions. However, they impose some standards for the Data Items and the character sets when information is exchanged in the Common Domain.

About XML Character Set Support, please refer to chapter VII.1.2.

If the standards used for the exchanges in National Domain, differ with those used in Common Domain, then every NA should foresee character set conversion and Data Item conversion.
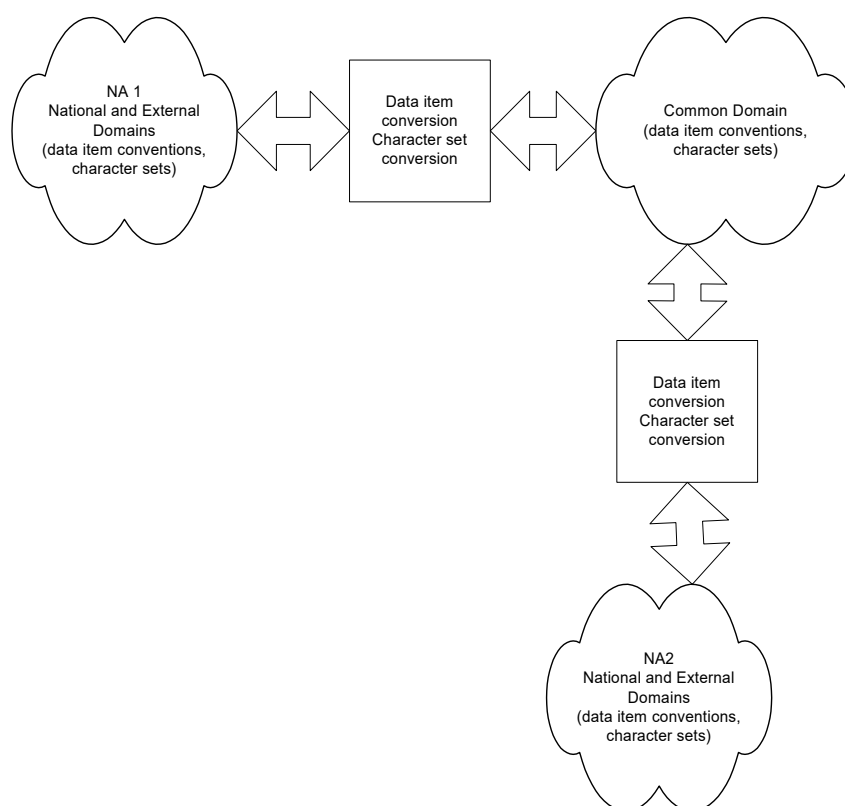
Figure 11: Character sets and conventions in use

The Common Domain standards are given below. Recommendations for National and External Domain exchanges are given next.

V.2.1 *Common Domain exchanges*

V.2.1.1 Data Item conventions

Every Data Item within a TMS will be either a numerical field or a text field. A number of rules and conventions have been defined for the possible data formats when present in the Common Domain. These rules are the same for data exchanged in EDIFACT format and in XML format.

V.2.1.1.1 *Numerical fields*

Concerning numerical fields, it should be noted that these are either a cardinal value (positive integer value) or a decimal value[16], unless otherwise specified by a Codelist or rule applied to the numerical field.

The decimal separator is the decimal point ".". No other symbols are permitted as decimal separator.

Triad separators, such as a comma, shall not be used.

Signs, whether positive or negative, shall not be used (all values are intrinsically positive).

For decimal values, the decimal notation (with the decimal point) should only be used when there is a reason to indicate precision.

E.g., for a mass value:

- 89 kg, with a precision of 1 kg;
- 89.2 kg, with a precision of 0.1 kg;
- 89.20 kg, with a precision of 0.01 kg.

For numerical values, leading zeroes shall not be used[17]. Trailing zeroes should only be used to indicate precision.

If the decimal point is present, at least one digit shall be present before the decimal point.

If the decimal point is present, at least one digit shall be present after the decimal point.

---

[16] The numeric value zero (0) is not considered as positive integer or as positive decimal value. The only exception is time numerical fields where the numeric value zero (0) may be used.

[17] The only exception is time numerical fields where leading zeros may be used.

Examples for a n..11,3 type.

- 12345678.123   Valid
- 123456789.123   Invalid – too many digits before decimal point and too many digits in total
- 12345678.1234   Invalid – too many digits after decimal point and too many digits in total
- 0123   Invalid – leading zero not permitted
- +123   Invalid – plus sign not allowed
- -123   Invalid – minus sign not allowed
- 1,234   Invalid – triad separator not allowed
- .3   Invalid – no digit before decimal point
- 12345.   Invalid – no digit after decimal point
- 0.3   Valid
- 1.3E1   Invalid – only digits and decimal point allowed
- 12345678901   Valid – n..11,3 can have maximally 11 digits of which maximally 3 after decimal point

It is to be noted that the rules above also apply to numerical values within Codelists. Codelist values must be kept according to the format definition in CS/RD2:

- For numeric format Codelists the leading zero(s) are removed;

- For alphanumeric format Codelists the leading and/or trailing zero(s) are kept.

If the leading zeroes are indeed omitted a comparison should always work, regardless of whether the comparison was done on a numerical or character basis.

Code lists format is defined in the XSDs used for the validation of generic XML as specified in Annex 9 of DDRDA [R27].

V.2.1.1.2 Text fields

Leading and trailing spaces (both normal spaces and non-breaking spaces) shall not be used within text fields.

The EDIFACT separator characters (see EDIFACT message formatting) can be used within such a field. The EDIFACT release character (?) can be used to include the separator characters in fields.

For XML, certain characters cannot be used in its content because they have special meaning. Adding control characters ('<', '>' etc) into XML data could cause the parser to misunderstand the resulting data. The solution (see [S4]) is to escape the control characters so that the parser can interpret them correctly as data, and not confuse them for markup. These characters have to be escaped with the following predefined entities. To use one of the characters listed below, substitute it with the appropriate string.

Character	Entity
& (ampersand)	**Must be** escaped to &
> (greater-than character)	Should be escaped to >
< (less-than character)	**Must be** escaped to <
" (straight quotation mark)	Should be escaped to "
' (single straight quotation mark)	Should be escaped to '

Table 23: characters to be escaped with predefined entities

Note: Only the characters "<" and "&" are strictly illegal in XML. The greater than character is legal, but it is a good practice all the characters mentioned in the above table to be replaced. To avoid any confusion, it's recommended that all the above characters are escaped when they appear in the exchanged XML instances. Furthermore, although the use of line feeds is legal, it is strongly recommended not to be inserted in the data.

The application must evaluate the length of the string by counting each escaped character as 1 character (i.e. "&" is 1 and not 5 characters). If the format of a data item is an..100, the following value is valid:

"This string of 100 'characters' must be <always> valid & not rejected, also with format "an..100" !"

Moreover, text fields shall be case sensitive (i.e. text fields with letter(s) as uppercase and text fields with same letter(s) as lowercase shall be considered as different).

V.2.1.1.3 Date/Time Fields (NCTS-P5 and AES-P1)

The specification of Date and/or Time fields used in TMS (Technical Message Structure and Appendix Q2 of system-specific DDNA) is based on W3C XML Schema specification [S18] except that:

- all years in DateTime and Date fields are in the Common Era (i.e. AD), hence the negative sign is not permitted;

- for all times in DateTime fields the time zone must be omitted. For the Common Domain messages, the time in all DateTime fields must be the UTC time. The local time can be used for the External Domain messages, but the NCA must convert the local time into the UTC time before sending the message over the CCN. It is recommended that the recipient also store the DateTime fields in UTC (even if displayed for the NCA's end user in local time);

- the fractional seconds must not be used in DateTime fields.

Based on the W3C XML Schema specification [S19] (Part2: Datatypes) and ISO 8601 Date and Time format [S20], the following table (Table 24) defines the format for each type and their corresponding regular expression , as it is applicable for NCTS-P5 and AES-P1.

It is worth noting that during the Transitional Period, no conversion of DateTime and Time fields to UTC time will be performed by the ieCA.

The NA in TO-BE phase will:

- send Common Domain messages with UTC time in all DateTime and Time fields.

- receive Common Domain messages with UTC or local time in all DateTime and Time fields.

Type	Regular Expression
Date	YYYY '-' MM '-' DD \d{4}-\d{2}-\d{2}
Time	hh ':' mm ':' ss \d{2}:\d{2}:\d{2}
Date/Time	YYYY '-' MM '-' DD 'T' hh ':' mm ':' ss \d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}

Table 24: Date/Time fields format and their corresponding regular expressions

Where:

- YYYY is four digit;

- the remaining '-'s are separators between parts of the date portion;

- MM is a two-digit numeral that represents the month;

- DD is a two-digit numeral that represents the day;

- 'T' is a separator indicating that time-of-day follows;

- hh is a two-digit numeral that represents the hour;

- ':' is a separator between parts of the time-of-day portion;

- mm is a two-digit numeral that represents the minute;

- ss is a two-integer-digit numeral that represents the seconds, while leap seconds are not allowed.

It should be noted that, all characters used in date and time expressions and representations are part of the ISO/IEC 646 repertoire, except for "hyphen", "minus" and "plus-minus". In an environment where a character repertoire based on ISO/IEC 646 is used, "hyphen" and "minus" should be both mapped onto "hyphen-minus".

Based on the above, the following XSD Types will be associated with data elements per case:

XSD restriction for Data Items of type *Date (DateType)* as per Table 24:

```xml
<xs:simpleType name="DateType">
            <xs:annotation>
                    <xs:documentation>Calendar dates are represented YYYY-MM-DD
format, following ISO 8601. This is a W3C XML Schema date type, but without the
optional timezone data.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:date">
                    <xs:pattern value="\d{4}-\d{2}-\d{2}(\.\d+)?" />
            </xs:restriction>
</xs:simpleType>
```

Table 25: XSD restriction for Data Items of type Date (*DateType*)

XSD restriction for Data Items of type *Time (TimeType)* as per Table 24:

```xml
<xs:simpleType name="TimeType">
            <xs:annotation>
                    <xs:documentation>The Coordinated Universal Time (UTC). The
UTC time is defined without offsets. UTC is used to avoid confusion about time
zones and daylight saving time. Local time maybe used for the External Domain
messages (not recommended) and must be converted in UTC before sending this
information on the Common Domain.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:time">
                    <xs:pattern value="\d{2}:\d{2}:\d{2}(\.\d+)?" />
            </xs:restriction>
</xs:simpleType>
```

Table 26: XSD restriction for Data Items of type Time *(TimeType)*

XSD restriction for Data Items of type *Date/Time (DateTimeType)* as per Table 24:

```xml
<xs:simpleType name="DateTimeType">
            <xs:annotation>
                    <xs:documentation>DATE: The date is in the Common Era (minus
sign in years is not permitted). TIME: The Coordinated Universal Time (UTC). The
UTC time is defined without offsets. UTC is used to avoid confusion about time
zones and daylight saving time. Local time maybe used for the External Domain
messages (not recommended) and must be converted in UTC before sending this
information on the Common Domain.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:dateTime">
              <xs:pattern value="\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}(\.\d+)?" />
            </xs:restriction>
</xs:simpleType>
```

Table 27: XSD restriction for Data Items of type Date/Time (*DateTimeType*)

V.2.1.2   Character set usage

A distinction should be made for the character sets when messages are transported. Indeed EDIFACT only supports byte based character sets, while XML supports Unicode.

V.2.1.2.1 Exchanges in EDIFACT format (for NCTS-P4, ECS-P2, NCTS-P5 and AES-P1)

Text fields can be either language-sensitive (with an associated LNG field) or not. There are some specific rules for both described below.

V.2.1.2.1.1 Language-sensitive text fields

These fields can be in any of the following character sets taken from EDIFACT syntax version 3 for EDIFACT message exchanges in the Common Domain:

- UNOC: Latin-1, ISO 8859-1;
- UNOD: Latin-2, ISO 8859-2 (Central Europe);
- UNOG: Latin-3, ISO 8859-3;
- UNOH: Latin-4, ISO 8859-4;
- UNOE: Latin-5, ISO 8859-5;
- UNOF: Greek, ISO 8859-7;
- UNOK: Turkish, ISO 8859-9.

V.2.1.2.1.2 Non-language sensitive text fields

Only ASCII printable characters (characters #32 to #126 decimal) can be used for these fields, unless otherwise specified by a Codelist or rule applied to the text field.

V.2.1.2.2 Exchanges in XML format

Messages exchanged in XML format shall use the UTF-8 encoding of UNICODE both for language sensitive fields and for non-language sensitive fields when these are present. The concept of language sensitive fields and for non-language sensitive fields in XML messages is present only in ICS.

However, during NCTS-P4, ECS-P2, and the Transitional Period of NCTS-P5[18] and AES-P1[18], it should be possible to map all the characters of any one language-sensitive field to a single character set to be chosen between UNOC, UNOD, UNOG, UNOH, UNOE, UNOF and UNOK unless otherwise specified by a Codelist or rule applied to the text field. Failure to comply with this statement would make it impossible to properly translate the message to EDIFACT.

---

[18] In case of Common Domain exchanges between NCA during the transitional phase of NCTS-P5/AES-P1 and NCA in NCTS-P4/ECS-P2

V.2.1.3   Transliteration for language–sensitive text fields

The associated LNG indicator, if present, denotes the language in which the original text was written. From this, the character set used can be derived.

If the LNG field is not present, the character set can be derived from the first characters of the original text. Transliteration can then be done, if necessary, from one character set to the other.

If more than one character set is used in a same free text field, the first identified character set will be used for the transliteration ignoring the other character sets.

It is therefore recommended to use only one character set per free text field.

Every NA should therefore have the capabilities to receive data in any of the character sets above and transliterate them into the character set(s) that is (are) in local use at the NA. Every NA should be capable of transliterating the character set(s) that is (are) in local usage at the NA into one of the character sets specified above.

The NA is expected to establish additional rules on language and character set usage in a later stage. These should clarify which languages and character sets are in local use at the NA and how the character sets can be derived from the language codes.

V.2.2   National and External Domain exchanges

It is highly recommended to use the standards, defined above, to the maximum possible extent in the National and External Domains.

V.3 Exception Handling

V.3.1 Introduction

"Exception" is the generic term used to refer to any behaviour of one or more system components of a movement system that is not in accordance with the specification given in DDNA.

On detecting an exception, an NCA must notify another NCA of that error. There are three possible error notification mechanisms:

- Functional errors: a message is not filled according to its TMS (e.g. a required Data Group is missing, or a Data Item violates a Code List) or is violating the State Transition Diagrams defined in DDNA Main Document (e.g. out of sequence message, only applicable if it can not be responded with one of the 'negative response' messages defined in the DDNA Main Document):

  o A Functional NACK (IE906: C_FUN_NCK) that is sent by the National Application detecting the error to the National Application that has sent the erroneous functional message across the Common Domain;

  o Specific error messages are sent in the External Domain and are identified in each specific DDNA volume.

- Format errors:

  o EDIFACT errors: a EDIFACT interchange and its EDIFACT message(s) is not filled according to its specification given in Design principles:

    ▪ An EDIFACT NACK (IE907: CONTRL) is sent by the National Application detecting the error to the National Application that has sent the erroneous interchange;

  o XML errors: an XML message is not filled according to the XSD included in the Appendix X of the DDNA volume. :

    ▪ An XML NACK (IE917) is sent by the National Application detecting the error to the National Application that has sent the erroneous message;

- Communication errors: some error occurs during the exchange of a CCN/CSI message across the Common Domain:

  o The interface software with CSI needs to handle various errors and the Confirm On Arrival and Confirm On Delivery options of the Quality of Service are set to ensure delivery by CCN to a receiving National Application (see also Transport of messages via CCN/CSI).

Section IX of FTSS [R26] specifies exception handling in detail for EDIFACT exchanges. This section specifies the possible error types and codes and the way they are exchanged in the Functional NACK, the Declaration Rejected and the EDIFACT NACK.

This section only covers exceptions regarding the exchange of EDIFACT or XML messages and their functional message structure.

More information regarding the automatic duplication of the error messages (Functional NACK, EDIFACT NACK and XML NACK) to CS/MIS is available in section II.2.5.

V.3.1.1 Architectural assumptions

The mechanisms specified in this section are based on the following assumptions:

1. Fallback and recovery procedures are outside the scope of DDNA. In principle, every action related to Information Exchanges needs to be logged to allow recovery and identification of a failed component.

2. There is a layered approach to error detection upon reception of information. It consists of the following three layers:
    - CCN/CSI layer: communication errors are handled by CCN/CSI software (see also Transport of messages via CCN/CSI);
    - Message formatting (EDIFACT or XML) layer: syntax errors are detected in addition to the ones detected by CCN/CSI;
    - Functional layer: Functional errors are detected on top of those detected by the message formatting (EDIFACT or XML) and CCN/CSI layers.

    Security functions in the Common Domain are offered by CCN/CSI. Security functions in the External Domain have to be specified by each NA.

3. EDIFACT is used as specified in EDIFACT message formatting, paragraph VI.2.1, e.g. one CSI message contains one EDIFACT interchange with one EDIFACT message.

4. XML is used as specified in XML message formatting e.g. one CSI message contains one XML message.

5. The FMS is the basis for identifying Functional errors. Although the FMS as such may not be implemented in National Applications, it is assumed that Data Group sequencing of sender and recipient is identical. Sequencing provides an easy mechanism for an error pointer.

V.3.1.2 Examples of error causes

The following error causes have been identified:

Error cause	Description
Failure of components	A distinction is made between three types of failures: • Failure of an application; • Failure of the network; • Failure of the link between an application and the network. Failures will cause errors in message sequencing; e.g. one of the applications involved did not receive a message and has not been able to produce the proper answer. This may cause applications to be out of sync.
Software bug	A function of a receiving or sending application does not reach its proper state because a required function is missing, incomplete or incorrect. Errors may be detected in another function; e.g. the recipient of a message may detect errors. For example, a software bug can cause the production of a message of an incorrect type (message sequencing) and/or the incorrect content of a message. The sending application is then likely to be out of sync with the receiving application.
Human mistake	A mistake is a wrong action due to incorrect human intervention; e.g. another MRN is selected than was intended. A human mistake can cause incorrect contents of a message and incorrect sequencing of a message.
Incorrect Code List	Improper Code Lists are used by a sending or receiving application, e.g. a sender uses an outdated Code List when preparing a message or a recipient does the same when verifying the data of a received message. An incorrect Code List will produce incorrect contents of a message.

Table 28: Error causes

V.3.2 Scenarios for exception handling

V.3.2.1 General procedure

In general, all errors must be logged upon their detection. Depending on their circumstances, one of the following scenarios has to be initiated:

- Exchange of Functional errors;

- Exchange of EDIFACT errors or exchange of XML errors.

In order to avoid entering an endless looping, the following applies:

- The IE906 will not be rejected with a message IE906, it can be rejected with an IE907 or IE917;

- The IE907 will never be rejected, neither with a message IE906 nor with an IE907;

- The IE917 will never be rejected, neither with a message IE906 nor with an IE917.

Each of those exceptional cases will be rapidly analysed by the involved National Customs Helpdesks.

Errors regarding the use of CCN are discussed in Section VIII: Transport of messages via CCN/CSI.

V.3.2.1.1 Functional errors

Every Information Exchange exchanged across the Common Domain can contain Functional errors, e.g. a required Data Item is missing or has a value that is not allowed or a Data Item is not allowed to have a value due to a rule specified by DDNA ([R28], [R29], [R16], [R17] and [R18]). The possible values of these errors are specified in Codelist CL049 (CD906A and CD906B) and in Codelist CL180 (CD906C).

Figure 12 shows an example of a Functional error in NCTS-P4 and relates to the reception of an AAR by the Office of Destination.
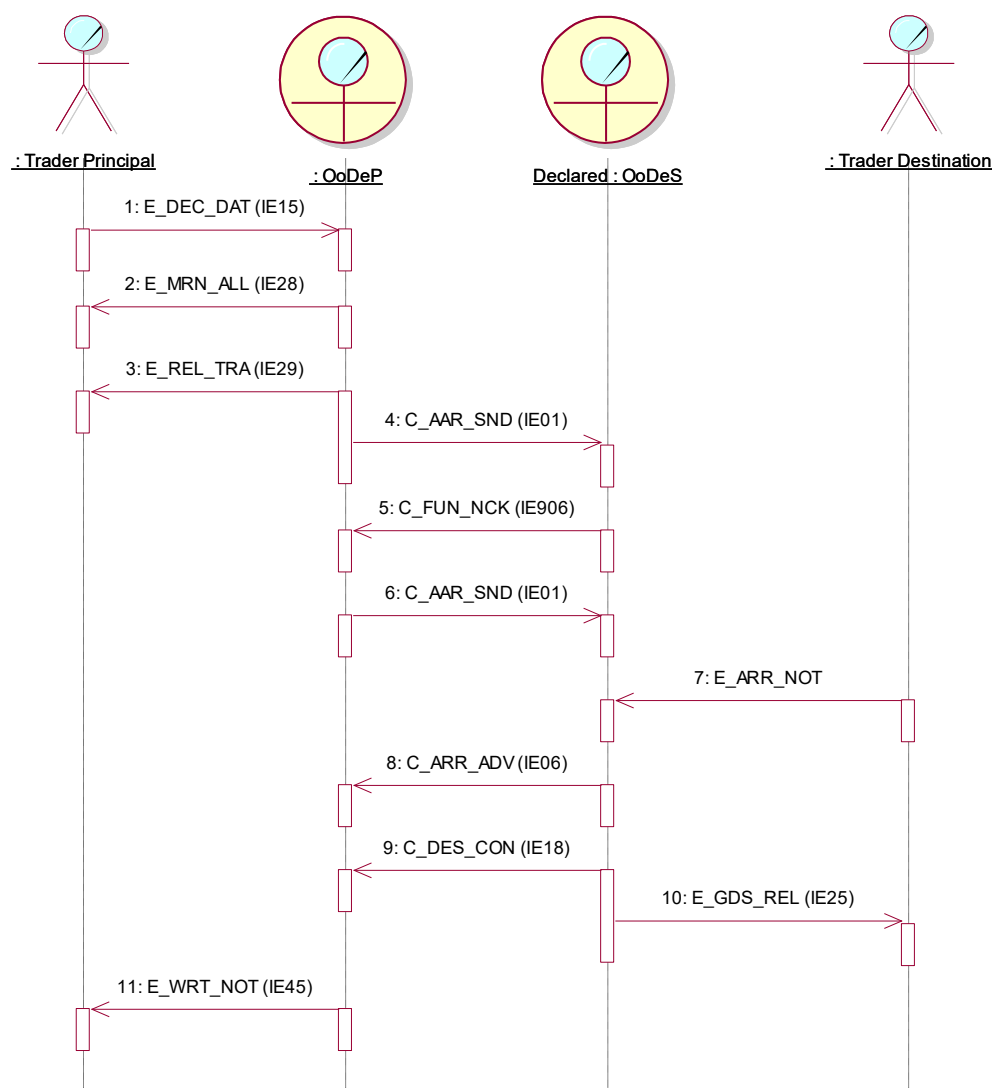
Figure 12: Functional error across the Common Domain (NCTS)

This figure shows the detection of an AAR with a Functional error. It causes a rejection of that AAR by the Office of Destination with a C_FUN_NCK. The correct AAR is sent after correction of the application by the Country of Destination or Departure, or the manual correction of the declaration message.

The CD906A Functional error (V.4) shall be used in NCTS-P4, ECS-P2 and the CD906B Functional error (V.4) in ICS-P1.

The CD906C Functional error (V.5) shall be used in NCTS-P5 (V.3.2.1.4) - (V.3.2.1.5) and AES-P1 (V.3.2.1.4) – (V.3.2.1.5).

With respect to EDIFACT exchanges, if messages are resent after correction of an error, the interchange in which they are resent requires a new interchange reference in the UNB segment (otherwise, a duplicate will be detected by an EDIFACT translator and a CONTRL with error code '26' is exchanged). A message is only unique in the context of an MRN and messages with the same reference in the UNH segment can be received (see EDIFACT message formatting). As the message has not yet been processed by the receiving application, the latter will not detect a duplicate.

It is not permitted to re-send a message other than after correction of the error(s) that caused the previous rejection.

V.3.2.1.2 EDIFACT errors

Every interchange exchanged across the Common Domain can contain EDIFACT errors, e.g. a missing segment or use of a syntax version that is not allowed. Figure 13 shows the exchange of an EDIFACT CONTRL message after detection of an error in an interchange. The original interchange and message within the interchange are referred to in the CONTRL. The possible values of these errors are maintained in CS/RD2 and specified in the Codelist CL023 applicable to the corresponding Customs Systems.
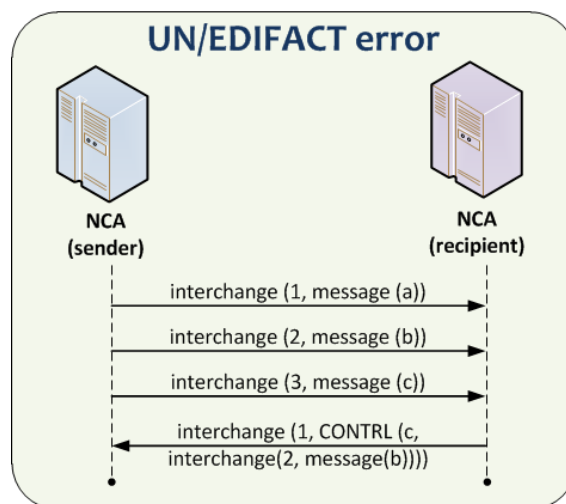
Figure 13: EDIFACT error

Figure 13 shows the exchange of an error detected in the interchange with reference '2' and message with reference 'b'. As this figure shows, the recipient returns an interchange with reference '1' containing a CONTRL message that refers to the original interchange in which the error has been detected.

This use of reference numbers of interchanges and messages is arbitrary, as long as an interchange reference is unique between a sender/recipient pair and a message reference is unique within a Movement identified with its unique MRN (Design principles).

A CONTRL message carries its own interchange and message reference, in the figure '1' and 'c' respectively. The reference to the interchange and message in which an error has been detected is exchanged in the UCI and UCM segments respectively (EDIFACT message formatting).

Figure 13 only shows a sending and receiving role of an organisation whereas an organisation can have both roles at the same time. Therefore, this figure is a simplification of the actual communication between two organisations.

V.3.2.1.3 XML error

The XML error message (IE917: C_XML_NCK) shall be used to report XML format and structure errors.

Every interchange exchanged across the Common/External Domain can contain XML validation errors, e.g. a missing mandatory data item or use of a message version of XML that is not allowed. Figure 14 shows the exchange of a XML CONTRL error message after detection of an error in an XML interchange. The original interchange and message within the interchange are referred to in the XML CONTRL. The reporting of XML errors using the XML NACK is specified in XML error (CONTRL) message.
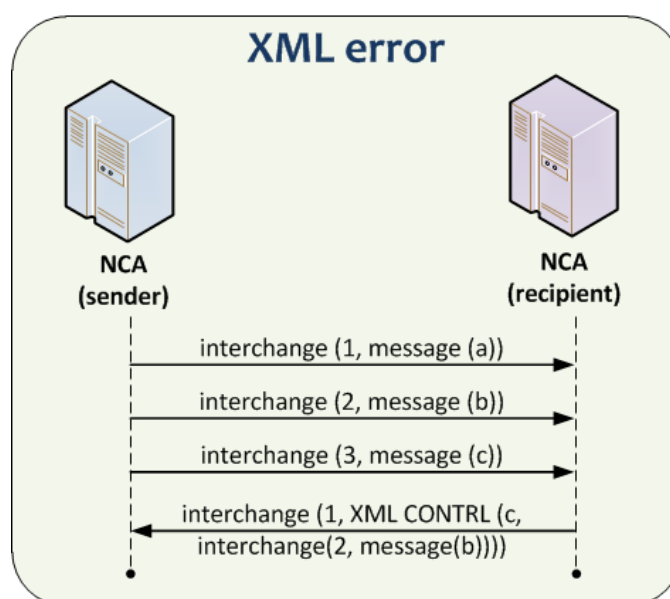
Figure 14: XML Control error

Figure 14 shows the exchange of an error detected in the interchange with reference '2' and message with reference 'b'. As this figure shows, the recipient returns an interchange with reference '1' containing a XML CONTRL message that refers to the original interchange in which the error has been detected.

The "Message identification" must be a unique identifier between sender/recipient. The response will not re-use the 'Message identification' of the request (ensured by duplicate detection using code '26' of the code list CL180 in CD906C).

A CONTRL message carries its own interchange and message reference, in the figure '1' and 'c' respectively. The reference to the interchange and message, in which an error has been detected, is exchanged in the Header of the Message respectively.

Moreover, Figure 14 shows only a sending and receiving role of an organisation, whereas an organisation can have both roles at the same time. Therefore, this figure is a simplification of the actual communication between two organisations.

Finally, if messages are resent after correction of an error, the interchange in which they are resent requires a new interchange reference (Message Identification) in the Message Level. A message is only unique in the context of an MRN and interchange. As the message has not yet been processed by the receiving application, that latter application will not detect a duplicate. It is recommended to re-send a message only after the correction of the error(s) that caused its rejection.

For ICS domain, the XML error codes are defined in tcl_ics.xsd and maintained in CS/RD2.

For NCTS-P5 and AES-P1 domains, the XML error codes are defined and maintained in CS/RD2.

V.3.2.1.4 Exception handling after the Transitional Period of "To Be" for NCTS-P5 and AES-P1

The exception handling for NCTS-P5 and AES-P1 operations started after Transitional Period is defined below.

The NCA shall respond per level of error as follows:

- Functional errors should be reported as specified in (V.3.2.1.1) using CD906C (V.5)

- XML error should be reported as specified in (V.3.2.1.3) using CD917C (VII.5) and with Error Codes (Codelist CL030) applicable to NCTS-P5 and AES-P1.

V.3.2.1.5 Exception handling during the Transitional Period of NCTS-P5 and AES-P1

IMPORTANT

READ ALSO the section 3 (ieCA Exception Handling Use Cases) of the document **ieCA Use Cases** [R42] that complements this version of the DDCOM.

The exception handling for NCTS-P5 and AES-P1 operations during Transitional Period is defined in the next sections.

The Common domain exchange patterns and the respective Common Domain policy are defined in Section IV of pertinent DDNXA for AES-P1 [R40] and DDNTA for NCTS-P5 [R41] during the Transitional Period of NCTS-P5 and AES-P1.

Table 29 defines exception handling per CD exchange pattern (please refer to column "Applicable Exception Handling"):

Pattern	Group	Sending NA operational mode	Receiving NA operational mode	Applicable Exception Handling
1	CD exchanges between NAs in "Legacy"	"Legacy"	"Legacy"	Exception Handling of "Legacy" protocol (ECS-P2/NCTS-P4)
2	CD exchanges between NA in "Legacy" and NA "To Be"	"Legacy"	"To Be"	Exception Handling of "Legacy" protocol and as elaborated in section V.3.2.1.5.1 in case conversion is involved.
3		"To Be"	"Legacy"	
4	CD exchanges between NAs in "To Be"	"To Be" (sending in "To Be" Interface)	"To Be"	Exception Handling of "To Be" protocol and as mentioned in section V.3.2.1.5.2
5		"To Be" (sending in "Legacy" Interface)[19]	"To Be"	Exception Handling of "Legacy" protocol and as elaborated in section V.3.2.1.5.1 in case conversion is performed by Receiving NA.

Only cases "Upgrade of message" are applicable as per sections V.3.2.1.5.1.2 and V.3.2.1.5.1.4. |

Table 29: Common Domain exchanges patterns during TP

---

[19] If IE is produced from "Legacy" system of NA, then it is highly strongly recommended to use the native format ("Legacy" interface) to minimize conversion needs.

V.3.2.1.5.1 Exception handling for CD exchanges between NA in "Legacy" [NCTS-P4/ECS-P2] and NA "To Be" [NCTS-P5/AES-P1] – CD Exchange pattern#2 and 3

The exception handling for <u>Common Domain exchanges</u> between NA "To Be" and NA "Legacy" shall be performed as per "legacy" protocol, i.e.:

- Functional errors should be reported as specified in (V.3.2.1.1) using CD906A (V.5);

- EDIFACT (TMS) error should be reported as specified in (V.3.2.1.2) using CD907A.

However, a distinction shall be made at this point for exception handling depending on whether conversion is used by NA:

Type A. NA "To Be" requiring to employ conversion of messages for Common Domain exchanges;

Type B. NA "To Be" without the need of conversion of messages for Common Domain exchanges with "Legacy" NA and being able to submit and receive Functional errors and EDIFACT errors with exact error codes, error pointers and error reasons as operating in "legacy".

For **NA "To Be" of type A**, the following challenges shall be considered and especially when the errors are found in the **"converted"** message:

1. NCTS-P4/ECS-P2 supports EDIFACT message while NCTS-P5/AES-P1 XML messages;

2. Error pointers are different from NCTS-P4/ECS-P2 phases to NCTS-P5/AES-P1 phases;

3. Different error codes between NCTS-P5/AES-P1 and NCTS-P4/ECS-P2;

4. Error is identified by the receiving application in a processed/converted message and not into original received;

5. Error does not always imply error in the original received message. It might concern the converted message and therefore must be investigated under incident management:

    o Error in the original message;

    o Conversion/data mapping problem;

    o Erroneous implementation of R/C/TRT/BRT or Technical Rule.

✓ The exception handling for NA "To Be" of **type A** <u>using the TAXUD ieCA convertor</u> must be in accordance with the principles for Common Domain exchanges defined in Table 29:

- If error found on **originally submitted message (before conversion)**, NA "To Be" of **type A** <u>using the TAXUD ieCA</u> shall respond with Functional error (CD906A) message and EDIFACT CONTRL message (CD907A) having **specific error reporting** (error code/type, error pointer/location and error location) as per "Legacy" NCTS-P4/ECS-P2 principles.

- If error found **on converted message**, NA "To Be" of **type A** <u>using the TAXUD ieCA</u> shall:

  o respond with Functional error (CD906A) having **generic error reporting** (error code/type, error pointer/location and error location) in case errors found on an "Upgraded" message. The Functional error (CD906A) shall be in alignment with "Legacy" NCTS-P4/ECS-P2 principles as described in Upgrade scenarios (V.3.2.1.5.1.2).

  The NA "To Be" of **type A** <u>using the TAXUD ieCA</u> will support Functional error (CD906C)/XML CONTRL messages (CD917C) for "To Be" (see V.3.2.1.5.2). Therefore, a "conversion" of Functional error (CD906C)/ XML CONTRL messages (CD917C) from one phase to another is necessary since different approaches are followed between "To Be" and "Legacy". Consequently, as mentioned above, the **generic error reporting** (error code/type, error pointer/location and error location) shall be used during the Transitional Period of NCTS-P5 and AES-P1 and for the "conversion" of Functional error (CD906C)/ XML CONTRL messages (CD917C) from "To Be" to "Legacy" approach and depending on the error at different levels (Table 30):

Validation Error	Error Message from NA "To Be"	Convertor	Error Message sent to NA "Legacy"
XML Validation Errors	**CD917C** *Specific Error Reporting*	➡	**CD906A** *Error type: 14* *Error pointer:* Root Element *Error Reason:* NCAvC
Business Validation Errors	**CD906C** *Specific Error Reporting*	➡	**CD906A** *Error type: 15* *Error pointer:* Root Element *Error Reason:* NCAvC

Table 30: Conversion of error messages in case of errors other than 90, 92 or 93 on an "Upgraded" message (received from NA "Legacy")

Table 30 error messages might also be sent from the <u>TAXUD ieCA</u> during output format XML validation or Business Validation Errors (BRT, TRT, Rules & Conditions and Codelists for "To Be") of converted "Upgraded" message prior submission to NA "To Be".

In this case, the ieCA will send to the receiving NA ("To-Be"):
- the post-conversion message (i.e. the "To-Be" IE in this case), for example the (erroneous) IE501C that is the result of the upgrade by the TAXUD ieCA of an IE501B;
- the *Error Details Report* in which the detected error will be depicted to inform the NA "To-Be" about the error to be investigated. This *Error*

Details Report will contain a CD917C or a CD906C error message generated by ieCA, depending on the type of error detected;

- the CD906A Error Message (see Table 30) produced by ieCA by downgrading the *Error Details Report* (that could be sent by the "To Be" NA to the "Legacy" NA where it would be readable).

The NA "To-Be" will be responsible to perform the format and business validation of the post-conversion message and depending on the result:

- either accept it and continue the movement flow (on successful validation) or
- produce the CD917C or CD906C (depending on which validation failed) and send it to TAXUD ieCA for downgrade in order to be sent to NA "Legacy".

The figure below (Figure 15) illustrates the above case:

Figure 15: Handling of errors (other than 90, 92 or 93) following Upgrade of message with NA "To Be" of type A using the validation results from TAXUD ieCA

o process the received Functional error (CD906A)/EDIFACT CONTRL message (CD907A) from NA "Legacy" in case errors found on a submitted "Downgraded" message. The Functional error (CD906A)/EDIFACT CONTRL message (CD907A) shall be in alignment with the "Legacy" principles as described in Downgrade scenarios (V.3.2.1.5.1.1).

The NA "To Be" using the TAXUD ieCA will support Functional error (CD906C) for "To Be" (see V.3.2.1.5.2). Therefore, a "conversion" of received Functional error (CD906A)/EDIFACT CONTRL message (CD907A) from one phase to another is necessary since different approaches are followed between "To Be" and "Legacy". Consequently, a **generic error reporting** (error code/type, error pointer/location and error location) shall be used during NCTS-P5 and AES-P1 and for the "conversion" of Functional error (CD906A)/EDIFACT CONTRL message (CD907A) from "Legacy" to "To Be" approach and depending on the error at different levels (Table 31):

Validation Error	Error Message from NA "Legacy"	Convertor	Error Message sent to NA "To Be"
TMS (EDIFACT)	***CD907A.edifact*** *Specific Error Reporting*	➡	***CD906C.xml*** *Error type: 51* *Error pointer:* Root Element *Error Reason:* NCAvB
FMS (sequencing, optionalities, repetitions, formatting)	***CD906A.edifact*** *Specific Error Reporting*	➡	***CD906C.xml*** *Error type: 52* *Error pointer:* Root Element *Error Reason:* NCAvB
Business Validation (R/C/T and Codelist validation)	***CD906A.edifact*** *Specific Error Reporting*	➡	***CD906C.xml*** *Error type: 52* *Error pointer:* Root Element *Error Reason:* NCAvB

Table 31: Conversion of error messages in case of errors other than 90, 92 or 93 on a submitted "Downgraded" message submitted by NA "To Be"

Table 31 error messages might also be sent from the TAXUD ieCA during output format FMS validation, Business Validation Errors (Rules & Conditions and Codelists for "Legacy") or output TMS (EDIFACT) validation of converted "Downgraded" message prior submission to NA "Legacy". Table 31 error messages might also be sent from the TAXUD ieCA during output format FMS validation, Business Validation Errors (Rules & Conditions and Codelists for "Legacy") or output TMS (EDIFACT) validation of converted "Downgraded" message prior submission to NA "Legacy".

o For error codes 90, 92 or 93, the error reporting (error code/type, error pointer/location to MRN for error code 90 and 93 or Message Type for error code 92) is expected to be re-used in case:

▪ Errors found by NA "To Be" on an "Upgraded" message (Table 32):

Validation Error	Error Message from NA "To Be"	Convertor	Error Message sent to NA "Legacy"
Error Code 90, or 93	***CD906C.xml*** *Error code:* 90 or 93 *Error pointer:* MRN *Error reason:* NCAvC	➡	***CD906A.edifact*** *Error type:* 90 or 93 *Error pointer:* MRN *Error reason:* NCAvC
Error Code 92	***CD906C.xml*** *Error code:* 92 *Error pointer:* Root Element *Error reason:* NCAvC	➡	***CD906A.edifact*** *Error type:* 92 *Error pointer:* Message Type *Error reason:* NCAvC

Table 32: Conversion of error messages in case of errors 90, 92 or 93 on an "Upgraded" message (received from NA "Legacy")

▪ Errors received by NA "To Be" on a "Downgraded" message (Table 33):

Validation Error	Error Message from NA "Legacy"	Convertor	Error Message sent to NA "To Be"
Error Code 90 or 93	***CD906A.edifact*** *Error type:* 90 or 93 *Error pointer:* MRN	➡	***CD906C.xml*** *Error code:* 90 or 93 *Error pointer:* MRN *Error reason:* NCAvB
Error Code 92	***CD906A.edifact*** *Error type:* 92 *Error pointer:* Message Type	➡	***CD906C.xml*** *Error code:* 92 *Error pointer:* Root Element *Error reason:* NCAvB

Table 33: Conversion of error messages in case of errors 90, 92 or 93 on a submitted "Downgraded" message submitted by NA "To Be"

▪ The above "conversion" of Functional errors is performed by NA "To Be" of **type A** using the TAXUD ieCA

✓ The exception handling for NA "To Be" of **type A** using a NCO must be in accordance with the principles for Common Domain exchanges defined in Table 29.

- If error found on **originally submitted message (before conversion)**, NA "To Be" using a NCO shall respond with Functional error (CD906A) message and EDIFACT CONTRL message (CD907A) having **specific error reporting** (error code/type, error pointer/location and error location) as per "Legacy" principles.

- If error found on **converted message**, NA "To Be" using a NCO shall:

   o respond with Functional error (CD906A) having **generic error reporting** (error code/type, error pointer/location and error location) in case errors found on an "Upgraded" message by NA "To Be". The Functional error (CD906A) shall be in alignment with "Legacy" principles as described in Upgrade scenarios (V.3.2.1.5.1.4) – Please see Table 30.

   o process Functional error (CD906A)/EDIFACT CONTRL message (CD907A) received from NA "Legacy" in case errors found on a submitted "Downgraded" message. The Functional error (CD906A)/EDIFACT CONTRL message (CD907A) shall be in alignment with "Legacy" NCTS-P4/ECS-P2 principles as described in Downgrade scenarios (V.3.2.1.5.1.3) – Please see Table 31.

   o For error codes 90, 92 or 93, the error reporting (error code/type, error pointer/location to MRN for error code 90 and 93 or Message Type for error code 92) is expected to be re-used in case:

      ▪ Errors found by NA "To Be" on an "Upgraded" message. Please see Table 32.

      ▪ Errors received by NA "To Be" on a "Downgraded" message. Please see Table 33.

      ▪ The above "conversion" of Functional errors is performed by NA "To Be"of **type A** using a NCO.

- Interface between between NA "To Be" and NCO is up to National Administration.

