

OWNER: DG TAXUD	ISSUE DATE: 10/08/2011	VERSION: 2.2
<p style="text-align: center;">EXCISE COMPUTERISATION PROJECT EMCS SYSTEM SPECIFICATIONS (ESS), COMMUNICATION AND INFORMATION PROGRAMME</p> <p style="text-align: center;">SUBJECT:</p> <p style="text-align: center;">Security Excise System Specifications (SESS)</p> <p style="text-align: center;">Framework Contract TAXUD/2004/CC/076</p> <p style="text-align: right;"><i>ECP1-ESS-SESS</i></p>		

[Blank for duplex printing]

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
DOCUMENT HISTORY	

Document History

Ed.	Rev.	Date	Description	Action (*)	Pages
0	01	01/06/2005	Creation.	I	All
0	02	04/07/2005	Document structure elaboration.	U	All
0	03	25/07/2005	Security Framework.	I	§3.1
			Compliance Matrix.	I	§4.2
			Security Domains.	I	§5.2
0	04	05/08/2005	Technical Security Infrastructure.	U	§5
0	05	22/08/2005	Technical Security Infrastructure.	U	§5
			Application Security Architecture.	U	§6
0	06	12/09/2005	CDEA Cartography.	I	§3.3
			EMCS Business Communication Channels.	I	§3.4
			Security Requirements Analysis.	I	§4
			Security Domains.	U	§5.2
0	07	26/01/2006	Entirely reworked after TESS Submission for Review (SfR) on 11/01/06. Version Submitted for Information (SfI).	U	All
0	08	06/02/2006	Integrates DG TAXUD comments made on SfI version. Version submitted for internal quality control.	U	All
0	09	10/02/2006	Version Submitted for Review (SfR) to DG TAXUD.	U	All
1	00	24/02/2006	Version integrating review workshop decisions. Quality checked. Version Submitted for Acceptance (SfA).	U	All

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
DOCUMENT HISTORY	

1	01	18/09/2006	Version integrating meeting decisions further to ECWP held on 19-20/09/06. Version Submitted for Review (SfR).	U D I	All §3.7.3, §4.6 Appendix D
2	00	02/10/2006	Version integrating DG TAXUD comments. Quality checked. Version Submitted for Acceptance (SfA).	U	§8.2.4, §10.2.1
2	1	02/12/2009	Update to the EMCS Security Compliance Certificate	U I	§8.2.3 §11. Appendix E
2	2	10/08/2011	Update to the EMCS Security Compliance Certificate	U I	§8.2.3 §11. Appendix E

(*) Action: I = Insert, R = Replace, U = Update, D = delete

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
TABLE OF CONTENTS	

Table of Contents

1. Management Summary / Kurzfassung / Résumé	15
1.1. English	15
1.1.1. Purpose of the Document	15
1.1.2. Intended Readership	15
1.1.3. Document Summary	15
1.1.4. Document Structure	16
1.1.5. Guidance to the Reader	17
1.1.6. Changes to this Document	17
1.2. Deutsch	19
1.2.1. Zielsetzung des Dokuments	19
1.2.2. Zielgruppe	19
1.2.3. Zusammenfassung des Dokuments	19
1.2.4. Dokumentstruktur	20
1.2.5. Hinweis für den Leser	22
1.2.6. Änderungen an diesem Dokument	22
1.3. Français	23
1.3.1. Objectif du document	23
1.3.2. Lecteurs concernés	23
1.3.3. Résumé du document	24
1.3.4. Structure du document	24
1.3.5. Guide pour le lecteur	26
1.3.6. Changements apportés à ce document	26
2. References	27
2.1. Documents	27
2.2. Acronyms	30
2.3. Security Standards	32
2.3.1. ISO/IEC 17799	32
2.3.2. ISF Standard	32
3. EMCS Background Information	35
3.1. Introduction	35
3.2. EMCS Architecture Overview	35
3.2.1. Domains and Applications	35

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
TABLE OF CONTENTS	

3.2.2.	References to the Technical Excise Systems Specifications (TESS)	36
3.3.	EMCS Security Objectives	37
3.3.1.	Availability	37
3.3.2.	Confidentiality	38
3.3.3.	Integrity	38
3.3.4.	Legitimate Use of the System	38
3.4.	EMCS Security Domains	39
3.5.	EMCS Business Communication Channels	41
3.6.	EMCS Infrastructure Communication Channels	45
3.6.1.	Introduction	45
3.6.2.	CCN/CSI Channel	47
	3.6.2.1. Intended Usage	47
	3.6.2.2. Description	47
	3.6.2.3. Compliance with EMCS Security Objectives	48
3.6.3.	CCN Intranet Channel	49
	3.6.3.1. Intended Usage	49
	3.6.3.2. Description	49
	3.6.3.3. Compliance with Security Objectives	50
3.6.4.	CCN Mail 2 Channel	51
	3.6.4.1. Intended Usage	51
	3.6.4.2. Description	51
	3.6.4.3. Compliance with EMCS Security Objectives	52
3.7.	EMCS Security Requirements	53
3.7.1.	Introduction	53
3.7.2.	Security Requirements	53
4.	EMCS Common Domain Security Measures	58
4.1.	Introduction	58
4.2.	Security Management	58
4.2.1.	Management Commitment	58
4.2.2.	Security Policy	59
4.2.3.	Security Coordination	60
4.2.4.	Business Continuity	61
4.2.5.	Security Audit/Review and Monitoring	61
4.2.6.	Public Key Infrastructure (PKI)	61
4.3.	EMCS Common Domain Infrastructure	62
4.3.1.	Installation Management	62
	4.3.1.1. Roles and Responsibilities	62