✓ The exception handling for NA "To Be" of type B must be in accordance of principles for Common Domain exchanges defined in V.3.2.1.5.1. If error found on submitted message (no conversion is considered), then NA "To Be" of type B shall respond with Functional error (CD906A) message and EDIFACT CONTRL message (CD907A) having error reporting (error code/type, error pointer/location and error location) as per "Legacy" principles.

V.3.2.1.5.1.1 Handling of errors (other than 90, 92 or 93) following Downgrade of message with Sender NA "To Be" of type A using TAXUD ieCA – Error Reported by "Legacy"

The scenario starts when a message must be submitted by NA "To Be" to a NA "Legacy". This means that the message shall be converted Downgraded as per Technical Conversion Specifications using the TAXUD ieCA prior submission to Common Domain according to the "Legacy" specifications (message structure and message formatting) **[Seq. 1-3].** In this scenario is assumed that downgrade conversion is performed successfully by TAXUD ieCA.

Upon receiving the message, the NA "Legacy" might identify errors at the following levels and for which error handling is defined per case as illustrated in Figure 16:

- TMS (EDIFACT)

- FMS (sequencing, optionalities, repetitions, formatting)

- Business Validation (R/C/TR and Codelist validation)

In case TMS Validation Errors are reported by NA "Legacy" via EDIFACT CONTRL message (CD907A.edifact) **[Seq. 6]**, then

1. the NA "To Be" shall forward the received EDIFACT CONTRL message (CD907A) to <u>TAXUD ieCA</u> along with the originally submitted message (e.g. IE501C.xml) and the converted message, which was rejected by NA "Legacy" (e.g. IE501B.edifact) **[Seq. 7]**;

2. Messages from point 1 shall be used for incident analysis purposes – further investigation is needed in the context of exception handling;

3. the <u>TAXUD ieCA</u> shall submit IE906C.xml using generic error reporting as follows **[Seq. 8]**:

    - Error code:51

    - Error pointer: <root element>

    - Error reason: "NCAvB"

In case FMS Validation Errors or Business Validation Errors are reported by NA "Legacy" via Functional error message (CD906A.edifact) **[Seq. 10] and [Seq. 14]** then

1. the NA "To Be" shall forward the received Functional error message (CD906A.edifact) to <u>TAXUD ieCA</u> along with the originally submitted message (e.g. IE501C.xml) and the converted message, which was rejected by NA "Legacy" (e.g. IE501B.edifact) **[Seq. 11] and [Seq. 15]**.

2. Messages from point 1 shall be used for incident analysis purposes – further investigation is needed in the context of exception handling;

3. the <u>TAXUD ieCA</u> shall submit IE906C.xml using generic error reporting as follows **[Seq. 12] and [Seq. 16]**:

    - Error code: 52

    - Error pointer: <root element>

    - Error reason: "NCAvB"
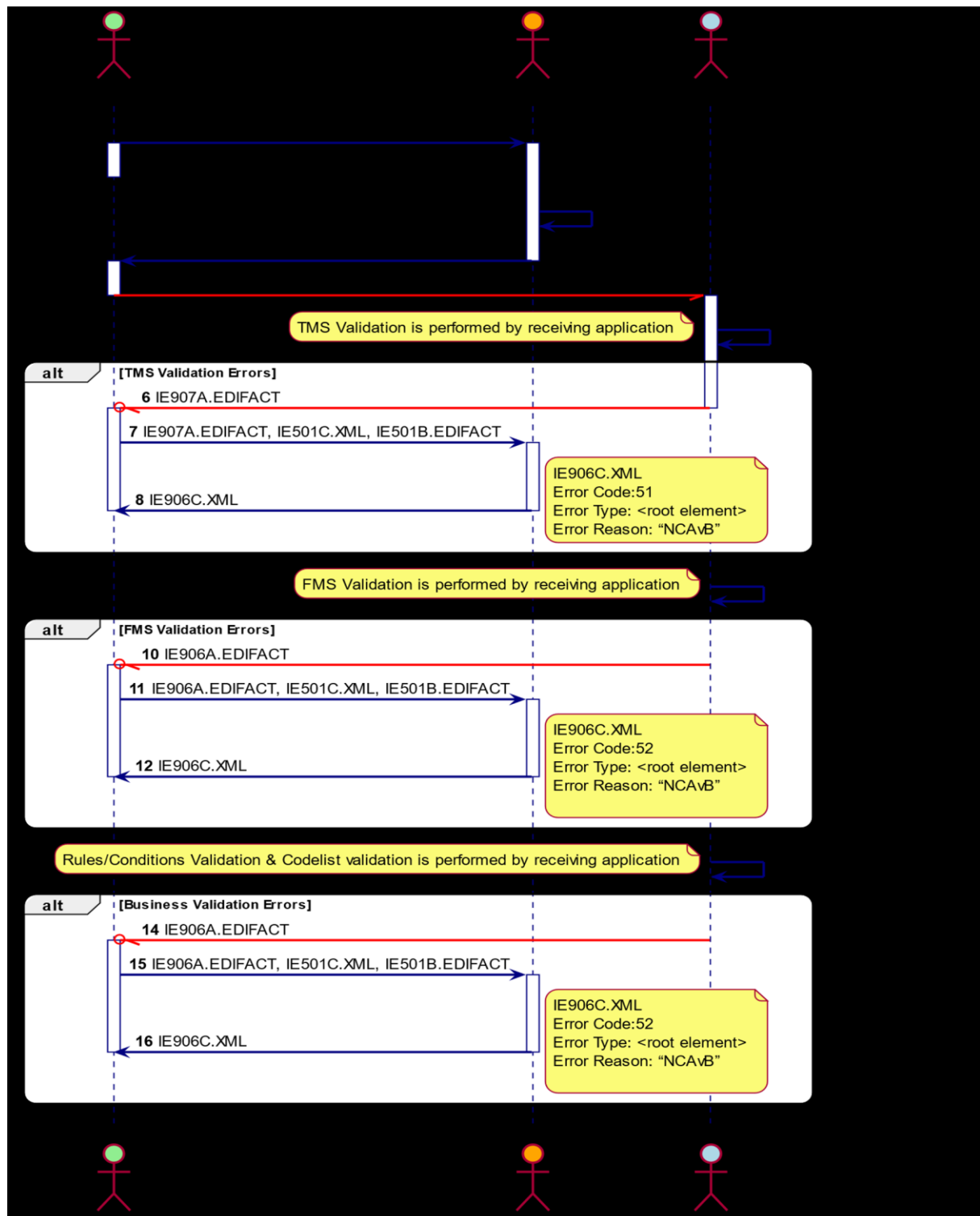
Figure 16: Handling of errors (other than 90, 92 or 93) following Downgrade of message with Sender NA "To Be" of type A using <u>TAXUD ieCA</u> – Error Reported by "Legacy"

V.3.2.1.5.1.2 Handling of errors (other than 90, 92 or 93) following Upgrade of message with NA "To Be" of type A using <u>TAXUD ieCA</u> – Error Reported by NA "To Be"

The scenario starts when a message is submitted by NA "Legacy" to an NA "To Be" according to the "Legacy" specifications (message structure and message formatting). This means that the message shall be converted (Upgraded) by NA "To Be" as per Technical Conversion Specifications using the TAXUD ieCA convertor following reception from the Common Domain **[Seq. 1-3].** In this scenario is assumed that upgrade conversion is performed successfully by ieCA.

Upon receiving the converted message (e.g. IE501C), the NA "To Be" might identify errors at the following levels and for which error handling is defined per case as illustrated in Figure 17:

- XML Validation Errors (as per XSD)

- Business Validation (R/C/T and Codelist validation)

In case XML Validation Errors are reported by NA "To Be" via XML CONTRL message (CD917C.xml) **[Seq. 6]**, then

1. the NA "To Be" shall forward the received XML CONTRL message (CD917C.xml) to TAXUD ieCA along with the originally submitted message (e.g. IE501B.edifact) and the converted message, which was rejected by NA "To Be" (e.g. IE501C.xml) **[Seq. 6]**;

2. Messages from point 1 shall be used for incident analysis purposes – further investigation is needed in the context of exception handling;

3. the TAXUD ieCA shall submit IE906A.edifact to NA "To Be" using generic error reporting as follows **[Seq. 7]**:

   - Error type:14

   - Error pointer: <root element>

   - Error reason: "NCAvC"

4. NA "To Be" shall subsequently submit the IE906A.edifact above to NA "Legacy"

In case Business Validation Errors are reported by NA "To Be" via Functional error message (CD906C.xml) **[Seq. 10]**, then

1. the NA "To Be" shall forward the received Functional error message (CD906C.xml) to TAXUD ieCA convertor along with the originally submitted message (e.g. IE501B.edifact) and the converted message, which was rejected by NA "To Be" (e.g. IE501C.xml) **[Seq. 6]**;

2. Messages from point 1 shall be used for incident analysis purposes – further investigation is needed in the context of exception handling;

3. the TAXUD ieCA convertor shall submit IE906A.edifact to NA "To Be" using generic error reporting as follows **[Seq. 12]**:

   - Error type:15

   - Error pointer: <root element>

   - Error reason: "NCAvC"

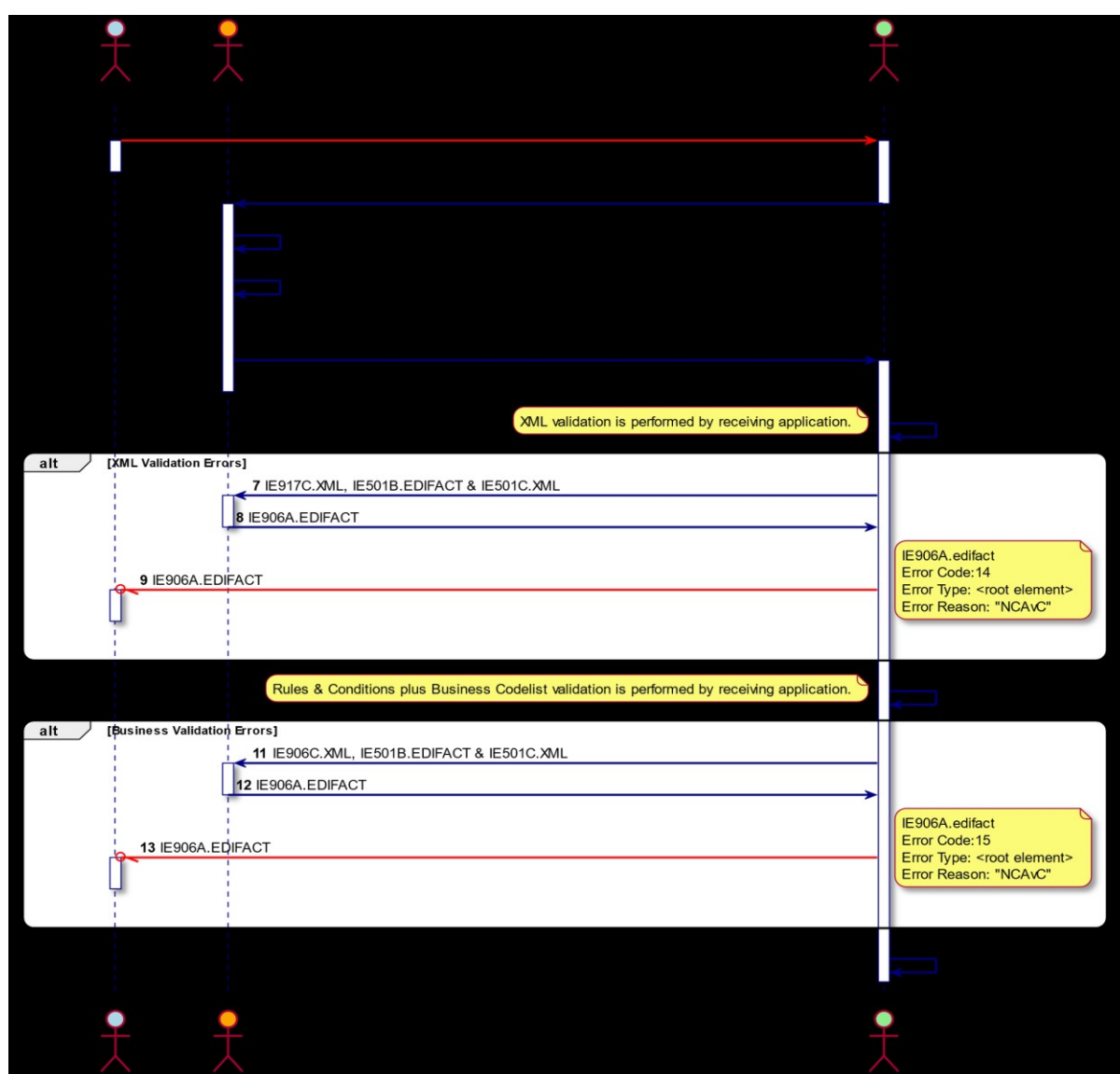4. NA "To Be" shall subsequently submit the IE906A.edifact above to NA "Legacy"
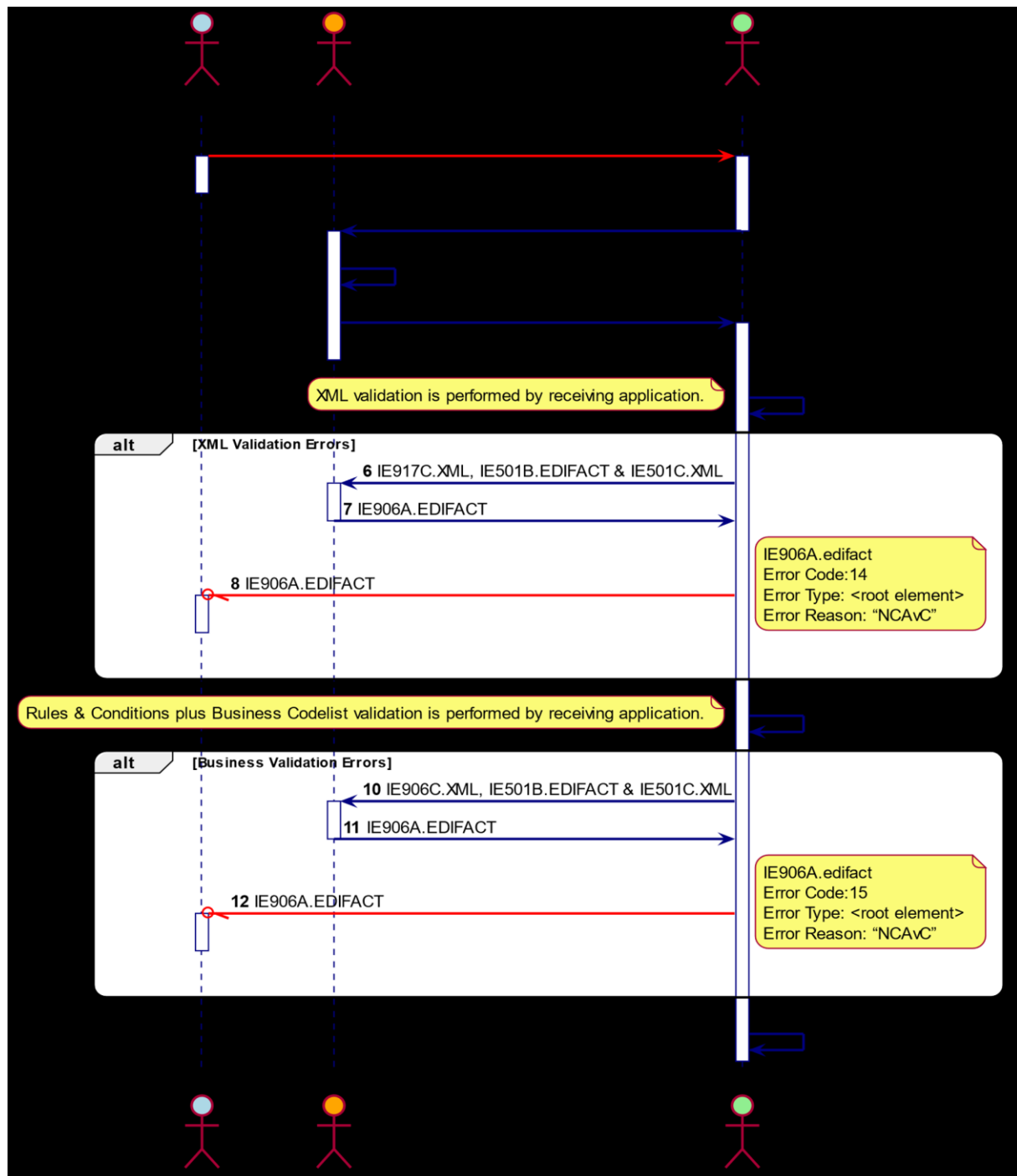
Figure 17: Handling of errors (other than 90, 92 or 93) following Upgrade of message with NA "To Be" of type A using <u>TAXUD ieCA</u> – Error Reported by NA "To Be"

V.3.2.1.5.1.3 Handling of errors (other than 90, 92 or 93) following Downgrade of message with Sender NA "To Be" of type A using <u>NCO</u> – Error Reported by NA "Legacy"

The scenario starts when a message must be submitted by NA "To Be" to a NA "Legacy". This means that the message shall be converted Downgraded as per Technical Conversion Specifications using the <u>NCO</u> prior submission to Common Domain according to the "Legacy" specifications (message structure and message formatting) **[Seq. 1].** In this scenario is assumed that downgrade conversion is performed successfully. Please note that the conversion of messages (IE501C.xml to IE501B.edifact) is a national issue however must be performed as per Technical Conversion Specifications.

Upon receiving the message, the NA "Legacy" might identify errors at the following levels and for which error handling is defined per case as illustrated in Figure 18:

- TMS (EDIFACT)

- FMS (sequencing, optionalities, repetitions, formatting)

- Business Validation (R/C/T and Codelist validation)

In case TMS Validation Errors are reported by NA "Legacy" via EDIFACT CONTRL message (CD907A.edifact) **[Seq. 3]**, then

1. The processing of EDIFACT CONTRL message (CD907A) by the NA "To Be" and the communication or involvement of <u>NCO</u> is a national issue (e.g. whether CD906C.xml will be created with error pointer similar to ieCA approach (V.3.2.1.5.1.1).

2. Messages IE907A.edifact, IE501C.XML, IE501B.edifact and IE501B.XML must be available for incident analysis– further investigation is needed in the context of exception handling.

In case FMS Validation Errors are reported by NA "Legacy" via Functional error message (CD906A.edifact) **[Seq. 5]**, then

1. The processing of Functional error message (CD906A.edifact) by NA "To Be" and the communication or involvement of <u>NCO</u> is a national issue (e.g. whether CD906C.xml will be created with error pointer similar to ieCA approach (V.3.2.1.5.1.1).

2. Messages IE906A.edifact, IE501C.XML, IE501B.edifact and IE501B.XML must be available for incident analysis– further investigation is needed in the context of exception handling.

In case Business Validation Errors are reported by NA "Legacy" via Functional error message (CD906A.edifact) **[Seq. 7]**, then

1. The processing of Functional error message (CD906A.edifact) by NA "To Be" and the communication or involvement of <u>NCO</u> is a national issue (e.g. whether CD906C.xml will be created with error pointer similar to ieCA approach (V.3.2.1.5.1.1).

2. Messages IE906A.edifact, IE501C.XML, IE501B.edifact and IE501B.XML must be available for incident analysis– further investigation is needed in the context of exception handling.
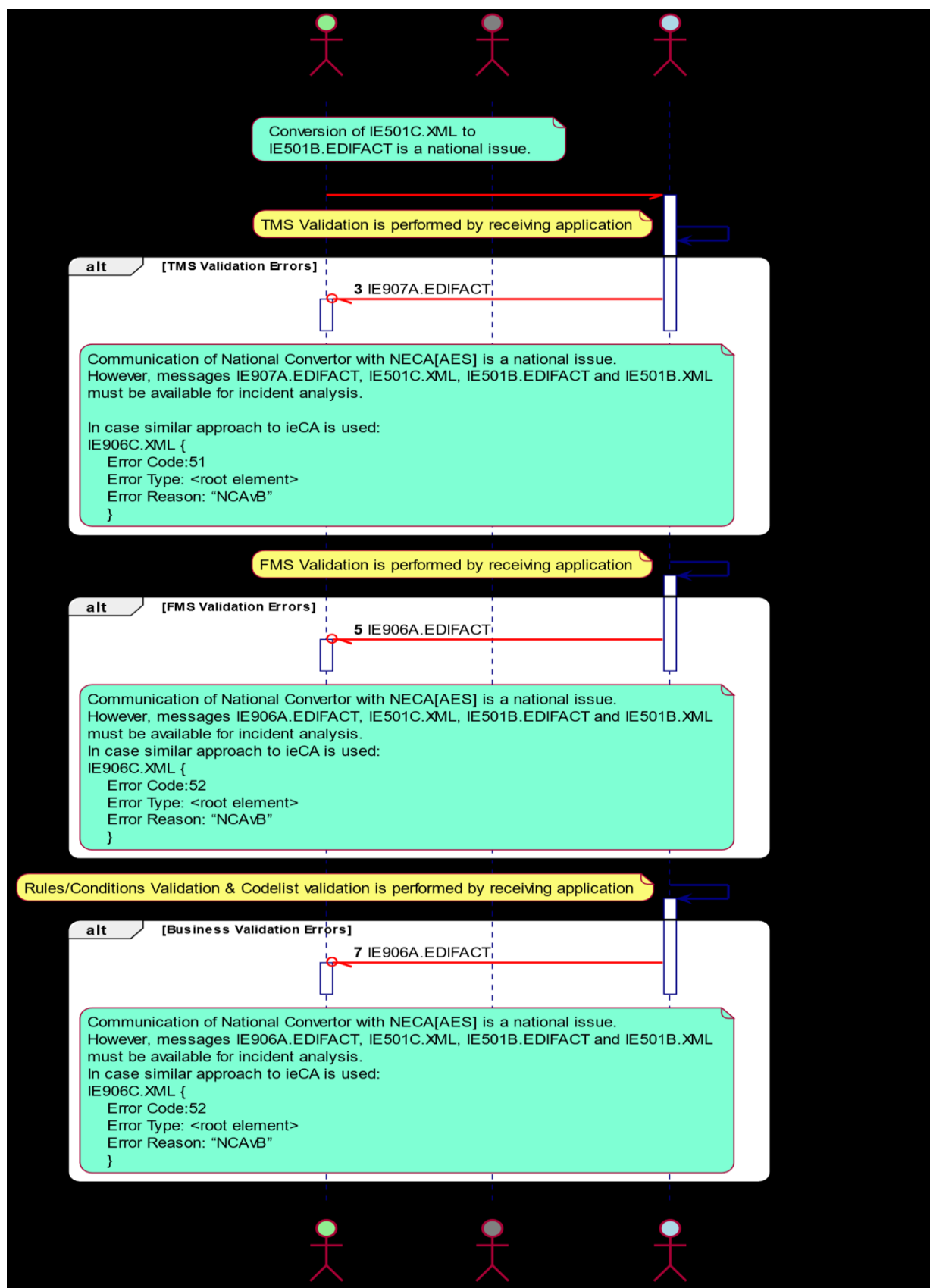
Figure 18: Handling of errors (other than 90, 92 or 93) following Downgrade dof message with Sender NA "To Be" of type A using <u>NCO</u> – Error Reported by NA "Legacy"

V.3.2.1.5.1.4 Handling of errors (other than 90, 92 or 93) following Upgrade of message with NA "To Be" of type A using <u>NCO</u> – Error Reported by NA "To Be"

The scenario starts when a message is submitted by NCA[NCTS-P4/ECS-P2] to an NA "To Be" according to the "Legacy" specifications (message structure and message formatting). This means that the message shall be converted (Upgraded) by NA "To Be" as per Technical Conversion Specifications using the <u>NCO</u> following the reception of the message from the Common Domain **[Seq. 1].** In this scenario is assumed that upgrade conversion is performed successfully. Please note that the conversion of messages (IE501B.edifact to IE501C.xml) is a national issue however must be performed as per Technical Conversion Specifications.

Following conversion of message (Downgrade from IE501B to IE501C), the NA "To Be" might identify errors at the following levels and for which error handling is defined per case as illustrated in Figure 19:

- XML Validation Errors (as per XSD)

- Business Validation (R/C/T and Codelist validation)

In case XML Validation Errors are reported by NCA [NCTS-P5/AES-P1] **[Seq. 2]**, then

1. The communication or involvement of <u>NCO</u> is a national issue (e.g. whether CD917C.xml will be created by NA "To Be" similar to the scenario of ieCA approach (V.3.2.1.5.1.2) and how this will be converted to CD906A.edifact).

2. the NCA [NCTS-P5/AES-P1] shall submit IE906A.edifact to NA "Legacy" using generic error reporting as follows **[Seq. 3]**:

   - Error type:14

   - Error pointer: <root element>

   - Error reason: "NCAvC"

3. Messages IE906A.edifact, IE501B.edifact, IE501C.xml and IE501B.xml must be available for incident analysis– further investigation is needed in the context of exception handling.

In case Business Validation Errors are reported by NA "To Be" **[Seq. 4]**, then

1. The communication or involvement of <u>NCO</u> is a national issue (e.g. whether CD906C.xml will be created by NA "To Be" similar to the scenario of ieCA approach (V.3.2.1.5.1.2) and how this will be converted to CD906A.edifact).

2. the NCA [NCTS-P5/AES-P1] shall submit IE906A.edifact to NA "Legacy" using generic error reporting as follows **[Seq. 5]**:

   - Error type:15

   - Error pointer: <root element>

   - Error reason: "NCAvC"

3. Messages IE906A.edifact, IE501B.edifact, IE501C.xml and IE501B.xml must be available for incident analysis– further investigation is needed in the context of exception handling.
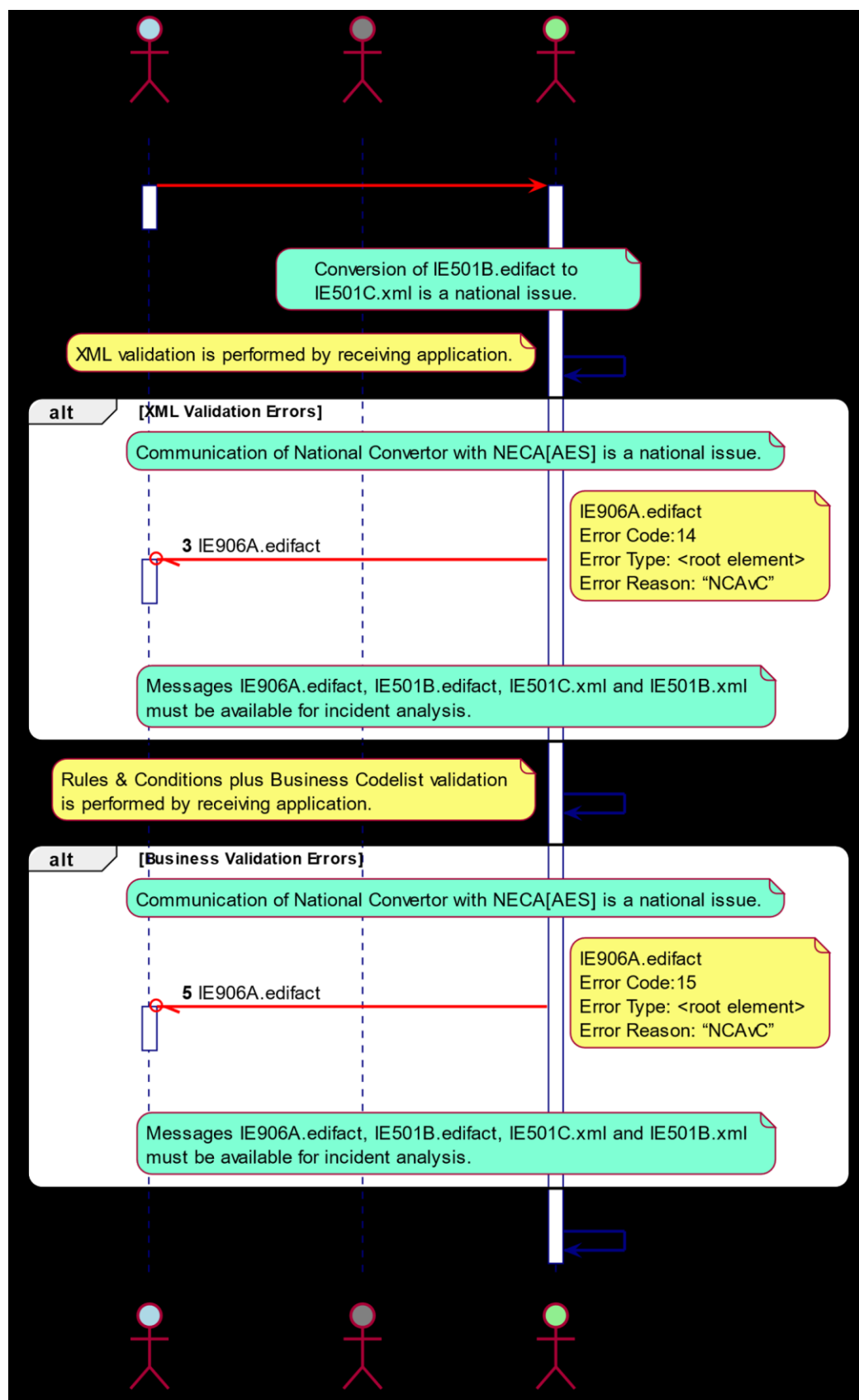
Figure 19: Handling of errors (other than 90, 92 or 93) following Upgrade of message with NA "To Be" of type A using <u>NCO</u> – Error Reported by NA "To Be"

V.3.2.1.5.2 Exception handling for CD exchange between NAs in "To Be" <u>with Sending NA being "To Be" (sending in "To Be" Interface) – CD Exchange pattern#4</u>

The exception handling for CD exchange between NAs in "To Be" with Sending NA being "To Be" (sending in "To Be" Interface) shall be performed as per principles of Exception handling after the Transitional Period. Please refer to V.3.2.1.4.

V.3.2.1.5.3 Exception handling for CD exchange between NAs in "To Be" <u>with Sending NA being "To Be" (sending in "Legacy" Interface) – CD Exchange pattern#5</u>

The exception handling for CD exchange between NAs in "To Be" with Sending NA being "To Be" (sending in "Legacy" Interface) shall be performed as per principles of Exception handling of "legacy" protocol (ECS-P2/NCTS-P4).

The case where conversion is needed by Receiving NA if further elaborated in section V.3.2.1.5.1. The *Sending NA being "To Be" (sending in "Legacy" Interface)* should be seen in this case <u>from exception handling point of view</u> as "Legacy NA".

Since the case concerns Sending NA being "To Be" (sending in "Legacy" Interface), only the cases "Upgrade of message" by Receiving NA are applicable as per sections 0 and V.3.2.1.5.1.4

V.3.3   *Functional error codes*

This section explains the error codes that can be used by the Functional error messages, the EDIFACT FUN NACK and XML FUN NACK (specified as C_FUN_NCK in DDNxA volumes). The XML NACK is described in section VII.5 XML error (CONTRL) message and EDIFACT NACK is described in VI.7 EDIFACT CONTRL Message.

The Functional error codes values are a subset of the generic table provided by EDIFACT and are based on the use of EDIFACT for Customs systems.

For the errors identified at functional level, different error codes are used:

- for **IE906A**, error codes are maintained in CS/RD2 (CL049);
- for **IE906B**, error codes are maintained in CS/RD2 (CL049) and are also available in tcl.xsd;
- for **IE906C**, error codes are specified in tcl.xsd and maintained in CS/RD2 (CL180).

The table below presents the list of functional error codes and their usage as defined in CS/RD2 (CL180).

Value	Description	Remark	Applicable[20]
12	**Codelist violation**	The value of a Data Item is outside the predefined set of values (i.e. not part of the applicable (business or technical) Codelist). *Example: The Data Element with CL027 ('0' or '1') includes the value '2'. It violates the CL027.*	• During TP • After TP
13	**Missing Required element violation**	A condition (Cxxxx or Txxxx) is violated due to missing Data Group or Data Item is missing (while "R"). *Example: Violation of C0569 - Declared number of seals is '2' and no seals are declared.* *(IF /*/GoodsShipment/Consignment/TransportEquipment/numberOfSeals is GREATER than '0'* *THEN /*/GoodsShipment/Consignment/TransportEquipment/Seal = "R"* *ELSE /*/GoodsShipment/Consignment/TransportEquipment/Seal = "N".)*	• During TP • After TP
14	**Rule violation**	A rule (Rxxxx or Txxxx) is violated and consequently a Data Group or a Data Item includes an invalid value. *Example: Violation of R0007 - The first declared Goods item number is 2.* *(Each <GOODS SHIPMENT - GOODS ITEM.Goods item number> is unique throughout the declaration. The items shall be numbered in a sequential fashion, starting from '1' for the first item and* *incrementing the numbering by '1' for each following item.)*	• During TP • After TP
15	**Condition violation – presence**	A condition (Cxxxx or Txxxx) is violated and consequently a Data Group or Data Item is present despite it shall not be present (it is present while "N").	• During TP • After TP

---

[20] It defines whether an error code is applicable during the Transitional Period, after the Transitional Period or both.

Value	Description	Remark	Applicable[20]
	not allowed	*Example: Violation of C0569 - Declared number of seals is '0' and seals are declared.* *(IF /*/GoodsShipment/Consignment/TransportEquipment/numberOfSeals is GREATER than '0'* *THEN /*/GoodsShipment/Consignment/TransportEquipment/Seal = "R"* *ELSE /*/GoodsShipment/Consignment/TransportEquipment/Seal = "N")*	
26	Duplicate Message ID	The message includes the same 'Message identifier' as another message already received and processed.	• During TP • After TP
50	Transitional constraint Violation	A transitional constraint (Exxxx or Bxxxx) is violated. A Data Group is missing or too many repetitions are in the message. A Data Item is missing or is present despite it may not be present, or a Data Item includes an incorrect value (including violation of the format). *Example: Violation of E1108 – Declaration with 10.000.000 packages.* *(IF <Decisive Date> is LESS than or EQUAL to <TPendDate>* *THEN /*/ExportOperation/totalNumberOfPackages* *format shall be set to n..7)*	• During TP • After TP
51	EDI violation post downgrade	After the downgrade conversion (from "Legacy" to "To Be") the EDIFACT message is syntactically incorrect (a CD906C is generated and sent back to the application that initiated the conversion).	• During TP
52	Functional violation post downgrade	After the 'downgrade' conversion (from "Legacy" to "To Be") the EDIFACT message is semantically incorrect: - FMS (sequencing, optionalities, repetitions, formatting) is violated - Business Validation (Rxxx, Cxxx or TRxxxx and Codelist validation) is violated	• During TP
90	Unknown MRN	A message is received with MRN unknown to the destination (exception is the IEx01 messages concerning movement creation). To be used only	• During TP • After TP

Value	Description	Remark	Applicable[20]
		when there is no 'negative response' *Example: The CDx02C is received and MRN is unknown, it must be responded with negative CDx03C; not with CD906C.* *But: If a message CD115C is received and MRN is unknown, it must be responded with a CD906C with code '90'.*	
92	**Message out of sequence**	The message cannot be processed, because the receiver's states machine is not in the state that does not allow to process the received message. *Example: the NTA (Office of Departure) receives the message CD018C while the movement is still in the state 'Under control'.*	• During TP • After TP
93	**Invalid MRN**	The message includes a value for the Data Item <MRN> that violates the structure defined in the DDCOM. *Example: the 'Check digit' is not valid.*	• During TP • After TP

Table 34: Functional error codes for NCTS-P5 and AES-P1

It is assumed that errors are detected by reception of a message. This implies that Functional errors are specified in more detail than message formatting errors (EDIFACT or XML). FMS specify more detail on the functional level with respect to:

- Status of a Data Item: a EDIFACT data element can be optional, whereas the related Data Item of an FMS is required;

- Code values: code values are specified at functional level, with the exception of those codes that are specific to EDIFACT (e.g. qualifier values);

- Dependency rules: values of Data Items can be dependent on each other as specified by additional conditions (see FSS [R26], [R13] and [R14]).

V.3.4 Technical Error codes

This section explains the error codes that can be used by the EDIFACT NACK and XML NACK error messages, (specified as C_EDI_NCK and C_XML_NCK in DDNxA volumes). The XML NACK is described in section VII.5 XML error (CONTRL) message and EDIFACT NACK is described in VI.7 EDIFACT CONTRL Message.

For the formatting errors identified, different error codes are used:

- for **IE907A**, error codes are maintained in CS/RD2 (CL023);

- for **IE917B**, error codes are maintained in CS/RD2 (CL030) and also available in tcl_ics.xsd;

- for **IE917C**, error codes are specified in tcl.xsd and maintained in CS/RD2 (CL030).

In particular, for the EDIFACT, the following table shows the EDIFACT segment that has to be used for a particular EDIFACT error code.

EDIFACT error segment	EDIFACT error code
UCI	2, 7, 12, 13, 14, 16, 18, 19, 21, 22, 23, 26, 28, 29, 32, 33.
UCM	3, 12, 13, 14, 19, 21, 22, 28, 29.
UCS	6, 13, 15, 35, 36.
UCD	12, 13, 14, 15, 16, 19, 21, 22, 37, 38, 39, 40.

Table 35: Segment position of EDIFACT error codes

V.4 Functional error in IE906 (CD906A/CD906B)

This section describes the use of Functional error data group in IE906 (CD906A/CD906B). The CD906A message must be used for Functional error reporting in the following cases:

1. Common Domain exchanges in NCTS-P4

2. Common Domain exchanges in ECS-P2

3. Common Domain exchanges between NTA of transitional NCTS-P5 and NTA [NCTS-P4]

4. Common Domain exchanges in between NECA of transitional AES-P1 and NECA [ECS-P2]

5. ICS-P1 is using CD906B in Common Domain exchanges.

More information for cases 3, 4 and 5 can be found in section V.3.2.1.4.

The Data Group 'FUNCTIONAL ERROR' has been introduced to enable the exchange of Functional errors. This Data Group is the technical implementation of Rule 123 in the FMS specified in FSS ([R26] Appendix B, [R13] Appendix B1 and [R14] Appendix B1).

The Data Group consists of the following Data Items:

Data Item	Content	Status	Format
Error type	Values taken from CS/RD2 (CL049).	Required	n2
Error pointer	This Data Item points to the Data Item or Data Group that caused the error by listing the hierarchy of that Data Item and its occurrence in the hierarchy. In case of error type 90 or 93, the error pointer points to the MRN. In case of error type 92, the error pointer points to the \<MessageType\> (i.e. CDxxxC). The syntax for the value of the error pointer is as follows: (Data Group code ['(' (occurrence) ')']'.')+ [(Data Item name)] For the NCTS-P5 and AES-P1 operations during the Transitional Period, in case of error reported other than 90, 92 or 93 by an NCA [NCTS-P5/AES-P1] following Upgrade of messages, the Error type = 14 or 15 will be used with Error pointer to the \<MessageType\> (i.e. CDxxxX).	Required	an..210
Error reason	This Data Item contains the identification of the Condition, Code List or Rule in case error type '15' is detected due to an error related to a Condition or a Rule or a Code List or a Technical Rule (for example 'C099' to denote a violation of condition C099, 'TR0001' to denote a violation of technical rule TR0001 and 'CL031' denote a violation of Code List CL031). In case a specific C_DES_CON or C_EXT_RES building rule is violated the particular error reason code 'TRxxxx' is used. Please refer to DDNTA or DDNXA Appendix Q1 about technical rules defined for the constructions of control results (IE018/IE518). For the NCTS-P5 and AES-P1 operations during the Transitional Period, in case of error reported other than 90, 92 or 93 by an NCA [NCTS-P5/AES-P1] following Upgrade of messages, the Error type = 14 or 15 will be used with Error reason: • "ieCAvB" if exception is thrown by ieCA or • "NCAvB" if exception is thrown by NTA or NECA	Dependent	an..6
Original attribute value	This Data Item is used to exchange the original value in case sequencing of Data Groups is changed at reception of a message.	Optional	an..140

Table 36: Data Items for Functional error data group in IE906 (CD906A/CD906B)

Notes to the Functional error Data Group:

- The Data Group codes used for the error pointer are listed in the corresponding Appendix Y. The notation used for specifying the pointer is as follows:

Pattern	Semantics	Example
A B	A followed by B	(Data Group code) (Data Item name)
[A]	A or nothing	[occurrence]
A^+	One or more occurrences of A	(Data Group code)$^+$
(expression)	Expression is treated as unit and may be combined as described in this list	(Data Group code)
'string'	A literal string	'(' or '.'[21]

Table 37: Notation of error pointer

- Occurrence is a sequence number for a Data Group. An occurrence is only given for repeatable or erroneously repeated Data Groups and is, therefore, optional. An occurrence relates to the sequence in which a message is received. This sequence is not necessarily equal to the sending sequence because the FMS structure may not be implemented as such by a National Customs Application;

- The Data Item names of the FMS are listed in the corresponding Appendix Q of this DDNA. Examples of the error pointer are as follows:

Error pointer value	Semantics
HEA.Containerised indicator	Pointer to 'Containerised indicator' of the Header Data Group.
GUA(3).REF(5).Access code	Pointer to 'Access code' of the fifth Guarantee reference Data Group within the third Guarantee Data Group.
GDS(3).GS2(4).Kind of packages	Pointer to 'Kind of packages' of the fourth Package Data Group within the third goods item.
CE1	Pointer to '(CONSIGNEE) TRADER' Data Group.

Table 38: Examples of error pointer

---

[21] The syntax of the Error pointer value defined in Table 36 specifies what string literals are applicable and how those can be used as part of the notation.

V.5 Functional error in IE906 (CD906C)

This section describes the use of Functional error data group in IE906 (CD906C). The CD906C message must be used for Functional error reporting in the following cases:

1. Post-transitional Common Domain exchanges in NCTS-P5 and AES-P1;

2. Transitional Common Domain exchanges in between NCAs in NCTS-P5 and AES-P1.

More information about case 2 can be found in section V.3.2.1.4.