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
TABLE OF CONTENTS	

4.3.1.2. Asset Management	62
4.3.2. Environment	62
4.3.2.1. Physical Security	62
4.3.2.2. Equipment Sitting and Protection	63
4.3.2.3. Power Supplies	63
4.3.2.4. Equipment Maintenance	63
4.3.3. System Operation	64
4.3.3.1. Backup	64
4.3.3.2. Incident and Change Management	64
4.3.3.3. Media Handling	64
4.3.3.4. Protection against Malicious Software	65
4.3.3.5. Patch Management	65
4.3.4. Access Control	65
4.3.4.1. Access control Arrangements	65
4.3.4.2. Registration	66
4.3.4.3. Authorisation	67
4.3.4.4. Authentication	67
4.3.4.4.1. CCN/CSI Authentication	68
4.3.4.4.2. CCN Intranet Authentication	68
4.3.4.4.3. CCN Mail 2 Authentication	69
4.4. CCN Network Security	69
4.4.1. Network Management	71
4.4.1.1. Roles and Responsibilities	71
4.4.1.2. Network Resilience	71
4.4.1.2.1. Protection of CCN Exchanges	71
4.4.1.2.2. NDCP Equipment Redundancy	72
4.4.1.2.3. Central Backup Site	73
4.4.1.2.4. CCN Mail 2 Fallback	73
4.4.2. Traffic Management	74
4.4.2.1. Network Routing Control (Enforced Path)	74
4.4.2.2. Firewalls	74
4.4.2.3. Network Encryption	75
4.4.2.4. External Access	75
4.4.3. Network Operations	75
4.4.3.1. Network Monitoring	75
4.4.3.2. Event Logging	76
4.4.3.3. Remote Maintenance	76
4.5. Systems Development	77
4.5.1. Roles and Responsibilities	77
4.5.2. System Design and Build	77
4.5.2.1. CSI-based Application Development	77
4.5.2.2. HTTP-based Application Development	78

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
TABLE OF CONTENTS	

5. EMCS Central Services Security Measures	79
5.1. Introduction	79
5.2. Central Services Security Components	79
5.2.1. Central Services Gateway	80
5.2.2. Central Security Services	81
5.2.2.1. Security Server	81
5.2.2.2. EMCS Central Services CA (CSCA)	81
5.2.2.2.1. CSCA Options	82
5.3. Security Management	83
5.3.1. Management Commitment	83
5.3.2. Security Policy	83
5.3.3. Security Coordination	83
5.3.4. Business Continuity	84
5.3.5. Security Audit/Review and Monitoring	85
5.4. CEA Security	85
5.4.1. Application Management	85
5.4.1.1. Roles and Responsibilities	85
5.4.2. User Environment	85
5.4.2.1. Registration	85
5.4.2.2. Access Control	86
5.4.2.2.1. CEA Access Control (CCN/CSI Channel)	86
5.4.2.2.2. CEA Access Control (CCN Intranet Channel)	86
5.4.3. System Management	86
5.4.3.1. Event Logging and Accounting	86
5.5. EMCS Central Services Infrastructure	88
5.5.1. Installation Management	88
5.5.1.1. Roles and Responsibilities	88
5.5.2. Environment	88
5.5.2.1. Physical Security	88
5.5.2.2. Equipment Siting and Protection	89
5.5.2.3. Power Supplies	89
5.5.2.4. Equipment Maintenance	89
5.5.3. System Operation	89
5.5.3.1. Backup	89
5.5.3.2. Incident and Change Management	90
5.5.3.3. Media Handling	90
5.5.3.4. Protection against Malicious Software	90
5.5.3.5. Intrusion Detection	91
5.5.3.6. Patch Management	92

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
TABLE OF CONTENTS	

5.6. SNET Network Security	92
5.6.1. Network Management	92
5.6.1.1. Roles and Responsibilities	92
5.6.2. Traffic Management	92
5.6.2.1. Network Routing Control (Enforced Path)	92
5.6.2.2. Firewalls	93
5.6.2.3. Network Encryption	93
5.7. Systems Development	94
5.7.1. Web-enabled Development	94
5.8. CEA Access Control (CCN Intranet Channel)	96
5.8.1. HTTP Session-level Security	96
5.8.1.1. Topology	96
5.8.1.2. Authentication	97
5.8.1.3. Authorisation	99
5.8.2. SOAP Message-level Security	100
5.8.3. CEA Web Services Addressing Scheme	100
6. Standard Excise Application (SEA) Security Measures	102
6.1. Introduction	102
6.2. Security Measures	103
6.2.1. Development Management	103
6.2.1.1. Roles and Responsibilities	103
6.2.1.2. Development Methodology	103
6.2.1.3. Quality Assurance	103
6.2.1.4. Development Environments	104
6.2.2. Requirements Definition	104
6.2.2.1. Confidentiality Requirements	105
6.2.2.2. Integrity Requirements	105
6.2.2.3. Availability Requirements	106
6.2.2.4. Logging and Auditing	106
6.2.3. Design and Build	107
6.2.3.1. Design	107
6.2.3.2. Application Controls	107
6.2.3.3. System Build	108
6.2.4. Testing	108
6.2.4.1. Testing Process	108
6.2.5. Deployment	109
6.2.5.1. System Deployment Criteria	109

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
TABLE OF CONTENTS	

7. Appendix A: Compliance Matrix	110
8. Appendix B: National Domain Security Guidance	118
8.1. Introduction	118
8.2. Security Management	118
8.2.1. Security Policy	118
8.2.2. Security Organisation	118
8.2.3. Issuance of the EMCS Security Compliance Certificate & EMCS Security Measures Questionnaire	119
8.2.4. Access Control Policy	120
8.2.5. Economic Operators Privacy Policy	122
8.3. EMCS National Domain Infrastructure	123
8.3.1. Installation Management	123
8.3.1.1. Roles and Responsibilities	123
8.3.1.1.1. NDCP Equipment	123
8.3.1.1.2. NEA Equipment	123
8.3.1.2. Asset Management	123
8.3.2. Environment	124
8.3.2.1. Physical Security	124
8.3.2.2. Equipment Sitting and Protection	125
8.3.2.3. Power Supplies	125
8.3.2.4. Equipment Maintenance	125
8.3.2.5. Provide security of equipment off-premises	126
8.3.2.6. Secure disposal or re-use of equipment	126
8.3.3. System Operation	126
8.3.3.1. Backup	126
8.3.3.2. Incident and Change Management	126
8.3.3.2.1. Incident Management	127
8.3.3.2.2. Change Management	127
8.3.3.3. Media Handling	127
8.3.3.4. Protection Against Malicious Software	127
8.3.3.5. Patch Management	128
8.3.3.6. MSA Officials Workstation Security	128
8.3.4. Access Control	129
8.3.4.1. Registration of MSA Users	129
8.3.4.2. Registration of Economic Operators	129
8.4. MSA Network Security	130
8.4.1. Network Management	130
8.4.1.1. Roles and Responsibilities	130
8.4.2. Traffic Management	131

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
TABLE OF CONTENTS	

8.4.2.1. Network Routing Control (Enforced Path)	131
8.4.2.2. Firewalls	131
8.4.2.3. Network Encryption	132
8.5. NEA Development (NDEA)	132
8.5.1. Development Management	132
8.5.2. Requirements Definition	132
8.5.2.1. Application Access Control	132
8.5.2.2. Secure Audit Logs (SAL)	133
9. Appendix C: Web Service Channel Security – Authentication and Authorisation Scheme	135
10. Appendix D: Proposal for the EMCS Common Domain PKI (CDPKI)	140
10.1. Introduction	140
10.2. Cryptographic Controls Requirements	140
10.2.1. Strong Authentication [SR21.1]	140
10.2.2. Shared Identity between National and Common Domains [SR21.2]	141
10.2.3. Secure Audit Logs (SAL) [SR21.3]	141
10.2.4. Excise Movement Authenticity [SR21.4]	142
10.3. EMCS Common Domain PKI (CDPKI)	144
10.3.1. Problem Statement	144
10.3.2. Architecture	146
10.3.2.1. Basic Principle	146
10.3.2.2. Links between CAs	148
10.3.3. Bridge CA/VA	148
10.3.3.1. Objective	148
10.3.4. Trust Relationship Establishment	149
10.3.5. Technical Operability Tests	152
10.3.6. Certificate Management	152
10.3.6.1. X.509 Certificates	152
10.3.6.2. Certificate Services	153
10.3.6.3. Certificate Authority (CA)	153
10.3.6.4. Certificate Revocation List (CRL)	153
10.3.6.5. Certificate Policy (CP) and Certificate Practice Statements (CPS)	153
10.3.6.6. Certificate and CRL Repositories	153
11. Appendix E: EMCS Security Compliance Certificate	154
11.1. Sample 'EMCS Security Compliance Certificate'	154