The Data Group 'FUNCTIONAL ERROR' consists of the following Data Items:

Data Item	Content	Status	Format
Error code	Values taken from CS/RD2 (CL180).	Required	n2
Error pointer	The Error pointer is to be denoted as singular XPath expression starting at the root element of the document ("abbreviated absolute location path"). *Example:* • *"/CD501C/GoodsShipment/GoodsItem[10]/Packaging[5]/shippingMarks"* Below, the expected *Error pointer* per *Error code* is defined: IF *Error code* = (90 or 93), THEN the *Error pointer* points to the <MRN>. IF *Error code* = (92, 51 or 52), THEN the *Error pointer* points to the <Root Element> (i.e. CDxxxX). ELSE the *Error pointer* points to the <Data Item or Data Group that caused the error>. **Example for C0105** *Error pointer*:/CD001C/CustomsOfficeOfTransit(Declared) *Error code*:13 *Error reason*:C0105 *Original attribute value*: N/A	Required	an..512

Data Item	Content	Status	Format
Error reason	The *Error reason* is used to report the reason of Functional error. IF *Error code* = 12, THEN the *Error reason* shall point to the Codelist number against which the validation failed (using the string 'CL999' where CL999 is the number of the codelist as defined in Appendix Q2. The length of the number is fixed to 3 digits). IF *Error code* = 13 or 15, THEN the *Error reason* shall point to the Condition or Technical Rule number(s) against which the validation failed (using the string 'C9999' or 'T9999' where 9999 is the number of the R&C as defined in Appendix Q2). IF *Error code* = 14, THEN the *Error reason* shall point to the Rule or Technical Rule number(s) against which the validation failed (using the string 'R9999' or 'T9999' where 9999 is the number of the R&C as defined in Appendix Q2). IF *Error code* = 50, THEN the *Error reason* shall points to the Transitional Constraint number against which validation failed (using the string 'E9999' or 'B9999' where 9999 is the number of the R&C as defined in Appendix Q2). IF *Error code* = 51 or 52, THEN the *Error reason* shall be: • "ieCAvB" if exception is thrown by ieCA • "NCAvB" if exception is thrown by NTA or NECA ELSE, the *Error reason* shall have the value "N/A". **Example for the violation of R0994** *Error pointer:* /CD001C/Consignment/grossMass *Error code:*13 *Error reason:* R0994 *Original attribute value:* 45887 (e.g. for the value of the erroneous data element in the erroneous message). **Example for the violation of CL217** *Error pointer:* /CD001C/TransitOperation/security *Error code:*12 *Error reason:* CL217 *Original attribute value:* 8 (e.g. for the value of the erroneous data element in the erroneous message). Note: for the CL number and the R & C number, it must include the leading zeros if applicable.	Required	an..7

Data Item	Content	Status	Format
Original attribute value	It is used to provide the value of the data element where the error occurred as per *Error pointer* in the erroneous message.	Optional	an..512

Table 39: Data Items for Functional error data group in IE906 (CD906C)

V.6 Constraints

V.6.1 Introduction

This section describes constraints that National Applications must fulfil in order to participate in one of the Customs systems. The following types of constraints are considered:

- Performance constraints;
- Timing constraints;
- Availability constraints.

V.6.2 Performance Constraints

V.6.2.1 External domain

Performance constraints related to Information Exchanges crossing the External Domain (communication between a NA and its Traders) or within the National Domain (communications between different locations of the same NA) are a national matter and should be fixed individually by each NA.

V.6.2.2 Common Domain

The time constraints applied to Information Exchanges crossing the Common Domain (communication between two NAs - directly or via TAXUD ieCA - or between a NA and Central Reference Site) must permit meeting the performance constraints defined in FSS ([R26], [R13] and [R14]). A number of relevant performance constraints are specified by the timer values in the specific Customs system volumes.

V.6.3 Timing constraints

All timing constraints are described in the specific domain volume.

V.6.4 Availability Constraints

The requirements for systems availability for NCAs only consider the international requirements, i.e. the NCAs availability required to support interoperability with other participating NAs through the Common Domain. This also means that this constraint does not apply to the External Domains.

During Initial Implementation, all participating NAs have to guarantee that in the event of a failure of their National Application, or when their National Application is deliberately taken off-line because of business or technical requirements, all Information Exchanges received from CCN will be held until the National Application comes back on-line. They can then be processed as normal, subject to the National Applications fallback rules. This minimum level of availability is met by the CCN functionality.

Sending NCAs should not re-send IEs for which there has been no reply as a result of unavailability of the receiving NCA. The re-send should occur only upon request of the NCA, or receipt of an exception report.

V.6.4.1   Suspension of sending messages

Suspension of sending messages must apply only in case of System Unavailability Type "N" as described in II.2.4.

Each domain specific DDNA volume ([R16], [R17], [R18], [R40] and [R41]) contains a table that specifies which messages should not be sent to an NA when a specific Business Service is unavailable at that NA.

V.6.5   Size constraints

The maximum size of messages exchanged over CCN is defined in section VIII.2.26. As defined in Terms of Collaboration [A16] each NA must inform DG TAXUD before any National change that might have an impact on the size and numbers of messages exchanged on the Common Domain.

V.7 MRN and GRN structure

V.7.1   Structure of the Master Reference Number (MRN) for NCTS-P4, ECS-P2 and ICS-P1

The Master Reference Number is a unique identifier for a movement and is allocated by the NCA which (after validation) accepts/registers the received declaration data from the Person lodging it.

The MRN contains 18 characters - letters used must be upper case - and is composed of following elements:

Field	Content	Field type	Examples
1	Last two digits of year of formal acceptance of a movement (YY)	Numeric 2	12
2	Identifier of the country from which the MRN originates.	Alphabetic 2 (ISO alpha 2 country code)	LV
3	Unique identifier for a movement per year and country	Alphanumeric 13	9876AB8890123
4	Check digit	Numeric 1	5

Table 40: Structure of MRN for NCTS-P4, ECS-P2 and ICS-P1

- Field 1 and 2 as explained above.

- Field 3 has to be filled in with an identifier for a transaction. The way that field is used is under the responsibility of national administrations but each transaction handled during one year within the given country must have a unique number. National administrations that want to have the office reference number of the competent authorities included in the MRN, could use up to the first 6 characters to insert the national number of the office.

- Field 4 has to be filled with a value that is a check digit for the whole MRN. This field allows for detection of an error when capturing the whole MRN.

Based on the above, the following XSD Type (**MRNType**) will be associated with MRN data item per system **(DocNumHEA5** and **MRN)** in NCTS-P4, ECS-P2 and ICS-P1 as per **Table 40**:

```
<xs:simpleType name="MRNType">
          <xs:annotation>
                    <xs:documentation>MRN (format: an18), (alias:
MRNType)</xs:documentation>
          </xs:annotation>
          <xs:restriction base="AlphaNumType">
                    <xs:pattern value="[0-9]{2}[A-Z]{2}[A-Z0-9]{13}[0-9]"/>
          </xs:restriction>
</xs:simpleType>
```

Table 41: XSD restriction for MRN data item in NCTS-P4, ECS-P2 and ICS-P1 _(MRNType)_ as per Table 40

where **AlphaNumType** is defined as follow**s:**

```
<xs:simpleType name="AlphaNumType">
        <xs:annotation>
                <xs:documentation>Base class for all anN and an..N types
                </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:token" />
</xs:simpleType>
```

Table 42: XSD definition of _AlphaNumType_ simple type base class for all anN and an..N types

V.7.1.1   Check character algorithm for the MRN

The algorithm for calculating the check digit character for the MRN is based on the ISO 6346 algorithm. Each character of the reference numbers is given a numeric value as determined by Table 43.

Each individual number is then multiplied by a different factor. The factors are in the range 2^0 to 2^{16} producing 17 sub-totals for the MRN.

These individual sub-totals are totalled and that result is then divided by 11. The remainder of the calculation is then used to determine the check digit by using Table 44.

ASCII Character	Check Character Value
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
A	10
B	12
C	13
D	14
E	15
F	16
G	17
H	18
I	19
J	20
K	21
L	23
M	24
N	25
O	26
P	27
Q	28
R	29
S	30
T	31
U	32
V	34
W	35
X	36
Y	37
Z	38

Table 43: Check character values

Remainder	Check character
10	0
9	9
8	8
7	7
6	6
5	5
4	4
3	3
2	2
1	1
0	0

Table 44: Remainder of the calculation

V.7.1.2 MRN Check Character Calculation Example

MRN (without check character)																
9	9	I	T	9	8	7	6	A	B	8	8	9	0	1	2	0
Check character value (Table 18)																
9	9	19	31	9	8	7	6	10	12	8	8	9	0	1	2	0
Multiplier																
1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536
Values																
9	18	76	248	144	256	448	768	2560	6144	8192	16384	36864	0	16384	65536	0

Total 154031

$154031/11 = 14002 + 9/11$; thus, the remainder is '9' and is used as the check digit (Table 44).

Resulting MRN (with check digit) = 99IT9876AB8890120**9**

V.7.2 Structure of the Master Reference Number (MRN) for NCTS-P5 and AES-P1

The Master Reference Number is a unique identifier for a movement and is allocated by the NCA which (after validation) accepts/registers the received declaration data from the Person lodging it.

The following structure shall be used for export and transit operations accepted in NCTS-P5/AES-P1.

The MRN contains 18 characters - letters used must be upper case - and is composed of following elements as defined in UCC/IA [A18]:

Field	Content	Field type	Examples
1	Last two digits of year of formal acceptance of the declaration (YY)	Numeric 2	21
2	Identifier of the country where the declaration/proof of the customs status of Union goods/ notification is lodged (alpha 2 country code)	Alphabetic 2 (ISO alpha 2 country code)	RO
3	Unique identifier for a movement per year and country	Alphanumeric 12	9876AB889012
4	Procedure identifier	Alphabetic 1	B
5	Check digit	Numeric 1	6

Table 45: Structure of MRN for NCTS-P5 and AES-P1

- Field 1 and 2 as explained above.

- Field 3 shall be filled in with an identifier for a transaction. The way that field is used is under the responsibility of national administrations but each transaction handled during one year within the given country must have a unique number in relation to the procedure concerned. National administrations that want to have the reference number of the competent customs office included in the MRN, may use up to the first 6 characters to represent it

- Field 4 shall be filled in with an identifier of the procedure (please see below).

- Field 5 shall be filled with a value that is a check digit for the whole MRN. This field allows for detection of an error when capturing the whole MRN. Please refer to sections V.7.1.1 and V.7.1.2.

About Field 4, the following values are allowed:

- Subset of Codes to be used in field 4 Procedure identifier for AES-P1, as defined in UCC/IA [A18].

Code	Procedure	Corresponding columns in Annex B of Title I, Chapter 2, Section 1 of [A19]
A	Export only	B1, B2, B3 or C1
B	Export and exit summary declaration	Combinations of A1 or A2, with B1, B2, B3 or C1
C	Exit summary declaration only	A1 or A2
D	Re-export notification	A3
E	Dispatch of goods in relation with special fiscal territories	B4

Table 46: Codes to be used in MRN field 4 Procedure identifier for AES-P1

- Subset of Codes to be used in field 4 Procedure identifier for NCTS, as defined in UCC/IA [A18].

Code	Procedure	Corresponding columns in Annex B of Title I, Chapter 2, Section 1 of UCC DA [A19]
J	Transit declaration only	Columns D1 (Special procedure — Transit declaration) or D2 (Special procedure –Transit declaration with reduced dataset – (transport by rail, air and maritime transport)); possibly complemented by D4 (Presentation Notification in relation to the pre-lodged transit declaration).
K	Transit declaration and exit summary declaration	Combinations of columns D1 or D2 with (A1 (Exit summary declaration) or A2 (Exit summary declaration — Express consignments)); possibly complemented by D4.
L	Transit declaration and entry summary declaration	Combinations of columns D1 or D2 with Entry summary declaration data as defined in the UCC TDA [A20]; possibly complemented by D4.
M	Transit declaration and exit summary declaration and entry summary declaration	Combinations of columns (D1 or D2) with (A1 or A2) and Entry summary declaration data as defined in the UCC TDA [A20]; possibly complemented by D4.

Table 47: Codes to be used in MRN field 4 Procedure identifier for NCTS-P5

Considering the fundamental requirement of having same XSDs during and after transition (IV.3), the following XSD Type (`MRNType`) will be associated with MRN data item for **NCTS-P5** (see also Appendix X of DDNTA [R16])**:**

```
<xs:simpleType name="MRNType">
  <xs:annotation>
    <xs:documentation>MRN (format: an18), (alias: MRNType)</xs:documentation>
  </xs:annotation>
  <xs:restriction base="AlphaNumType">
   <xs:pattern value="([0-1][0-9]|[2][0-4])[A-Z]{2}[A-Z0-9]{13}[0-9]" />
      <!-- ================================================================ -->
      <!-- 'Legacy' MRN structure - - - - - - - - - - - - - - - - - - - -- -->
      <!-- ================================================================ -->
      <!-- Definition of the structure of the MRN produced by an NCTS-P4 -- --->
      <!-- application for an NCTS-P4 movement (i.e. initiated during the- - -->
      <!-- Transitional Period) - - - - - - - - - - - - - - - - - - - - - -->
      <!-- Until the end of 2024, the NCTS-P5 applications will use this -  --->
      <!-- pattern to validate any MRN received (i.e. MRN received for - -- --->
      <!-- movements initiated by an NCTS-P4 application and  MRN received - -->
      <!-- for movements initiated by an NCTS-P5 application) - - - - - -  - -->
      <!-- ================================================================ -->
   <xs:pattern value="([2][4-9]|[3-9][0-9])[A-Z]{2}[A-Z0-9]{12}[J-M][0-9]" />
      <!-- ================================================================ -->
      <!-- 'To Be' MRN structure (NCTS-P5)- - - - - - - - - - - - - - -- -->
```

```xml
        <!-- =============================================================== -->
        <!-- Definition of the structure of the MRN produced by an NCTS-P5 -  --->
        <!-- application for NCTS-P5 movements initiated *after* 01.01.2024  - -->
        <!-- (considering the date of the end of Transitional Period in 2023) --->
        <!-- From 01.01.2024, the NCTS-P5 applications will use this pattern to ->
        <!-- validate any MRN *received*  - - - - - - - - - - - - - - - - - - - --->
        <!-- The structure of the MRN *produced* by the NCTS-P5 applications ----->
        <!-- will be  "([2][1-9]|[3-9][0-9])[A-Z]{2}[A-Z0-9]{12}[J-M][0-9]" -- -->
        <!-- for the first NTAs starting Phase 5 operations in 2021. - - - -- --->
        <!-- =============================================================== -->
    </xs:restriction>
 </xs:simpleType>
```

and for AES-P1 (see also Appendix X of DDNXA [R17]):

```xml
<xs:simpleType name="MRNType">
  <xs:annotation>
    <xs:documentation>MRN (format: an18), (alias: MRNType)</xs:documentation>
  </xs:annotation>
  <xs:restriction base="AlphaNumType">
    <xs:pattern value="([0-1][0-9]|[2][0-4])[A-Z]{2}[A-Z0-9]{13}[0-9]" />
        <!-- =============================================================== -->
        <!-- 'Legacy' MRN structure - - - - - - - - - - - - - - - - - - - - - -->
        <!-- =============================================================== -->
        <!-- Definition of the structure of the MRN produced by an ECS-P2 - - - -->
        <!-- application for an ECS-P2 movement (i.e. initiated during the  - - -->
        <!-- Transitional Period) - - - - - - - - - - - - - - - - - - - - - - - -->
        <!-- Until the end of 2023 (i.e. at least during the Transitional - - - -->
        <!-- Period, the AES-P1 applications will use this pattern to validate- -->
        <!-- any MRN received (i.e. MRN received for movements initiated by - - -->
        <!-- an ECS-P2 applications and  MRN received for movements initiated - -->
        <!-- by an AES application) - - - - - - - - -->
        <!-- =============================================================== -->
  <xs:pattern value="([2][4-9]|[3-9][0-9])[A-Z]{2}[A-Z0-9]{12}[A-E][0-9]" />
        <!-- =============================================================== -->
        <!-- 'To Be' MRN structure (AES-P1)- - - - - - - - - - - - - - - - - - -->
        <!-- =============================================================== -->
        <!-- Definition of the structure of the MRN produced by an AES-P1 - - - -->
        <!-- application for AES-P1 movements initiated *after* 01.01.2024 - - ---->
        <!-- (considering the date of the end of Transitional Period in 2023)- --->
        <!-- From 01.01.2024, the AES-P1 applications will use this pattern to --->
        <!-- validate any MRN *received*  - - - - - - - - - - - - - - - - - - ---->
        <!-- The structure of the MRN *produced* by the AES-P1 applications - - -->
        <!-- will be  "([2][1-9]|[3-9][0-9])[A-Z]{2}[A-Z0-9]{12}[A-E][0-9]" - - -->
        <!-- for the first NECAs starting AES operations in 2021. - - - - - - - -->
        <!-- =============================================================== -->
    </xs:restriction>
  </xs:simpleType>
```

where **AlphaNumType** is defined Table 42.

In addition to the above XSD restriction, Rules shall be defined in DDNxA and applied to MRN data element

- in the Technical Message Structure of CC528C, CC571C, CC628C, (MRN ALLOCATED) defining that the 17th character of MRN must be (depending of the message) 'A', 'B', 'C', 'D' or 'E', for AES-P1 [R16]

- in the Technical Message Structure of CC028C (MRN ALLOCATED) defining that the 17th character of MRN must be 'J', 'K', 'L' or 'M', for NCTS-P5 [R17].

During the Transitional Period, there will be no validation of the 'To Be' MRN structure to enable the upgrade of messages in Common Domain since the NCTS-P4 and ECS-P2 format does not guarantee that the 17th character of MRN will be one of the values defined in Table 46 and Table 47 above. Nevertheless, the export and transit operations in AES-P1 and NCTS-P5 respectively will be assigned with MRN as per structure defined in Table 46 and Table 47 above.

V.7.3 Structure of the Guarantee Reference Number (GRN)

Each NCTS guarantee is referenced by a unique Guarantee Reference Number (GRN) which is used for validation in the guarantee management sub system.

The "Guarantee Reference Number" (GRN) is allocated by the office of guarantee to identify each single guarantee. The GRN contains 17 or 24 characters - letters used must be upper case - and it is structured as follows:

Below, extract from Annex D1, Title II, paragraph B of the Convention and Annex 37a, Title II, paragraph B, IP.

Field	Content	Field type	Examples
1	Last two digits of the year at which the guarantee was accepted (YY)	Numeric 2	12
2	Identifier of the country where the guarantee is lodged (ISO alpha 2 country code)	Alphabetic 2	IT
3	Unique identifier for the acceptance given by the Office of Guarantee per year and country	Alphanumeric 12	1234AB788966
4	Check digit	Numeric 1	8
5	Identifier of the individual guarantee by means of voucher (1 letter + 6 digits) or NULL for other guarantee types	Alphanumeric 7	A001017

Table 48: Structure of GRN

Field 1 and 2 as explained above.
Field 3 has to be filled with a unique identifier per year and country for the acceptance of the guarantee given by the office of guarantee. National Administrations which want to have the Customs Office Reference Number of the office of guarantee included in the GRN, could use up to the first six characters to insert the national number of the office of guarantee.

Field 4 has to be filled with a value that is a check digit for the fields 1 to 3 of the GRN.
This field allows the detection of an error when capturing the first four fields of the GRN.

Field 5 is only used when the GRN is related to an individual guarantee by means of vouchers registered in the computerised transit system. In that case, this field has to be filled with the identifier of the voucher.

Based on the above, the following XSD Type (`GRNType`) will be associated with GRN data item in NCTS-P4 and NCTS-P5 as per Table 48:

```
<xs:simpleType name="GRNType">
        <xs:annotation>
                <xs:documentation> GRN (format: an..24),
(alias:GuaRefNumGRNREF21)</xs:documentation>
        </xs:annotation>
        <xs:restriction base="AlphanumericCapitalType">
                <xs:pattern value="[0-9]{2}[A-Z]{2}[A-Z0-9]{12}[0-9]([A-Z][0-
9]{6})?"/>
        </xs:restriction>
</xs:simpleType>
```

Table 49: XSD restriction for GRN data item in NCTS-P4 and NCTS-P5 *(GRNType)* as per Table 48

where `AlphanumericCapitalType` is defined as follows:

```
<xs:simpleType name="AlphanumericCapitalType ">
        <xs:restriction base="AlphaNumType">
                <xs:pattern value="[A-Z0-9]*" />
        </xs:restriction>
</xs:simpleType>
```

Table 50: XSD definition of *AlphanumericCapitalType* simple type

where `AlphaNumType` is defined Table 42.

V.7.3.1   GRN Check Character Calculation Example

The check character algorithm for the GRN is almost the same as the check character algorithm for the MRN (see section V.6.1.1). The difference is that the factors are in the range 2^0 to 2^{15} producing 16 sub-totals for the GRN.

In this example the check character (yet to be calculated) is represented as *

GRN = 05DE3300BE000106*A001017

0	5	D	E	3	3	0	0	B	E	0	0	0	1	0	6

Check character value (Table 18)

0	5	14	15	3	3	0	0	12	15	0	0	0	1	0	6

Multiplier

1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768

Values

0	10	56	120	48	96	0	0	3072	7680	0	0	0	8192	0	196608

Total   215882

215882/11= 19625 + 7/11; thus, the remainder is '7' and is used as the check digit (Table 44)

Resulting GRN (with check digit) = 05DE3300BE0001067A001017

V.8   GNSS (Global Navigation Satellite System)

In order to define the coordinates of a location, the *Information Exchange*s will include the *Data Group* 'GNSS' value with two separate *Data Items*: the *Latitude* and the *Longitude*. In order to identify the *Longitude* and *Latitude*, the WGS84 system which is the standard for GNSS is used. The regular expression provided in the table below allows *Latitude* to vary from -90 to +90 degrees (mandatory sign '-' for Southern latitude, optional sign '+' for Northern latitude) and *Longitude* from -180 to +180 degrees (mandatory sign '-' for Western longitude, optional sign '+' for Eastern longitude), thus providing global coverage. The format used must be in decimal degrees (DD). Decimal digits are always required (e.g 170.000000) and accuracy of at least 5 to maximum 7 digits must be provided.

Field	Regular Expression	Example	Len
Latitude	[+-]?([0-8]?[0-9]\.[0-9]{5,7}|90.000000?0?)	+50.842372	an..11
Longitude	[+-]?((0?[0-9]?|1[0-7])[0-9]\.[0-9]{5,7}|180.000000?0?)	+4.383993	an..12

Table 51: GNSS Coordinates format

NOTE: the value '00.000000' is a valid *Longitude* and a valid *Latitude*.

V.9   Identification Number Structure

The Identification number used for Trader identification in the context of AES-P1 and NCTS-P5 has the following format by XSD definition.

```
<xs:simpleType name="TINNewType">
    <xs:annotation>
        <xs:documentation>EORI or TCUI Number (format:
                 an..17)</xs:documentation>
    </xs:annotation>
    <xs:restriction base="AlphaNumType">
        <xs:minLength value="3"/>
        <xs:maxLength value="17"/>
        <xs:pattern value="[A-Z]{2}[!-~]{1,15}"/>
    </xs:restriction>
</xs:simpleType>
```

Table 52: XSD definition of *TINNewtype* simple type

The applicability of this XSD pattern to specific data elements is defined in DDNXA [R40] and DDNTA [R41]. Trader Identification Number should follow the EOS specifications [R23] since after the end of the Transitional Period, a valid EORI number needs to be provided for specific data elements.

The first 2 characters must be capital alphabetic characters restricted from A to Z, while the minimum length is 3 characters and the maximum is 17 characters. Whitespaces are not allowed by XSD definition (also not allowed by EOS).

VI EDIFACT message formatting

VI.1 Introduction

EDIFACT [S1] is a standard for representation of data during transmission between parties. Version 3 of this standard is used for the Customs systems.

EDIFACT anticipates a number of standard messages for various business purposes. Within Customs systems, it is foreseen to use the standard directory [S2]. Within this directory, the usage of the following standard EDIFACT messages is foreseen: CUSDEC, CUSRES, CUSCAR, PARTIN (renamed to PARTTC in this document), GESMES, GENRAL, and BANSTA. In addition, it is foreseen to use the CONTRL message [S3].

Every EDIFACT message is built according to a number of conventions:

- At the bottom, there are a number of *data elements*. These data elements have a predefined name and a type. For some data elements, the standard is foreseeing the usage of predefined *Code Lists*. The collection of data elements is common to a directory definition (all EDIFACT messages are built upon a common collection of data elements);

- *Composite data elements* are built as a sequence of individual data elements and EDIFACT *segments* are built as a sequence of composite data elements and single data elements. The collection of segments is common to all messages that are part of a directory (all EDIFACT messages are built with the same segments). A segment has a name, optionality (Mandatory or Conditional) and a maximum repeat count. Within a segment, the sequence of composite data elements and data elements is fixed. A composite data element is either Mandatory or Conditional; an individual data element is also Mandatory or Conditional. Within a composite data element, it is common to use *qualifier* values in order to denote the meaning of a particular data element (one data element then contains the qualifier while another data element contains the actual value). The standard also foresees a number of predefined qualifier values;

- EDIFACT messages are built as structures of segment groups or individual segments. A segment group is a sequence of segments. Within the structure of an EDIFACT message, there can be hierarchic levels. Within a hierarchy, every segment will have a predefined position, with an associated optionality and repeat count.

When a system is using the EDIFACT standard, it is common to define an *Interchange Agreement*. This agreement specifies how the different standards are to be applied and which common conventions need to be maintained. This section, together with the corresponding section in each Customs system specific volume, is acting as the EDIFACT interchange agreement for the Customs systems.

To be noted is that changes can be applied to the various items that are part of the EDIFACT standard:

- Overall EDIFACT message structure;

- Optionality and repeat count of the segments;

- Structure of the segments (data elements and composite data elements), optionality of these elements;

- Data types;

- Usage of Code Lists;

- Usage of qualifier values.

This section, therefore, first, specifies a number of common conventions (such as common message header structure), applying to all Information Exchanges that are exchanged using EDIFACT). Next, it defines which Information Exchanges are mapped upon which EDIFACT messages. It, then, defines, in detail, which changes have been applied to the EDIFACT standard. Finally, it defines the mapping rules (correlation between Information Exchanges and EDIFACT messages).

Messages that are exchanged by other means only (XML-format, paper, fax…) are not discussed in this chapter.

VI.2 EDIFACT conventions for Customs

The following section contains a number of rules for exchanges in the Common Domain. It is highly advisable to use the same (or similar) rules for exchanges in other Domains.

VI.2.1   EDIFACT choices

This section lists a number of choices made with respect to EDIFACT syntax options. These choices are identical to the ones made in the Single Administrative Message (SAM) Mapping Guide. They are:

1. A EDIFACT interchange starts with an interchange header segment (UNB). **The UNA segment is not used**.

2. One EDIFACT interchange contains only one message. One Information Exchange will correspond to one EDIFACT interchange, which will correspond to one EDIFACT message. Conceptually, EDIFACT enables the transmission of several messages in one interchange. Within the Common Domain, this will be restricted to one message per interchange only.

3. The following separator set is used:

   - '   Segment separator;
   - +   Data element separator;
   - :   Composite data element separator;
   - ?   Release character.

4. The decimal notation is a '.' (point).

5. Functional grouping is not used (UNG/UNE segments).

6. Nesting indicators are not used.

7. This document specifies the technical aspects of the Customs systems Interchange Agreement. Separate reference to this agreement is not required because other mechanisms like technical message structures and queue naming conventions are provided.

VI.2.2 *Common Message Header Structure*

Information Exchanges are mapped to EDIFACT UNSMs as specified in this section. Instances of these UNSMs are exchanged in interchanges. The common specification for the use of the interchange service segment UNB (present in every EDIFACT message for Customs systems) is according to the SAM Mapping Guide:

```
UNB[0], INTERCHANGE HEADER, M, 1 x                          | MESSAGE
S001    SYNTAX IDENTIFIER                         M         |
0001     SYNTAX IDENTIFIER                        M   A4    | SYNTAX IDENTIFIER (A4)
0002     SYNTAX VERSION NUMBER                    M   N1    | SYNTAX VERSION NUMBER (N1)
                                                            |
S002    INTERCHANGE SENDER                        M         |
0004     SENDER IDENTIFICATION                    M   AN..35 | MESSAGE SENDER (AN..35)
0007     IDENTIFICATION CODE QUALIFIER            C   AN..4 | SENDER IDENTIFICATION CODE QUALIFIER (AN..4)
0008     ADDRESS FOR REVERSE ROUTING              C   AN..14 | -
                                                            |
S003    INTERCHANGE RECIPIENT                     M         |
0010     RECIPIENT IDENTIFICATION                 M   AN..35 | MESSAGE RECIPIENT (AN..35)
0007     IDENTIFICATION CODE QUALIFIER            C   AN..4 | RECIPIENT IDENTIFICATION CODE QUALIFIER (AN..4)
0014     ROUTING ADDRESS                          C   AN..14 | -
                                                            |
S004    DATE/TIME OF PREPARATION                  M         |
0017     DATE                                     M   N6    | DATE OF PREPARATION (N6)
0019     TIME                                     M   N4    | TIME OF PREPARATION (N4)
                                                            |
0020    INTERCHANGE CONTROL REFERENCE             M   AN..14 | INTERCHANGE CONTROL REFERENCE (AN..14)
                                                            |
S005    RECIPIENTS REFERENCE, PASSWORD            C         |
0022     RECIPIENT'S REFERENCE/PASSWORD           M   AN..14 | RECIPIENT'S REFERENCE/PASSWORD (AN..14)
0025     RECIPIENT'S REFERENCE/PASSWORD QUALIFIER C   AN2   | RECIPIENT'S REFERENCE/PASSWORD QUALIFIER (AN2)
                                                            |
0026    APPLICATION REFERENCE                     C   AN..14 | APPLICATION REFERENCE (AN..14)
                                                            |
0029    PROCESSING PRIORITY CODE                  C   A1    | PRIORITY (A1)
                                                            |
0031    ACKNOWLEDGEMENT REQUEST                   C   N1    | ACKNOWLEDGEMENT REQUEST (N1)
                                                            |
0032    COMMUNICATIONS AGREEMENT ID.              C   AN..35 | COMMUNICATIONS AGREEMENT ID. (AN..35)
                                                            |
0035    TEST INDICATOR                            C   N1    | TEST INDICATOR (N1)
```

Table 53: Common message header structure

The left part of this table shows the EDIFACT definition of the segment. The right part shows the corresponding Data Items. All these Data Items belong to the Data Group MESSAGE, as specified for every Information Exchange.

The different items of the UNB segment are now discussed in detail. Mandatory EDIFACT data elements are the following:

Syntax Identifier: this data element is specifying the character set used in the message. This should be equal to 'UNOC". Within an EDIFACT message, the UNOC character set will be used, except for some free text fields (these may be encoded in a different character set).

Syntax version number is the current version of the EDIFACT standard. This is always equal to '3'.

In the Common Domain MESSAGE Data Group, the Data Items "Message sender" and "Message recipient" should contain the EDIFACT address within Transit or Export as defined below:

```
<Application Name>.<Country ISO Code>
```

Where <Application Name> and <Country ISO Code> can have the following values:

- <Application Name> is a valid application used in Customs, e.g. NTA, TTA, CSMIS and NECA[22];

- <Country ISO Code> is a valid ISO Country Code with the addition of 'EC' for addressing of the EC (see Transport of messages via CCN/CSI).

Examples of valid addresses are NTA.DE, TTA.EC, CSMIS.EC, NECA.DE, ATIS.EC and EUECN.EC.

This approach does not impose restrictions on an application with respect to the use of CCN/CSI. A mapping between EDIFACT addresses and CCN/CSI addresses is provided by the interface specification.

Date and **Time** are also required, being the date and time when the Information Exchange was put in an EDIFACT representation. As syntax version 3 is used, the date format in data element 0017 is limited to n6.

The **Test Indicator** requires a value '1' for communication between an NCA on the one hand and an STTA or TTA on the other hand (also during the CT Mode 3, or in PROD). Otherwise, its value is '0'. When it is not present, this should also be considered as an operational message.

Interchange Control Reference (ICR) needs to be unique for every EDIFACT interchange created by a specific Customs application. Every EDIFACT message created by the same Customs application (even if it was the same Information Exchange sent twice) should contain a unique ICR. No rules are specified for External and National Domain exchanges, although it is highly recommended to use similar conventions.

All other elements of the UNB segment currently do not have a specific meaning for Common Domain exchanges and are optional.

VI.2.3   UNH segment

Every EDIFACT exchange will contain a UNH segment. Within this segment, the only mandatory data element is the message type string. The message type is a short string denoting the Information Exchange type and the Domain in which it is interchanged. Message type strings are defined in the next chapter.

VI.2.4   Segment conventions

Some clarifications on EDIFACT standards:

---

[22] For exchanges with OLAF in the context of NCTS P4 and ATIS, the Application Name shall be "ATIS". For exchanges with the EC SPEED2 Platform in the context of the pilot project NCTS/TIR-DATA, the Application Name shall be "EUECN".

- Within every message, the last but one segment will be a UNT segment, denoting the count of the number of segments in the message. This count should include every segment in the EDIFACT message, including UNH and UNT itself but not UNB and UNZ (last segment) from the EDIFACT interchange;

- Some EDIFACT messages need to point to other segments in an EDIFACT message. In this case, segment number one is the UNH segment;

- Some segments require the presence of a segment at a higher level. This higher-level segment must always be present (even if it does not contain any data at all);

- Some segments are defined as optional. If the relevant data is not present, these segments are not to be included in the EDIFACT message.

VI.2.5   Amendments to UNSMs

The detailed structure of the UNSMs to be used for Customs systems is documented as follows:

The overall message structure is defined in the corresponding Appendix G. This Appendix defines the structure and the hierarchy of the UNSMs and the exact location of the various segments in the UNSMs.

The detailed specification of the segments is included in the corresponding Appendix H. (left-hand side).

The following paragraphs define how UNSMs have been modified in order to meet the needs of Customs systems.

It is assumed that the Customs systems' Information Exchanges need to be supported by an EDIFACT UNSM. Directory D96B is used for mapping the templates to UNSMs. If no UNSM supports the FMS requirements, an existing UNSM is adjusted to support the FMS.

In various cases, the repeat factor of segments UNSMs is insufficient. The repeat factor has been raised to meet the requirements whenever necessary. Requirements of repeat factors higher than offered by the UNSMs, is due to two reasons:

- **Proper mapping, repeat count too low**

    The first reason is the correct mapping of repeating Data Groups or Data Items to a segment with a repeat count that is too low.

- **Stuffing**

    The second reason is a semantically incorrect mapping of Data Items to segments or misusing data elements to qualify a segment, because, otherwise, the required FMS hierarchy and repeating of Data Groups would be violated.

These types of errors cannot be solved by simply reducing the repeat count of Data Groups in the FMS. It may imply deleting Data Items if repeat counts of UNSMs need to be adhered to. Therefore, the repeat factors of UNSMs have been adjusted.

The detailed list of all changes being made to the UNSM is included in Appendix H for consistency reasons. This Appendix defines the mapping of the TMS to the UNSM. This

Appendix therefore starts by providing the reader with the full list of changes to the UNSM standard.

VI.3 Mapping of Information Exchanges

For each domain specific NCTS and ECS DDNA volume ([R17] and [R18]), a corresponding chapter contains the structure of all messages and various tables that list which Information Exchanges are mapped to each EDIFACT message, e.g. CUSDEC, CUSRES, PARTTC, etc. The messages are all part of the D96B-directory.

VI.3.1 Mapping overview

In general, an Information Exchange is mapped to CUSDEC D96B when it is used to exchange declaration data or when it is the first message initiated between two communicating organisations. If an Information Exchange is a response to a received Information Exchange and is not used to exchange declaration data, it is mapped to CUSRES D96B. The other UNSMs serve specific purposes. The tables in each volume also define the message type string (to be included in segment UNH) for the various Information Exchanges.

VI.4 Message Hierarchies

The correct order of the Data Groups can be found in Appendix Y.

VI.5 Correlation tables

The correlation tables list the correlation between the Message Hierarchies (which are each mapped to one particular UNSM) and the Information Exchanges and can be found in the Appendix I of the NCTS and ECS domain specific DDNA volumes ([R17] and [R18]).

Thus, only Information Exchanges that need to be sent in EDIFACT-format will be found in these correlation tables.

The right-hand side of Appendix H defines the direct correlation between the UNSM segments and the Data Items.

VI.5.1 EDIFACT Mapping

- Appendix I of NCTS and ECS domain specific DDNA volume ([R17] and [R18]) specifies the correlation between the Technical Message Structure (and all its composites) and the data elements of the EDIFACT messages. For each mapping of a message to an EDIFACT message, a Correlation Table is given. Many Information Exchanges can be mapped to the same EDIFACT messages.

These correlation tables contain the following columns:

- **SAD Box**

  It specifies the box used in the SAD (Single Administrative Document). It is only given for those Data Items for which a SAD box has been identified in the SAM project. This column is only applicable to the mapping of the Core Information Exchanges.

- **Name**

  It specifies the name of the box used in the SAD (Single Administrative Document). It is only given for those Data Items for which a SAD box has been identified in the SAM project. This column is only applicable to the mapping of the Core Information Exchanges.

- **Elements**

  Hierarchy level, specifying the origin of the information to map into the EDIFACT element. The higher level Data Groups are separated from the (lower level) Data Groups by a '-'. An example is 'GOODS ITEM – PACKAGES' where 'GOODS ITEM' is the higher level Data Group and 'PACKAGES' is the concerned Data Group. The information in this column refers to the *Message* Hierarchy.
  Data Item (after the full stop) specifies the actual name of the application Data Item to map into the EDIFACT data element.

- **Data type**

  It describes the type and the length of the Data Item. When a data-type includes a decimal, the maximum number of decimals after the decimal sign is included in the length of the data-type. For instance, the format n..11,3 can have 3 decimals included in its maximum total length of 11 numeric digits. Neither the decimal point nor the sign are included in the length of a data-type, so allowance has to be made for this where necessary.

- **Status (numbered columns)**

  It specifies if the Data Item is required [R], dependent [D] or optional [O] per Functional Message Structure. The status given in a column needs to be read in conjunction with the status of the Data Group specified by the message hierarchy. For instance, the status in a column may read R (required), whereas the status of the related Data Group in the message hierarchy reads O (optional, see Appendix Q). In those cases, the entry in the column is required only when the related Data Group is used.

- **Pos**

  It identifies the EDIFACT segment according to its position in the standard message. The position refers to the branching diagram. The UNB segment is shown as position 0 as it is the interchange header and not part of the message. (Although not part of the formal DDNA review package, branching diagrams are provided in Appendix G for information).

- **EDIFACT mapping**

  It gives the mapping information referring to one particular data element in a segment of a particular EDIFACT message, possibly with reference to all applicable qualifier

values. Furthermore, the position number of the segment is given. An example is given by FTX[11](4451=ABL).C108.4440, which is the mapping to data element 4440 of composite C108 with qualifier value 'ABL' for element 4451 of the FTX segment at position 11 of the EDIFACT message. In some occasions, a data element is not uniquely identified within a composite or a segment. In those cases, the mapping information is followed by '#' and the sequence number of that particular data element. For instance, FTX[11](4451=ABL).C108.4440#2, is a mapping to the second free text data element of the composite identified by C108 in the segment FTX. In case no qualifier value is required, e.g. a mapping is constructed to a qualified segment only for one Data Item, this is indicated by a '-' as the value for a qualifier (the qualifier data element is conditional in those occasions). In case all qualifier values are allowed for a particular mapping, this is indicated by a '*' as the value for a qualifier.

It may appear occasionally that, although this is not mentioned, the number of occurrences of an EDIFACT segment is higher than the maximum allowed by the CUSDEC. However, the number of occurrences always needs to be read in conjunction with the status given by one of the columns.

In some instances, the Correlation Table does not have an entry for data elements of the service segments. This is applicable to those data elements that have a fixed value; e.g. data element 0002 always has the value '3' identifying the syntax version. Those EDIFACT service elements that cannot be found in the Correlation Table are available in the segment description.

Mappings can be constructed to repeating composite data elements within one segment. EDIFACT prescribes that the first composites of a segment need to be filled, which implies that the filling of a composite is independent of its position in a segment. However, if the composite does not contain a composite qualifier and the mapping of a Data Item is fixed by a composite's position in a segment, it implies that data for such a Data Item is always mapped to the same position in a segment independent of empty composites before that position.

- **Code List**

  If a Code List can and should be applied to the Data Item, the reference number of this Code List is listed in this column. The full set of Code Lists is maintained in CS/RD2. For NCTS-P4 and ECS-P2, where EDIFACT message exchange is applicable, the Technical code lists are also maintained in Appendix C of DDNA.

VI.6 Functional error message in EDIFACT

VI.6.1   Functional error CUSRES Hierarchy

The Data Group 'FUNCTIONAL ERROR' of IE906 points to a certain Data Item in an FMS.

The IE906 refers to the message in which the error has been detected with the reference number of that message (MESSAGE.Original message identification). A message reference number is uniquely assigned by a sender of a message (Technical Message Structure).

Functional errors are exchanged by D96B CUSRES. The Data Group 'FUNCTIONAL ERROR' is mapped to an FTX segment.

The hierarchy is given as follows:

```
    MESSAGE                                    1 x,     R
        HEADER                                 1 x,     D
        FUNCTIONAL ERROR                     999 x,     R
```

VI.6.2   EDIFACT Mapping of Functional error message

The Data Item HEADER.Declaration type is required to be able to map to the mandatory EDIFACT BGM segment and to be in line with all other FMS mapped to CUSRES.

The correlation tables can be found in the corresponding Appendix I of this DDNA.

VI.7 EDIFACT CONTRL Message

VI.7.1.1   General

The EDIFACT CONTRL message structure is used to exchange errors detected in a received interchange. The minimal requirement is to report the first error detected. All other detected errors should be reported if possible.

The structure of CONTRL is based on four segments: UCI (Interchange Level), UCM (Message Level), UCS (Segment Level) and UCD (Data Element Level), each containing a reference to a part of the subject interchange. The parts of the subject interchange are:

- The UNB and UNZ segments, referenced in the UCI segment. UCI refers to the original EDIFACT interchange in which errors have been detected, by copying the sender identification, recipient identification, and interchange reference of that erroneous interchange;

- The UNH and UNT segments, referenced in the UCM segment. UCM refers to the original EDIFACT message in which errors have been detected, by copying the message reference and the message type/version/release number/controlling agency/association assigned code of that erroneous message. The action taken by the recipient of the erroneous message as well as the specific error information (error code – message segment – position in this segment) is transmitted;

- A segment in a message, referenced in the UCS segment. UCS refers to a position of a segment for which an error has been detected in the original EDIFACT message, by means of a segment position. The segment position is a sequence number of the erroneous segment in the EDIFACT message. It starts with and includes the UNH segment as segment number '1'. To report a missing segment, this is the numerical count of the last segment that was processed before the position where the missing segment was expected to be. Identifying the first segment in the group as missing denotes a missing segment group;

- A simple, composite or component data element referenced in the UCD segment. UCD refers to a position of a data element in a segment for which an error has been detected in the original EDIFACT message. EITHER the data element position is a counter of all fields starting at '1' for the segment tag OR, if the information can be supplied by the EDI-converter, the data element position is a counter of simple and composite fields starting at '1' for the segment tag and the data component position is the position of the component within the composite field.