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
TABLE OF CONTENTS	

11.2. 'EMCS Security Measures Questionnaire'

155

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
LIST OF TABLES	

List of Tables

TABLE 1: REFERENCE DOCUMENTS	30
TABLE 2: ABBREVIATIONS AND ACRONYMS	32
TABLE 3: CCN/CSI CHANNEL - COMPLIANCE WITH EMCS SECURITY OBJECTIVES	48
TABLE 4: CCN INTRANET CHANNEL - COMPLIANCE WITH EMCS SECURITY OBJECTIVES	51
TABLE 5: CCN MAIL 2 CHANNEL - COMPLIANCE WITH EMCS SECURITY OBJECTIVES	52
TABLE 6: SECURITY REQUIREMENTS	57
TABLE 7: CONTROLLED ACCESS POINTS – CCN NETWORK	74
TABLE 8: CONTROLLED ACCESS POINTS – CENTRAL SERVICES	93
TABLE 9: EMCS SECURITY COMPLIANCE MATRIX	117
TABLE 10: ACCESS CONTROL POLICY	122
TABLE 11: CONTROLLED ACCESS POINTS – NATIONAL DOMAIN AND EXTERNAL DOMAIN	131
TABLE 12: AUTHENTICATION AND AUTHORISATION SCHEME – SEQUENCES	135

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
LIST OF FIGURES	

List of Figures

FIGURE 1: ISF FRAMEWORK	33
FIGURE 2: EMCS OVERVIEW	36
FIGURE 3: EMCS SECURITY DOMAINS	39
FIGURE 4: EMCS BUSINESS COMMUNICATION CHANNELS	41
FIGURE 5: EMCS INFRASTRUCTURE CHANNELS - OVERVIEW	46
FIGURE 6: EMCS INFRASTRUCTURE COMMUNICATION CHANNEL (CSI)	47
FIGURE 7: EMCS INFRASTRUCTURE COMMUNICATION CHANNEL (WEB SERVICES)	49
FIGURE 8: EMCS INFRASTRUCTURE COMMUNICATION CHANNELS (EMAIL-BASED INTERFACE)	51
FIGURE 9: RESPONSIBILITY MODEL	60
FIGURE 10: ACCESS CONTROL – REGISTRATION	67
FIGURE 11: CCN INTRANET AUTHENTICATION	68
FIGURE 12: CCN NETWORK	70
FIGURE 13: CCN NETWORK RESILIENCE – EQUIPMENT REDUNDANCY	72
FIGURE 14: CENTRAL SERVICES SECURITY COMPONENTS – OVERVIEW	80
FIGURE 15: CEA SECURITY - PROTECTION AGAINST MALICIOUS SOFTWARE	91
FIGURE 16: HTTP SESSION-LEVEL SECURITY – TOPOLOGY	97
FIGURE 17: NEA TO CEA AUTHENTICATION – CERTIFICATE-BASED	98
FIGURE 18: CEA AUTHORISATIONS	99
FIGURE 19: CEA WEB SERVICES ADDRESSING – HTTPS TRANSPORT	101
FIGURE 20: STANDARD EXCISE APPLICATION ARCHITECTURE	102
FIGURE 21: SERVICE BROKER TECHNICAL ARCHITECTURE	105
FIGURE 23: NATIONAL DOMAIN – PHYSICAL SECURITY	124
FIGURE 24: SECURE AUDIT LOGS (SAL)	133
FIGURE 25: ARROWS CONVENTIONS	135
FIGURE 26: WEB SERVICE CHANNEL SECURITY – AUTHENTICATION AND AUTHORISATION (PART 1)	136
FIGURE 27: WEB SERVICE CHANNEL SECURITY – AUTHENTICATION AND AUTHORISATION (PART 2)	137
FIGURE 28: WEB SERVICE CHANNEL SECURITY – AUTHENTICATION AND AUTHORISATION (PART 3)	138
FIGURE 29: WEB SERVICE CHANNEL SECURITY – AUTHENTICATION AND AUTHORISATION (PART 4)	139
FIGURE 30: EXCISE MOVEMENT AUTHENTICITY - DIGITAL SIGNATURE	142
FIGURE 31: PKI ARCHITECTURE TYPES	145
FIGURE 32: CA COMBINATIONS	145
FIGURE 33: EMCS COMMON DOMAIN PKI (CDPKI) – OVERVIEW	147
FIGURE 34: EMCS COMMON DOMAIN PKI (CDPKI) – BRIDGE CA/VA	149
FIGURE 35: TRUST RELATIONSHIP ESTABLISHMENT PROCESS	150

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

1. Management Summary / Kurzfassung / Résumé

1.1. English

1.1.1. Purpose of the Document

The Security Excise System Specifications (SESS) address the security issues of EMCS applications, which fall under the responsibility of DG TAXUD – the Central Excise Applications (CEA). It also addresses security issues relating to the interfaces between the Common Domain and the National Domains and, in so far as a National Excise Application (NEA) is in use, the secure interoperability between the National Domain and the External Domain. The SESS indicates how the high-level security requirements identified in the EMCS Security Policy (SEP) [\[R3\]](#), where applicable to the CEA applications, will be applied.

The SESS complies with the recommendations of the Information Security Forum (ISF) [\[R35\]](#) and covers the five building blocks of Information Security as defined by the ISF: Security Management, Critical Business Applications, Computer Installations, Networks, and Systems Development. In short, Computer Installations and Networks provide the underlying infrastructure (or “*IT facilities*”) on which the Critical Business Applications run. Systems Development deals with how new applications are created and Security Management addresses high-level direction and control.

The SESS provides a guidance on “*Who does What?*”: Managers take care of security management; Developers and their team leaders feed secure software into the systems; System administrators install and maintain systems; and Network engineers take care of the secure connectivity between the systems¹.

1.1.2. Intended Readership

The intended readership of this document is:

- Central and national project teams involved in the EMCS specifications, development and operations;
- MSA Security Officers in charge of enforcing security procedures and controls;
- ECP Management.

Refer to the SEP [\[R3\]](#) for more details about the roles and responsibilities of the intended readership.

1.1.3. Document Summary

As indicated in the SEP, “*the use of EMCS system should never be an obstacle to the free exchange of goods on the Single Market, nor represent a bottleneck in the daily activity of Economic Operators.*”

A necessary condition to meet this objective is to make sure that the EMCS target architecture (as specified in the TESS [\[R9\]](#)) meets the security requirements (i.e. the “*What*”) formulated

¹ For further information regarding security roles please refer to the SEP [\[R3\]](#).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

in the SEP and consequently to specify the security measures (i.e. the “*How*”) that need to be implemented by the EMCS.

To reach this goal, the SESS is elaborated on a two-step basis:

- *Gathering EMCS background information* (see Chapter 3) with regards to the EMCS Architecture Overview, EMCS Security Objectives, EMCS Security Domains, EMCS Business Communication Channels, EMCS Infrastructure Communication Channels, and EMCS Security Requirements. This information comes from two main sources: the SEP [R3] and the TESS [R9];
- *Specifying security measures*, ensuring that the requirements formulated in the SEP can be met by the EMCS target architecture. This specification process focuses on three main areas (corresponding to the TESS Sections II, III, and IV):
 - EMCS Common Domain Security Measures (see Chapter 4);
 - EMCS Central Services Security Measures (see Chapter 5);
 - Standard Excise Application Security Measures (see Chapter 6).

It is to be noted that only security specifications provided in the Chapter 4 are of a compulsory nature for the Member State Administrations, as they correspond to the part of the EMCS system that *must be enforced at national level* to ensure the interoperability between national excise systems. The other Chapters do not impose specific constraints to the National Domain.

However, as the overall EMCS security also relies on the assurance that every MSA has effectively implemented the necessary security measures for the proper running of its national system (NEA), a “*National Domain Security Guidance*” is provided in [Appendix B](#) so as to help MSAs in the implementation of the national EMCS security measures.

It is also important to mention that the SESS has been elaborated *in parallel* with the TESS, so that security aspects could be considered at an early stage in the EMCS design and that consistency between both documents could be ensured.

1.1.4. Document Structure

The SESS is made up of six main Chapters and three Appendices, as follows:

- Chapter 1 **Management Summary.** Provides the reader with an overview of the SESS document goals and content.
- Chapter 2 **References.** Provides pointers to reference documents, the list of acronyms used in the SESS (and not yet included in the Glossary of Terms [R1]), and information about the security standards used as guidance for the SESS elaboration.
- Chapter 3 **EMCS Background Information.** Provides background information with regards to the EMCS Architecture Overview, EMCS Security Objectives, EMCS Security Domains, EMCS Business Communication Channels, EMCS Infrastructure Communication Channels, and EMCS Security Requirements.
- Chapter 4 **EMCS Common Domain Security Measures.** Provides the specifications of the security measures to be implemented at the Common Domain level (Central Services excluded) to meet the

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

identified security requirements.

- Chapter [5](#) **EMCS Central Services Security Measures.** Provides the specifications of the security measures to be implemented at the Central Services level to meet the identified security requirements.
- Chapter [6](#) **Standard Excise Application (SEA) Security Measures.** Provides the specifications of the security measures to be implemented at the Standard Excise Application level to meet the identified security requirements.
- Appendix A **Compliance Matrix.** Allows the assessment of the coverage of all security requirements in the SESS. Takes the form of a table indicating for each requirement the related general security measures to be implemented (as indicated by the SEP [\[R3\]](#)) and provides pointers to the paragraphs where those security measures are further specified.
- Appendix B **National Domain Security Guidance.** Provides guidance to Member State Administration for the implementation of security measures in the National Domain.
- Appendix C **Web Service Channel Security – Authentication and Authorisation Scheme.** Provides the detailed specification of the authentication and authorisation scheme that is to be followed to access CEA backend applications resources.
- Appendix D **Proposal for the EMCS Common Domain PKI (CDPKI).** Provides the description of the public key infrastructure that could be implemented in the Common Domain to answer EMCS specific cryptographic controls requirements.