On receipt of a CONTRL message, it must be possible to display and/or print the position of an error, regardless of whether a component position is present or not

The UCI segment can only report one error. If more than one error is detected at interchange level, the receiver of the interchange is free to choose which error to report.

It is not allowed to exchange more than one CONTRL message to report several errors in the same interchange.

The list of allowed error codes is maintained in CS/RD2 (CL023) and also in the Appendix C of DDNA.

The structure of the CONTRL is based on the assumption of one message per EDIFACT interchange.

The message type as exchanged in the association assigned code of the EDIFACT message header (UNH.S009.0057) of the EDIFACT CONTRL is CD907A, where CD indicates the exchange across the Common Domain. The use of the CONTRL in the External Domain is up to each NA.

Should an error be detected in a CD907A, no further message is exchanged but as much data as possible provided for manual intervention.

VI.7.1.2 CONTRL correlation table

The correlation table can be found in the corresponding Appendix I of this DDNA.

VI.7.1.3 CONTRL building rules

At every one of the levels UCI, UCM, UCS or UCD an error, detected at the corresponding level (UNB, UNH, segment, and data element) in the subject interchange, can be specified. Logically, only the error at the right level (and only up to that level) needs to be specified.

Note that the Data Item specifying the error at UCI level is called 'Syntax Error' because at this level, it will always concern an error against EDIFACT syntax rules.

This leads to two Technical Rules for IE907 (TR0901, TR0902), which are documented in Appendix Q.

VII XML message formatting

VII.1 Introduction

VII.1.1 XML

The Extensible Markup Language (XML) is a subset of SGML. Its goal is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML[23].

VII.1.2 Character set support

XML documents always use one encoding, which is specified in the prologue of the document. This encoding will be UTF-8. Unicode is obligatory from the moment that the document contains characters from more than one ISO-8859 character set. The character sets supported by CS/RD2 and used in XML messages as Codelist values are defined in DDRDA [R27].

VII.2 XML mapping of Information Exchanges

The XML mapping of all Information Exchanges for movement systems can be found in the corresponding Appendix R of DDNA volumes. This Appendix includes the XML definition of all Information Exchanges for movement systems.

---

[23] The complete specification of XML 1.0 can be found at http://www.w3.org/TR/xml/

VII.3 XML mapping of Information Exchanges for AES-P1 and NCTS-P5

For all XML mappings (XML Tags) the following naming convention will be applied:

Data Element Type	XSD Type	Naming Convention	Examples	
			Data Element	**XML Tag**
Data Item	Simple	IF acronym THEN Upper Case all letters ELSE camel**C**ase format	MRN	MRN
			Declaration date	declarationDate
			Presentation notification rejection date	presentationNotificationRejectionDate
Data Group	Complex	IF acronym THEN Upper Case all letters ELSE **P**ascal**C**ase format	GNSS	GNSS
			GOODS SHIPMENT	GoodsShipment
			TRANSPORT EQUIPMENT	TransportEquipment
			ADDITIONAL SUPPLY CHAIN ACTOR	AdditionalSupplyChainActor

Table 54: XML Tags naming conventions for NCTS-P5 and AES-P1

VII.4 Document Type Definition

The DTDs for all messages used in NCTSP4 and ECSP2 are described in the corresponding Appendix T. DTDs are not applicable for AES-P1 and NCTS-P5 where the message structure is specified only by the XSDs included in Appendix X.

VII.5 XML error (CONTRL) message

The XML CONTRL message structure (IE917) is used to exchange errors detected in a received XML message. The minimal requirement is to report the first error detected. All other detected errors should be reported if possible.

It is not allowed to exchange more than one XML CONTRL message to report several errors in the same interchange. The structure of the XML CONTRL is based on the assumption of one message per XML interchange. The message type of this XML CONTRL is the CD917B (ICS-P1) or CD917C (NCTS-P5 and AES-P1), where CD indicates the exchange across the Common Domain.

Data Item	Content	Status	IE917B Format	IE917C Format
Error line Number	The line and column of the error are two required numeric data items used to specify the location of the error. The XML parser or the XML validator can be used to provide values for the two data items.	Required	n..9	n..9
Error column Number		Required	n..9	n..9
Error code	This data item is required and it is used to codify the error on a message. The values for this data item are specified in the relevant Codelist of CS/RD2 (Also in Appendix C for ICS [R18]).	Required	n2	n2
Error reason	The Error reason is a required alphanumeric data item that contains the text of the error returned by the XML parser or the XML validator.	Required	an..350	an..512
Error pointer	The Error pointer is an optional alphanumeric data item that may contain the XPath location of the error. Since XPath locations require a valid XML file, this data item is optional in case of an XML parsing error. Even for XML schema error, this data item is optional since not all XML parsers report the location of the error as XPath. If the XPath string is to be truncated (i.e. if the length of the string is greater than 350 characters long), then the data item should not be used.	Optional	an..350	an..512
Original attribute value	The Original attribute value is an optional alphanumeric data item that should be used when the error is an XML schema error concerning invalid values. The reasons for considering an attribute value invalid might be the format and/or a value for a technical code list. For such cases, the data item should contain the value of the invalid value in order to indicate which value was perceived invalid.	Optional	an..350	an..512

Table 55: Data Items for XML Error data group in IE917

Should an error be detected in a CD917B/CD917C, no further message is exchanged but as much data as possible provided for manual intervention.

The CD917C uses the same Message Header for NCTS-P5 and AES-P1 (see section VII.7).

It is recommended that NAs are following the same approach in External Domain exchanges for XML errors.

VII.6 Message Header for ICS-P1

This section provides information about the data items of the MESSAGE data group of XML messages.

VII.6.1 Message Sender and Message Recipient

In the MESSAGE Data Group, the Data Items "Message sender" and "Message recipient" contain the address within the specific Customs domain (e.g. NCTS, ECS or ICS), defined as follows:

- **Message Sender** field is required for detecting the proper sender at reception. The following structure shall be used for this field: `<Application Name>.<Country ISO Code>`

- **Message Recipient** field is required for sending a message to its proper destination. The following structure shall be used for this field: `<Application Name>.<Country ISO Code>`

Where:

- `<Application Name>` is a valid application used in Customs, e.g. NICA in ICS domain, TTA, CSMIS, etc;

- `<Country ISO Code>` is a valid ISO Country Code with the addition of 'EC' for addressing of the EC (see Transport of messages via CCN/CSI).

Examples of valid addresses are NICA.DE, TTA.EC, and CSMIS.EC.

The above approach does not impose restrictions on an application with respect to the use of CCN/CSI. A mapping between XML addresses and CCN/CSI addresses is provided by the interface specification.

VII.6.2 Message Type

Message Type field is required since it contains a string identifying the number of the IE, the domain in which it is used, and the version.

The Message Type shall have the following structure:

- **External/National Domain Exchanges** = CC[24]<IE Number>A or B[25] or <ISO Country Code><IE Number>A or B

---

[24] Optionally CC may be replaced with the ISO Country Code of the NA that exchanges an Information Exchange within the National domain.

[25] Represents the version of the FMS structure.

- **Common Domain Exchanges** = CD<IE Number>A or B or C[26]

Please note that the aforementioned message type for External/National Domain exchanges should be considered only as recommendation. Only the structure for Common Domain Exchanges is required.

The message types for the Common Domain Exchanges in NCTS, ECS and ICS are defined in the Codelist CL060 in CS/RD2.

Examples of valid message types for NCTS, ECS and ICS are: "CD301A" and "CD319A".

VII.6.3   Date & Time of preparation

Date and **Time** are also required, being the date and time when the Information Exchange was put in an XML representation.

VII.6.4   Test Indicator

The **Test Indicator** requires a value '1' for communication between an NCA on the one hand and STTA or TTA (or CTA once available for ICS-P1) on the other hand. The same applies for CT Mode 3. Otherwise, its value is '0'. When it is not present, this should also be considered as an operational message.

VII.6.5   Message Identification

The Data Item 'Message Identification' needs to be unique for every XML interchange created by a specific Customs application. Every XML message created by the same Customs application (even if it was the same Information Exchange sent twice) must contain a unique Message Identification. No rules are specified for External and National Domain exchanges, although it is highly recommended to use similar conventions.

VII.6.6   Original Message Identification

In case of Functional errors or XML errors in ICS-P1, the Message identification of the rejected message must be filled in the "Original message identification" data item of the XML header.

VII.6.7   Correlation Identifier

In case of Functional errors or XML errors in ICS, the message identification of the rejected messages must be filled in the "Correlation identifier" data item of the MESSAGE data group. This data item must also be used in case of response messages to indicate the message identification of the pertinent request message. Otherwise, this data item shall not be used.

---

[26] Represents the version of the FMS structure.

VII.7 Message Header for NCTS-P5 and AES-P1

This section provides information about the data items of the MESSAGE data group of XML messages.

VII.7.1   *Message Sender and Message Recipient*

In the MESSAGE Data Group, the Data Items "Message sender" and "Message recipient" contain the address within the specific Customs domain , defined as follows:

- **Message Sender** field is required for detecting the proper sender at reception. The following structure shall be used for this field: `<Application Name>.<Country ISO Code>`

- **Message Recipient** field is required for sending a message to its proper destination. The following structure shall be used for this field: `<Application Name>.<Country ISO Code>`

Where:

- `<Application Name>` is a valid application used in Customs, e.g. NECA in AES-P1 domain, CSMIS, etc;
- `<Country ISO Code>` is a valid ISO Country Code with the addition of 'EC' for addressing of the EC (see Transport of messages via CCN/CSI).

Examples of valid addresses are NECA.FI, NTA.GB and CSMIS.EC.

The above approach does not impose restrictions on an application with respect to the use of CCN/CSI. A mapping between XML addresses and CCN/CSI addresses is provided by the interface specification.

VII.7.2   *Message Type*

Message Type field is required since it contains a string identifying the number of the IE, the domain in which it is used, and the version.

The Message Type shall have the following structure:

- **External/National Domain Exchanges**[27] =

    CC<IE Number>C[28] or <ISO Country Code><IE Number>C[28]

- **Common Domain Exchanges** = CD<IE Number>C[28] or D[29]

---

[27] Optionally CC may be replaced with the ISO Country Code of the NA that exchanges an Information Exchange within the National domain.

[28] Represents the version of the FMS structure.

[29] This is applicable for IE411.

Please note that the aforementioned message type for External/National Domain exchanges should be considered only as recommendation. Only the structure for Common Domain Exchanges is required.

The message types for the Common Domain Exchanges in NCTS-P5 and AES-P1, are defined in the Codelist CL060 in CS/RD2.

Examples of valid message types: "CD501C" and "CD001C".

VII.7.3   *Message Timestamp*

Message Timestamp is also required and provided in a single element, being the date and time when the Information Exchange was put in an XML representation.

Please refer to Date/Time definition in section V.2.1.1.3.

VII.7.4   *Message Identification*

Message Identification needs to be unique for every XML interchange created by a specific Customs application. Every XML message created by the same Customs application (even if it was the same Information Exchange sent twice) must contain a unique Message Identification. No rules are specified for External and National Domain exchanges, although it is highly recommended to use similar conventions.

VII.7.5   *Correlation Identifier*

In case of Functional error (e.g. CD906C), XML error (e.g. CD917C) and response message (e.g. CD503C), the "Message identification" of the response or rejected message must be filled in the "Correlation identifier" data item of the XML header of the control or response message, to facilitate the correlation of messages at business level. The correlation of messages at network level for use by external application (e.g. CS/MIS) is performed at CCN/CSI envelope and it is described in VIII.2.1.

VII.8 XSD Principles for NCTS-P4, ECS-P2 and ICS-P1

The herein section defines the XSD Conventions as well as the proposed structure of the XSDs to be used for NCTS/ECS/ICS domains. These conventions primarily ensure the compliance with the current DTD structure. The assembled XSDs should respect that no structural modification is imposed to DTDs after the introduction of XSDs for validation of NCTS/ECS/ICS XML messages. The Specs Manager application holds the message structure information for the aforementioned domains and exports the DTDs and XSD files that are compliant to the XSD conventions mentioned in this section.

VII.8.1   XSD Conventions

The following conventions shall be respected by the generated XSDs:

- **Inter-domain XSDs:** XSDs export mechanism shall identify simple types that are shared between the domains and define them in inter-domain XSDs. In order for a simple type to be regarded as common it shall share the same code, name, format and values amongst the domains for which the export takes place. The resulting inter-domain XSDs shall be consequently imported by all message-specific XSDs;

- **Domain Specific XSDs:** XSD files shall be categorised, in the context of a single domain, as shared or Message_specific. Shared XSDs shall contain definitions of simple or complex types that have been identified to be shared between more than one messages of the domain. Message_specific XSDs shall contain the structural definition of a specific XML message and thus message-specific XSDs shall have one to one cardinality with the XMLs of each domain. All shared XSDs of a domain shall be referenced by the Message_specific ones in order to make use of the simple or complex types defined in the former;

- **Common Simple types:** shall be defined in a single, common XSD for all data items that are based on a specific pattern (e.g. MRN) or have a common format (e.g. date);

- **Common Complex types:** shall be defined in a common XSD per domain. Complex types shall be identified as common as long as they share the same structure;

- **Technical Codelists:** shall be defined as simple types in a separate, domain-specific or inter-domain XSD. Whenever a data item of a message is linked to a technical Codelist , this item shall have the corresponding type defined in the technical Codelists' domain-specific XSD (see section VII.8.4.4);

- **Message-specific XSDs:** shall define the structure of each message and reference the shared domain or inter-domain XSDs when required. A data element that is associated to a Codelist will be defined by either a type of domain-specific or inter-domain XSD where common Codelists are defined;

- **Datagroups repetitions:** shall be defined in the XSDs using the attribute "maxOccurs";

- **Optionality:** optional data items or data groups shall be defined in the XSDs by setting the "minOccurs" attribute of the corresponding element equal to zero. If this attribute is not used, the data item or data group is required;

- **Root Element:** each message shall have its Message Type as root element and the children of the Root Element will be a list of data items (simple types) and data groups (complex types);

- **XSD documentation:** definition of each simple or complex type shall be documented by specific elements. Those elements shall contain information related to description, and applicable rules or conditions. Those documentation elements shall in turn be defined in a shared XSD;

- **Comments:** each generated XSD shall begin with a comment indicating the DDNA and/or RFC-List version to which is aligned to at the moment of extraction;

- **Namespaces**: each XSD has to "import" the required namespaces and then reuse the necessary components by using its origin (i.e. the namespace) as a prefix. Each XSD file is associated with a distinct namespace;

- **Hiding of namespaces:** in order to eliminate impact on existing applications and to hide the namespaces within schemas, the 'elementFormDefault' and 'attributeFormDefault' attributes for all schemas have defined value 'unqualified'. When the namespaces must be exposed, the attributes value must be set to 'qualified' for all involved schemas.

VII.8.2 XSDs' File Structure

The current sub-section describes how the XSD conventions defined in VII.8.1 are realised in terms of XSDs file structure. The XSDs to be generated can be at high level distinguished as "domain specific" and "inter-domain". Inter-domain XSDs as already mentioned shall be applicable to message-specific XSDs of all domains. Domain Specific XSDs shall be applicable per domain containing definition of Simple and Complex types. Domain Specific XSDs can be further categorised as Message_specific and Domain shared XSDs. The following figure provides a high level visualisation of the XSDs categorisation.
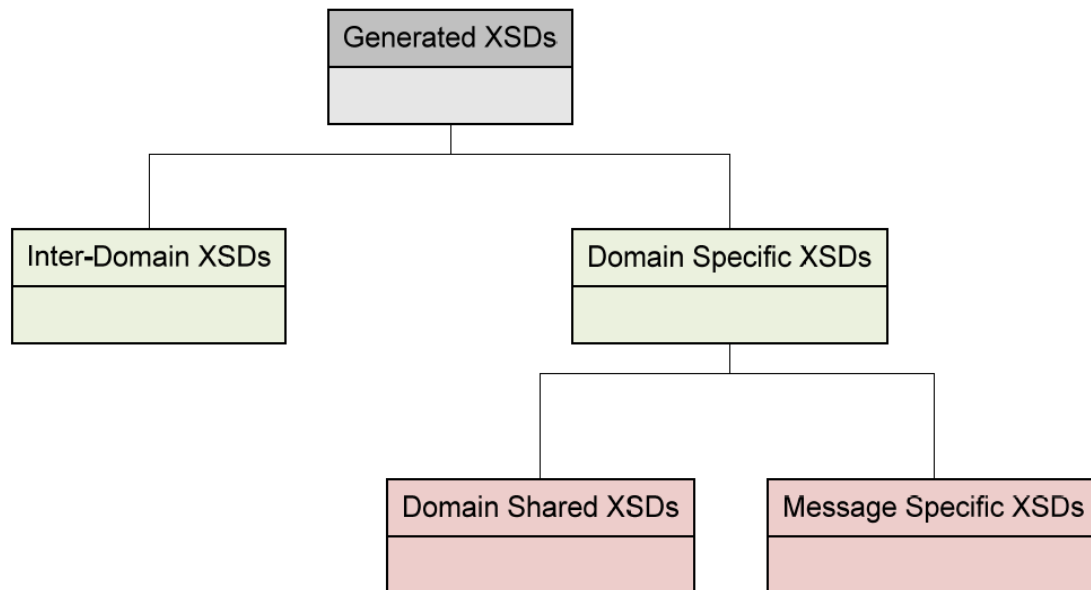
Figure 20: XSDs' Categorisation

Domain Shared XSDs shall contain definition of Simple and Complex types that are shared between messages of the specific domain. Simple types defined in Inter-Domain XSDs shall not be redefined in the Domain Specific ones. Message_specific XSDs shall contain the definition of the structure for each domain message and shall exist for each message of the domain.

The following figure provides an illustration of the structure of the XSD files as they will be extracted from the Specs Manager for a single domain.
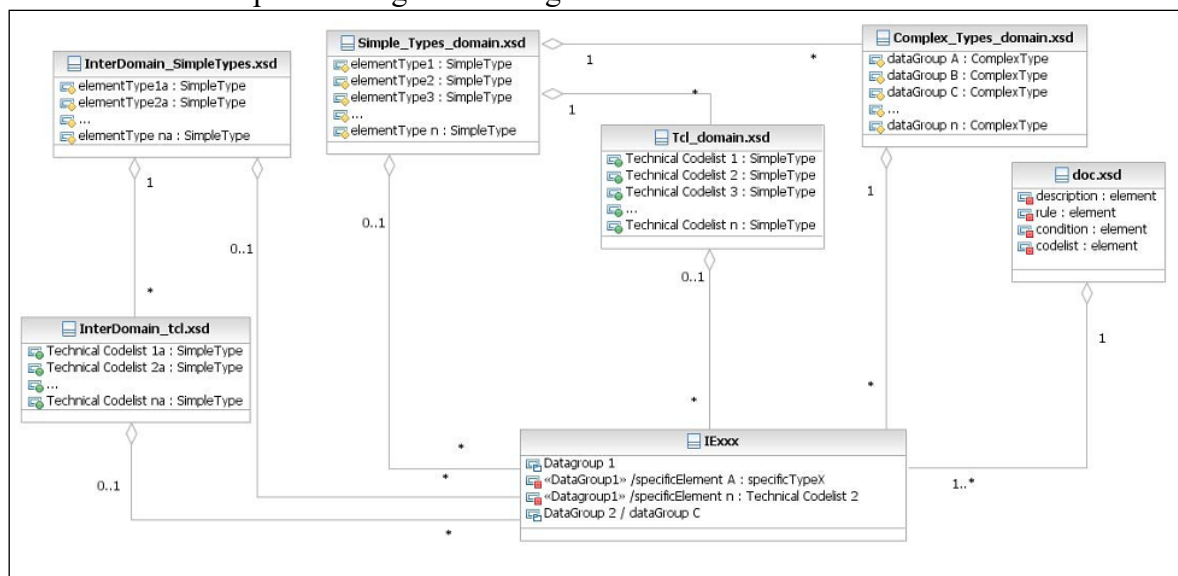
Figure 21: XSDs' File Structure

A short description of the Domain Shared XSDs is provided below:

- **Documentation (doc.xsd):** shall contain the template definition of documentation elements (rules, conditions, Codelists and descriptions) that are being further declared in the message-specific or common XSDs. The specific file shall be used for documentation purposes only and no validation of Codelists, rules or conditions shall be performed by the elements of that file;

- **Simple Types XSD (Simple_types_domain.xsd):** shall contain the definition of data items that are used in the message-specific as well as in other common XSDs. Definition of those types shall contain the type (alphanumeric, numeric etc) and format, pattern definition. Simple Types that are identified to be repeatedly defined in messages of the same domain shall be grouped under a common definition;

- **Technical Codelists XSD (tcl_domain.xsd):** shall contain the definition of technical Codelists for a specific domain as simple types. It shall provide the definition of their type (e.g. string,integer, etc.) and an enumeration of the applicable values;

- **Common Complex Types XSD (Complex_types_domain.xsd):** shall contain the definition of data groups used in message-specific XSDs. Complex Types that are identified to be repeatedly defined in messages of the same domain shall be grouped under a common definition;

- **Message_specific XSD (IExxx):** shall define only the structure of each message. Definition of simple or complex types shall be achieved by referencing the domain or inter-domain XSDs that contain the required definition.

As with the case of common files in a single domain, inter-domain common files shall be also referenced by Message_specific XSDs of all domains as shown above. A short description of the inter-domain XSDs follows:

- **Common Simple Types XSD (Simple_types.xsd):** shall contain the definition of data items that are commonly used in all message-specific XSDs of all domains;

- **Technical Codelists XSD (tcl.xsd):** shall contain the definition of shared technical Codelists for all domains. Values are maintained in CSRD2 and are part of Appendix X.

VII.8.3   XSDs Binding

As shown in Figure 21 there is a certain degree of interdependency between the XSD files, whether those are message-specific or common. In order to realise that interdependency and assemble the XSDs, XML Schemas <import> element will be used.

VII.8.4   Internal Structure of XSD Files

The current section provides an overview of the internal structure per XSD type as well an example of their application to define simple and complex types.

VII.8.4.1   Message-specific XSDs

Each message-specific XSD shall define the structure of the pertinent IE. In order for data items and groups to be defined, each Message_specific XSD shall contain reference to the Common XSDs of its domain as well as to the inter-domain ones. The XSD structure is compliant to the characteristics presented below:

- **Root Element:** is the type of message. As shown in Figure 22, CD301A is the root element of the XSD;

Message Structure / Datagroups: Datagroups ordered under Root Element define the message structure as shown in Figure 22. Data-groups in dashed line shall be defined as required while those with solid line are defined as optional. Documentation elements provide additional information per datagroup, such as description and applicable rules/conditions. Each datagroup consists of data items. Datagroups identified during generation to have a common list of elements are defined in shared XSD (Common complex type XSD for domain) and referenced in the Message_specific XSD;

Figure 22: Root Element and Message data-groups

- **Message Structure / Data Items:** data items and data groups ordered under XSD root element define message structure, thus the format of information related to the message. Data-items that share common definitions in terms of format are defined in domain or inter-domain shared XSDs and referenced in Message_specific XSDs.

The XSD conventions should follow the principles that are currently in place. As a result, the Root Element of the XSD shall define the Message Type. The Root Element shall contain the structure of the message according to its TMS presented in Appendix Q2 and T of the relevant DDNA specific volume ([R16], [R17] and [R18]). A list of simple type data items and a list

of complex type data groups shall be ordered as in the pertinent DTD. It should be also mentioned that the same XML tags shall be preserved.

In addition, a message-specific XSD per CS/RD2 message shall be present for each domain, maintaining the current structure of the CS/RD2 messages.

VII.8.4.2 Simple Types XSD (Simple_Types_domain.xsd / Simple_Types.xsd)

Simple types shall be defined in domain (Simple_Types_domain.xsd) or inter-domain (Simple_Types.xsd) XSDs depending on their scope.

Simple types whose scope is limited to a single domain shall be defined in XSDs specific to a domain (e.g. Simple_Types_NCTS.xsd, Simple_Types_ECS.xsd, Simple_Types_ICS.xsd). Simple types that have been identified as shared between more than one domain shall be defined in a shared XSD (simple_types.xsd). Internal structure of both domain specific and inter-domain XSDs shall be similar. Each XSD shall initially define Base Types. Base types shall merely define the type and or size of simple types. Base types shall be further restricted by patterns and or size limitations and thus Specific types shall be defined. An example is presented in Figure 24, where a specific type DocNumHEA5Type is defined for the DocNumHEA5 data item by applying an additional pattern restriction[30] to the Alphanumeric which in that case is the base type.

If a data item is not associated to a technical Codelist in Appendix Q2 of the relevant DDNA specific volume ([R16], [R17] and [R18]), this data item shall be defined in the Message_specific XSD with the corresponding specific type that represents the format of the data item in the types' domain-specific XSD.

As already mentioned in case of multi-domain XSDs generation, Specs Manager shall identify all commonly defined simple types and define them in an inter-domain XSD for Simple Types.

```
<xs:simpleType name="Alphanumeric">
<xs:restriction base="xs:token">
      <xs:pattern value="."/>
</xs:restriction>
```

Figure 23: Abstract type definition for alphanumeric format

```
<xs:simpleType name="DocNumHEA5Type">
      <xs:restriction base="Alphanumeric">
            <xs:length value="21"/>
            <xs:pattern value="[0-9]{2}[A-Z]{2}[A-Z0-9]{13}[0-9] "/>
      </xs:restriction>
</xs:simpleType>
```

Figure 24: Specific type definition for DocNumHEA5

---

[30] This pattern restriction is based on the definition that appears in the "Proposal for Structure of Reference Numbers in NCTS-DGXXI/0627/97-Rev.3" and in the "Check Character Algorithm for the MRN and GRN-DGXXI/0879/99- Rev.3".

VII.8.4.3   Complex Types XSD (Complex_Types_Domain.xsd)

Complex Types that shall be identified to be shared between more than one messages of the same domain shall be defined in common XSD per domain (e.g. Complex_Types_NCTS.xsd, Complex_Types_ECS.xsd, Complex_Types_ICS.xsd). That way definition of commonly used Complex types per domain shall be shared for the Message_specific XSDs. Structurally wise, Complex_Types_Domain.xsd shall be fairly simple as it will comprise of a list of complex types definitions.

Complex types XSD shall define the structure of complex types that have been identified as common in Message_specific XSDs of the same domain. Complex types shall be referenced in the Message_specific XSDs where the structure of a message shall be defined. The following example in Figure 25 illustrates the definition of Risk Analysis complex type in complex_types_ics.xsd. The specific complex type has been identified to be shared between multiple Message_specific XSDs of ICS.
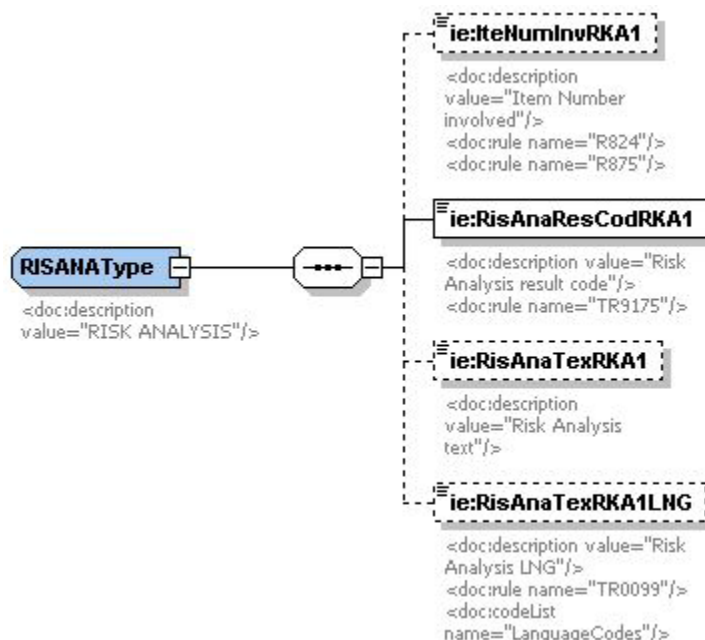
Figure 25: Definition of Risk Analysis complex type

The following figure illustrates how RISANAType is referenced in Message_specific XSD in order to define data-group CD301A.RISANA.
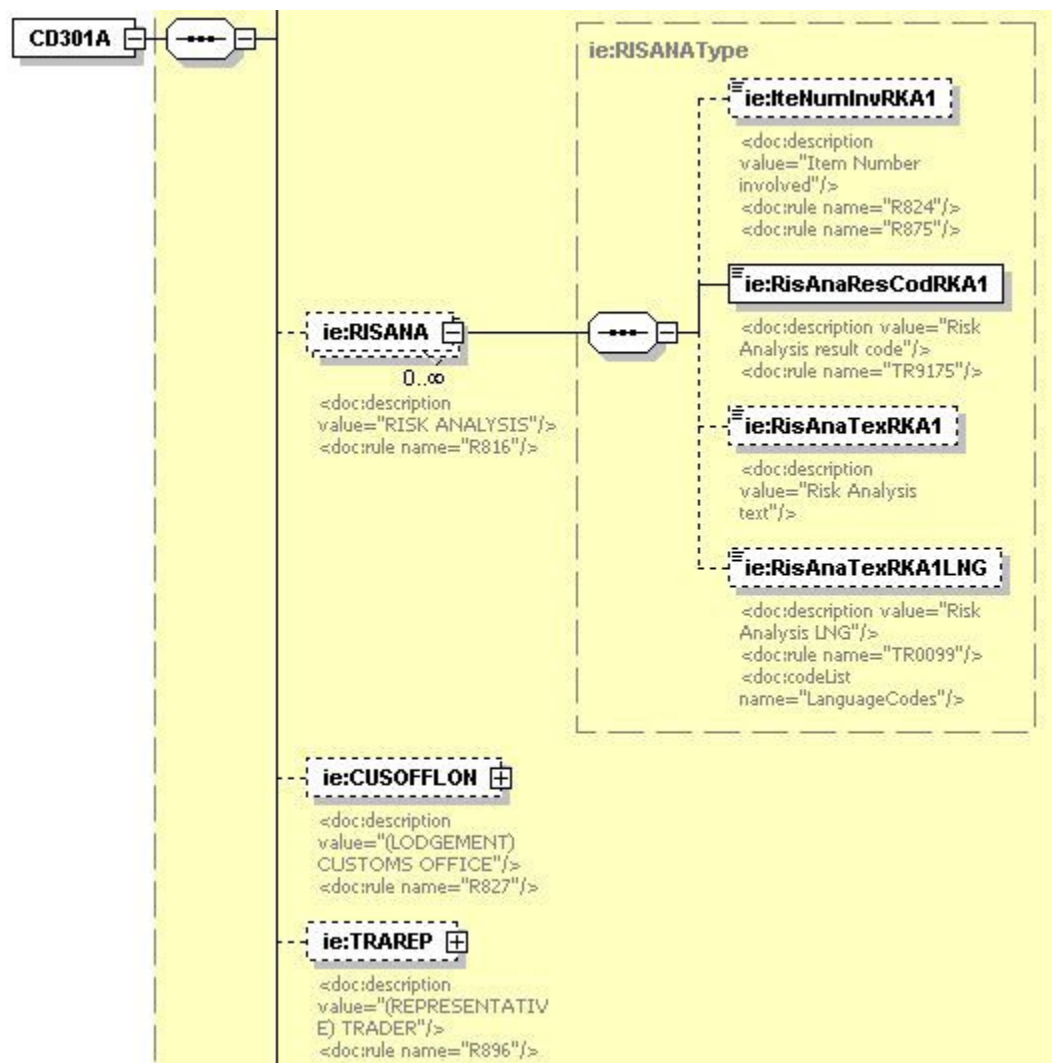
Figure 26: Definition of CD301A.Risk Analysis

VII.8.4.4   Technical Codelists XSD (Tcl_domain.xsd / Tcl.xsd)

Technical Codelists shall be defined in domain (Tcl_domain.xsd) or inter-domain (Tcl.xsd) XSDs depending on their scope. Structure of abovementioned XSDs shall be similar, since both shall consist by a list of simple types as the one shown in Figure 27.

Technical Codelists whose scope is limited to a single domain shall be defined in XSDs that apply to the specific domain (Tcl_NCTS.xsd, Tcl_ECS.xsd, Tcl_ICS.xsd). Technical Codelists that have been identified as shared between more than one domain shall be defined in a shared XSD (tcl.xsd). The latter shall be referenced by Message_specific XSDs of all domains. If a data item is associated with a technical Codelist, according to Appendix Q2 of the relevant DDNA specific volume ([R16], [R17] and [R18]), this data item shall be defined in the message-specific XSD by reference to the pertinent Codelist definition in the technical Codelists' common XSD (tcl_domain.xsd or tcl.xsd).

If a data item is associated with a technical Codelist, according to Appendix Q2 of the relevant DDNA specific volume ([R16], [R17] and [R18]), this data item shall be defined in the message-specific XSD by reference to the pertinent Codelist definition in the technical Codelists' common XSD (tcl_domain.xsd or tcl.xsd).

An example is presented in Figure 27, where the Message Type data item is defined as of type "MessageTypes", which represents the relevant technical Codelist in the technical Codelists' XSD.

Codelists are maintained in CS/RD2. For NCTS-P4, ECS-P2 and ICS-P1, the Technical code lists are also maintained in Appendix C and are part of Appendix X of DDNA.

```xml
<!--==========================================-->
<!--===== Message Types =====-->
<!--==========================================-->
<xs:simpleType name="MessageTypes">
    <xs:annotation>
        <xs:documentation>Message Types</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:token">
        <xs:enumeration value="CC004A">
            <xs:annotation>
                <xs:documentation>Amendment acceptance
</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="CC005A">
            <xs:annotation>
                <xs:documentation>Amendment Rejection
</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="CC007A">
            <xs:annotation>
                <xs:documentation>Arrival notification
</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="CC008A">
            <xs:annotation>
                <xs:documentation>Arrival notification
rejection</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="CC009A">
            <xs:annotation>
                <xs:documentation>Cancellation decision
</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="CC014A">
            <xs:annotation>
                <xs:documentation>Declaration cancellation
request</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="CC015B">
            <xs:annotation>
                <xs:documentation>Declaration data
</xs:documentaxion>
            </xs:annotation>
```

```
            </xs:enumeration>
            <xs:enumeration value="XXXX">
                    ....

            </xs:enumeration>

        </xs:restriction>

</xs:simpleType>
```

Figure 27: Technical Codelist definition for MessageTypes

VII.9 XSD Principles for NCTS-P5 and AES-P1

The herein section defines the XSD Conventions as well as the proposed structure of the XSDs to be used for NCTS-P5 and AES-P1 domains. Specs Manager application has been adapted in order to export XSD files that are compliant to the XSD conventions mentioned in this section.

VII.9.1   XSD Conventions

The following conventions shall be respected by the generated XSDs:

- **Domain Specific XSDs:** XSD files shall be categorised, in the context of a single domain/phase (e.g. AES-P1), as shared or Message_specific. Shared XSDs shall contain definitions of simple and complex types that have been identified to be shared between more than one messages of the domain. Message_specific XSDs shall contain the structural definition of a specific XML message and thus message-specific XSDs shall have one to one cardinality with the XMLs of each domain. All shared XSDs of a domain shall be referenced by the Message_specific ones in order to make use of the simple or complex types defined in the former;

- **Simple types:** shall be defined in a single, common XSD for all data items that are based on a specific pattern (e.g. MRN) or have a common format (e.g. date). Shall contain the definition of data items that are used in the message-specific XSDs as well as documentation.

- **Complex types:** shall be defined in a common XSD per domain. Complex types shall be identified as common as long as they share the same structure. Shall contain the definition of data groups that are used in the message-specific XSDs as well as documentation.

- **Message_specific XSD:** shall define only the structure of each message by providing the data groups and data items including their type.

- **Technical header:** The technical header elements types are defined in a separate XSD file;

- **Technical Codelists:** shall be defined as simple types in a separate, domain-specific XSD. Whenever a data item of a message is linked to a technical Codelist according to Appendix Q2 of the relevant DDNA specific volume ([R16] and [R17]), this item shall have the corresponding type defined in the specific tcl_domain.xsd (see section VII.8.4.4) as defined in CS/RD2;

- **Datagroups repetitions:** shall be defined in the XSDs using the attribute "maxOccurs";

- **Optionality:** shall be defined in the XSDs for data items or data groups by setting the "minOccurs" attribute of the corresponding element equal to zero. If this attribute is not used, the data item or data group is required;

- **Root Element:** each message shall have its Message Type as root element and the children of the Root Element will be a list of data items (simple types) and data groups (complex types);

- **XSD documentation:** definition of each simple or complex type shall be documented by specific elements. Those elements shall contain information related to description, message type applicability and applicable rules, conditions and Codelists;

- **Comments:** each generated XSD shall begin with a comment indicating the DDNA and/or RFC-List version to which is aligned to at the moment of extraction;

- **Namespaces:** targetNamespace will have the values http://ncts.dgtaxud.ec and http://ecs.dgtaxud.ec for NCTS-P5 and AES-P1 respectively. The namespaces used for all XSDs are:
  o http://www.w3.org/2007/XMLSchema-versioning and;
  o http://www.w3.org/2001/XMLSchema .

- **XSD version:** The vc:minVersion="1.1" attribute will be used to indicate for XSDL processors that XSD has version XSD v1.1;

- **Qualified elements:** The 'elementFormDefault' and 'attributeFormDefault' attributes are set to 'unqualified' for all schemas;

- **XML tags:** Each business functionality (i.e. MRN) will correspond to a single unique XML tag. XML tags naming convention is defined in section VII.3.

VII.9.2   XSDs' File Structure

This sub-section describes how the XSD conventions defined in VII.9.1 are realised in terms of XSDs file structure. Only "domain specific" XSDs are to be generated. Domain Specific XSDs can be further categorised as Message_specific and Domain shared XSDs. The following figure provides a high level visualisation of the XSDs categorisation.
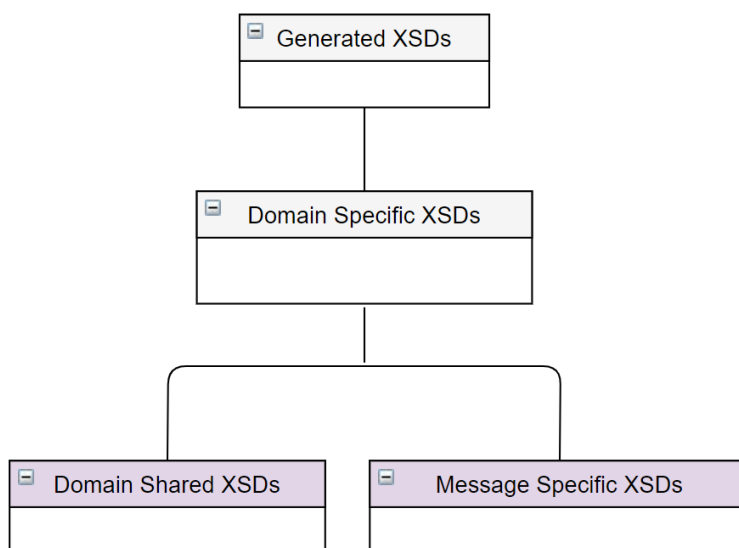
Figure 28: XSDs' Categorisation

Domain Shared XSDs shall contain definition of Simple and Complex types that are shared between messages of the specific domain. Message_specific XSDs shall contain the definition of the structure for each domain message and shall exist for each message of the domain.

The following figure provides an illustration of the XSD files as they will be extracted from the Specs Manager for a single domain.
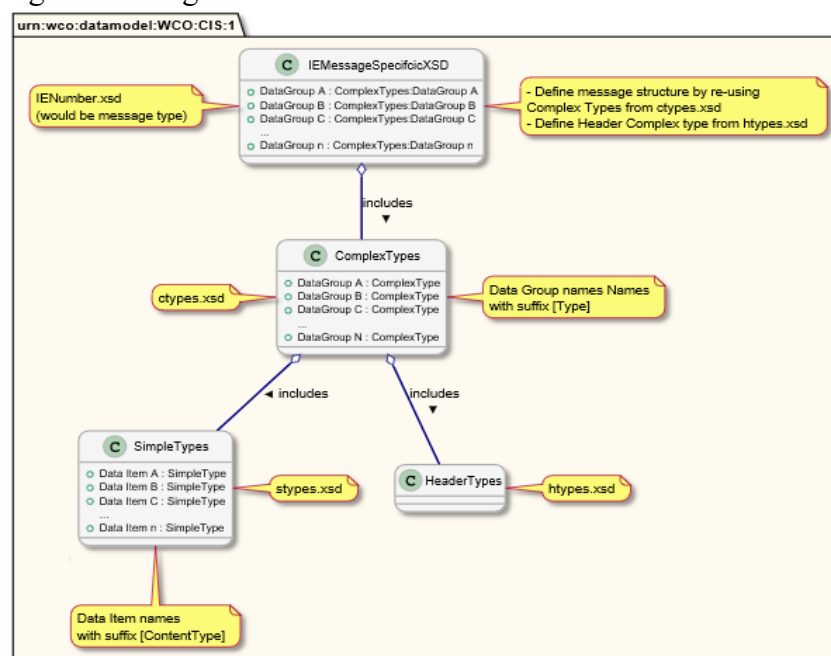
Figure 29: XSDs' File Structure

A short description of the Domain Shared XSDs is provided below:

- **Simple Types XSD (stypes.xsd):** shall contain definition of simple types by type, format and pattern definition. Each data item may have more than one Simple Type. Simple types follow the naming convention [Description][ContentType][n] with few exceptions (Date, Time, Country Code etc.) where the naming convention followed for ECSP2 and NCTS-P4 will be used;

- **Common Complex Types XSD (ctypes.xsd):** shall contain the definition of data groups used in message-specific XSDs and documentation. Complex Types that are identified to be repeatedly defined in messages of the same domain shall be grouped under a common definition. Each complex type definition contains documentation and reference to the data items (and their simple types) that consist the data group. Data item optionality, max repetitions, Rules & Conditions and CL is provided. Complex types follow the naming convention [Description][Type][n]. In the documentation section of the XSD it is explicitly documented if the applicable CL for each complex type is used in the Common or External domain;

- **Header types (htypes.xsd):** shall contain the simple and complex type definitions for the technical header elements. It is common for all messages;

- **Message_specific XSD (CDxxxV.xsd):** shall define only the structure of each message by providing the data groups and data items including their type. Multiplicity and optionality

is also defined and documentation is provided. Each data group definition is consisted by the element name, type, optionality and repetitions.