1.1.5. Guidance to the Reader

The SESS document shall be read in conjunction with the following documents, which bring complementary information to the specifications:

- The Glossary of Terms (GLT) [\[R1\]](#), which defines all business concepts used in EMCS and the IT-related terms of use in the ESS project;
- The Security Excise Policy (SEP) [\[R3\]](#), which defines the security policy in EMCS;
- The Technical Excise System Specifications (TESS) [\[R9\]](#), which provides the technical specifications of the EMCS architecture incorporating business, application, and infrastructure requirements;
- The Central Operation Specification (COS) [\[R6\]](#), which defines the functions of the EMCS Central Operations (EMCS/CO).

1.1.6. Changes to this Document

Changes to the present document shall follow the Change Management Procedures described in EMCS Terms of Collaboration [\[R2\]](#).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

1.2. Deutsch

1.2.1. Zielsetzung des Dokuments

Die Sicherheitsspezifikationen des Verbrauchsteuersystems (SESS) behandeln die Aspekte der Sicherheit der EMCS-Anwendungen, die in den Zuständigkeitsbereich der DG TAXUD fallen - die Zentralen Verbrauchsteueranwendungen (CEA). Sie behandeln auch Sicherheitsfragen bezüglich der Schnittstellen zwischen dem Gemeinsamen Bereich und den Nationalen Bereichen und, sofern eine Nationale Verbrauchsteueranwendung (NEA) verwendet wird, die sichere Interoperabilität zwischen dem Nationalen Bereich und dem Externen Bereich. Die SESS geben an, wie die in der EMCS-Sicherheitspolitik (SEP) [\[R3\]](#) festgelegten hochrangigen Sicherheitsanforderungen angewendet werden, sofern sie für die CEA-Anwendungen gelten.

Die SESS entsprechen den Empfehlungen des Informationssicherheitsforums (ISF) [\[R35\]](#) und decken die fünf Bausteine der Informationssicherheit gemäß der Definition des ISF ab: Sicherheitsmanagement, kritische Geschäftsanwendungen, Datenverarbeitungsanlagen, Netzwerke und Systementwicklung. In Kürze kann folgendes festgestellt werden: Datenverarbeitungsanlagen und Netzwerke bilden die zugrunde liegende Infrastruktur (oder „IT-Anlagen“), auf der die kritischen Geschäftsanwendungen laufen. Der Bereich Systementwicklungen behandelt die Frage, wie neue Anwendungen angelegt werden, während es im Bereich Sicherheitsmanagement um Leitung und Kontrolle auf höchster Ebene geht.

Die SESS bieten Leitlinien bezüglich des „Wer macht was“: Manager, die sich um das Sicherheitsmanagement kümmern; Entwickler und ihre Teamleiter, die sichere Software in die Systeme einspeisen; Systemverwalter, die Systeme installieren und warten; und Netzwerkingenieure, die für die sichere Verbindungsfähigkeit zwischen den Systemen verantwortlich sind².

1.2.2. Zielgruppe

Die Zielgruppe dieses Dokuments ist folgende:

- zentrale und nationale Projektteams, die an EMCS-Spezifikationen, Entwicklung und Vorgängen beteiligt sind;
- MSA-Sicherheitsmitarbeiter, die für die Durchführung von Sicherheitsverfahren und Kontrollen zuständig sind;
- ECP-Management.

Der SEP [\[R3\]](#) sind weitere Einzelheiten über die Aufgaben und Zuständigkeiten der Zielgruppe zu entnehmen.

1.2.3. Zusammenfassung des Dokuments

Gemäß der SEP *„darf der Einsatz des EMCS-Systems unter keinen Umständen den freien Güterverkehr auf dem Binnenmarkt behindern oder beim Tagesgeschäft der Wirtschaftsbeteiligten einen Engpass darstellen.“*

² Für weitere Information über Sicherheitsvorschriften bitte verweisen Sie auf die SEP [\[R3\]](#).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

Zur Erreichung dieser Zielsetzung muss sicher gestellt werden, dass die EMCS-Zielarchitektur (so wie sie in der TESS [R9] festgelegt ist) den in der SEP enthaltenen Sicherheitsanforderungen entspricht, und es müssen folglich die vom EMCS umzusetzenden Sicherheitsmaßnahmen festgelegt werden.