- **Technical Codelists XSD (tcl.xsd):** shall contain the definition of technical Codelists for a specific domain as simple types. It shall provide the definition of their type (e.g. string,integer, etc.) and an enumeration of the applicable values;

VII.9.3   XSDs Binding

As shown in Figure 29 there is a certain degree of interdependency between the XSD files, whether those are message-specific or common. In order to realise that interdependency and assemble the XSDs, XML Schemas <include> element will be used.

VII.9.4   Internal Structure of XSD Files

The current section provides an overview of the internal structure per XSD type as well an example of their application to define simple and complex types.

VII.9.4.1   Message-specific XSDs

Each message-specific XSD shall define the structure of the pertinent IE. In order for data items and groups to be defined each Message_specific XSD shall contain reference to the Common XSDs of its domain. The XSD structure is compliant to the characteristics presented below:

- **Root Element:** is the type of message. As shown in Figure 30, CD501C is the root element of the XSD;

- **Message Structure / Datagroups:** Datagroups ordered under Root Element define the message structure as shown in Figure 30. Data-groups in dashed line shall be defined as required while those with solid line are defined as optional. Documentation elements provide additional information per datagroup, such as description and applicable rules/conditions. Each datagroup consists of data items. Datagroups identified during generation to have a common list of elements are defined in shared XSD (Common complex type XSD for domain) and referenced in the Message_specific XSD;

Figure 30: Root Element and Message data-groups

- **Message Structure / Data Items:** data items and data groups ordered under XSD root element define message structure, thus the format of information related to the message. Data-items that share common definitions in terms of format are defined in domain or inter-domain shared XSDs and referenced in Message_specific XSDs.

The XSD conventions are following the principles that are currently in place for the ECSP2 and NCTS-P4. As a result, the Root Element of the XSD is defining the Message Type. The Root Element shall contain the structure of the message according to its TMS presented in Appendix Q2 of the relevant DDNA specific volume ([R16] and [R17]). It should be also mentioned that the same XML tags shall be preserved.

VII.9.4.2   Simple Types XSD (stypes.xsd)

Simple types shall be defined in domain (stypes.xsd) XSDs.

The naming convention that will be used is stypes.xsd. The Base Types are restricted to the standard 'token', 'dateTime', 'integer' and 'decimal'. Base types shall merely define the type and or size of simple types. Base types shall be further restricted by patterns and or size limitations and thus Specific types shall be defined. An example is presented in Figure 31, where a specific type ModeOfTransportAtTheBorderContentType is defined for the Mode of Transport data item by applying an additional pattern restriction to the 'token' which in that case is the base type.

Those data items associated to a Codelist in Appendix Q2 of the relevant DDNA specific volume ([R16] and [R17]) with this Codelist been a technical one (part of tcl.xsd), shall be also defined in stypes.xsd. The allowed values for technical Codelists are maintained in CS/RD2 and also included in tcl.xsd.

```xml
<xs:simpleType name="ModeOfTransportAtTheBorderContentType">
    <xs:annotation>
      <xs:documentation>
        <usedBy>Used by 2/5 messages: CC515C, CD501C</usedBy>
      </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:token">
      <xs:pattern value="[0-9]"/>
    </xs:restriction>
  </xs:simpleType>
```

Figure 31: Specific type definition for ModeOfTransportAtTheBorderContentType

VII.9.4.3   Complex Types XSD (ctypes.xsd)

Complex Types that shall be identified to be shared between more than one messages of the same domain shall be defined in common XSD per domain. The naming convention that will be used is ctypes.xsd. That way definition of commonly used Complex types per domain shall be shared for the Message_specific XSDs. Structurally wise, each complex type definition is comprised by the definitions of the simple types that represent the data items of the complex type data group. Because each data group may be used with a different set of data items among different message types, multiple complex types are foreseen for each data group and denoted by the [n] in the naming of the complex type. An example is provided in the Figure 32 below:

Complex types shall be referenced in the Message_specific XSDs where the structure of a message shall be defined. The following example in Figure 32 illustrates the definition of Risk Analysis complex type in ctypes.xsd. The specific complex type has been identified to be shared between multiple Message_specific XSDs of AES-P1.

```xml
<xs:complexType name="RiskAnalysisResultType01">
    <xs:annotation>
      <xs:documentation>
        <usedBy>Used by 1/5 messages: CD501C</usedBy>
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="riskAnalysisTypeCode" type="RiskAnalysisTypeCodeContentType">
```

```xml
        <xs:annotation>
          <xs:documentation>
            <description value="Risk analysis type code" />
            <codeList code="CL739" type="business" name="RiskAnalysisType" />
            <format value="a1" />
            <optionality value="R" />
          </xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="riskAnalysisResultCode" type="RiskAnalysisResultCodeContentType">
        <xs:annotation>
          <xs:documentation>
            <description value="Risk analysis result code" />
            <codeList code="CL737" type="business" name="RiskAnalysisResult" />
            <format value="an..17" />
            <optionality value="R" />
          </xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="riskAnalysisResultText" minOccurs="0"
 type="RiskAnalysisResultTextContentType">
        <xs:annotation>
          <xs:documentation>
            <description value="Risk analysis result text" />
            <format value="an..350" />
            <optionality value="O" />
          </xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="controlRecommendationCode" minOccurs="0"
 type="ControlRecommendationCodeContentType">
        <xs:annotation>
          <xs:documentation>
            <description value="Control recommendation code" />
            <format value="an..17" />
            <optionality value="O" />
          </xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="controlRecommendationText" minOccurs="0"
 type="ControlRecommendationTextContentType">
        <xs:annotation>
          <xs:documentation>
            <description value="Control recommendation text" />
            <format value="an..350" />
            <optionality value="O" />
          </xs:documentation>
        </xs:annotation>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
```
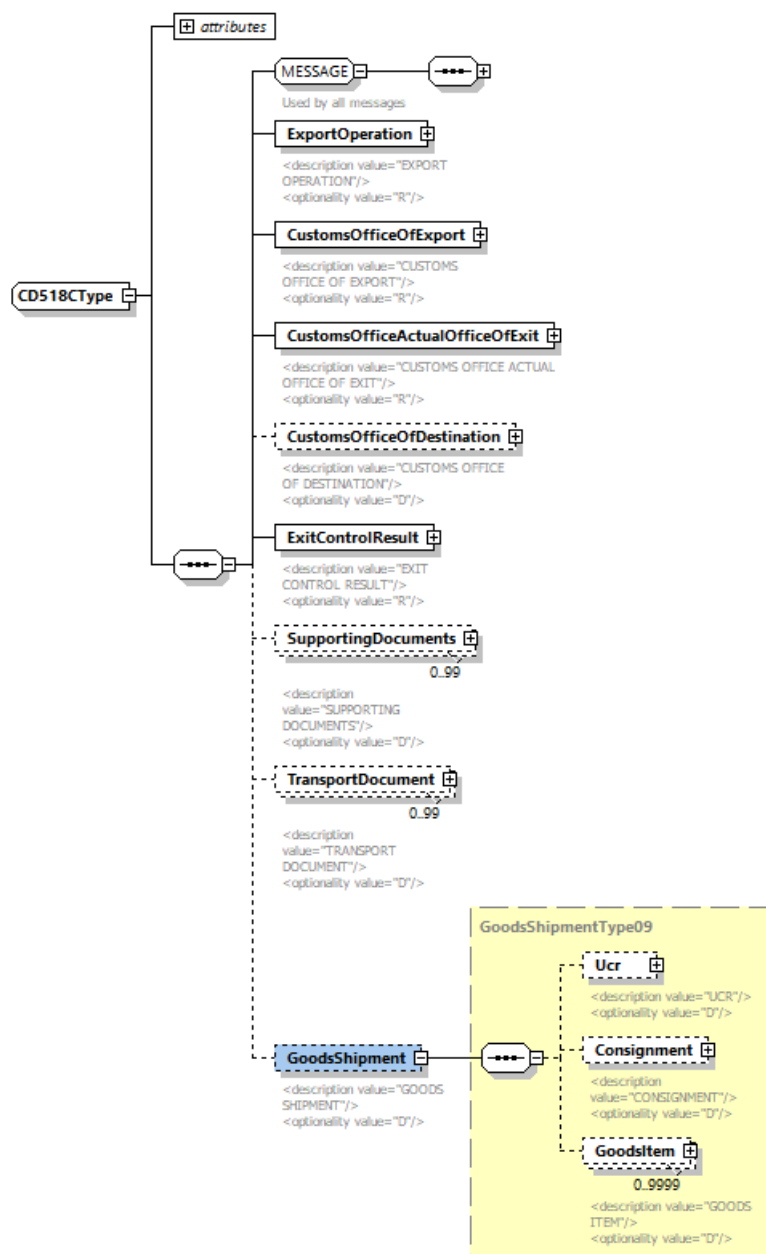
Figure 32: Definition of Risk Analysis complex type

The following figure illustrates how GoodsShipmentType is referenced in Message_specific XSD in order to define data-group CD501C.GoodsShipment.
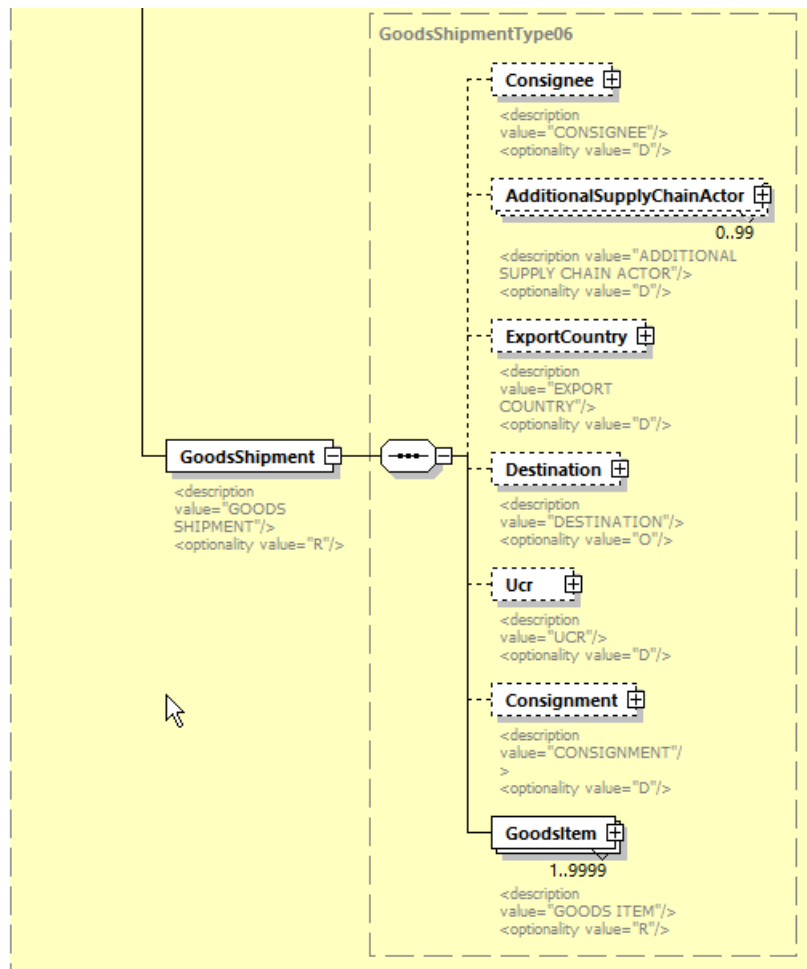
Figure 33: Definition of CD501C.GoodsShipment

VII.9.4.4 Technical Codelists XSD (tcl.xsd)

Technical Codelists shall be defined in CS/RD2. Those are listed in one XSD (tcl.xsd) that is referenced by ctypes.xsd and htypes.xsd of each domain.

VIII Transport of messages via CCN/CSI

VIII.1 Introduction

VIII.1.1 Summary

This section specifies the exchange of messages through the Common Domain.

The specification consists of a set of specified items that are grouped in two parts:

- The mandatory items: these consist of all choices that need agreement in the Common Domain to ensure end-to-end communication between National Applications.

- The recommended items: these consist of all recommendations that are of benefit for the best possible performance of the communication means, beyond what is mandatory and taking into account the fact that varied architectural constraints may exist on different NCA platforms.

VIII.1.2 Architectural Assumptions

1. The exchanges in the Common Domain use the communication services provided by the CCN/CSI infrastructure. The CCN/CSI infrastructure has the main objective of exchanging CCN messages across the Common Domain: a CCN message is an object that is created, sent and received through the CSI API. A CCN message has a structure composed of service elements and Application data.

2. The CCN infrastructure consists of a set of interconnected Gateways; each NCA is able to use the CCN services by connecting an NCA front end to a nationally located Gateway and accessing this Gateway through the CSI API.

3. Only the subset of CCN asynchronous communication services is used in Customs systems.

4. The CCN asynchronous services operate on persistent storage objects named "queues". In this mode, CCN messages are exchanged between queues by the CCN services. There exists a consistent naming convention for all queues defined for Customs systems.

5. In Customs systems, the Application data within a CCN message consist of one Information Exchange. The EDIFACT or XML interchange that carries one Information Exchange consists of one EDIFACT or XML message[31] respectively.

6. The responsibility for routing a CCN message coming from the Common Domain, once it is present in the receiving queue, entirely lies upon the NCA. This includes

---

[31] If in future versions this assumption changes, this section will need to be reviewed in that respect. Only EDIFACT messages of the same priority are combined in one interchange

the steps of (a) reading from the receiving queue; (b) dispatching the message contents to processes and destinations within the National Domain; (c) extracting where appropriate the EDIFACT or XML message from the CCN message; (d) reacting appropriately to the EDIFACT or XML message contents in accordance with the Customs systems business process threads, rules and conditions.

7. The Information Exchanges do not require an immediate answer. Response times for National and central applications are defined in the SLA [R30].

8. A National Application is interacting with CCN/CSI via CCN/CSI API calls. It is mandatory to check the result of any API call (by checking the API return and reason codes) to assure the proper execution of the API call and to take corrective actions in case of problems.

9. Whenever an Information Exchange is sent, CCN/CSI enables to request report messages indicating the state of the message transfer. The usage of these report messages is mandatory. The sender must check the reception of the report messages and corrective action needs to be taken in case of problems.

10. CCN/CSI enables automated MRN nursing, whereby an automated application can track all CCN/CSI exchanges related to a single MRN, including the exchange of the various CCN/CSI reports. In order to support MRN nursing, the National and Central applications must follow the conventions defined for the usage of MsgId and CorrelId in the CCN/CSI exchanges.

11. In Customs systems when two Information Exchanges are sent to the same queue on the same Gateway and the sequence of these is significant (e.g. IE006/IE018 in NCTS), then it is the responsibility of the sending NCA to ensure that this sequence is maintained under all conditions. This may be achieved by delaying the sending of the second until receipt of the first has been acknowledged.

12. In order to prevent a message from being deleted from a queue before it has actually been processed, the queue should first be browsed to get the message and then delete the message from it (after the message has been processed). The usage of the verb to get and delete is not allowed since it does not guarantee a correct handling of the message.

13. Sending NCAs should not re-send IEs for which there has been no reply as a result of unavailability of the receiving NCA. The re-send should occur only upon request of the NCA, or receipt of an exception report. Specifically for NTAs, the sending NTA should "enable" the sequence check mechanism in order to respect the correct sequence of messages, when this is explicitly defined, as is the case for IE006 and IE018.

VIII.1.3   References to CCN/CSI

This document does not describe CCN/CSI. That information is available in the relevant CCN/CSI manuals. The document provides a short reminder of the CCN communication with the aim of helping the reader to find his/her way into the CCN/CSI documentation and it also defines the programming choices applicable to Customs systems.

General Introduction lists specific references related to CCN/CSI and the C language ([A1] to [A3] and [R34] to [R10]).

The definitions of data structures, of data types and of constants are found in "include" files (for the C language) or "COPY" files (for the COBOL language). "Library" files providing the compiled code that must be linked with the application-compiled code are also provided. The indications of the files to use are given in:

- For the C language: see [A1] chapter 12 "Building an application on UNIX systems";

- For the COBOL language on BS1000: see [A2] heading 6.6;

- For the COBOL language on CICS: see [A3] heading 6.6.

VIII.2 The CCN communication reminder

This chapter presents those elements of CCN/CSI that are agreed to ensure end-to-end communication between two CCN Gateways.

In this chapter, the word "message" is to be understood as "CCN message".

CCN carries messages between Gateways. The messages are prepared and sent by a sending Application, using CSI API; the messages are received and interpreted by a receiving Application. The communication uses the asynchronous mode.

An application is said to communicate in asynchronous mode when this application is able to send a message without having established a connection with its peer application. Messages are exchanged by placing them in and extracting them from the queues.

Figures available from an application currently operational on CCN/CSI demonstrate that the total request/reply round trip delay is in the range of 5 to 10 seconds with all accesses performed in asynchronous mode. This is the time between the moment that the sender puts a Request on its sending queue and the moment when the reply is available for the sender to retrieve from its receiving queue.

The structure of the message consists of:

- A description of the message or "**message descriptor**" (see [A6] chapter 4.3.2.2);

- A description of the data or "**data descriptor**" (see [A6] chapter 4.3.3.2); the data descriptor is said to 'contain' the data, even when actually it contains only a description consisting of length (in bytes) and address in memory or location in the file system;

- A description of specific parameters, called "**quality of services**". These parameters describe particular handling that has to be applied (when sending) or was applied (when receiving), on the data contained in the data descriptor during execution of a CSI verb.

These three structure components are further detailed in the three paragraphs (0, VIII.2.2, and VIII.2.6) that follow.

The sending and receiving of CCN messages may occur after the application has connected itself to the CCN Gateway, has created a security context and has connected to the queue manager: these steps are further detailed in the paragraphs (VIII.2.8, VIII.2.9, VIII.2.10 and 0) that follow.

An NCA will always interact with CCN/CSI via CCN/CSI API calls. It is essential that the correct execution be checked after each API call (by checking the API return code) and that appropriate action is taken when the API call has failed. Possible API return codes are documented in [A7].

VIII.2.1   The message descriptor

The message descriptor consists of a CSIMQMD structure.

This structure is to be prepared, prior to sending a message with the CSI_mq_put verb.

This structure is to be interpreted and some of its elements have to be copied back in an equivalent structure when an Information Exchange is replied with another Information Exchange, in line with the Time Sequence Diagram demonstrated in paragraph VIII.2.7.

Table 56 details the CSIMQMD structure members.

Typedef struct tag		Value on SEND	Value for CCN Report	Notes
CSIMQMD {				
CSICHAR4	StrucId;	CSIMQMD_STRUC_ID	CSIMQMD_STRUC_ID	
CSILONG	Version;	CSIMQMD_VERSION_1	CSIMQMD_VERSION_1	
CSILONG	Report;	0L	0L	
CSILONG	MsgType;	CSIMQMT_REQUEST or CSIMQMT_DATAGRAM	CSIMQMT_REPORT	
CSILONG	Expiry;	3 456 000L	(DNC)	
CSILONG	Feedback;	CSIMQFB_NONE		
CSILONG	Encoding;	0L	(DNC)	
CSILONG	CodedCharSetId;	0L	(DNC)	
CSICHAR8	Format;	Empty string	(DNC)	
CSILONG	Priority;	0L	(DNC)	
CSILONG	Persistence;	CSIMQPER_PERSISTENT	(DNC)	Message persistence
CSIBYTE24	MsgId;	CSIMQCI_NONE	=MsgId of reported Msg	Message identifier
CSIBYTE24	CorrelId;	=MRN or = MsgId of Request message or =MsgId of Rejected message	= CorrelId of reported Msg	
CSILONG	BackoutCount;	0L	(DNC)	Backout counter
CSICHAR48	ReplyToQ;	Empty string	(DNC)	Not used
CSICHAR48	ReplyToQMgr;	Empty string	(DNC)	Not used
CSICHAR12	UserIdentifier;	Empty string	(DNC)	Not used
CSICHAR32	AccountingToken;	Empty string	(DNC)	Not used
CSICHAR32	ApplIdentityData;	Empty string	(DNC)	Not used
CSILONG	PutApplType;	0L	(DNC)	Not used
CSICHAR28	PutApplName;	Empty string	(DNC)	Not used
CSICHAR8	PutDate;	Empty string	(DNC)	Not used
CSICHAR8	PutTime;	Empty string	(DNC)	Not used
CSICHAR4	ApplOriginData;	Empty string	(DNC)	Not used
} CSIMQMD;				

Table 56: MQ Message Descriptor

Notes:

1. Column "Value on SEND" exhibits the value that an application has to set in each structure member.

2. Column "Value for CCN report" defines the value set in the CCN reports.

3. The indication "(DNC)" means: "Do not consider".

4. Values in uppercase are CCN/CSI constants defined in the header files.

5. The value CSIMQMT_REQUEST has the effect of requesting a reply. The name of the queue to which the reply is to be sent is contained in ReplyToQ field of CSIQOS structure. See paragraph VIII.2.5.

6. The CCN Gateway buffers incoming messages in case the application is temporarily unable to process them. The requirement is to be able to buffer the messages for 96 hours (in tenths of second, this duration amounts to: 96 x 3600 x 10 = 3 456 000).

7. Value in 'Feedback' is set by the queue manager to indicate, within a report message, how the original message was handled on the Destination queue.
   The reports are sent back to the sender as specified by the parameters set in the configuration (see chapter VIII.4).

   Possible values are:

▪ A value comprised in the range from CSIMQFB_SYSTEM_FIRST and CSIMQFB_SYSTEM_LAST (those limits included)	*Exception report*
▪ CSIMQFB_EXPIRATION	*Expiration report*
▪ CSIMQFB_COA	*Confirm on Arrival report*
▪ CSIMQFB_COD	*Confirm on Delivery report*

8. The MsgId value is an identifier used by the application to correlate a Report Message with the Information Exchange it reports about. As an Expiration report may only be generated after 96 hours (see Note 2 for 'Expiry' field above), it is recommended that the MsgId generating rule uses a counter that does not "rewind" in less than 96 hours.
   As the field MsgId presents 24 bytes, the NCA designer is able to choose a MsgId definition that covers this condition and well beyond.
   The MsgId is a binary value that can be defined automatically by CCN/CSI or that can be defined by the sending application itself. When automatically created by CCN/CSI, the MsgId is based upon system date and time and is satisfying the criterion defined above.
   In order to support MRN nursing, the following conventions must be followed:
   - The MsgId is generated automatically by CCN/CSI or by the sending application itself.
   - The CorrelId is filled in with:

- o For the IE906, IE907 and IE917, the Message ID (MSGID) of the rejected message;
- o For the response messages (i.e. a message responding to a message request), the Message ID (MSGID) of the corresponding request message;
- o For the other messages, the MRN (in an ASCII format).

This will enable the correlation of the ErroneousMessage/ErrorMessage and Request/Response.

When a Report is sent back:

- the MsgId is equal to the MsgId of the original message;

- the CorrelId is equal to the CorrelId of the original message.

If the MsgId is set to CSIMQMI_NONE, then the queue manager will generate a unique message identifier upon sending.

The MsgId of the original message is copied into the MsgId of the Report message by setting the appropriate flag CSIMRQRO_PASS_MSG_ID in the ReportRequest field of the QOS. The CorrelId of the original message is copied into the CorrelId of the report message by setting the appropriate flag CSIMRQRO_PASS_CORREL_ID in the ReportRequest field of the QOS (see section VIII.2.6).

9. In order to support MRN nursing, the value of CorrelId needs to be equal to the MRN. The CorrelId of the original message is copied into the CorrelId of the report message by setting the appropriate flag CSIMRQRO_PASS_CORREL_ID in the ReportRequest field of the QOS (see section VIII.2.6).

A report message is sent back to the sender:
- Confirm on Delivery (CoD) report when the message has been read by the receiving application and deleted from the queue;

- Confirm on Arrival (CoA) report when the message has arrived on the remote Gateway;

- Expiration (EXP) report when a value of time lapse set in the CSIMQMD.Expiry variable (see Note 2) has expired and an application tries to retrieve this message after the elapsed expiration time: the message, once arrived on Destination queue (CoA), was not fetched from this queue by an application program during the time allotted;

- Exception (EXC) report when other technical errors that are related to the queuing system, have occurred.

The usage of the four report messages (CoA, CoD, EXP and EXC) is mandatory. An NCA will have to request all four types of reports whenever an Information Exchange is sent and will have to wait for the reception of the reports for any Information Exchange sent. In case of problems, corrective action needs to be taken. This usage is further discussed in chapter VIII.2.7.

The report messages are to be read from the queue whose name is given by the element "ReplyToQ" of the Quality of Service structure. See Table 59. The report messages do not contain the original message.

In case the report message could not be delivered to the queue indicated by this element, it will be stored on the so-called dead-letter queue (CSIMQRO_DEAD_LETTER_Q) on the gateway that sent the report. Each CCN Gateway needs to have this type of queue.

VIII.2.2   The data descriptor

The data descriptor is implemented by a CSIDD structure shown in Table 57.

Typedef struct tag		Value on SEND	Data descriptor
CSIDD {			
CSICHAR4	StrucId;	CSIDD_STRUC_ID	Structure identifier
CSILONG	Version;	CSIDD_VERSION_1	Structure version
CSILONG	Flags;	O_MEMORY or O_FILE	
CSICHAR256	FileName;	See VIII.2.4	
CSIULONG	DataLength;	See VIII.2.4	
CSIBYTE	*Data;	See VIII.2.4	
} CSIDD;			

Table 57: CSI Data Descriptor

Notes:

1. Column "Value on SEND" exhibits the value that an application has to set in each structure member.

2. The CSIDD structure allows the representation of data:
   ▪ Either located in core memory: the structure element 'Flags' must have the value O_MEMORY;
   ▪ Or located in a file: the structure element 'Flags' must have the value O_FILE.

   The choice of which method to use for passing the application data is strongly dependent on the design choices taken for the application: it is recommended that the "O_MEMORY" method be used whenever possible.

VIII.2.3   Allocation of a CSIDD

The CSIDD has to be allocated dynamically and initialised with the function HL_alloc(), documented in [A6]:

```
    CSILONG HL_alloc    (
     CSIULONG SizeRq,
     CSIDD    **DataOut,
     CSILONG  *ReturnCode,
     CSILONG  *ReasonCode
    );
```

If the data are represented in core memory, the value of argument SizeRq must be at least equal to or greater than, the length of the application data (expressed in octets).

Upon successful call to HL_alloc(), some elements of the allocated CSIDD structure are initialised:

- StrucId = CSIDD_STRUC_ID;

- Version = CSIDD_VERSION_1;

- Flags = O_MEMORY;

- DataLength = 0L.

When a CSIDD structure is not used anymore, it has to be given back to system resources by performing the HL_free() verb, documented in [A6]:

```
CSILONG HL_free(
CSIDD    **DataOut,
CSILONG  *ReturnCode,
CSILONG  *ReasonCode
);
```

The example for allocation of a CSIDD structure is part of the listing in Table 58.

VIII.2.4   Inserting the application data into the CSIDD structure

The application data consist of an Information Exchange in EDIFACT or XML format. In the example provided in Table 58, they are represented as a core memory value named 'Request'.

- If the application data are represented in core memory:
  They have to be copied from their current location into the buffer allocated and pointed to by CSIDD.Data and the element "DataLength" must be entered as the exact length (expressed in octets) of the application data. It cannot be assumed that the Information Exchange is represented in memory as a NULL-terminated string according to the ANSI C convention. The example for this case is provided (as statement "**memcpy**") in Table 58;

- If the application data are represented in a file:
  The elements of the CSIDD structure must be set to:

  o Flags = O_FILE.

  o DataLength = length of useful contents in the File.

  o FileName = full path name of the file. 'FileName' is set to the path name of a file containing application data.

VIII.2.5   Encoding the CSIDD

When the CSIDD is prepared, with elements either FileName or Data (as well as DataLength) correctly initialised by the application, it has to be presented, on the sending side to the HL_encode() verb. Conversely, after being received, a CSIDD structure must be presented to the HL_decode().

The prototype of the `HL_encode` verb is:

```
CSILONG HL_encode(
    IN    CSIDD      *DataIn,
    IN    CSICHAR32 MsgTypeId,
    IN    CSILONG   CodePage,
    IN    CSICHAR128    HostFormat,
    OUT   CSIDD      *DataOut,
    OUT   CSILONG   *ReturnCode,
    OUT   CSILONG   *ReasonCode
);
```

The parameter MsgTypeId must have a value within a pre-determined set of values that are listed in each domain specific DDNA volume ([R16], [R17] and [R18]).

See chapter VIII.4 for an explanation of arguments 'CodePage' and 'HostFormat' as obtained from configuration information.

The listing in Table 58 illustrates the usage of `HL_alloc` and `HL_encode` verbs, as well as the initialisation of the CSIDD structure with the EDIFACT Information Exchange.

```
REQUEST   Request;
CSIDD     pCSIrequest;
CSILONG   ReturnCode;
CSILONG   ReasonCode;


The variable Request has been prepared in REQUEST structure.
Assume Request is the EDIFACT_interchange for a CD001A message

Steps are:
   (1)   (See VIII.2.3) Allocate Data Descriptors for request
         HL_alloc (sizeof (REQUEST), &pCSIRequest, &ReturnCode,
         &ReasonCode);
   (2)   Copy REQUEST structure into "Data" field of request
         CSIDD structure
         memcpy (pCSIrequest->Data (CSICHAR *) &Request, sizeof
         (REQUEST));

   pCSIrequest->DataLen = sizeof (REQUEST);


   (3)   Encode request
         HL_encode  (pCSIrequest,  "CD001A-MSG.NCTS",  CODEPAGE,
         HFMT, \

   pCSIrequest, &ReturnCode, &ReasonCode);

   After  these  steps:  the  CSIDD  will  be  sent  with
   HL_mq_put() verb. Logging of this CSI movement will take
   a record of "CD0001A"
```

Table 58: Example of CSIDD allocation, initialisation with Information Exchange and encoding

This code is not intended to be used directly as actual working code. All API return codes (and possibly reason codes) will have to be checked after every API call.

VIII.2.6   *The quality of service*

CCN specifies a Quality of Service (QoS) with a number of parameters (see [A6] Section 4.3.3.3). These parameters are used in the CSI verbs that handle data; the values of these parameters apply to the data exchanged in the same verb.

When a specific parameter is not mentioned in the QoS (vector QoSToApply in [A6] Section 4.3.3.3), its default value as defined at configuration time (see paragraph VIII.4.7 of Transport of messages via CCN/CSI) applies.

The Quality of Service is represented by the CSIQOS structure shown in Table 59. The fields applicable in this structure are ticked with a "√" in the right-hand column of this Table.

typedef struct tag		value on SEND	Notes	
CSIQOS{				
CSICHAR4	StrucId;	CSIQOS_STRUC_ID	Structure id.	√
CSILONG	Version;	CSIQOS_VERSION_1	Structure version	√
CSILONG	QoSToApply;		Specified QoS	√
CSILONG	AppliedQoS;	(DNC)	Applied QoS	√
CSILONG	Priority;		Priority value	√
CSILONG	ReportRequest;		Report/Request flag	√
CSICHAR48	ReplyToQ;		Name of reply queue	√
CSICHAR48	ReplyToQMgr;	(DNC)	Name of reply queue mgr	√
CSIBYTE24	CorrelId;	Empty string	Correlation id.	√
CSILONG	Integrity;		Integrity flag	√
CSILONG	Confidentiality;		Confidentiality flag	√
CSILONG	Compression;		Compression flag	√
CSICHAR8	CompressionId;		Comp. Algorithm id.	√
CSICHAR16	CoT;	DEFAULTCOT	Class of Traffic	√
CSICHAR48	VASScript;	Empty string	VAS script name	√
CSILONG	DegradedMode;	(DNC)	Degraded mode flag	
} CSIQOS;				

Table 59: CCN/CSI Quality of Service structure

Notes:

1. Column "Value on SEND" exhibits the value that an application has to set in each structure member.

2. 'QoSToApply' is a vector of bits obtained by adding once or by performing a bitwise OR operation between, the set of values that follow:
    QoSToApply =
       CSI_QOS_PRIORITY +
       CSI_QOS_REPLYTO_Q +
       (0 or CSI_QOS_INTEGRITY: see Note 6.1) +
       (0 or CSI_QOS_CONFIDENTIALITY: see Note 6.2) +
       (0 or CSI_QOS_COMPRESSION: see Note 6.3) +
       (0 or CSI_QOS_COMPRESSION_ID: see Note 6.3)

3.   Two priority values are distinguished (these values are written with the C language convention for long integers):

- High priority: QoS priority parameter has value 7L. This priority is applied to the Information Exchanges listed in the respective tables in the domain specific DDNA volumes ([R16], [R17] and [R18]).

- Normal priority: QoS priority parameter has value 5L. Normal priority is applicable to the other Information Exchanges exchanged across the Common Domain.

For AES-P1 and NCTS-P5, all Information Exchanges shall be sent with Normal priority and therefore appropriate QoS priority parameter shall be used. [R41] and [R40] do not specify high priority Information Exchanges compared to ECS-P2 and NCTS-P4.

When a message is retrieved from a Destination queue, it is accompanied with the QoS that was set at the time of sending. Therefore, the priority set when sending has to be used to fetch the received message in accordance with the rule:

Rule for fetching messages from a receiving queue:
High priority messages will always be processed first and, within the same priority level,"first in, first out" behaviour will be used.

4.   'ReportRequest' specification is fully defined by configuration (see chapter VIII.4) and hence is not to be set for each individual message. One thus has the choice either to use the default value set by configuration or to use an individual value for every individual message sent. In any case it is required to request all four types of reports (CoA, CoD, EXC, EXP) whenever an Information Exchange is sent. In addition, the following flags need to be set for copying MsgId and CorrelId from the original message to the report message:

- CSIMQRO_PASS_MSG_ID

- CSIMQRO_PASS_CORREL_ID

5.   'ReplyToQ' is to be set to the name of a queue that exists on the CCN Gateway used by the sending application. This name is of no use for the receiving application (because the report message is constructed and sent by the CCN software and not by the receiving application).

6.   The attributes "Integrity", "Confidentiality" and "Compression" apply to the link between the NA platform and the CCN gateway. Therefore, the choice of modifying the values preset at Configuration time (see paragraph VIII.4.3) depends of the strength of this link as perceived by the NA Local Security Officer. The notes 6.1, 6.2 and 6.3 apply to the situation where the decision is taken to change the default values.

6.1   See chapter VIII.4 for the explanation of the configuration options set for the Integrity (data are accompanied with a signature). If the NCA chooses to set the Integrity for a specific message differently from the configured value, then

- Value CSI_QOS_INTEGRITY must be added to QoSToApply;

- Element 'Integrity' in CSIQOS takes the value CSI_INTEGRITY_REQUIRED.

Else:

- Value CSI_QOS_INTEGRITY must not be added to QoSToApply;

- Element 'Integrity' in CSIQOS takes the value CSI_INTEGRITY_NOT_REQUIRED.

6.2   See chapter VIII.4 for the explanation of the configuration options set for the Confidentiality (data are encrypted). If the NCA chooses to set the Confidentiality for a specific message differently from the configured value, then:

- Value CSI_QOS_CONFIDENTIALITY must be added to QoSToApply;

- Element 'Confidentiality' in CSIQOS takes the value CSI_ CONFIDENTIALITY _REQUIRED.

Else:

- Value CSI_QOS_CONFIDENTIALITY must not be added to QoSToApply;

- Element 'Confidentiality in CSIQOS takes the value CSI_ CONFIDENTIALITY _NOT_REQUIRED.

6.3   See chapter VIII.4 for the explanation of the configuration options set for the Compression and CompressionId. If the NCA chooses to set these parameters for a specific message differently from the configured value, then:

- Value CSI_QOS_COMPRESSION and CSI_QOS_COMPRESSION_ID must be added to QoSToApply;

- Element 'Compression' in CSIQOS takes the value CSI_ COMPRESSION _REQUIRED;

- Element 'CompressionId' in CSIQOS takes the value CSI_ COMPRESSIONID_LZW.

Else

- Value CSI_QOS_CONFIDENTIALITY must not be added to QoSToApply;

- Element 'Confidentiality in CSIQOS takes the value CSI_ COMPRESSION_NOT_REQUIRED;

- Element 'CompressionId' in CSIQOS takes the value CSI_ COMPRESSIONID_NONE.

6.4   High priority messages are defined in each domain specific DDNA volume ([R16], [R17] and [R18]) for the specific domain.

VIII.2.7   Illustration of the use of the QOS parameters

This section illustrates by means of Time Sequence Diagrams (Time Sequence Diagrams) the use of the QoS parameters and of the CCN report messages. It shows the communication between a sending CSI stack, a sending CCN Gateway, a receiving CCN Gateway and a receiving CSI stack. It shows several cases starting with the normal case in which a Confirm on Arrival and Confirm on Delivery are received. Based on this normal case, several exceptions are shown in Figure 34.
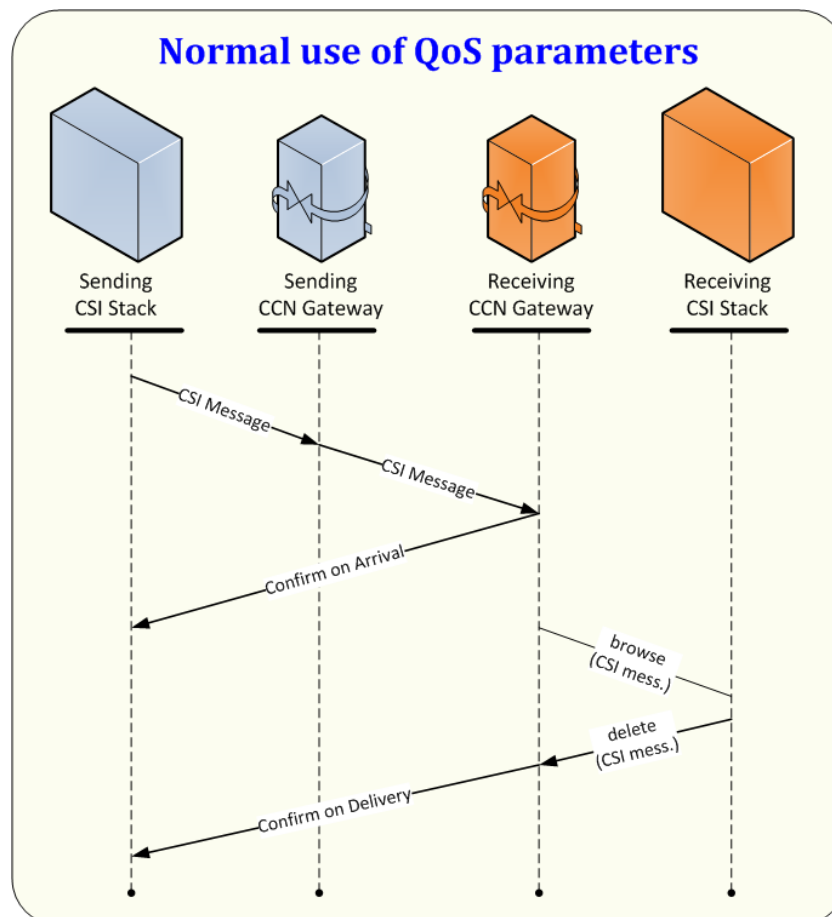
Figure 34: Normal use of QoS parameters for NCA

The figure shows that a queue is to be first browsed for a message, before the message is deleted (after having processed the message). This use of CSI verbs is mandatory in order to prevent a message from being deleted from a queue before it has actually been processed. The usage of the verb HL_mq_get is not allowed.

It should be noted that, for every Information Exchange sent, the user will have to wait for the reception of the CoA and CoD before concluding that the message has been transferred successfully. The CoA is denoting that the Information Exchange has reached the destination queue, while the CoD is denoting that the Information Exchange has been successfully processed at (and deleted from) the destination queue. Please also note that CCN/CSI does not assure the delivery of CoA and CoD in sequence (in rare occasions, the CoD may be returned first).

If a message cannot be sent to a Destination CCN Gateway, the result is indicated in the CSI verb (HL_mq_put). This type of error needs to be handled by the sending CSI stack. In such a case, the CSI message will never arrive at its Destination CCN Gateway and no CCN report message will be generated.

An exception report can be generated for various reasons and can be generated by both sending and receiving Gateways. Whenever a sending application is submitting a message to CCN/CSI via the `HL_mq_put` verb, the message will first be stored in the internal technical queues of the CCN/CSI stack on the sending Gateway. CCN/CSI will then attempt to forward the message from the internal technical queues on the sending Gateway to the internal technical queues on the receiving Gateway and from these to the destination queue on the destination Gateway. An exception report is generated whenever an anomaly is detected in the internal CCN/CSI behaviour (at either sending or receiving Gateway). This can e.g. be:

- Incorrect addressing at CCN/CSI level, either at sending or receiving side (e.g. invalid Gateway or invalid queue name);

- Unavailability of the receiving Gateway when attempting to transfer the message.

The ITSM CONTRACTOR is maintaining a number of availability flags for the different Gateways. Whenever a Gateway is marked as down, an EXC report will immediately be generated upon sending to this Gateway. When the Gateway is not marked as down, CCN/CSI will attempt to transfer the message; if this does not succeed, an EXC report can still be generated by the sending Gateway.

The Expiration report can be created when the message has arrived at the destination Gateway (Confirm On Arrival has been created) and when the original message has not been read from the Destination queue before the timer set by the 'Expiry' field of the message descriptor expires. The Destination CCN Gateway handles the expiration timer. The destination timer is only checked whenever the destination queue is accessed (no expiration reports will be sent when the queue is not accessed at all). Therefore, EXP reports will not always be generated when the expiry took place (they may actually be generated afterwards).

For all these reasons it is therefore mandatory to wait for the processing reports after sending an Information Exchange and to maintain a timer for every Information Exchange sent. When this timer expires, one should check the availability of the destination Gateway (and possibly re-send the message).
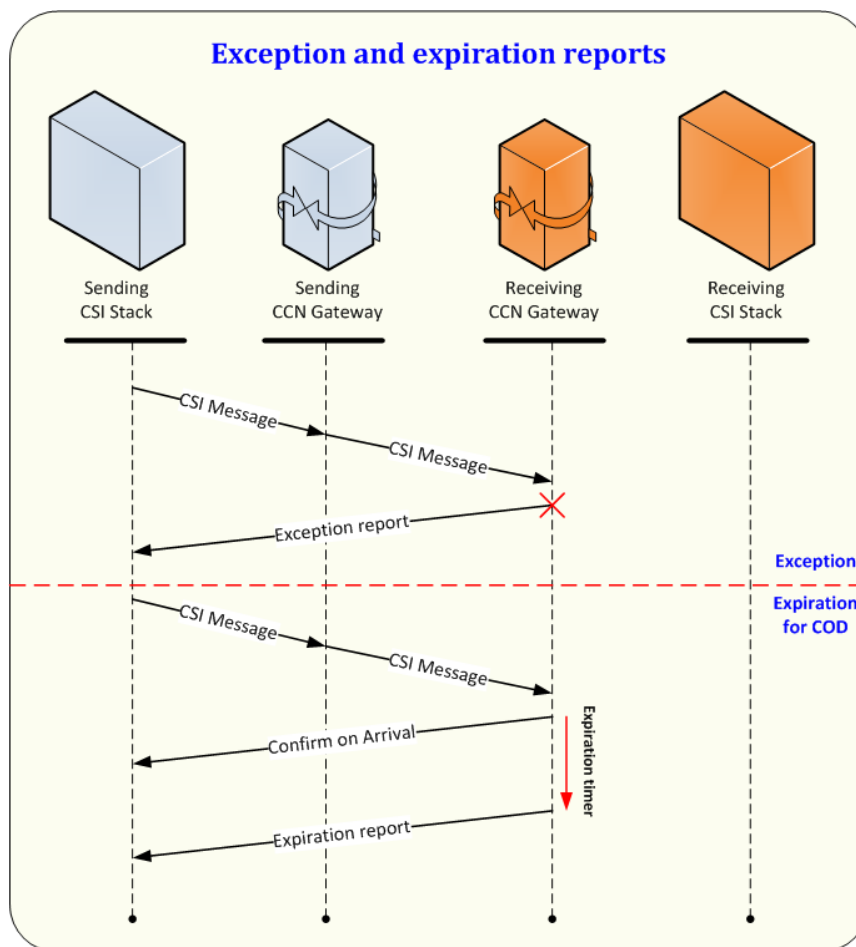
Figure 35: Exception and expiration reports

All possible options for the use of the QoS parameters and their exceptions are shown in the State Transition Diagram in Figure 36. This State Transition Diagram specifies the states of one CSI message present in the sending CSI stack, with respect to the use of CCN. It assumes that the binding of the CSI stack to the CCN Gateway has successfully taken place.
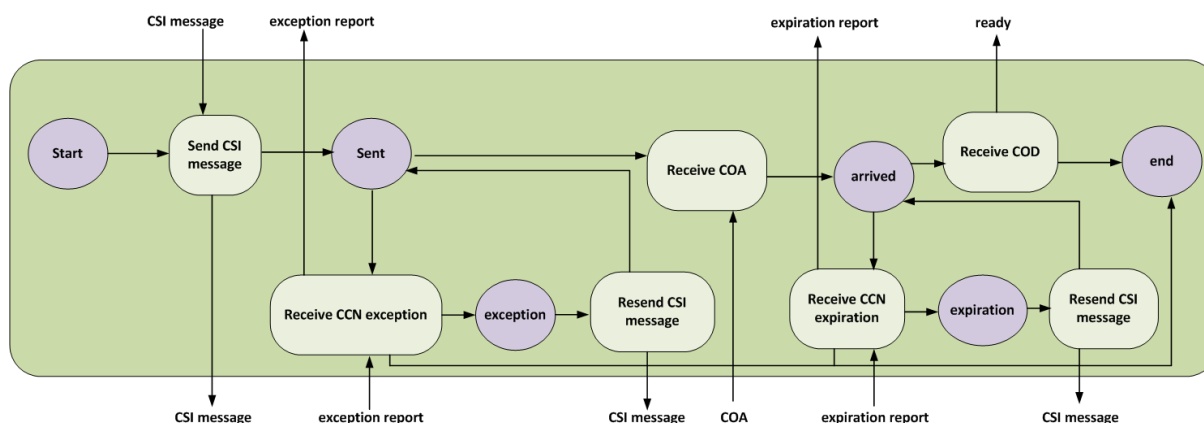
Figure 36: State Transition Diagram of the sending CSI stack

Each of the transitions shown in the previous figure consists of CSI verbs.

VIII.2.8 Connecting the application to the CCN Gateway

Any instance of any application establishes a CSI session by using the HL_bind() verb:

```
CSILONG HL_bind(
    CSICHAR48   AppliName,
    CSICHAR48   ProxyName,
    CSIQOS      *DefaultQoS,
    CSILONG     *ReturnCode,
    CSILONG     *ReasonCode
);
```

"AppliName" is a value previously registered to the CCN Gateway (see paragraph VIII.4.3 of Transport of messages via CCN/CSI). A remote proxy name must have been set together with the ApplicationName at configuration time. This default value may not be overridden: therefore the "ProxyName" argument in the HL_bind() call must be an empty string.

Closing a CSI session occurs with the verb HL_unbind().

Note that the session, when established, has no identifier on its own.

VIII.2.9 Creating a security context for an application

Within the session, a security context has to be created by using the verb HL_init_sec_context and is destroyed with the verb HL_delete_sec_context. The parameter of the HL_init_sec_context verb is a CSISECINFO containing (in the current version of CSI software) a GSSNAME structure:

```
typedef struct tagGSSNAME {
    char user_id[GSS_NAME_LENGTH];
    char application_id[GSS_NAME_LENGTH];
    char user_password[GSS_PASSWD_LENGTH];
    char application_key[GSS_PASSWD_LENGTH];
} GSSNAME;
```

The components of the GSSNAME structure are:

- A user identification;
- An application name;
- A user password;
- An application key.

These four values must have been configured previously by the NA Local Security Officer (see Table 67).

The structure GSSNAME is referenced (i.e. pointed) by a structure CSISECINFO :

```
typedef struct tagCSISECINFO {
    CSILONG securityType;
    CSIVOID securityInfoP;        / here: GSSNAME */
} CSISECINFO;
```

'securityType' is set to the value BI_SEC_TYPE ([A4]).

Finally the verb HL_init_sec_context() is used with the structure CSISECINFO that was initialised:

```
CSILONG HL_init_sec_context(
    CSISECINFO    *credentialInfo,
    CSILONG  *ReturnCode,
    CSILONG  *ReasonCode
);
```

Note that the security context, when established, has no identifier on its own.

The verb HL_delete_sec_context() is used for deleting the security context.

VIII.2.10 *Connecting to the queue manager*

The application has to connect itself to the queue manager in order to be able to issue commands related to queue access. The verb HL_mq_conn() is used for this purpose:

```
CSILONG HL_mq_conn(
    CSICHAR48 Name,
    CSIMQHCONN    *Conn,
    CSILONG  *ReturnCode,
    CSILONG  *ReasonCode
);
```

 "Name" value must be set to an empty string for current version of CSI.

"Conn" is initialised by this function and has to be used subsequently for opening any queue.

The verb HL_mq_disc() is used to disconnect from the queue manager:

```
CSILONG HL_mq_disc(
    CSIMQHCONN    *Conn,
    CSILONG  *ReturnCode,
    CSILONG  *ReasonCode
);
```

Argument "Conn" in this call must be identical to the one obtained from previously using HL_mq_conn().

VIII.2.11 Opening a queue

The application has to open a queue before performing any access to it. See in Table 61 the list of verbs that may be used once a queue has been successfully opened.

The verb HL_mq_open() is used to open a queue:

```
CSILONG HL_mq_open(
    CSIMQHCONN    Conn,
    CSIMQOD  *ObjDesc,
    CSILONG   Options,
    CSIMQHOBJ *Obj,
    CSILONG   *ReturnCode,
    CSILONG   *ReasonCode
);
```

Value of argument "Conn" is identical to the one obtained from HL_mq_conn().

Value of argument "Options" is obtained by adding values that control the HL_mq_open() behaviour. There is no mandatory value of this argument in DDNA because the policy for reading and writing into Gateway queues by the application is a local matter. However, the recommended use of the verb HL_mq_browse() for retrieving messages from a queue (see VIII.2.15), as well as the use of default configured values, mandates the use of at least the options CSIMQOO_BROWSE and CSIMQOO_INPUT_AS_Q_DEF. Hence:

Options = CSIMQOO_BROWSE + CSIMQOO_INPUT_AS_Q_DEF.

Successful call of the verb HL_mq_open() for a certain queue provides a value "Obj", called a "handle", that will be subsequently used in all verbs (listed in Table 61) that deal with this queue.

Argument "ObjDesc" is a CSIMQOD structure that must be initialised as follows:

Typedef	struct tag	Initial value	Notes
CSIMQOD {			
CSICHAR4	StrucId;	CSIMQOD_STRUC_ID	Structure id.
CSILONG	Version;	CSIMQOD_VERSION_1	Structure version
CSILONG	ObjectType;	CSIMQOT_Q	
CSICHAR48	ObjectName;		Name of queue
CSICHAR48	ObjectQMgrName;	(DNC)	This field must not be used
CSICHAR48	DynamicQName;	(DNC)	This field must not be used
CSIBYTE12	AlternateUserId	(DNC)	This field must not be used
} CSIMQOD;			

Table 60: MQ Object Descriptor

Notes:

The Queue Name is inserted here. This allows a maximum length of 47 characters for the Queue Name.

The rules for queue naming are explained in paragraph VIII.2.18.1.

When not used anymore, a queue must be closed by using the verb CSI_mq_close:

```
CSILONG HL_mq_close(
     CSIMQHCONN    Conn,
     CSIMQHOBJ *Obj,
     CSILONG   Options,
     CSILONG   *ReturnCode,
     CSILONG   *ReasonCode
);
```

Value of argument "Conn" is identical to the one obtained from HL_mq_conn().

Value of argument "Obj" is identical to the one obtained from HL_mq_open().

Value of argument "Options" must be set to CSIMQCO_NONE.

VIII.2.12 CSI verbs allowed for queue accesses

When a queue was successfully opened, it is identified by a handle Obj, of type CSIMQHOBJ.

The following verbs may be used to deal with the "Obj" queue contents:

Class of verbs	Verb	Usage
close queue	HL_mq_close()	Mandatory.
write in queue	HL_mq_put()	Mandatory (see also 0 however).
read from queue	HL_mq_browse	Mandatory
delete from queue	HL_mq_delete	Mandatory. A message must have been successfully read and processed before deleting.

Table 61: CSI verbs for queue access

It is the responsibility of the application to organise the reading from a receiving queue in order to avoid loss of messages.

VIII.2.13 *Putting a message into a queue: HL_mq_put()*

```
CSILONG HL_mq_put(
    CSIMQHCONN     Conn,
    CSIMQHOBJ ObjDesc,
    CSIMQMD   *MsgDesc,
    CSIMQPMO  *PutMsgOpts,
    CSIDD     *DataIn,
    CSIQOS    *QoS,
    CSILONG   *ReturnCode,
    CSILONG   *ReasonCode
);
```

Value of argument "Conn" is identical to the one obtained from HL_mq_conn().

Value of argument "Obj" is identical to the one obtained from HL_mq_open().

Argument "MsgDesc" points to a CSIMQMD structure that was prepared as explained in paragraph VIII.2.1. The values present in this structure after a successful call of the HL_mq_put() are not to be considered.

Argument "DataIn" points to a CSIDD structure that was prepared as explained in paragraph VIII.2.2.

Argument "QoS" points to a CSIQOS structure that was prepared as explained in section VIII.2.6.

Argument "PutMsgOpts" is to be initialised with the statements:

(a) Define a static variable s_DefMQPMO of type CSIMQPMO initialised with constant values:

```
CSIMQPMO s_DefMQPMO = {CSIMQPMO_DEFAULT};
```

(b) Each time the HL_mq_put() verb will be used, define and initialise dynamically a variable s_MQPMO of type CSIMQPMO by using the static variable s_DefMQPMO :

```
CSIMQPMO s_MQPMO;
memcpy(&s_MQPMO, s_DefMQPMO, sizeof(CSIMQPMO));
```

VIII.2.14 Putting a message into a queue: HL_mq_put1()

The verb HL_mq_put1() is identical to the verb HL_mq_put(), with the exception that it uses an additional argument to specify the queue that has to be written to, instead of a queue handle. This verb performs in one call the function of the three operations: HL_mq_open(), HL_mq_put(), HL_mq_close().

Reading a message from a queue: HL_mq_get()

```
CSILONG HL_mq_get(
    CSIMQHCONN      Conn,
    CSIMQHOBJ  ObjDesc,
    CSIMQMD   *MsgDesc,
    CSIMQGMO  *GetMsgOpts,
    CSIDD     *DataOut,
    CSILONG        *MsgLen,
    CSIQOS         *QoS,
    CSILONG *ReturnCode,
    CSILONG *ReasonCode
);
```

Beware: As soon a message has been retrieved from a queue using the HL_mq_get() verb, this message is deleted from the queue.

Value of argument "Conn" is identical to the one obtained from HL_mq_conn().

Value of argument "Obj" is identical to the one obtained from HL_mq_open().

The "MsgDesc" argument contains, as input parameter, a set of attributes the message to retrieve must have and as output parameter the set of attributes the retrieved message actually has.

Method 1
When the application is in such a state that it is waiting for a report message, it has to set two attributes in the "MsgDesc" as follows:

```
MsgDesc.MsgId = CSIMQMI_NONE ;
MsgDesc.CorrelId = {value of the MsgId in the original
message, for which a report is now awaited};
```

This initialisation is to be performed before each HL_mq_get() invocation.

Method 2
When the application is in such a state that it is waiting for any kind of message, it has to set two attributes in the "MsgDesc" as follows:

```
MsgDesc.MsgId = CSIMQMI_NONE ;
MsgDesc.CorrelId = CSIMQCI_NONE ;
```

This initialisation is to be performed before each HL_mq_get() invocation.

While the policy for reading messages from a queue with HL_mq_get() depends on the design of the application architecture, it is recommended though to use the Method 2 in combination with a priority value explained in attribute "Priority" of the "QoS".

This means in practical terms that, within a set of messages read with a uniform "Priority" (see argument "QoS"), the messages will be read in their order of appearance.

They have then to be handled separately in line with the value of the "MsgDesc.MsgType" (either CSIMQMT_REQUEST, CSIMQMT_DATAGRAM or CSIMQMT_REPORT, as stated in Table 56). Any message with its MsgType equal to CSIMQMT_REPORT must be matched to its own originator by the rule:

[report_message.CorrelId] is equal to [original_message.MsgId]

To be able to correlate a report with the related Information Exchange, it is recommended that the software controlling the sending CSI stack maintains a dynamic table that cross-references the state of a CSI message and its message identification. Message identification consists of:

- Value of field CSIMQMD.MsgId in the message sent by the sending NTA;

- Value of field CSIMQMD.CorrelId in a report message given by the sending NTA (exception, COA, expiration, COD).

The "GetMsgOpts" argument is a structure that controls the behaviour of the HL_mq_get() verb. The structure is shown in Table 62:

typedef struct tag		**Initial value**
CSIMQGMO{		
CSICHAR4	StrucId;	CSIMQGMO_STRUC_ID
CSILONG	Version;	CSIMQGMO_VERSION_1
CSILONG	Options;	
CSILONG	WaitInterval;	
CSILONG	Signal1;	(DNC)
CSILONG	Signal2;	(DNC)
CSICHAR48	DynamicQName;	(DNC)
} CSIMGMO;		

Table 62: CSIMQGMO Object Descriptor

Notes:

1. It is a design issue related to the NCA architecture, to choose between an applicative polling of a queue or a triggering mechanism initiated by CCN/CSI software, to be awakened upon a new message forthcoming in the queue. Regarding polling of a queue two processing mechanisms can be used:

   o Constant CSIMQGMO_NO_WAIT is related to first choice;

    o   While CSIMQGMO_ WAIT and value of WaitInterval set relate to second choice.

Whichever the choice taken, two precautions must be taken:

    o   "WaitInterval" cannot be set to CSIMQWI_UNLIMITED when "Options" has value CSIMQGMO_WAIT;

    o   When applicative polling is used ("Options" has value CSIMQGMO_NO_WAIT), then there must be a grace period foreseen in the application between two successive readings in the queue.

Value of argument "DataOut" represents the location of the data, when the value of the "MsgDesc.MsgType" is CSIMQMT_REQUEST or CSIMQMT_DATAGRAM. Otherwise (in the case of a CSIMQMT_REPORT) the CSIDD "DataOut" is left undefined (check this with the value of argument "MsgLen", that must be 0L).

When a value for "DataOut" is defined, the attribute "Flags" of this CSIDD structure defines the way the information in CSIDD is to be represented.

Value of argument "MsgLen" represents the actual length in bytes of the application data in the retrieved message. It must be compared to the attribute "DataOut.DataLen" (see [A4]).

The argument "QoS" represents a CSIQOS structure that describes the particular handling that was applied on "DataOut". Within this structure, only the "Priority" attribute is to be considered in order to satisfy the **Rule for fetching messages from a receiving queue** highlighted in section VIII.2.6.

VIII.2.15 *Browsing through a queue: HL_mq_browse()*

```
CSILONG HL_mq_browse(
     CSIMQHCONN     Conn,
     CSIMQHOBJ ObjDesc,
     CSIMQMD   *MsgDesc,
     CSIMQGMO  *GetMsgOpts,
     CSIDD     *DataOut,
     CSILONG        *MsgLen,
     CSIQOS         *QoS,
     CSILONG *ReturnCode,
     CSILONG *ReasonCode
);
```

All arguments used in this verb are explained as for the HL_mq_get() verb.

The HL_mq_browse() verb does not delete the message read from the queue. An explicit use of the verb HL_mq_delete() is required for deleting it.

Within the "QoS" structure, only the "Priority" attribute is to be considered in order to satisfy the **Rule for fetching messages from a receiving queue** highlighted in section VIII.2.6.

VIII.2.16 Deleting an element from a queue: HL_mq_delete()

```
CSILONG HL_mq_delete(
    CSIMQHCONN      Conn,
    CSIMQHOBJ ObjDesc,
    CSIMQMD    *MsgDesc,
    CSIMQGMO   *GetMsgOpts,
    CSIDD      *DataOut,
    CSILONG        *MsgLen,
    CSIQOS         *QoS,
    CSILONG *ReturnCode,
    CSILONG *ReasonCode
);
```

All arguments used in this verb are explained as for the HL_mq_browse() verb.

Important advice: message may not be left indefinitely in a queue; it must be deleted at some time by using HL_mq_delete(). Otherwise, if the policy of the application is to neglect this message repeatedly, this message will always be in first position to be read after, hence will block the queue for reading any other message.

VIII.2.17 Queue naming and addressing

Messages on CCN are always exchanged between **Gateways**. In Customs systems, two kinds of Gateways have to be considered:

- **National Gateways** used by all the NAs to perform Customs systems business;

- **Commission Gateways** used by Taxation and Customs Union DG, European Anti-fraud Office (OLAF) or its contractors to operate the Customs systems, including SPEED2 Platform, or to develop the CDCA.

It has to be noted that countries and Commission always have multimode Gateways, i.e. both operational and back-up.

On every Gateway, **Environments** will be defined. An environment can be seen as a 'layer' in which messages are exchanged.

Within Customs systems, four environments are defined:

- The **Operational Environment** is used to exchange messages in operations;

- The **National Testing Environment** is used to exchange messages for national testing purposes. In practice, this environment has to be used for National Testing of an NCA using STTA or a National Test Application[32];

- The **Common Domain Testing Environment** is used to exchange messages for testing purposes on the Common Domain. In practice, this environment has to be used

---

[32] This environment will be configured to work in loopback mode, not to exchange messages with other Gateways.

for Conformance Testing with ITSM and International Testing between two or more countries or between two or more countries and Partner Countries via the EC SPEED2 Platform;

- The **Training Environment** is used to exchange messages for training purposes.[33]

The Operational Gateway contains the Operational Environment. The Back-up Gateway contains the Common Domain Testing Environment, the National Testing Environment and the Training Environment.

In every environment, **queues** have to be defined on the different Gateways. It has to be noted that messages should only be exchanged between queues belonging to the same Environment.

Every queue always has the following syntax:

<div style="border:1px solid;">

<QUEUE NAME.XXXX@GATEWAY NAME>

</div>

Where "XXXX" represents the specific Customs system name e.g. NCTS, ECS and ICS.

Within Customs systems, the queues can be divided in several groups based upon their function:

- **'Core flow'** is used for the messages marked as such in Tables residing in the Customs systems' DDNA volumes;

- **'Administration'** is used for IE903, IE904, IE905, IE906, IE907, IE913 and IE917;

- **'Reports'** is used for the CCN/CSI Reports (IE908, IE909, IE910 and IE911). The CCN/CSI reports are returned for every message type. It is received by a sending application in the queue that was indicated by the QoS "ReplyToQ" argument when sending the Information Exchange. It is highly recommended to request these reports in the associated REPORT queue. In this manner, pending reports can be recognised quickly and problems can be identified in a straightforward manner. It is recommended to use the REPORT queue solely for storing those CCN/CSI reports;

- **'Technical Statistics'** is used for CCN/CSI technical statistics from ITSM CONTRACTOR ;[34]

- **'Audit'** is used for CCN/CSI audit files from ITSM CONTRACTOR .[35]

Additional queue group defined for NCTS-P4:

- **'ATIS'** for sending the IE011 to OLAF.

Additional queue group used within NCTS-P4, NCTS-P5, ECS-P2, AES and ICS:

- **'Business Statistics'** is used for IE411[36].

---

[33] This environment will be configured to work in loopback mode, not to exchange messages with other Gateways.

[34] Please note that no queues are defined for NAs for this function.

[35] Please note that no queues are defined for NAs for this function.

Additional queue groups used within NCTS-P5 and AES:

- **'Availability'** is used for IE974, IE975;

- **'Link'** is used for IEx78.

In the following chapters, the queues per environment are defined as well as the actual names to be used for the queues and the Gateways.[37]

Important for users of the ieCA application

READ ALSO the section 6 (Technical Integration with TAXUD ieCA) of
the document **ieCA Use Cases** [R42] that complements this version of the DDCOM.

VIII.2.18   *National Gateways*

VIII.2.18.1   Queue Name

Every National Gateway has to be configured to contain the following queues as shown in Table 63:

Environment	Queue Function	Queue Name
Normal Operation	Core flow	CORE-QUE CORE-IECA-QUE
	Administration	ADMIN-QUE ADMIN-IECA-QUE
	Reports	REPORT-QUE REPORT-IECA-QUE
	Business Statistics	-
	Technical Statistics	-
	Audit	-
	Availability	CSMIS-AVAIL-SEND-QUE[38]
	Link	-

---

[36] Please note that no queues are defined for NAs for this function.

[37] Please note that these chapters focus on the queues to be used by the National Applications. The queues on the Taxation and Customs Union DG gateway and the European Anti-fraud Office gateway that are not part of country-specific configuration are added, as well. Otherwise, they are made available to all NAs.

[38] This queue will be used to receive IE974 messages.

Environment	Queue Function	Queue Name
Common Domain Testing[39]	Core flow	CORE-RCT-QUE CORE-RIT-QUE CORE-CTA-RCT-QUE CORE-IECA-RCT-QUE CORE-IECA-RIT-QUE
	Administration	ADMIN-RCT-QUE ADMIN-RIT-QUE ADMIN-CTA-RCT-QUE ADMIN-IECA-RCT-QUE ADMIN-IECA-RIT-QUE
	Reports	REPORT-RCT-QUE REPORT-RIT-QUE REPORT-CTA-RCT-QUE REPORT-IECA-RCT-QUE REPORT-IECA-RIT-QUE
	Business Statistics	-
	Technical Statistics	-
	Audit	-
	Availability	-
	Link	-
National Testing[40]	Core flow	CORE-LCT-QUE CORE-xx-LCT-QUE
	Administration	ADMIN-LCT-QUE ADMIN-xx-LCT-QUE
	Reports	REPORT-LCT-QUE REPORT-xx-LCT-QUE
	Business Statistics	-
	Technical Statistics	-
	Audit	-
	Availability	-
	Link	-

[39] The CORE-RIT-QUE, ADMIN-RIT-QUE, REPORT-RIT-QUE are to be used for International Testing (Mode-3) between NAs. The ADMIN-RIT-QUE and the REPORT-RIT-QUE queues shall also be used for International testing with EC SPEED2 Platform.
The ADMIN-RCT-QUE and the REPORT-RCT-QUE queues shall be used for the SPEED2 Conformance Testing.
The [Queue Type]- CTA-RCT-QUE queues are used for testing with CTA in the context of NCTS-P5 and AES-P1.
The [Queue Type] -IECA-[Mode]-QUE are used for Conformarnce and International Testing, with the ieCA used as a conversion service in the context of NCTS-P5 and AES-P1.
[40] The CORE-LCT-QUE, ADMIN-LCT-QUE, REPORT-LCT-QUE, are queues mdeant to be attached to the National Customs Application (NCA), while the others are meant to be attached to the local Testing Application (STTA or NCTA). LST queues are not valid for AES-P1 and NCTS-P5.

Training[41]	Core flow	CORE-LST-QUE
		CORE-xx-LST-QUE
	Administration	ADMIN-LST-QUE
		ADMIN-xx-LST-QUE
	Reports	REPORT-LST-QUE
		REPORT-xx-LST-QUE
	Business Statistics	-
	Technical Statistics	-
	Audit	-
	Availability	-
	Link	-

Table 63: Queue Names for National Gateways

Notes:

- In the above table "xx" can take the value 01 – 10 (or value NCTA in case of Reports) to indicate different queues for use (i) by STTA or NCTA in National Testing environment or (ii) by any application in Training environment.

VIII.2.18.2   Gateway Site Names

The name of the CCN Gateway site for each country is published on CIRCABC eCustoms IT aspects.

- For NCTS:
    https://circabc.europa.eu/w/browse/d297088d-9cfa-4e5d-a6e8-d2e47ef33049
- For ECS-P2 / AES:
    https://circabc.europa.eu/w/browse/e7887955-d799-4392-acc1-6f0c11825c21
- For ICS-P1:
    https://circabc.europa.eu/w/browse/2b62dcc0-47a5-43a0-a902-88dd2ff99398

---

[41] The CORE-LST-QUE, ADMIN-LST-QUE, REPORT-LST-QUE are queues meant to be attached to the National Customs Application (NCA), while the others are meant to be attached to an application for Training purposes. LST queues are not valid for AES-P1 and NCTS-P5.

VIII.2.19 Taxation and Customs Union DG Gateways

VIII.2.19.1 Queue Name

The names of the Queues are defined as shown in Table 64:

Environment	Queue Function	Queue Name
Normal Operation	Core flow	EU2XX-CORE-QUE[42] CORE-IECA-[COUNTRY REF][43]-QUE
	Administration	ADMIN-QUE ADMIN-IECA-[COUNTRY REF]-QUE REPORT-IECA-[COUNTRY REF]-QUE
	Reports	REPORT-QUE XX2EU-REPORT-QUE[44]
	Business Statistics	CSMIS-QUE[45]
	Technical Statistics	CSMIS-STATP -QUE[46] CSMIS-STATT-QUE[47]
	Audit	CSMIS-AUDITP-QUE[48] CSMIS-AUDITT-QUE[49]
	Availability	CSMIS-AVAIL-RECEIVE-QUE[50]

---

[42] These queues will be used by the EC SPEED2 Platform to receive the IE012 messages from NTAs for the different NCTS/TIR-DATA Partner Countries. XX will be replaced by the ISO-3166 code of each NCTS/TIR-DATA Partner Country. For example, in the scope of the pilot project NCTS/TIR-RU, the queue EU2RU-CORE-QUE will be used by the EC SPEED2 Platform to receive the IE012 messages that are sent by the NTAs for Russia.

[43] COUNTRY REF: It will be defined during the configuration request. Preferable the country iso code or a code that will distinct the queues that will be configured for the incoming traffic.

[44] These queues will be used by the EC SPEED2 Platform to receive the CCN/CSI Reports from NTAs for the IE907 messages. The IE907 message is sent by the EC SPEED2 Platform in response to an invalid message IE012. For example, in the scope of the pilot project NCTS/TIR-RU, the queue RU2EU-REPORT-QUE will be used by the EC SPEED2 Platform to receive the CCN/CSI reports that are generated by the NTAs when receiving an IE907 message.

[45] The National Customs Applications will use this queue for sending of IE411 operational messages to ITSM.

[46] This queue will be used by the CS/MIS application at ITSM to collect ITSM CONTRACTOR technical statistics files from the Operation environment.

[47] This queue will be used by the CS/MIS application at ITSM to collect ITSM CONTRACTOR technical statistics files from the Backup environment.

[48] This queue will be used to collect CCN/CSI audit files from ITSM CONTRACTOR for the Operation environment

[49] This queue will be used to collect CCN/CSI audit files from ITSM CONTRACTOR for the Backup environment.

Environment	Queue Function	Queue Name
	Link	CSMIS-LINK-QUE[51]
Common Domain Testing[52]	Core flow	CORE-axx-RCT-QUE COR[reference]-[country:id]-RCT-QUE CORE-IECA-[COUNTRY REF]-RCT-QUE CORE-IECA-[COUNTRY REF]-RIT-QUE EU2XX-CORE-xx-RCT-QUE EU2XX-CORE-RIT-QUE
	Administration	ADMIN-axx-RCT-QUE ADM[reference]-[country:id]-RCT-QUE ADMIN-IECA-[COUNTRY REF]-RCT-QUE ADMIN-IECA-[COUNTRY REF]-RIT-QUE
	Reports	REPORT-axx-RCT-QUE REP-[country:id]-RCT-QUE REPORT-IECA-[COUNTRY REF]-RCT-QUE REPORT-IECA-[COUNTRY REF]-RIT-QUE XX2EU-REPORT-xx-RCT-QUE XX2EU-REPORT-RIT-QUE
	Business Statistics	CSMIS-RCT-QUE
	Technical Statistics	CSMIS-STATP-RCT-QUE
	Audit	CSMIS-AUDITP-RCT-QUE
	Availability	CSMIS-AVAIL-RECEIVE-RCT-QUE CSMIS-LINK-RCT-QUE
	Link	CSMIS-LINK-RIT-QUE
National Testing[53]	-	
Training[54]	-	

---

[50] This queue will be used to receive IE975 messages.

[51] This queue will be used to receive IEx78 messages.

[52] The Common Domain Testing environment at the Taxation and Customs Union DG Gateway is used for several purposes:
- **NCTS-P4** Conformance Testing using the TTA or STTA and **ECS-P2** Conformance Testing using the TTA or STTA (CORE-axx-RCT-QUE, ADMIN-axx-RCT-QUE, and REPORT-axx-RCT-QUE) The exact configuration of the queues and their name used for Conformance Testing will be communicated by ITSM to the NAs;
- **NCTS-P5** Conformance Testing using the CTA and **AES-P1** Conformance Testing using the CTA;
- **NCTS/TIR-DATA** Conformance Testing using the SSTA (EU2XX-CORE-xx-RCT-QUE, XX2EU-REPORT-xx-RCT-QUE). The exact configuration of the queues and their name used for Conformance Testing will be communicated to the NAs on the CIRCABC web site;
- **International Testing** will be performed using the EU2XX-CORE-RIT-QUE, XX2EU-REPORT-RIT-QUE queues, which shall be used for the communication with the EU MS.

[53] The National Testing queues defined on the Taxation and Customs Union DG gateway are not use for any interaction with NAs and are, therefore, not defined in DDNA. Taxation and Customs Union DG uses these queues for internal testing purposes.

Table 64: Queue Names for Taxation and Customs Union DG Gateways

Notes:

- In the above table for NCTS-P4, ECS-P2 and ICS-P1, "a" is the TTA Role and "xx" is a value 01 – YY creating a string, which indicates the different queues for use by TTA in Common Domain Testing environment (e.g. "CORE-OoDep01-RCT-QUE"). The TTA roles are defined in the TTA SRD [R22];

- In the above table for NCTS-P5 and AES-P1, the following naming convention is used for the CTA queues:

  - reference = "1 .. n" // Order of the country impersonated by CTA in a specific scenario. Not used for REPORT.

  - country:id = "nn" //A 2-digit numeric ID for each country

- In the above table, "xx" is a value 01 – YY creating a string, which indicates the different queues for use by SSTA in Common Domain Testing or National Testing environment (e.g. "EU2RU-CORE-01-RCT-QUE"). Currently, the SSTA will play the role of EC SPEED2 Platform for the Common Domain Testing with the Member States of EU and the role of Member State of EU for the National testing environment;

- In the above table, "XX" is the ISO-3166 Country Code creating a string, which indicates the different queues for use with NCTS/TIR-DATA Partner Country (e.g. "EU2MD-CORE-01-RCT-QUE").

VIII.2.19.2   Gateway Names

The Gateway name of the Taxation and Customs Union DG Gateways is 'ITSM.TC'.

---

54 The Training queues defined on the Taxation and Customs Union DG gateway are not use for any interaction with NAs and are therefore not defined in DDNA. Taxation and Customs Union DG uses these queues for training purposes.

VIII.2.20 European Anti-fraud Office Gateway

VIII.2.20.1   Queue Name

The names of the Queues are defined as shown in Table 65:

Environment	Queue Function	Queue Name
Normal operation	ATIS	TRANSIT-MSG-QUE.NCTS@OLAF.EC EXPORT-MSG-QUE.ECS@OLAF.EC
Common Domain Testing[55]	ATIS	TRANSIT-MSG-RCT-QUE.NCTS@OLAF.EC EXPORT-MSG-RCT-QUE.ECS@OLAF.EC TRANSIT-MSG-RIT-QUE.NCTS@OLAF.EC EXPORT-MSG-RIT-QUE.ECS@OLAF.EC
National testing[56]	-	
Training[57]	-	

Table 65: Queue Names for European Anti-fraud Office Gateway

VIII.2.20.2   Gateway Names

The name of the Gateway Site for OLAF must be available to all MSs.

VIII.2.21 Queue usage Overview

The following chapters provide an overview of the usage of the queues in the different environments by the NCA.

In every figure, the left side is the NCA and the right side shows the application with which it is communicating. To be noted:

If the CCN/CSI network is coloured grey, it indicates the Back-up Gateway has to be used. Otherwise, the Operational Gateway has to be used.

The queues that are coloured grey, are those defined at the Commission Gateways. The others are defined at the NA Gateways.

---

[55] The Common Domain Testing queues defined on the European Anti-fraud Office Gateway are used for International Testing (Mode-3) between NA and OLAF.

[56] The National Testing queues defined on the European Anti-fraud Office Gateway are not used for any interaction with NAs and are therefore not defined in DDNA. European Anti-fraud Office (OLAF) uses these queues for internal testing purposes.

[57] The Training queues defined on the European Anti-fraud Office Gateway are not used for any interaction with NAs and are therefore not defined in DDNA. European Anti-fraud Office (OLAF) uses these queues for training purposes.

VIII.2.22 Operational Environment

The following diagrams graphically depict the normal operations of an NCA that interacts with another NCA or with the Central Services Applications.
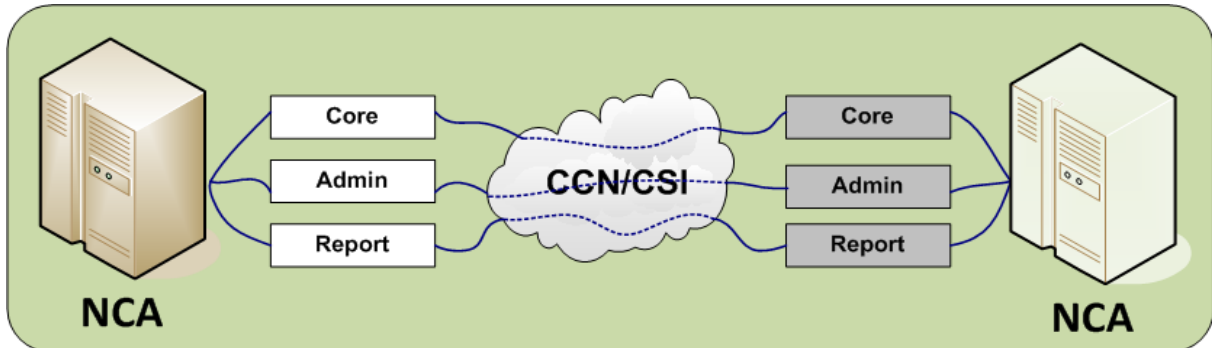
Figure 37: Normal Operations with an NCA
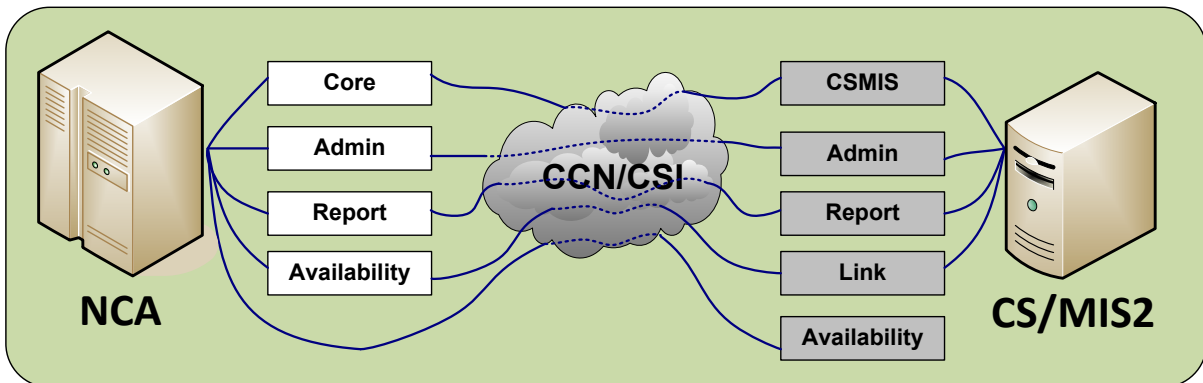
Figure 38: Normal Operations with CS/MIS2
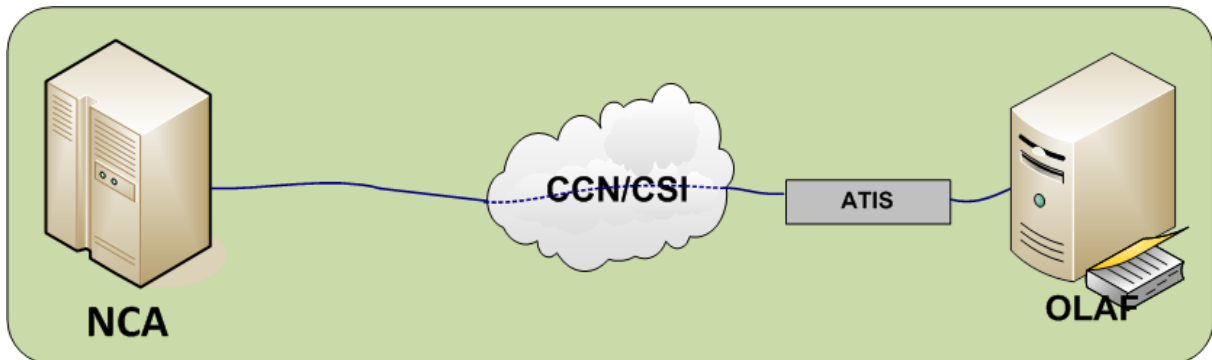
Figure 39: Normal Operations with OLAF (ATIS)

The following diagram graphically depicts the normal operations of an NCA that interacts with the EC SPEED2 Platform.
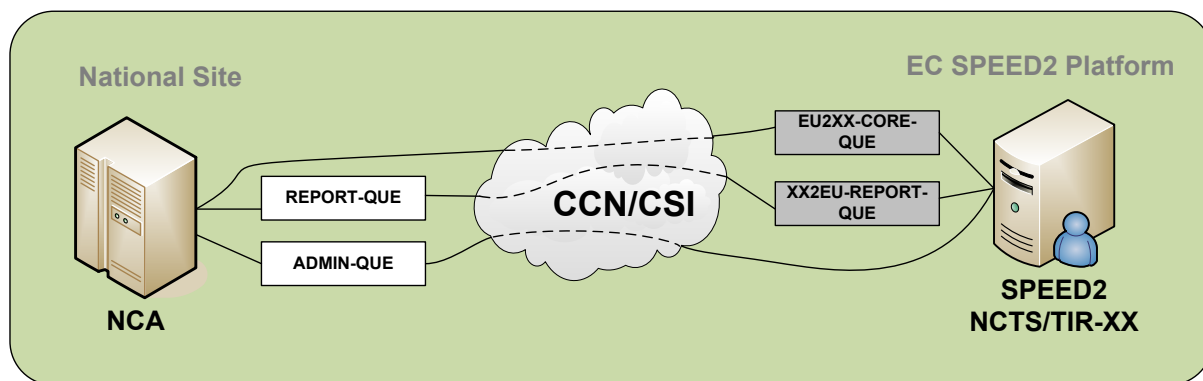
Figure 40: Interactions between an NCA and the EC SPEED2 Platform in Normal Operations environment [58]