Um diese Zielsetzung zu erreichen, werden die SESS in zwei Schritten erarbeitet:

- *Zusammentragen von EMCS-Hintergrundinformation* (siehe Kapitel 3), die sich auf EMCS-Architekturübersicht, EMCS-Sicherheitsziele, EMCS-Sicherheitsbereiche, EMCS-Geschäftskommunikationskanäle, EMCS-Infrastrukturkommunikationskanäle, EMCS-Sicherheitsanforderungen beziehen. Diese Informationen stammen aus zwei Hauptquellen: SEP [R3] und TESS [R9];
- *Festlegung der Sicherheitsmaßnahmen*, die gewährleisten, dass die in der SEP dargelegten Anforderungen von der EMCS-Zielarchitektur erfüllt werden können. Dieser Festlegungsprozess konzentriert sich auf drei Hauptbereiche (die den Abschnitten II, III und IV der TESS entsprechen):
 - Sicherheitsmaßnahmen des Gemeinsamen EMCS-Bereichs (siehe Kapitel 4);
 - Sicherheitsmaßnahmen der Zentralen EMCS-Dienstleistungen (siehe Kapitel 5);
 - Sicherheitsmaßnahmen der Standard-Verbrauchsteueranwendung (siehe Kapitel 6).

Es ist festzustellen, dass nur die in Kapitel 4 aufgeführten Sicherheitsspezifikationen für die Mitgliedstaatverwaltungen verbindlicher Art sind, da sie den Teil des EMCS-Systems darstellen, der *auf nationaler Ebene umgesetzt werden muss*, um die Interoperabilität zwischen den nationalen Verbrauchsteuersystemen zu gewährleisten. Die übrigen Kapitel schreiben für den Nationalen Bereich keine spezifischen Sachzwänge vor.

Da die Sicherheit des gesamten EMCS auch darauf beruht, dass gewährleistet wird, dass die einzelnen MSA die für das ordnungsmäßige Funktionieren ihres nationalen Systems erforderlichen Sicherheitsmaßnahmen auch tatsächlich umgesetzt haben, ist in Anhang B ein „Leitfaden für die Sicherheit des Nationalen Bereichs“ enthalten, der die MSA bei der Umsetzung der nationalen EMCS-Sicherheitsmaßnahmen unterstützen soll.

Es ist auch wichtig festzustellen, dass die Erarbeitung der SESS *parallel* zur Entwicklung der TESS erfolgt ist, damit die Sicherheitsaspekte zu einem frühen Stadium der EMCS-Gestaltung betrachtet und die Übereinstimmung zwischen den beiden Dokumenten gewährleistet werden konnte.

1.2.4. Dokumentstruktur

Die SESS bestehen aus den nachfolgend aufgeführten sechs Hauptkapiteln und drei Anhängen:

- Kapitel 1 **Kurzfassung**. Gibt dem Leser eine Übersicht über die SESS Dokumentziele und -inhalt.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

- Kapitel [2](#) **Referenzdokumente.** Enthält Hinweise auf Bezugsdokumente, die Liste der in den SESS verwendeten Abkürzungen (die noch nicht im Glossar enthalten sind [\[R1\]](#)) und Informationen über die bei der Erarbeitung der SESS als Leitfaden verwendeten Sicherheitsstandards.
- Kapitel [3](#) **EMCS-Hintergrundinformation.** Bietet Hintergrundinformationen zu EMCS-Architekturübersicht, EMCS-Sicherheitszielen, EMCS-Sicherheitsbereichen, EMCS-Geschäftskommunikationskanälen, EMCS-Infrastrukturkommunikationskanälen, und EMCS-Sicherheitsanforderungen.
- Kapitel [4](#) **Sicherheitsmaßnahmen des Gemeinsamen EMCS-Bereichs.** Enthält Spezifikationen der Sicherheitsmaßnahmen, die auf der Ebene des Gemeinsamen Bereichs umzusetzen sind (ohne Zentrale Dienstleistungen), um die festgelegten Sicherheitsanforderungen zu erfüllen.
- Kapitel [5](#) **Sicherheitsmaßnahmen der zentralen EMCS-Dienstleistungen.** Enthält die Spezifikationen der Sicherheitsmaßnahmen, die auf der Ebene der Zentralen Dienstleistungen umzusetzen sind, um die festgelegten Sicherheitsanforderungen zu erfüllen.
- Kapitel [6](#) **Sicherheitsmaßnahmen der Standard-Verbrauchsteueranwendung (SEA).** Enthält die Spezifikationen der Sicherheitsmaßnahmen, die auf der Ebene der Standard-Verbrauchsteueranwendung umzusetzen sind, um die festgelegten Sicherheitsanforderungen zu erfüllen.
- Appendix A **Befolgungsmatrix.** Lässt zu der Einschätzung der Abdeckung aller festgelegten Sicherheitsanforderungen der SESS. Weist die Form einer Tabelle auf, die für jede allgemeine umzusetzende Sicherheitsanforderung (so wie von der SEP [\[R3\]](#) angegeben) die damit verbundenen Sicherheitsmaßnahmen enthält und umfasst Verweise auf die Abschnitte, in denen diese Sicherheitsmaßnahmen weiter spezifiziert werden.
- Appendix B **Leitfaden für die Sicherheit des Nationalen Bereichs.** Bietet der Mitgliedstaatverwaltung einen Leitfaden für die Umsetzung der Sicherheitsmaßnahmen im Nationalen Bereich.
- Appendix C **Sicherheit des Web-Dienstleistungskanals – Authentisierungs- und Autorisierungsschema.** Enthält die umfassende Spezifikation für das Authentisierungs- und Autorisierungsschema, das im Bereich des Zugriffs auf die CEA-Back-End-Anwendungsressourcen zum Einsatz kommt.
- Appendix D **Vorschlag für die EMCS Common Domain PKI (CDPKI).** Enthält die Beschreibung der Public Key-Infrastruktur, die in dem Gemeinsamen Bereich eingeführt werden könnte, um EMCS spezifische Kryptographikskontrollenanforderungen zu beantworten.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