VIII.2.23 Common Domain Testing Environment

The following diagrams graphically depict the operations for Conformance Testing of an NCA.
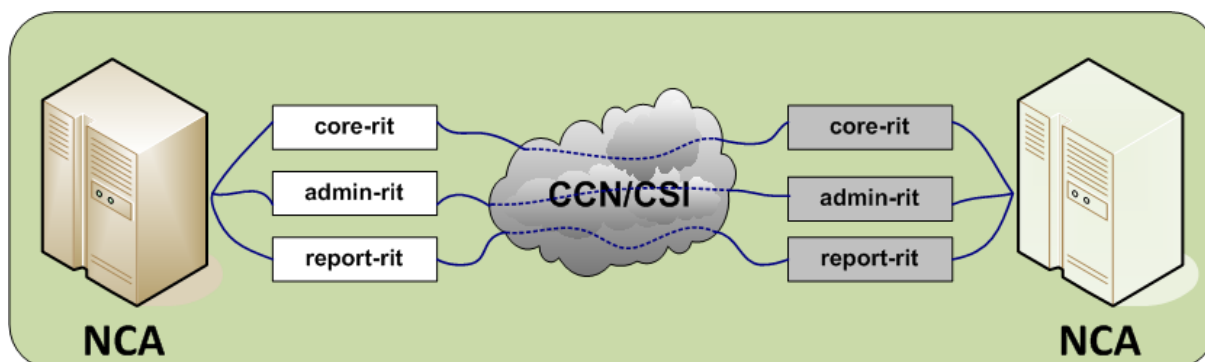
Figure 41: International Testing with another NCA
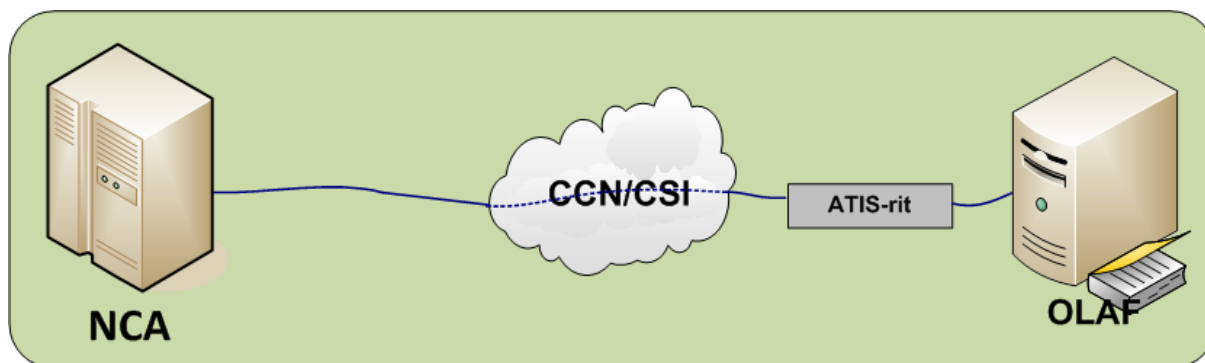
Figure 42: International Testing between NCA and OLAF

---

[58] Please note that the information exchange continues after SPEED2 Platform and Partner Country, however, this communication is not shown in this figure since it is out of scope of this document.
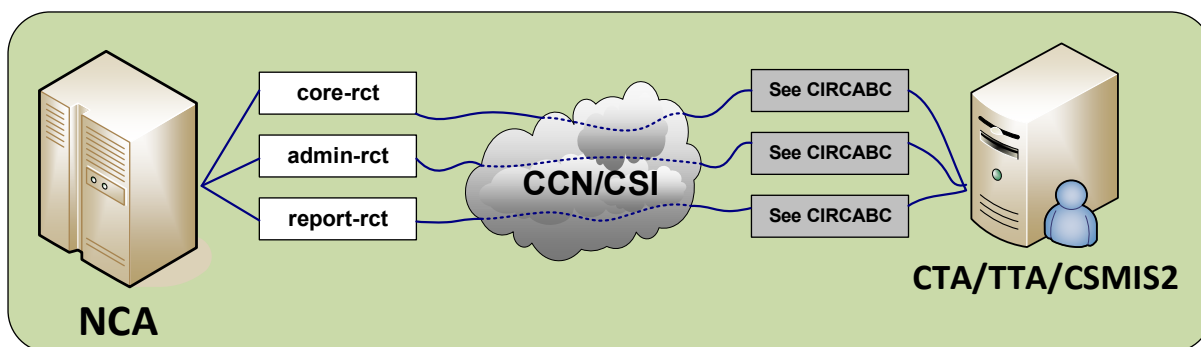
Figure 43: Conformance Testing

The following diagrams graphically depict the operations for Conformance and International Testing of an NCA that interacts with the EC SPEED2 Platform.
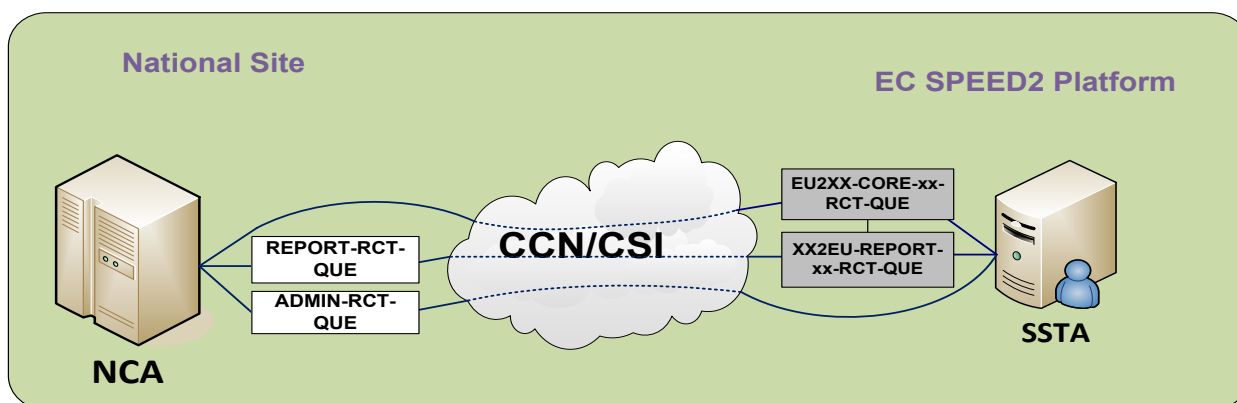
Figure 44: Interactions between an NCA and the EC SPEED2 Platform in Conformance testing environment with NCA
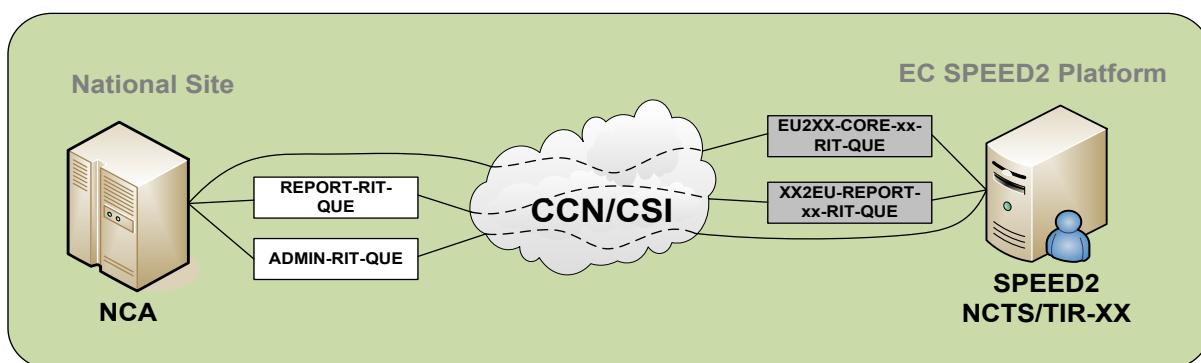
Figure 45: Interactions between an NCA and the EC SPEED2 Platform in International testing environment[59]

---

[59] Please note that the information exchange continues after SPEED2 and Partner Country, however, this communication is not shown in this figure since it is out of scope of this document.

VIII.2.24 National Testing and Training Environments

The following diagrams graphically depict the operations for National Testing of an NCA.
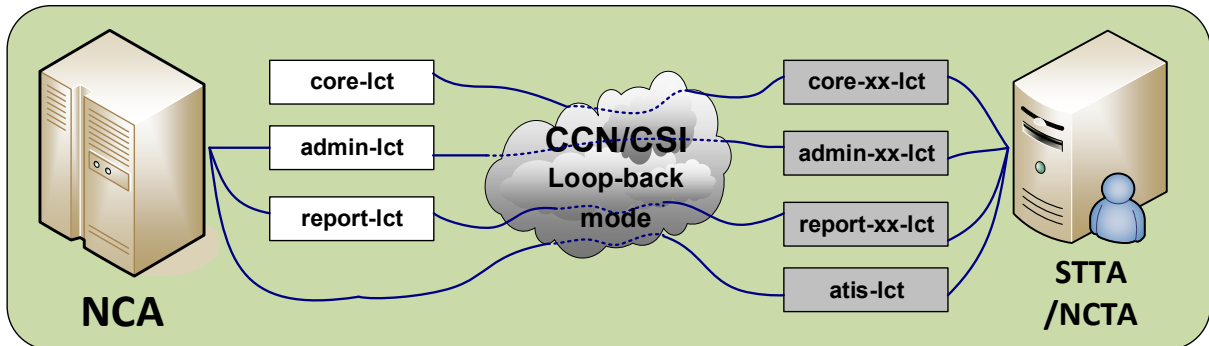
Figure 46: National Testing with STTA or NCTA
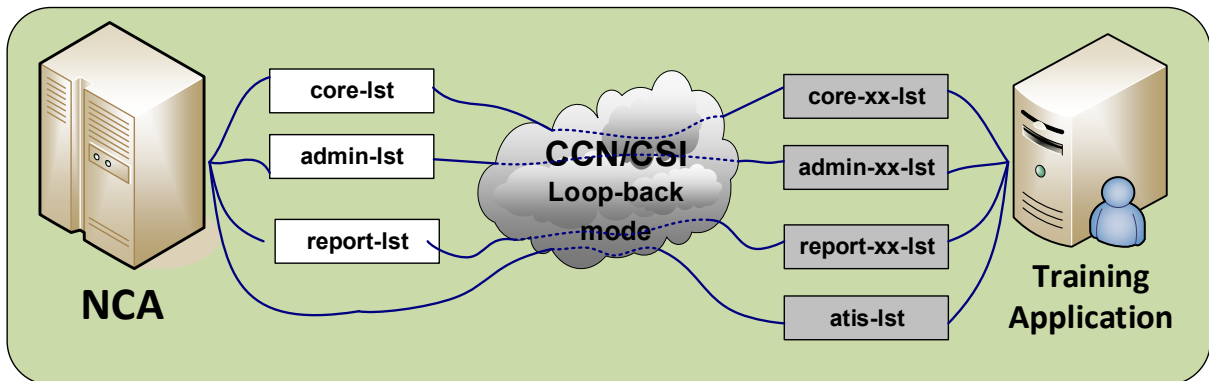
Figure 47: Training with a Training Application

VIII.2.25 Access Control List

User Profiles are defined by the ITSM at Configuration time (see paragraph VIII.4.6).

User Profiles are defined, corresponding to the different types of queues defined in each specific domain. The NA Local Security Officer associates User Identifiers with each of the User Profiles, as he/she deems useful.

These data are subsequently used when opening a security context (see paragraph VIII.2.9).

VIII.2.26 Maximum Message size

The maximum size of a message handled by the CSI stacks (NJCSI, C CSI) is 4GB. The recommended limit (for the data before encryption) is ~10% lower, if integrity or confidentiality is enabled in the applied Quality of Service.

For the purpose of NCTS-P5 and AES-P1, the maximum size of the CCN message (after compression) is fixed at 20 MBytes. Consequently, the National Applications must define and apply limits on the declaration messages, to avoid that a declaration message is accepted from

the declarant, but cannot be exchanged on the Common Domain. Each National Transit Application must be able to receive and process the Common Domain messages with the multiplicity defined in the Appendix Q2 (when the size of the message is below the limit of 20 MBytes per compressed message). A similar approach is applicable to AES-P1.

VIII.3 Recommended use of CCN/CSI

This section illustrates the use of CCN/CSI in a send and receive routine. This example is only a guide for implementation. It is up to each NA to implement its routines for sending and receiving. The specifications of both routines show the general sequence of synchronous interaction between the application and the corresponding CSI component on the Gateway ("Remote API Proxy"). They illustrate how and where the naming and addressing rules must be applied (examples of C-programs can be found in [A1]).

The routines are specified in a C-like pseudo-code. The setting of a number of parameters of CSI verbs is not shown when these are not relevant for this explanatory purpose.

VIII.3.1   Main routines

Typical execution phases are as follows:

1. Program Connection phase:

    o Program binding to the CSI stack (HL_bind);

    o Establishment of a security context (HL_init_sec_context);

    o Connection to the local Queue Manager (HL_mq_conn).

2. Sending phase:

    o Opening of a message queue with the appropriate options (HL_mq_open);

    o Encode the data descriptor passed by the application into another data descriptor, which will be handled by the Sending function, by using a Presentation profile, which corresponds to the Information Exchange type (HL_encode);

    o Send a message to a remote queue that has been opened for output (HL_mq_put). If a queue has not yet been opened, the verb HL_mq_put1 can be used. This latter verb also implies closing the queue after inserting the message into it;

    o Closing the opened message queue (HL_mq_close).

3. Receiving phase:

    o Opening of a message queue with the appropriate options (HL_mq_open);

    o Destructive extraction of a message from a local queue (HL_mq_browse, HL_decode, and HL_mq_delete). This sequence of verbs is recommended, rather than the verb HL_mq_get, to overcome deletion of a message if it does not fit in a memory buffer;

o Decode the received data descriptor into another data descriptor, for application usage. No application profile is to be communicated to this verb. This verb checks the correctness of the CodePage and HostFormat used;

o Closing the opened message queue (HL_mq_close).

4. Program Disconnection phase:

o Disconnection from the Queue Manager (HL_mq_disc);

o Destruction of the security context (HL_delete_sec_context);

o Disconnection from the CSI stack (HL_unbind).

These four execution phases can be executed in a sequence as is for instance shown by Figure 48. Other sequences are also possible, e.g. parallel sending and reception of messages or parallel sending of messages to different queues. Another option is to combine the Sending and Receiving phases into one routine. This routine may first send and secondly read messages out of queues.

It is recommended to distinguish between priorities in sending and receiving, e.g. first browsing a queue for high priority messages before the messages with normal priority are received from the same queue.

For reception, all available queues for reading identified via the Access Control List need to be browsed. A sequence of browsing and reading is up to each application developer.
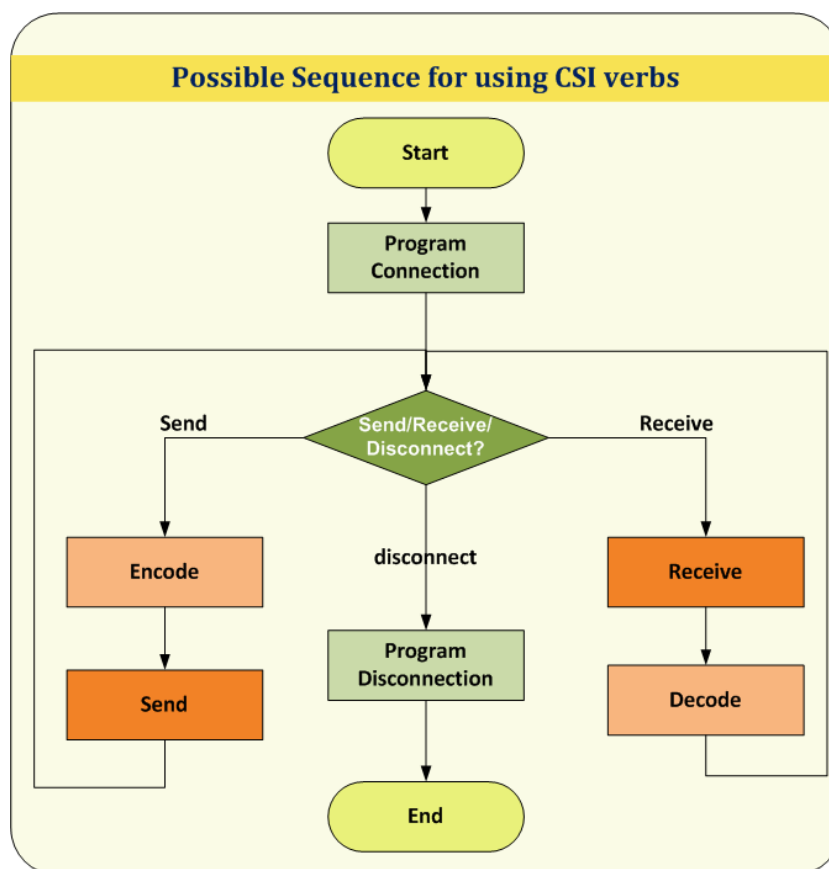
Figure 48: A possible sequence for using CSI verbs

Message queue opening and closing and queue access verbs, as shown in the Sending and Receiving phases, can be inter-mixed in any sequence with the restriction that queues must be properly opened before messages can be written to or read from it.

All program interactions are with the local Queue Manager running in the local CCN gateway. As a consequence, the transmission and processing delays do not slow sending or receiving programs and the response times are significantly improved.

Errors related to the use of CCN/CSI are specified in the appropriate CCN/CSI documentation. They have to be handled by an application program connecting to the CSI stack.

The next examples use the arguments (CSILONG) **pReturnCode, pReasonCode** as output parameters of a CSI verb. The first indicates success or failure and, in case of failure, the second gives the reason for failure. Working code should check these values after every CCN/CSI call.

VIII.3.2   *Program connection*

The following pseudo-code is given for connection of an application named "NCA" to the CCN Gateway.

Connect (out MQHCONN, Returncode)

- The result of the connection is an identifier that needs to be used for sending, receiving, and disconnecting a session with the CCN Gateway (MQHCONN). The result of the execution of this routine is given in Returncode. Errors for executing verbs can possibly be hidden in the connect routine by retrying to connect to the Gateway more than once. Some errors, e.g. there is no validated user password, which require a systems administrator to take action, need to be passed to the application.

HL_bind (in "NCA", "", out CSIQOS, pReturnCode, pReasonCode)

- *"NCA"* is now bound to the CSI stack. Default ProxyName was used (the empty string "").

- Default QoS for "NCA" is returned by the Gateway in parameter CSIQOS.

- The first CSILONG indicates the success or failure of the verb execution, whereas the second specifies an error reason. If CSILONG indicates a failure, a retry of Connect may be tried, depending on the error reason.

- The application is in charge of obtaining security credentials: UserName equals "NCA" and, "UserPassword" and "ApplicationKey" have to be valid parameter values checked by the CCN Gateway. The variable SecurityInfo, with type CSISECINFO, has been filled as explained above in paragraph VIII.2.9.

HL_init_sec_context (in SecurityInfo, out pReturnCode, pReasonCode)

- Security context between Application Platform and CCN gateway is established. If the security context could not be established, the CSILONG parameters contain the success or failure with the associated reason. The application key and username is checked by the X.500 directory of the Gateway. Both parameters need to be known to the application.

HL_mq_conn (in Mqman, out MQHCONN, pReturnCode, pReasonCode)

- Application is connected to the message queue management system identified by Mqman. The Gateway returns the status of the execution of the verb and an identifier to be used during exchange of information between the "NCA" and the Gateway (MQHCONN).

VIII.3.3 Sending

For sending a EDIFACT interchange to a given queue in the context of a connection previously set up, the pseudo-code is as follows:

queuename: name of a queue as defined in previous paragraphs, for example:

CORE-LCT-QUE.NCTS@CUSTTAX.NL

send(in EDIFACT_interchange, queuename, MQHCONN, Correlation Identifier out ReturnCode, Correlation Identifier)

- The send routine is specified as a high level routine that returns an error if something failed that could not be solved internally by this routine. The send routine can be extended by its internal error handling, thus hiding some specific results returned by a CCN Gateway. These results can be hidden by, for instance, retrying certain verbs several times. The Correlation Identifier parameter is a list to store the reference that is used by a CCN report message.

prepare_objdesc(in queuename, out ObjDesc)

- A structure ObjDesc is used to pass the name of the queue to be opened.

HL_mq_open (in MQHCONN, ObjDesc, CSIMQOO_OUTPUT, out Handle, pReturnCode, pReasonCode)

- The target queue is open for output. The MQHCONN refers to the connection between the NCA and the Queue Manager. The name of the queue to open is retrieved in ObjDesc. The option CSIMQOO_OUTPUT makes the queue available for writing messages. The CSILONG parameters contain the result of the execution of the verb. The Handle is to be used for further access to the queue, once it has been opened.

HL_alloc (in sizeof(EDIFACT_interchange), out * pDataDesc, pReturnCode, pReasonCode

memcpy(pDataDesc->Data, EDIFACT_interchange, sizeof(EDIFACT_interchange))

- A CSI Data Descriptor structure is allocated for the message to be queued. The CSILONG parameters contain the result of the execution of the verb;

- The actual buffer to be sent is copied into the CSI Data Descriptor structure.

HL_encode (in pDataDesc, MSG_TYPE_ID, CodePage, HostFormat, out pDataDesc, pReturnCode, pReasonCode)

- The HL_encode adds the coding information into the Header field of the data descriptor. The code page and host format can be found in the included files generated by the presentation tools on the Gateway;

- The data descriptor used is that returned by the HL_alloc. It is used for input of the EDIFACT interchange and the same data descriptor is given for output. This use is recommended to avoid any unnecessary duplication of data;

- MSG_TYPE_ID is a value stored in the X500 directory of the CCN Gateway; while not actually modifying the data, it tags the message for technical statistics purpose.

HL_mq_put (in MQHCONN, Handle, inout pMsgAttributes, pPutOptions, pDataDesc, in CSIQOS, out pReturnCode, pReasonCode)

- The message is queued in the local CCN gateway and will be forwarded to the remote queue identified by the Handle. The pDataDesc contains the information to send;

- The result of the execution of the verb, its applied QoS and a reason in case of failure is returned by the Gateway. Additional code is needed to act upon the result;

- The QoS parameters are either the default ones or the changed ones. They contain the reference for correlating the result. The result itself can be received in the administration queue of the NCA. Separate receive routines need to be developed to correlate a Confirm On Delivery with a message.

HL_mq_close (in MQHCONN, Handle, CSIMQCO_NONE, out pReturnCode, pReasonCode)

- The queue is now closed.

HL_free (in pDataDesc, out pReturnCode, pReasonCode)

- The data descriptor structure is cleaned up.

VIII.3.4   Receiving

queuename: name of a queue as defined in previous paragraphs, for example:

CORE-LCT-QUE.ECS@CUSTTAX.NL

which is the incoming queue for national testing of the core flow messages by the Dutch installation of the NECA.

receive(in queuename, Correlation Identifier, MQHCONN, out Returncode)

- Receive can be made such that either one interchange is received or several. The example does not show that a result is returned but the result is copied to a file on disk that can be used for conversion to the internal data structure of the NCA. The way in which errors will be handled can be similar to the approach taken for sending;

- The Correlation Identifier is used for receiving a CCN report message. It might be stored in memory or on file and used whenever a CCN report message is received.

prepare_objdesc(in queuename, out ObjDesc)

- A structure ObjDesc is used to pass the name of the queue to be opened.

HL_mq_open (in MQHCONN, ObjDesc, CSIMQOO_BROWSE, out Handle, pReturnCode, pReasonCode)

- The queuename is now open for browsing.

HL_alloc (in sizeof(EDIFACT_interchange), out pDataDesc, pReturnCode, pReasonCode)

- A CSI Data Descriptor structure is allocated for the incoming EDIFACT interchange(s) with enough space for incoming message. If the browsing of the queue (step below) detects that still more room is needed, then HL_free and again HL_alloc have to be applied in this order;

HL_mq_browse (in MQHCONN, Handle, inout pMSGDesc, pBrowseOptions, out pDataDesc, MSGLEN, CSIQOS, pReturnCode, pReasonCode))

- The message has been taken non-destructively from the local queue.

HL_decode (in pDataDesc, CodePage, HostFormat, out pDataDesc, pReturnCode, pReasonCode)

- The message needs to be decoded according to the CodePage and HostFormat;

- This verb operates without using a Presentation profile because of its very purpose, which is to free the application from this burden;

- It is recommended to put the message on a disk before deleting it from a queue. This is to prevent loss of messages in case of systems failure between deleting and storing a message.

**If
(pMSGDesc.MsgType = 'CSI_MQMT_REPORT' and pMSGDesc.Feedback in_set('CSIMQFB_COD','CSIMQFB_COA', 'CSIMQFB_EXPIRATION', 'CSIMQRC_*'))
then
checkCCN_REP (in Correlation Identification, pDataDesc.pMSGDesc, out returncode)**

- If the correlation of a received CCN report with an identifier contained in the Correlation Identification structure is not successful, an error is returned and the CCN report is deleted. The error needs to be logged. If it is successful, the Correlation Identification is updated to log the reception of the CCN report. These actions are not shown here.

HL_mq_delete (in MQHCONN, Handle, inout pMSGDesc, pDeleteOptions, out pReturnCode, pReasonCode))

- The message has been deleted from the local queue.

HL_mq_close (in MQHCONN, & Handle, CloseOptions, out pReturnCode, pReasonCode)

- The queue is now closed. The Handle is no longer valid.

HL_free (in pDataDesc, out pReturnCode, pReasonCode)

- The data descriptor structure is cleaned up.

VIII.3.5 Program disconnect

disconnect (in MQHCONN, out Returncode)

- The purpose is to release the session with the CCN Gateway. It can be successful or fail.

HL_mq_disc (inout MQHCONN, out ReturnCode, ReasonCode)

- The application is disconnected from the message queuing system or not. See 'ReasonCode' values for this verb in [A7].

HL_delete_sec_context (out ReturnCode, ReasonCode)

- The security context is deleted, either successful or not. See 'ReasonCode' values for this verb in [A6].

HL_unbind (out ReturnCode, ReasonCode)

- The session is terminated either successful or not. There is no entry for this verb [A6].

VIII.4 Configuration information

VIII.4.1 Introduction

This chapter presents the steps that need to be performed to set up the parameters on the CCN Gateways.

This chapter is divided into:

- The information to be prepared by a NA for all objects that are specific to each NA;

- The information to be prepared by ITSM and that are required to ensure end-to-end interoperability.

Chapter 5 of document [R9] presents a Responsibility Model that distributes the choices to be taken between several roles. It is applicable for all Customs systems. The roles applicable for Customs movement systems are:

Roles for Customs Systems	
CDIA	the ITSM CONTRACTOR Directory Administrator, responsible for the central management of the CCN directory
CASO	the Central Application Security Officer, responsible for security issues that concern a given application of the Taxation and Customs Union DG, running over the CCN/CSI system. This is actually the ITSM
CSO	ITSM CONTRACTOR Central Security Officer
LAD	a Local Application Designer, responsible for the design of an NDCA program. In the case of a CDCA, the contractor designer has to further subdivide the design issues between what the CDCA was able to decide and what is left to the NA development to decide
LSO	the Local Security Officer, responsible for security issues for an NDCA
LSYA	the Local System Administrator for the NDCA infrastructure, responsible for the system management
LAA	the Local Application Administrator for the NDCA infrastructure, responsible for the management of the CCN directory data related to the local users of NDCA: this amounts to maintaining the list of UserIds with respect to UserProfiles

Table 66: Roles for Customs Systems

VIII.4.2   Configuration information to be provided by the NA

Security aspects for Customs systems are defined in [R33].

Concerning CCN/CSI exchanges, a number of standard security features of the CCN/CSI network will be used. The NA only needs to set up the proper security configuration on their gateways, in co-ordination with the ITSM CONTRACTOR. For CCN/CSI exchanges, document [A5] is containing additional information on security aspects.

VIII.4.3   Collection of External Configuration Data

The words 'Entity' and 'Attributes' used in Table 67 refer to the ERD defined in [R9].

The associated values depend on the technical infrastructure that exists within an NA.

These values have to respect the "Formatting Rules" defined in heading 5.3 of [R9].

The values have to be entered onto forms in Annex C of [R9].

It is necessary to cooperate with ITSM for the practical handling of these forms as shown in Table 67.

Entity	Attribute	Provided by	Managed by
Application	ccnApplicationName	LAD	CDIA
	ccnApplicationType	LAD	CDIA
	ccnAddress	LAD	CDIA
	ccnAddressType	LAD	CDIA
	ccnAuthorizedSecurityMechanisms	LAD	CDIA
	ccnDefaultSecurityMechanisms	LAD	CDIA
	ccnDataRepresentationRules	LAD	CDIA
	ccnDefaultCodePage	LAD	CDIA
	ccnApplicationActivationMode	LAD	CDIA
	ccnApplicationExchangeMode	LAD	CDIA
	ccnConversationalModeEnabled	LAD	CDIA
	ccnApplicationSecurityKey	LSO	LSA or LAA
	ccnDefaultQOS	LAD	CDIA
	ccnOperationalStatus	LSYA	CDIA
	ccnPlatformName	LAD	CDIA
	ccnRAPName	LAD	CDIA
Platform	ccnPlatformName	LAD	CDIA
	ccnAddress	LAD	CDIA
	ccnAddressType	LAD	CDIA
	ccnAuthorizedSecurityMechanisms	LAD	CDIA
	ccnDefaultSecurityMechanisms	LAD	CDIA
	ccnDataRepresentationRules	LAD	CDIA
	ccnDefaultCodePage	LAD	CDIA
	ccnOperationalStatus	LSYA	CDIA
Queue	ccnQueueName	LAD	CDIA

Entity	Attribute	Provided by	Managed by
	ccnTriggerEnabled	LAD	CDIA
	ccnTriggerType	LAD	CDIA
	ccnMaxQueueDepth	LAD	CDIA
	list of ccnApplicationName	LAD	CDIA
Remote API Proxy	ccnRAPName	LAD	CDIA
	ccnMinNbOfRAPInstances	LAD	CDIA
	ccnMaxNbOfRAPInstances	LAD	CDIA
User	ccnUserName	LSO	LSA or LAA
	ccnUserPassword	LSO	LSA or LAA
	ccnUserDisabled	LSO	LSA or LAA
	ccnOrganisationName	LSO	LSA or LAA
	list of ccnUserProfileId	LSO	LSA or LAA

Table 67: External Configuration Data defined by NA

VIII.4.4   Message configuration procedure

The message configuration procedure is performed by ITSM. NAs are using the ACT tool to request the creation of queues.

Note that the information 'ccnDataRepresentationRules' and 'ccnDefaultCodePage' presented in paragraph VIII.4.3 will be used by the ITSM to generate files specific to the NCA development.

VIII.4.5   Configuration information to be provided by the Customs systems Central Operation

VIII.4.6   Collection of External Configuration Data

Entity	Attribute	Provided by	Managed by
Application	ccnDefaultQOS	LAD-CAD	CDIA
CCN/CSI organisation	ccnOrganisationName	CDIA	CDIA
CCN gateway	ccnGatewayName	CDIA	CDIA
Message	ccnMessageId	CAD	CDIA
	ccnMessageFormalDefinition	CAD	CDIA
Queue	list of ccnUserProfileId	CASO	CSA
	list of ccnUserProfileId	CASO	CSA
	ccnGatewayName	CAD	CDIA
Remote API Proxy	ccnGatewayName	CAD	CDIA
User profile	ccnUserProfileId	CASO	CSA

Table 68: External Configuration Data defined by ITSM

The values to be configured by ITSM are detailed below.

VIII.4.7   ccnDefaultQOS

As explained in the value configured on all Gateways for all applications may be overridden upon each call (HL_mq_put() or HL_mq_put1()) performed by an application. The values from Table 69 will be entered into CCN/CSI application configuration form -part 4:

▪ Priority:	5
▪ ReportRequest:	▪ Exception ▪ Expiration ▪ Confirm on Arrival ▪ Confirm on Delivery ▪ PassMessageId ▪ PassCorrelId
▪ ReplyToQ:	left empty
▪ Integrity:	Forbidden
▪ Confidentiality:	Forbidden
▪ Compression:	Forbidden
▪ CompressionId:	LZW
▪ DegradedMode:	NotAllowed -- N/A anyway
▪ CoT:	DEFAULTCOT

Table 69: Configuration of default QoS

VIII.4.8   ccnGatewayName

See Table 68.

VIII.4.9   ccnOrganisationName

See Table 67 and Table 68.

VIII.4.10 ccnMessageId

[Msg Type]**-MSG.[DOMAIN]**

Where

- ▪ [Msg Type] is the message type of the IE, defined in the domain specific DDNA volumes ([R16], [R17] and [R18]);

- ▪ [DOMAIN] is the domain (e.g. NCTS, ECS or ICS).

An indicative example for a *ccnMessageId* for NCTS is the following:

CD001C-MSG.NCTS

VIII.4.11 ccnMessageFormalDefinition

See paragraph VIII.4.13.

VIII.4.12 *ccnUserProfileId*

Syntax for defining the *ccnUserProfileId* is:

```
[UserProfileId][ApplicationModeSuffix]-PRF.DOMAIN
```

Where "DOMAIN" represents the specific Customs system name e.g. NCTS, ECS, ICS. The UserProfileIds correspond to the following queues:

- CORE-QUE
- EU2XX-CORE-QUE[60]
- ADMIN-QUE
- REPORT-QUE
- XX2EU-REPORT-QUE[61]
- CSMIS-QUE
- STAT-QUE
- AUDIT-QUE
- CORE-RCT-QUE
- ADMIN-RCT-QUE
- REPORT-RCT-QUE
- CORE-CTA-RCT-QUE
- ADMIN-CTA-RCT-QUE
- REPORT-CTA-RCT-QUE
- CORE-IECA-RCT-QUE
- ADMIN-IECA-RCT-QUE
- REPORT-IECA-RCT-QUE
- CORE-IECA-RIT-QUE
- ADMIN-IECA-RIT-QUE
- REPORT-IECA-RIT-QUE
- CSMIS-RCT-QUE
- STAT-RCT-QUE
- AUDIT-RCT-QUE
- CORE-LCT-QUE
- CORE-xx-LCT-QUE
- ADMIN-LCT-QUE
- ADMIN-xx-LCT-QUE
- EU2XX-CORE-xx-RCT-QUE
- EU2XX-CORE-RIT-QUE
- REPORT-LCT-QUE
- REPORT-xx-LCT-QUE

---

[60] "XX" being the ISO-3166 Country Code of the various NCTS TIR DATA Partner Countries.

[61] "XX" being the ISO-3166 Country Code of the various NCTS TIR DATA Partner Countries.

- CORE-LST-QUE
- CORE-xx-LST-QUE
- ADMIN-LST-QUE
- ADMIN-xx-LST-QUE
- REPORT-LST-QUE
- REPORT-xx-LST-QUE
- XX2EU-REPORT-xx-RCT-QUE
- XX2EU-REPORT-RIT-QUE
- COR[reference]-[country:id]-RCT-QUE
- ADM[reference]-[country:id]-RCT-QUE
- REP-[country:id]-RCT-QUE
- CORE-IECA-[COUNTRYREF]-RCT-QUE
- ADMIN-IECA-[COUNTRYREF]-RCT-QUE
- REPORT-IECA-[COUNTRYREF]-RCT-QUE
- CORE-IECA-[COUNTRYREF]-RIT-QUE
- ADMIN-IECA-[COUNTRYREF]-RIT-QUE
- REPORT-IECA-[COUNTRYREF]-RIT-QUE
- CORE-axx-RCT-QUE
- ADMIN-axx-RCT-QUE
- REPORT-axx-RCT-QUE
- CORE-RIT-QUE
- ADMIN-RIT-QUE
- REPORT-RIT-QUE

Notes:

In the above list,

1. "a" is the TTA Role, which are defined in the TTA SRD [R22];

2. "xx" is a value 01 – YY creating a string, which indicates the different queues for use by TTA/STTA;

3. The following queues EU2XX-CORE-QUE, XX2EU-REPORT-QUE, EU2XX-CORE-xx-RCT-QUE, EU2XX-CORE-RIT-QUE, XX2EU-REPORT-xx-RCT-QUE and XX2EU-REPORT-RIT-QUE are applicable only to NCTS domain.

4. - QUEUE TYPE = 'COR' || 'ADM' || 'REP' **// CORE, ADMIN, REPORT**

    - reference = "1 .. n" **// Order of the country impersonated by CTA in a specific scenario. Not used for REPORT.**

    - country:id = "nn" **// A 2-digit numeric ID for each NA**

VIII.4.13 Message configuration procedure

In Figure 49, an example of IDL definition is depicted (part of the IDL definition) for the NCTS messages, which are exchanged over the Common Domain. A full definition of all messages of each domain will be contained in the corresponding domain specific DDNA volumes ([R16], [R17] and [R18]). There, the MsgTypeId of each message is defined. The report messages are not defined with an IDL description.

The ITSM compiles this IFL definition and must forward to each NA the files obtained from this compilation. Section 6 of document [R9] has to be followed for this process.

The IDL definition of CCN Messages for each domain is based on the following syntax:

Figure 49: Example of IDL definition of CCN Messages for NCTS

VIII.5   Description of statistics

VIII.5.1   Introduction

The explanations in this chapter are extracted and summarised from documents produced by ITSM CONTRACTOR.

The CCN/CSI system includes a statistics service, which allows collection of various statistics information about the traffic generated by any application domain relying on the CCN/CSI infrastructure.

Files holding statistics information are first created locally on each CCN gateway, are later transferred and archived on a ITSM CONTRACTOR gateway and are finally dispatched to the ITSM. See [A1] for details about the CCN/CSI statistics generation, centralisation and dispatch processes and [A2] for the specification of the CSI application to be used by ITSM to receive the statistics files dispatched by the ITSM CONTRACTOR .

VIII.5.2   Requirement to be fulfilled by ITSM CONTRACTOR

Two pairs of daily statistics files must be generated on each CCN gateway participating in the Customs systems: one pair for each system and each pair will consist of two files.

The first file (**MSGS**) provides information about the Customs system application messages. It contains a detailed view of the type, number and size of the Customs system application messages exchanged between the NA participating in the Customs system during that day.

The second file (**REPS**) provides information about the report messages associated to these Customs system application messages. It contains a detailed view of the type and number of report messages associated to these Customs system application messages during that day.

VIII.5.3   Specification of the MSGS file

The **MSGS** file is a plain ASCII file, composed of a sequence of lines formatted as follows: NA;DIR;TYPE;NBMSG;AVSZ;MINSZ;MAXSZ (Table 70).

Specification of the MSGS file	
NA	Is the ISO identifier of the remote NA for which statistics are provided (**AT**, **BE**, …).
DIR	Indicates whether the statistics provided concern outgoing or incoming Customs system application messages ("O" for application messages sent to the Common Domain, "I" for application messages received from the Common Domain).
TYPE	Is the CCN/CSI message type identifier for which statistics are provided; it is identical to the MessageTypeId listed in the domain specific volumes.
NBMSG	Gives the number of Customs system application messages of type TYPE sent (DIR = "O") or received (DIR = "I") to or from administration NA.
AVSZ	Gives the average size of these NBMSG messages.
MINSZ	Gives the minimum message size among these NBMSG messages.
MAXSZ	Gives the maximum message size among these NBMSG messages.

Table 70: Specification of the MSGS file

VIII.5.4   *Specification of the REPS file*

The **REPS** file is a plain ASCII file, composed of a sequence of lines formatted as follows: NA;DIR;TYPE;NBARR;NBDEL;NBEXC;NBEXP (Table 71).

Specification of the REPS file	
NA	Is the ISO identifier of the remote NA for which statistics are provided (AT, BE, …).
DIR	Indicates whether the statistics provided concern outgoing or incoming Customs system application messages ("O" for application messages sent to the Common Domain, "I" for application messages received from the Common Domain).
TYPE	Is the CCN/CSI message type identifier for which statistics are provided.
NBARR	Gives the number of "confirmation on arrival" report messages, generated on Customs system application messages of type TYPE and sent (DIR = O) or received (DIR = I) to or from administration NA.
NBDEL	Gives the number of "confirmation on delivery" report messages, generated on Customs system application messages of type TYPE and sent (DIR = O) or received (DIR = I) to or from administration NA.
NBEXC	Gives the number of "exception" report messages, generated on Customs system application messages of type TYPE and sent (DIR = O) or received (DIR = I) to or from administration NA.
NBEXP	Gives the number of "expiration" report messages, generated on Customs system application messages of type TYPE and sent (DIR = O) or received (DIR = I) to or from administration NA.

Table 71: Specification of the REPS file

IX Transport of messages via the Inter(extra)net

IX.1 Introduction

Within this section, some common Internet principles are stated.

All exchanges are based upon exchanges via the HTTP 1.1 protocol (RFC-2068).

Some general principles hold for the HTTP communication.

- The client sends requests using the HTTP/1.0 Basic Access Authentication over SSL. This assumes that the server side knows the password of the user that is managed by use of the Project web site logon facility. As a consequence of this use of the HTTP authentication, the user's identity is sent with each HTTP request. More information on the security aspect can be found in chapter IX.2;

- Client requests in which parameters are passed to CS/MIS system conform to the MIME specifications (RFC-2045, RFC-2046, RFC-2047, RFC-2048 and RFC-2049). They are encoded using the media type "multipart/formdata" as described in RFC-1867. MIME defines a wrapper for the useful data. The use of MIME and RFC-1867 allows the client to send files to the HTTP-server using a web-browser;

- A client request parameter may have only one value unless specified otherwise;

- Some requests can take some time to process. The client gets an immediate reply when such a request has been received but the result of the processing is only available for download after some time. It is made available immediately after the processing.

IX.2 Security

For CS/MIS application, the most important security aspects that must be covered are identification and authentication. These are needed for functional and data access control and for logging purposes. Since the communication is HTTP based, the communication system described here inherits the security properties and possibilities of HTTP. The current recommended version is HTTP/1.1, which offers two authentication schemes.

The first scheme is called the "Basic" authentication scheme. The second scheme is the so-called "Digest" authentication scheme. The latter digest-based scheme, as described in RFC-2069, is safer.

In order to have extra security, the HTTP protocol can operate over a secure connection. For example, HTTP over SSL (HTTPS) can be used without major changes to the exchange procedure used, giving the client reason to trust the server. Optionally, SSL could be used by the HTTP-server for authentication of the client.

The use of HTTPS is mostly part of the system installation and only visible to the application through the use of different URIs (https://…). The use of HTTP over a secure layer improves the system with higher integrity guarantees.

X Annex A – Scope for Central Services (CS) and System Administration (SA) for NCTS-P4/ECS-P2 and ICS-P1

X.1 Introduction

This annex describes the functional scope of the Central Services (CS) and System Administration (SA) for NCTS-P4, ECS-P2 and ICS-P1. It presents the exclusions and restrictions applicable for NCTS-P4, ECS-P2 and ICS-P1.

It intends to classify the CS and SA specifications into:

- Excluded EBPs/IEs: NCTS/ECS/ICS exclude their implementation (nevertheless NAs can implement them in accordance with [R26], [R13] or [R14] as long as they do not have international impact);

- Recommended EBPs/IEs (covering Optional, Recommended and Strongly Recommended): NCTS/ECS/ICS recommends their implementation according to [R26], [R13] or [R14]. The NAs remain free to implement the recommended specifications or not, and in the former case, according to their specific constraints and needs;

- Mandatory EBPs/IEs: NCTS/ECS/ICS imposes their implementation in NTAs/NECAs/NICAs.

The term National Customs Applications (NCA) is used hereinafter to refer to the NTA for NCTS, NECA for ECS, NICA for ICS.

X.2 Exclusions and restrictions

X.2.1 Introduction

This section presents all the exclusions and restrictions defined by the implementation of CS and SA for NCTS, ECS and ICS. EBPs and IEs that are completely excluded from the scope are also defined inside this chapter.

X.2.2 Restriction on Fallback

Regarding NCTS, the fallback specifications, presented in [R26] section IX and Appendix D, must only be considered as a recommendation. If it is required to agree on mandatory set of specifications for Fallback, the issue will be escalated to the ECG (Electronic Customs Group).

The paper-based ECS fallback procedure for Export declarations is defined in general terms in Art. 787 (2) of the Customs Code Implementing Provisions and in Art. 842b (3) for Exit Summary Declarations. ECS specific exception handling is currently not described in Section IX of [R13].

Concerning ICS, the [R14] document does not address cases where one of the ICS components is not functioning (fallback procedures). In this respect, reference is made to doc. TAXUD1465/2007 which addresses on a high level basis, different occurrences of fallback.

Once this document is approved, an in-depth examination will be carried out and a proposal for an administrative arrangement will be drafted.

X.2.3   *Restriction on Statistics*

Statistics are included in the scope of NCTS, ECS and ICS for CS to collect and compile the Technical Statistics provided by CCN/CSI and the National Business Statistics that the NAs provide at a configurable periodicity.

The National Administrations (NA) must compile National Business Statistics according to the specifications in EBPs SA01 and CS15 as detailed in the EBPs list presented in Section X.3.

NCAs will send the nationally compiled Statistics (IE411), via CCN/CSI, to the CS for consolidation. The consolidated Statistics (IE412[10]) will then be posted on the CS/MIS application in a format which includes all elements of Business Statistics.

The CS will only provide a set of files publishing Business Statistics (IE412[10]), each one covering a given period for a given system (i.e. NCTS-P4, ECS-P2 or ICS-P1). The CS will not provide an online statistical database from which for example a user automatically obtains chronological series and performs statistical analysis of the information.

X.2.4   *Restriction on the Central Services*

NAs will have connections to the CS via the restricted ITSM portal and their NCAs will have connections to the CS via the CCN/CSI network.

For NCTS-P4, ECS-P2 and ICS-P1, in order to support exchange of information, Web access will be maintained. This is also necessary to allow all NAs to provide and access some critical information. This will be regardless of the state of readiness of the NAs to join the operation of NCTS-P4, ECS-P2 and ICS-P1. This is applicable for IE070, IE071 and IE971.

Additionally, for NCTS-P4, ECS-P2 and ICS-P1, Web access will also be available to support Business Statistics and is applicable to IE412[10] (NCTS, ECS and ICS).

For NCTS-P4, ECS-P2 and ICS-P1, the CCN/CSI will be used to transfer structured information in EDIFACT (NCTS and ECS) or XML (ICS, NCTS and ECS) format between the NCA and the CS.

Additional formats and transport mechanisms are available for CS, please refer to [R27].

In addition to NCTS, ECS and ICS CCN/CSI will also be used to support Business Statistics by transferring IE411 in EDIFACT (NCTS and ECS) or XML (ICS, NCTS and ECS) format. It will be mandatory for an NTA to transfer this information as soon as it will enter into operation.

The ITSM Portal[62] will also host other information required for the operation management (e.g. interaction with NCTS Central Help Desk).

The NAs are responsible for uploading and downloading the non-"technical" information on and from the ITSM Portal and, whenever appropriate, to import this information into their systems. Indeed, the CDCA covers neither the preparation in the National Domain of the information to be uploaded on the Web site nor the downloading and processing at National level of the information to be made available on the ITSM Portal.

Please refer to section X.4 to get the specifications of both formats and exchange mechanism for all the above-mentioned IEs.

X.2.5 *Exclusion on the Central Services*

Not applicable.

X.2.6 *Restriction on SA05, SA06, and SA08*

Regardless of whether they use NDCAs or CDCAs the NAs will be responsible for performing the following business processes, found in [R26]: The Configuration management and Version Control (SA05), the Data Management (SA06) and the Problem Tracking (SA08). The NAs will use their IT operation infrastructure, including COTS, to support these tasks. Considering the specificity of the National IT operational environment, it is not foreseen at this stage that the Central Project will provide or recommend any specific COTS to support these processes.

X.2.7 *Performance*

The performance of the applications should conform to the recommendations made in this document. NAs are invited to align their NCAs to these performance recommendations.

X.2.8 *Security scope*

The following points have to be emphasised regarding the security scope:

- The security must comply with the applicable Legal Base and the specifications found in [R3], in [R16], in [R17], in [R18], in this document;

- NAs are responsible for the security in the National Domain;

- DG TAXUD is responsible for the security in the Common Domain, and for the security of the CS;

- The Central Project Team is responsible for the security of the CS.

---

[62]URL: https://itsmtaxud.europa.eu/

X.3 The scope matrix of Central Services and System Administration

The matrix consists of a table in which the status of each process is identified according to the scope of NCTS, ECS or ICS.

The scope matrix illustrates all the EBPs for CS and SA.

When determining whether a process or message is mandatory the first deciding factor is that Common Domain IEs are de facto mandatory. Therefore the EBP which produces the relevant IE also becomes mandatory. It was decided, historically, that all processes which are required in order that the mandatory EBP can be provided are themselves also mandatory.

Column Name	Column content description	Possible Values[63]
EBP ID	The identifier of the Elementary Business Process.	FTSS Id
EBP Name	The name of the Elementary Business Process	Text
The **"NCTS"** columns display information about the processes that are included in the scope of **NCTS**. It makes a clear statement on which of the processes are computer assisted and which remain manual.		
NCTS Status	The status of the EBP in NCTS. "M", "SR", "R" and "O" mean that the process to be implemented is included in the scope of NCTS as "Mandatory", "Strongly Recommended", "Recommended" or "Optional" respectively. "X" means that process is "Excluded" from the scope of NCTS and therefore any applicable Transit procedures remain valid.	M, SR, R, O or X
NCTS Man./C.A.	The degree of automation of the process (Computer Assisted or Manual) for NCTS. This column is only completed for the processes that are in the scope.	Man. Or C.A.

[63] The legend for the values is:
M   : Mandatory
SR   : Strongly Recommended
R   : Recommended
O   : Optional
X   : Excluded
C.A.   : Computer Assisted
Man.   : Manual
P   : Print
S   : Screen
CS   : Central Services
CS/RD2 : Central Services/Reference Data 2
CS/MIS: Central Services/Management Information System

Column Name	Column content description	Possible Values[63]
The **"ECS"** columns display information about the processes that are included in the scope of **ECS**. It makes a clear statement on which of the processes are computer assisted and which remain manual.		
ECS Status	The status of the EBP in ECS. "M", "SR", "R" and "O" mean that the process to be implemented is included in the scope of ECS as "Mandatory", "Strongly Recommended", "Recommended" or "Optional" respectively. "X" means that process is "Excluded" from the scope of ECS and therefore any applicable Export procedures remain valid.	M, SR, R, O or X
ECS Man./C.A.	The degree of automation of the process (Computer Assisted or Manual) for ECS. This column is only completed for the processes that are in the scope.	Man. Or C.A.
The **"ICS"** columns display information about the processes that are included in the scope of **ICS**. It makes a clear statement on which of the processes are computer assisted and which remain manual.		
ICS Status	The status of the EBP in ICS. "M", "SR", "R" and "O" mean that the process to be implemented is included in the scope of ICS as "Mandatory", "Strongly Recommended", "Recommended" or "Optional" respectively. "X" means that process is "Excluded" from the scope of ICS and therefore any applicable Import procedures remain valid.	M, SR, R, O or X
ICS Man./C.A.	The degree of automation of the process (Computer Assisted or Manual) for ICS. This column is only completed for the processes that are in the scope.	Man. Or C.A.
The CDCA columns indicate the processes that will be supported by the CDCAs.		
CDCA Incl. IE	This column shows the IEs that are initiated from the triggering of the EBP.	IE+'number'
CDCA Application	It defines the application which will support the EBP: • **CS** : Central Services; • **CS/RD2** : Central Services/Reference Data 2 • **CS/MIS** : Central Services/Management Information System (alias Statistics) The indication "Blank" means that the CDCA will not support the process.	CS, CS/RD2, CS/MIS, "Blank"
CDCA Scr/Prt	It indicates, **for information only,** the interface proposed for CDCA with its environment. Note that these interfaces are likely to sustain substantial change at the design stage of the CDCA.	S, P "Blank"

Column Name	Column content description	Possible Values[63]
	• "S" means that a screen is foreseen for entering or receiving information via the man-machine interface. • "P" means that information is printed. The indication "Blank" means that no interface has been identified at the time of releasing the document.	
CDCA Excl. IE	This column shows the IEs that are excluded from CDCA. The IEs that are excluded from the EBPs follow the same pattern as the IEs that are included in the EBPs. Therefore, only those IEs that are initiated from the triggering of the EBP and are excluded are presented in this column.	IE+'number'

Table 72: Scope of EBPs matrix definitions

X.3.1 Scope of EBPs for Central Services and System Administration

EBP ID	EBP Name	NCTS-P4		ECS-P2		ICS-P1		CDCA			
		Status	Man/ C.A.	Status	Man/ C.A.	Status	Man/ C.A.	Incl. IE	Applic	Scr/Prt	Excl. IE
CS1A0100	Prepare modification of Customs Office for Common Domain	M	C.A.	M	C.A.	M	C.A.				
CS1A0200	Notify modification to Common Domain	M	C.A.	M	C.A.	M	C.A.		CS/RD2		
CS1A0300	Process modification from NA	M	C.A.	M	C.A.	M	C.A.		CS/RD2		
CS1A0400	Notify modification to all NA	M	C.A.	M	C.A.	M	C.A.		CS/RD2		
CS1A0500	Process modification from Common Domain into National Domain	M	C.A.	M	C.A.	M	C.A.				
CS1B0600	Extract COL in electronic form	SR	C.A.	SR	C.A.	SR	C.A.		CS/RD2		
CS2A0100	Maintain Trader information	SR	C.A.	SR	C.A.	SR	C.A.				
CS2B0201	Check guarantee for authorisation	X		X		X					
CS2C0202	Evaluate guarantee check	X		X		X					
CS2C0300	Analyse Trader	X		X		X					
CS2C0400	Establish Convention	X		X		X					
CS2C0500	Modify database	SR	C.A.	X		X					
CS030100	Import HS6 commodity codes from national tariff file	M	C.A.	M	C.A.	M	C.A.				

DG TAXUD – FC TAXUD/2013/CC/124 – SC25	REF: DDCOM-Main Document
DESIGN DOCUMENT FOR COMMON OPERATIONS AND METHODS	VER: 20.20

ANNEX A – SCOPE FOR CENTRAL SERVICES (CS) AND SYSTEM ADMINISTRATION (SA) FOR NCTS-P4/ECS-P2 AND ICS-P1 - THE SCOPE MATRIX OF CENTRAL SERVICES AND SYSTEM ADMINISTRATION

EBP ID	EBP Name	NCTS-P4		ECS-P2		ICS-P1		CDCA			
		Status	Man/C.A.	Status	Man/C.A.	Status	Man/C.A.	Incl. IE	Applic	Scr/Prt	Excl. IE
CS4A0100	Manage and maintain codes and other common reference data	M	C.A.	M	C.A.	M	C.A.		CS/RD2		
CS4A0500	Notify modification in reference data to NA	M	C.A.	M	C.A.	M	C.A.		CS/RD2		
CS4A0500 TI	Notify modification in reference data to NA	X		X		X					
CS4A0600	Process modification in reference data from Common Domain Central Services Office	M	C.A.	M	C.A.	M	C.A.				
CS4B0200	Maintain national reference data	M	C.A.	M	C.A.	M	C.A.				
CS4C0600	Extract Reference Data in electronic form	SR	C.A.	SR	C.A.	SR	C.A.				
CS5A0100	Prepare unavailability schedule update	M	C.A.	M	C.A.	M	C.A.				
CS5A0200	Send unavailability schedule update to Common Domain	M	C.A.	M	C.A.	M	C.A.		CS/MIS		
CS5A0300	Process unavailability schedule update from NA	M	C.A.	M	C.A.	M	C.A.		CS/MIS		
CS5A0400	Send unavailability schedule update to all NA	M	C.A.	M	C.A.	M	C.A.		CS/MIS		
CS5A0500	Process unavailability schedule update from Common Domain	M	C.A.	M	C.A.	M	C.A.			S	
CS5B0100	Process submitted IE	M	C.A.	M	C.A.	M	C.A.				
CS5B0200	Process waiting IE	M	C.A.	M	C.A.	M	C.A.				

DG TAXUD – FC TAXUD/2013/CC/124 – SC25 | REF: DDCOM-Main Document

DESIGN DOCUMENT FOR COMMON OPERATIONS AND METHODS | VER: 20.20

ANNEX A – SCOPE FOR CENTRAL SERVICES (CS) AND SYSTEM ADMINISTRATION (SA) FOR NCTS-P4/ECS-P2 AND ICS-P1 - THE SCOPE MATRIX OF CENTRAL SERVICES AND SYSTEM ADMINISTRATION

EBP ID	EBP Name	NCTS-P4		ECS-P2		ICS-P1		CDCA			
		Status	Man/C.A.	Status	Man/C.A.	Status	Man/C.A.	Incl. IE	Applic	Scr/Prt	Excl. IE
CS110100	Send request for statistics information to NA	X		X		X					
CS110200	Receive request for statistics information from Data Manager for Common Domain	X		X		X					
CS110200 TI	Receive request for statistics information from Data Manager for Common Domain	X		X		X					
CS110300	Retrieve statistics information	M	C.A.	X		X					
CS110400	Send statistics information	M	C.A.	X		X					
CS110500	Receive statistics information from NA	M	C.A.	X		X		CS/MIS			
CS110600	Generate common statistics	M	C.A.	X		X		CS/MIS			
CS110700	Send common statistics to NA	M	C.A.	X		X		CS/MIS			
CS110800	Receive common statistics	R	C.A.	X		X					
CS120200	Maintain Risk Analysis profiles	SR	C.A.	SR	C.A.	SR	C.A.				
CS130100	Locate movement data	R	C.A.	R	C.A.	R	C.A.			S	
CS130200	Reload data from off line support	R	C.A.	R	C.A.	R	C.A.			S	
CS130400	Analyse movement data	R	C.A.	R	C.A.	R	C.A.			S	
CS130500	Remove uploaded data	R	C.A.	R	C.A.	R	C.A.			S	
CS140100	Choose kind of statistics data	R	C.A.	X		X					
CS140200	Define analysis criteria	R	C.A.	X		X					
CS140300	Analyse trends	R	C.A.	X		X					

DG TAXUD – FC TAXUD/2013/CC/124 – SC25	REF: DDCOM-Main Document
DESIGN DOCUMENT FOR COMMON OPERATIONS AND METHODS	VER: 20.20

ANNEX A – SCOPE FOR CENTRAL SERVICES (CS) AND SYSTEM ADMINISTRATION (SA) FOR NCTS-P4/ECS-P2 AND ICS-P1 - THE SCOPE MATRIX OF CENTRAL SERVICES AND SYSTEM ADMINISTRATION

EBP ID	EBP Name	NCTS-P4		ECS-P2		ICS-P1		CDCA			
		Status	Man/ C.A.	Status	Man/ C.A.	Status	Man/ C.A.	Incl. IE	Applic	Scr/Prt	Excl. IE
CS140400	Analyse current situation	R	C.A.	X		X					
CS140500	Analyse system administration statistics data	R	C.A.	X		X					
CS150100	Update incoming messages statistics	R	C.A.	R	C.A.	R	C.A.				
CS150200	Update outgoing messages statistics	R	C.A.	R	C.A.	R	C.A.				
CS150400	Update failures data	R	C.A.	R	C.A.	R	C.A.				
CS150500	Update errors and irregularities statistics	R	C.A.	R	C.A.	R	C.A.				
CS150600	Update recoveries statistics	R	C.A.	R	C.A.	R	C.A.				
CS160100	National Domain Maintain user	R	C.A.	M	C.A.	M	C.A.				
CS160200	National Domain Maintain profile	R	C.A.	M	C.A.	M	C.A.				
CS160300	National Domain Maintain user-profile	R	C.A.	M	C.A.	M	C.A.				
CS170100	Common Domain Maintain user	M	C.A.	M	C.A.	M	C.A.		CS		
CS170200	Common Domain Maintain profile	M	C.A.	M	C.A.	M	C.A.		CS		
CS170300	Common Domain Maintain user-profile	M	C.A.	M	C.A.	M	C.A.		CS		
SA010100	Freeze movement data	M	C.A.	M	C.A.	M	C.A.				
SA010300	Update statistics	M	C.A.	M	C.A.	M	C.A.				
SA010400	Archive data to off line support	M	C.A.	M	C.A.	M	C.A.				
SA010500	Purge the database	M	C.A.	M	C.A.	M	C.A.				

DG TAXUD – FC TAXUD/2013/CC/124 – SC25	REF: DDCOM-Main Document
DESIGN DOCUMENT FOR COMMON OPERATIONS AND METHODS	VER: 20.20

ANNEX A – SCOPE FOR CENTRAL SERVICES (CS) AND SYSTEM ADMINISTRATION (SA) FOR NCTS-P4/ECS-P2 AND ICS-P1 - THE SCOPE MATRIX OF CENTRAL SERVICES AND SYSTEM ADMINISTRATION

EBP ID	EBP Name	NCTS-P4		ECS-P2		ICS-P1		CDCA			
		Status	Man/ C.A.	Status	Man/ C.A.	Status	Man/ C.A.	Incl. IE	Applic	Scr/Prt	Excl. IE
SA05	Configuration Management and version control	R	C.A.	R	C.A.	R	C.A.				
SA06	Data Management	R	C.A.	R	C.A.	R	C.A.				
SA07	Fallback procedure	R	C.A.	X		X					
SA08	Problem Tracking	R	C.A.	R	C.A.	R	C.A.				
SA09	Audit Trail	M	C.A.	M	C.A.	M	C.A.				

Table 73: EBPs for Central Services and System Administration

X.4 The scope of Information Exchanges

Besides the EBPs, the scope of CS and SA for NCTS, ECS, ICS and CDCA can be expressed in terms of IEs. The table below illustrates the IEs that are within the scope of the CS and SA functionality.

The meaning of each column should be taken as follows:

Columns Name	Columns content description	Possible Values[64]
IE	The IE identifier as defined in the [R26] (Appendix B), [R13] (Appendix B1) and [R14] (Appendix B2).	IE+'number'
Name	The name of IE as defined in the [R26] (Appendix B), [R13] (Appendix B1) and [R14] (Appendix B2).	Text
Reference	The reference of the IE as defined in [R16], [R17] and [R18]. IE starting with E_, N_ and C_ are messages exchanged respectively in the External, National and Common Domains.	X_xxx_xxx
NCTS-P4	This column determines if the specific IE is supported in the NCTS-P4 domain. A "Y" means that the IE is exchanged in the specific domain.	Y, blank
ECS-P2	This column determines if the specific IE is supported in the ECS-P2 domain. A "Y" means that the IE is exchanged in the specific domain.	Y, blank
ICS-P1	This column determines if the specific IE is supported in the ICS-P1 domain. A "Y" means that the IE is exchanged in the specific domain.	Y, blank
National Control Application This section defines which IEs are mandatory or (strongly) recommended for the MSs / NAs, the exchange mechanism and the format of the message.		
Send	This column determines if the construction and the submission of the IE have to be processed. An "M" means that the NA must implement the	M, SR, R, O, blank

---

[64] The legend for the values is:

M : Mandatory
SR : Strongly Recommended
R : Recommended
O : Optional
Y : Yes

Columns Name	Columns content description	Possible Values[64]
	construction and the sending of this IE in full compliance with [R26] (Appendix B), [R13] (Appendix B1) and [R14] (appendix B2), in order to comply with the legal base, while "R", "SR" and "O" indicate that it is recommended, strongly recommended and optional for the NA to do so, respectively. A blank cell means that in case of: • E_ IE, the IE does not need to be sent during NCTS, ECS or ICS when implementing the CS and the SA functionality; • C_ IE, the IE must not be sent during NCTS, ECS or ICS when implementing the CS and the SA functionality.	
Receive	This column determines if the reception and the processing of the IE have to be implemented. An "M" means that the NA must implement the reception and the processing of this IE in full compliance with [R26] (Appendix B), [R13] (Appendix B1) and [R14] (appendix B2) in order to comply with the legal base, while "R", "SR" and "O" indicate that it is recommended, strongly recommended and optional for the NA to do so, respectively. A blank cell means that in case of: • E_ IE, the IE does not need to be received during NCTS, ECS or ICS when implementing the CS and the SA functionality; • C_ IE, the IE must not be received during NCTS, ECS or ICS when implementing the CS and the SA functionality.	M, SR, R, O, blank
Exchange Mechanism	This section defines the exchange mechanism for the IE: paper, up to the NA s, CCN/CSI or Web.	
Paper	A "Y" or a "M" means that the IE has to be exchanged on paper: • An "M" indicates that the printing must be made according a layout imposed by the legal base; • A "Y" indicates that the printing must be made according to a nationally defined layout. This paper mechanism and its associated format are not specified further in this document. A blank cell means that the IE does not have to be exchanged on paper.	M, Y, blank
MS	A "Y" means that the NA must decide how to	Y, blank

Columns Name	Columns content description	Possible Values[64]
	implement the send/receive functions: choice of exchange mechanism (paper, fax, phone, DTI, etc) and choice of format (forms, EDI, format, etc). This mechanism is not specified in this document. This document provides only recommendation for the EDI format of the External IEs. A blank cell means that it is not left up to the NA to choose the exchange mechanism of the IE.	
CCN/CSI	An "M" means that the IE has to be exchanged via CCN/CSI. The CCN/CSI exchange mechanism is specified in the body of this document. A blank cell means that the IE has not to be exchanged via CCN/CSI.	M, blank
Web	An "M" means that the IE has to be exchanged via Internet. The Web exchange mechanism is specified in this document. A blank cell means that the IE does not have to be exchanged via Internet.	M, blank
EDI Format	This section defines the EDI format used for the IE: EDIFACT, XML or CCN/CSI.	
EDIFACT	This column determines if the IE has to be formatted according to EDIFACT standard. These IEs are specified in [R16], [R17] and [R18]. A "M" means that the NA must implement the IE in EDIFACT according to the specifications of [R17], [R16] or [R18], an "R", a "SR" or an "O" means that it is recommended, strongly recommended or optional for the NA to implement the IE according to the EDIFACT specification of this document. A blank cell means that the IE does not have to be formatted according to EDIFACT.	M, SR, R, O, blank
XML	This column determines if the IE has to be formatted according to XML. XML stands for "eXtended Mark-up Language" and is an emerging standard in the Web technology and for EDI over Internet. These IEs are specified in Appendix A of [R16], [R17] and [R18]. An "M" means that the NA must implement the IE in XML, an "R", a "SR" or an "O" means that it is recommended, strongly recommended or optional for the NA to implement the IE according to the XML format. A blank cell means that the IE does not to have to be formatted according to XML.	M, SR, R, O, blank

Columns Name	Columns content description	Possible Values[64]
CCN/CSI	This column determines if the IE has to be formatted according to the CCN message internal structure. An "M" means that the NA must implement the IE via CCN/CSI, an "R", an "SR" or an "O" means that it is recommended, strongly recommended or optional for the NA to implement the IE according to the CCN/CSI format. A blank cell means that the IE does not have to be formatted according to CCN/CSI.	M, SR, R, O, blank
The 'Central Services' This section defines which IEs are implemented in the Central Project CS, which includes CS/RD2[65], CS/MIS, the exchange mechanism and the format of the message.		
Send	This column determines if the construction and the submission of the IE will be implemented in NCTS, ECS or ICS. A "Y" means that the IE will be constructed and sent from NCTS, ECS or ICS. A blank cell means that the IE will not be sent in the scope of NCTS, ECS or ICS.	Y, blank
Receive	This column determines if the reception and the processing of the IE will be implemented in NCTS, ECS or ICS. A "Y" means that the IE will be received and processed in NCTS, ECS or ICS. A blank cell means that the IE will not be received in the scope of NCTS, ECS or ICS.	Y, blank
Exchange Mechanism	This section defines the exchange mechanism for the IE: paper, up to the NA s, Queues, CCN/CSI or Web."	
Paper	A "Y" means that the IE will be exchanged on paper according to a layout imposed by the legal base. A blank cell means that the IE does not have to be exchanged on paper	Y, blank
MS	A "Y" means that the NA must decide how to implement the send/receive functions: choice of exchange mechanism (paper, fax, phone, DTI, etc) and choice of format (forms, EDI, format, etc). The exchange mechanism is not specified in this document.	Y, blank

---

[65] Additional formats and transport mechanisms are available for CS/RD2, please refer to [R09].

Columns Name	Columns content description	Possible Values[64]
	This document provides only recommendation for the EDI format of the External IEs. A blank cell means that it is not left up to the NA to choose the exchange mechanism of the IE.	
CCN/CSI	This column determines if the IE will be formatted according to CCN message internal structure. A "Y" means that the IE will be implemented via CCN/CSI." A blank cell means that this exchange mechanism is not used.	Y, blank
Web	A "Y" means that the NA will be responsible for downloading the messages from the CS/RD2 Web site and placing them in the appropriate MCC or ECN+ queue. A blank cell means that this exchange mechanism is not used.	Y, blank
EDI Format	This section defines the EDI format used for the IE: EDIFACT, XML or CCN/CSI	
EDIFACT	A "Y" means that the IE will be implemented in EDIFACT format according to the specifications of [R17], [R18] or this document. A blank cell means that the IE will not be formatted according to EDIFACT.	Y, blank
XML	A "Y" means that the IE will be formatted in XML according to the specifications of [R16], [R17] or [R18]. A blank cell means that the IE will not be formatted according to XML.	Y, blank
CCN/CSI	A "Y" means that the IE will be formatted according to CCN message internal structure. A blank cell means that the IE will not be formatted according to CCN/CSI.	Y, blank

Table 74: Scope of Information Exchanges matrix definitions

X.4.1 Scope of IEs for Central Services and System Administration

Column groups: columns 7–15 belong to **National Customs Application**; columns 16–24 belong to **Central Services**. Within each group: Send, Receive, then Exchange Mechanism (Paper, NA/MS, CCN/CSI, Web), then EDI Format (EDIFACT, XML, CCN/CSI).

IE	Name	Reference	NCTS-P4	ECS-P2	ICS-P1	NCA Send	NCA Receive	NCA Paper	NCA NA/MS	NCA CCN/CSI	NCA Web	NCA EDIFACT	NCA XML	NCA CCN/CSI	CS Send	CS Receive	CS Paper	CS NA/MS	CS CCN/CSI	CS Web	CS EDIFACT	CS XML	CS CCN/CSI
					Y		M			M	M		M		Y				Y	Y		Y	
IE070	Notification of System Unavailability To CD	C_UNA_COM	Y	Y	Y	M					M		M			Y				Y		Y	
IE071	Notification of System Unavailability To ND	C_UNA_NAT	Y	Y	Y		M				M		M		Y					Y		Y	
IE411[66]	Sending of statistics data	C_STA_SND	Y	Y		M				M	M	M	M			Y			Y	Y	Y	Y	
					Y	M				M	M		M			Y			Y	Y		Y	
IE412[10]	Statistics generated sent to national domain	C_STA_GEN	Y	Y	Y		M				M		M		Y					Y		Y	
IE904	Status Request	C_STD_REQ	Y	Y		M	M			M		M											
IE905	Status Response	C_STD_RSP	Y	Y		M	M			M		M											
IE906	Functional NACK	C_FUN_NCK	Y	Y		M	M			M		M			Y	Y			Y		Y		
					Y	M	M			M				M	Y	Y			Y				Y
IE907	EDIFACT NACK (CONTRL)	C_EDI_NCK	Y	Y		M	M			M		M			Y	Y			Y		Y		
IE908	CCN/CSI Confirm On Delivery (COD) Acknowledgement	C_COD_ACK	Y	Y	Y	M	M			M				M									
IE909	CCN/CSI Confirm On Arrival (COA) Acknowledgement	C_COA_ACK	Y	Y	Y	M	M			M				M									
IE910	CCN/CSI Expiration notification	C_EXP_NOT	Y	Y	Y	M	M			M				M									

---

[66] The IE411 for NCTS and ECS must be sent to CS/MIS,
- either via CCN/CSI or via manual upload.
- either in EDIFACT format or in XML format.

One EDIFACT message may include information of NCTS only, or ECS only, or both NCTS+ECS.

One XML message may include data of NCTS, or ECS, or ICS or multiple domains

DG TAXUD – FC TAXUD/2013/CC/124 – SC25   REF: DDCOM-Main Document

DESIGN DOCUMENT FOR COMMON OPERATIONS AND METHODS   VER: 20.20

ANNEX A – SCOPE FOR CENTRAL SERVICES (CS) AND SYSTEM ADMINISTRATION (SA) FOR NCTS-P4/ECS-P2 AND ICS-P1 - THE SCOPE OF INFORMATION EXCHANGES

| IE | Name | Reference | NCTS-P4 | ECS-P2 | ICS-P1 | National Customs Application | | | | | | | | | Central Services | | | | | | | | |
						Send	Receive	Paper	NA/MS	CCN/CSI	Web	EDIFACT	XML	CCN/CSI	Send	Receive	Paper	NA/MS	CCN/CSI	Web	EDIFACT	XML	CCN/CSI
IE911	CCN/CSI Exception notification	C_EXC_NOT	Y	Y	Y	M	M			M				M									
IE917	XML NACK	C_XML_NCK			Y	M	M			M			M		Y	Y			Y			Y	
IE971	Full unavailability schedule	C_UNA_DAT	Y	Y	Y		M				M	M		Y				Y		Y	

Table 75: Scope of Information Exchanges

XI Annex B – Scope for Central Services (CS) and System Administration (SA) for NCTS-P5 and AES-P1

XI.1 Introduction

This annex describes the functional scope of the Central Services (CS) and System Administration (SA) for NCTS-P5 and AES-P1. It presents the exclusions and restrictions applicable for NCTS-P5 and AES-P1.

AES-P1/NCTS-P5 Architecture Overview [R38] defines the interactions of NCA with Central Services (e.g. with CS/RD2, CRS/CDMS, TARIC3) in scope of NCTS-P5 and AES-P1. Therefore, NCA must consider them for implementation.

This annex focus is to classify the CS and SA [R26] specifications into:

- Excluded EBPs/IEs: NCTS-P5/AES-P1 exclude their implementation (nevertheless NAs can implement them in accordance with the pertinent specifications as long as they do not have international impact);

- Recommended EBPs/IEs (covering Optional, Recommended and Strongly Recommended): NCTS-P5/AES-P1 recommends their implementation according to the pertinent specifications. The NAs remain free to implement the recommended specifications or not, and in the former case, according to their specific constraints and needs;

- Mandatory EBPs/IEs: NCTS-P5/AES-P1 imposes their implementation in NTAs/NECAs.

The term National Customs Applications (NCA) is used hereinafter to refer to the NTA for NCTS-P5 and NECA for AES-P1.

XI.2 Exclusions and restrictions

XI.2.1 Introduction

This section presents all the exclusions and restrictions defined by the implementation of CS and SA of the following EBPs applicable for NCTS-P5 and AES-P1:
- CS5A - Manage Scheduled Unavailability [R26]
- CS5B - Check National System Availability [R26]
- CS11 - Manage Transit Movement Statistics / L4-STE-01 Business Statistics for Transit and Export [R39]
- CS13 – Analyse Transit Movement Data [R26]
- CS15 - Manage System Administration Statistics [R26]
- CS16 - National Domain Maintains User and Profile Data [R26]
- SA01 - Archive Procedures [R26]

XI.2.2   Restriction on Fallback

The restrictions on fallback given in section X.2.2 are assumed for NCTS-P5 and AES-P1.

XI.2.3   Restriction on Statistics

Statistics are included in the scope of NCTS-P5 and AES-P1 for CS to collect and compile the Technical Statistics provided by CCN/CSI and the National Business Statistics that the NAs provide at a configurable periodicity.

The National Administrations (NA) must compile National Business Statistics according to the specifications in EBPs SA01 and CS15 as detailed in the EBPs list presented in Section XI.3.

NCAs will send the nationally compiled Statistics (IE411), via CCN/CSI, to the CS for consolidation. The consolidated Statistics (IE412[10]) will then be posted on the CS/MIS application in a format which includes all elements of Business Statistics.

The CS will only provide a set of files publishing Business Statistics (IE412[10]), each one covering a given period for a given system (i.e. NCTS-P5 or AES-P1). The CS will not provide an online statistical database from which for example a user automatically obtains chronological series and performs statistical analysis of the information.

XI.2.4   Restriction on the Central Services

The restrictions on the Central Services given in section X.2.4 are assumed for NCTS-P5 and AES-P1.

For integration with CS/RD2 and other Central Services please refer to AES-P1/NCTS-P5 Architecture Overview [R38].

Please refer to XI.4 to get the specifications of both formats and exchange mechanism for all the above-mentioned IEs.

XI.2.5   Exclusion on the Central Services

Not applicable.

XI.2.6   Performance

The restrictions on fallback given in section X.2.7 are assumed for NCTS-P5 and AES-P1.

XI.2.7   Security scope

The following points have to be emphasised regarding the security scope:
- The security must comply with the applicable Legal Base and the specifications found in [R3], in [R40], in [R41] and in this document;

- NAs are responsible for the security in the National Domain;

- DG TAXUD is responsible for the security in the Common Domain, and for the security of the CS;

- The Central Project is responsible for the security of the CS.

XI.3 The scope matrix of Central Services and System Administration

The matrix consists of a table in which the status of each process is identified according to the scope of NCTS-P5 or AES-P1.

The scope matrix is limited to the following EBPs:
- CS5A - Manage Scheduled Unavailability [R26]
- CS5B - Check National System Availability [R26]
- CS11 - Manage Transit Movement Statistics / L4-STE-01 Business Statistics for Transit and Export [R39]
- CS13 – Analyse Transit Movement Data [R26]
- CS15 - Manage System Administration Statistics [R26]
- CS16 - National Domain Maintains User and Profile Data [R26]
- SA01 - Archive Procedures [R26]

In addition, the AES-P1/NCTS-P5 Architecture Overview [R38] defines the interactions of NCA with Central Services (e.g. with CS/RD2, CRS/CDMS, TARIC3) in scope of NCTS-P5 and AES-P1. Therefore, NCA must consider them for implementation.

When determining whether a process or message is mandatory the first deciding factor is that Common Domain IEs are de facto mandatory. Therefore the EBP which produces the relevant IE also becomes mandatory. It was decided, historically, that all processes which are required in order that the mandatory EBP can be provided are themselves also mandatory.

| DG TAXUD – FC TAXUD/2013/CC/124 – SC25 | REF: DDCOM-Main Document |
| DESIGN DOCUMENT FOR COMMON OPERATIONS AND METHODS | VER: 20.20 |

ANNEX B – SCOPE FOR CENTRAL SERVICES (CS) AND SYSTEM ADMINISTRATION (SA) FOR NCTS-P5 AND AES-P1 - THE SCOPE MATRIX OF CENTRAL SERVICES AND SYSTEM ADMINISTRATION

Column Name	Column content description	Possible Values[67]
EBP ID	The identifier of the Elementary Business Process.	FTSS Id
EBP Name	The name of the Elementary Business Process	Text
The **"NCTS"** columns display information about the processes that are included in the scope of **NCTS-P5**. It makes a clear statement on which of the processes are computer assisted and which remain manual.		
NCTS-P5 Status	The status of the EBP in NCTS-P5. "M", "SR", "R" and "O" mean that the process to be implemented is included in the scope of NCTS as "Mandatory", "Strongly Recommended", "Recommended" or "Optional" respectively. "X" means that process is "Excluded" from the scope of NCTS-P5 and therefore any applicable Transit procedures remain valid.	M, SR, R, O or X
NCTS-P5 Man./C.A.	The degree of automation of the process (Computer Assisted or Manual) for NCTS-P5. This column is only completed for the processes that are in the scope.	Man. Or C.A.
The **"AES-P1"** columns display information about the processes that are included in the scope of **AES-P1**. It makes a clear statement on which of the processes are computer assisted and which remain manual.		
AES-P1 Status	The status of the EBP in AES-P1. "M", "SR", "R" and "O" mean that the process to be implemented is included in the scope of AES-P1 as "Mandatory", "Strongly Recommended", "Recommended" or "Optional" respectively. "X" means that process is "Excluded" from the scope of AES-P1 and therefore any applicable Export procedures remain valid.	M, SR, R, O or X

---

[67] The legend for the values is:

M   : Mandatory
SR   : Strongly Recommended
R   : Recommended
O   : Optional
X   : Excluded
C.A.   : Computer Assisted
Man.   : Manual
P   : Print
S   : Screen
CS   : Central Services
CS/RD2 : Central Services/Reference Data 2
CS/MIS: Central Services/Management Information System

Column Name	Column content description	Possible Values[67]
AES-P1 Man./C.A.	The degree of automation of the process (Computer Assisted or Manual) for AES-P1. This column is only completed for the processes that are in the scope.	Man. Or C.A.
The CDCA columns indicate the processes that will be supported by the CDCAs.		
CDCA Incl. IE	This column shows the IEs that are initiated from the triggering of the EBP.	IE+'number'
CDCA Application	It defines the application which will support the EBP: • **CS/MIS** : Central Services/Management Information System (alias Statistics) The indication "Blank" means that the CDCA will not support the process.	CS, CS/RD2, CS/MIS, "Blank"
CDCA Scr/Prt	It indicates, **for information only,** the interface proposed for CDCA with its environment. Note that these interfaces are likely to sustain substantial change at the design stage of the CDCA. • "S" means that a screen is foreseen for entering or receiving information via the man-machine interface. • "P" means that information is printed. The indication "Blank" means that no interface has been identified at the time of releasing the document.	S, P "Blank"
CDCA Excl. IE	This column shows the IEs that are excluded from CDCA. The IEs that are excluded from the EBPs follow the same pattern as the IEs that are included in the EBPs. Therefore, only those IEs that are initiated from the triggering of the EBP and are excluded are presented in this column.	IE+'number'

Table 76: Scope of EBPs matrix definitions

XI.3.1   Scope of EBPs[68] for Central Services and System Administration

EBP ID	EBP Name	NCTS-P5		AES-P1		CDCA			
		Status	Man/C.A.	Status	Man/C.A.	Incl. IE	Applic	Scr/Prt	Excl. IE
CS5A0100	Prepare unavailability schedule update	M	C.A.	M	C.A.				
CS5A0200	Send unavailability schedule update to Common Domain	M	C.A.	M	C.A.		CS/MIS		
CS5A0300	Process unavailability schedule update from NA	M	C.A.	M	C.A.		CS/MIS		
CS5A0400	Send unavailability schedule update to all NA	M	C.A.	M	C.A.		CS/MIS		
CS5A0500	Process unavailability schedule update from Common Domain	M	C.A.	M	C.A.			S	
CS5B0100	Process submitted IE	M	C.A.	M	C.A.				
CS5B0200	Process waiting IE	M	C.A.	M	C.A.				
L4-STE-01	Create business statistic records	M	C.A.	M	C.A.				
L4-STE-01	Retrieve business statistics information	M	C.A.	M	C.A.				
L4-STE-01	Send business statistics information	M	C.A.	M	C.A.				
L4-STE-01	Receive business statistics information from NA	M	C.A.	M	C.A.		CS/MIS		
L4-STE-01	Generate common business statistics	M	C.A.	M	C.A.		CS/MIS		
L4-STE-01	Send common business statistics to NA	M	C.A.	M	C.A.		CS/MIS		

---

[68] The scope matrix is limited to the following EBPs:
- CS5A - Manage Scheduled Unavailability [R26]
- CS5B - Check National System Availability [R26]
- CS11 - Manage Transit Movement Statistics / L4-STE-01 Business Statistics for Transit and Export [R39]
- CS13 – Analyse Transit Movement Data [R26]
- CS15 - Manage System Administration Statistics [R26]
- CS16 - National Domain Maintains User and Profile Data [R26]
- SA01 - Archive Procedures [R26]

DG TAXUD – FC TAXUD/2013/CC/124 – SC25	REF: DDCOM-Main Document
DESIGN DOCUMENT FOR COMMON OPERATIONS AND METHODS	VER: 20.20

ANNEX B – SCOPE FOR CENTRAL SERVICES (CS) AND SYSTEM ADMINISTRATION (SA) FOR NCTS-P5 AND AES-P1 - THE SCOPE MATRIX OF CENTRAL SERVICES AND SYSTEM ADMINISTRATION

EBP ID	EBP Name	NCTS-P5		AES-P1		CDCA			
		Status	Man/C.A.	Status	Man/C.A.	Incl. IE	Applic	Scr/Prt	Excl. IE
L4-STE-01	Receive common business statistics	R	C.A.	R	C.A.				
CS130100	Locate movement data	R	C.A.	R	C.A.				
CS130200	Reload data from off line support	R	C.A.	R	C.A.				
CS130400	Analyse movement data	R	C.A.	R	C.A.				
CS130500	Remove uploaded data	R	C.A.	R	C.A.				
CS150100	Update incoming messages statistics	R	C.A.	R	C.A.				
CS150200	Update outgoing messages statistics	R	C.A.	R	C.A.				
CS150400	Update failures data	R	C.A.	R	C.A.				
CS150500	Update errors and irregularities statistics	R	C.A.	R	C.A.				
CS150600	Update recoveries statistics	R	C.A.	R	C.A.				
CS160100	National Domain Maintain user	R	C.A.	M	C.A.				
CS160200	National Domain Maintain profile	R	C.A.	M	C.A.				
CS160300	National Domain Maintain user-profile	R	C.A.	M	C.A.				
SA010100	Freeze movement data	M	C.A.	M	C.A.				
SA010300	Update statistics	M	C.A.	M	C.A.				
SA010400	Archive data to off line support	M	C.A.	M	C.A.				
SA010500	Purge the database	M	C.A.	M	C.A.				

Table 77: EBPs for Central Services and System Administration

XI.4 The scope of Information Exchanges

Besides the EBPs, the scope of CS and SA for NCTS-P5 and AES-P1 CDCA can be expressed in terms of IEs.

Detailed information scope of IEs for interaction with CS/MIS are available under Appendix A of DDNTA [R41] and DDNXA [R40] documents.

***

*** End of document ***