1.2.5. Hinweis für den Leser

Das SESS-Dokument ist zusammen mit den folgenden Dokumenten, die zusätzliche Informationen zu den Spezifikationen enthalten, zu lesen:

- dem Glossar (GLT) [\[R1\]](#), in dem alle im EMCS verwendeten Geschäftskonzepte und die im ESS-Projekt verwendeten IT-spezifischen Begriffe definiert werden;
- der Sicherheitsverbrauchsteuerpolitik (SEP) [\[R3\]](#), die die Sicherheitspolitik im EMCS festlegt;
- der Technischen Spezifikation des Verbrauchsteuersystems (TESS) [\[R9\]](#), die die technischen Spezifikationen der EMCS-Architektur einschließlich Geschäfts-, Anwendungs- und Infrastrukturanforderungen enthält;
- den Zentralen Betriebsspezifikationen (COS) [\[R6\]](#), in denen die Funktionen der Zentralen EMCS-Vorgänge (EMCS/CO) dargelegt sind.

1.2.6. Änderungen an diesem Dokument

Änderungen an diesem Dokument müssen entsprechend den in den EMCS-Zusammenarbeitsbestimmungen [\[R2\]](#) beschriebenen Änderungsmanagementverfahren vorgenommen werden.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

1.3. Français

1.3.1. Objectif du document

Le document de spécifications de la sécurité du système d'accises (Security Excise System Specifications ou SESS) traite des enjeux en matière de sécurité des applications EMCS, lesquelles relèvent de la responsabilité de la DG Fiscalité et Union Douanière (TAXUD) – les applications centrales d'accises (CEA). Ces spécifications abordent également les enjeux de sécurité liés aux interfaces entre le domaine commun et les domaines nationaux ainsi que, lorsqu'une application d'accises nationale (NEA) est utilisée, la sécurité de l'interopérabilité entre le domaine national et le domaine externe. La SESS indique comment seront appliquées les exigences de sécurité de haut niveau identifiées dans la politique de sécurité EMCS (Security Policy ou SEP) [\[R3\]](#) lorsqu'elles s'appliquent aux applications centrales CEA.

La SESS est conforme aux recommandations du Forum pour la Sécurité Informatique (ISF) [\[R35\]](#) et couvre les cinq piliers de la sécurité informatique tels que définis par l'ISF : la gestion de la sécurité, la sécurisation des applications critiques, la protection des équipements informatiques, la sécurité des réseaux et des systèmes en développement. En bref, les équipements informatiques et les réseaux composent l'infrastructure de base (ou « *IT facilities* ») sur laquelle reposent les applications critiques. La sécurité des systèmes en développement porte sur la manière dont les nouvelles applications sont créées et la gestion de la sécurité définit les orientations générales en matière de sécurité et de contrôle.

La SESS apporte des indications sur le « Qui fait Quoi » : les décideurs responsables de la bonne gestion de la sécurité ; les programmeurs et les chefs d'équipes chargés de produire des systèmes constitués de logiciel sécurisé ; les administrateurs de systèmes chargés de l'installation et de la maintenance des systèmes informatiques ; et les ingénieurs réseaux assurant la sécurité des liaisons entre systèmes³.

1.3.2. Lecteurs concernés

Ce document s'adresse au groupe cible suivant :

- Les équipes de projet centrales et nationales impliquées dans les spécifications, le développement et les opérations EMCS ;
- Les responsables de la sécurité des administrations des Etats Membres chargés du respect des procédures de sécurité et des contrôles ;
- Le comité directeur ECP.

Veuillez consulter la SEP [\[R3\]](#) pour tout détail complémentaire quant aux rôles et aux responsabilités des lecteurs concernés.

³ Veuillez vous référer à la SEP [\[R3\]](#) pour davantage d'informations sur les rôles exercés dans le domaine de la sécurité.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

1.3.3. Résumé du document

Comme indiqué dans la SEP, « *l'utilisation du système EMCS ne devrait jamais faire obstacle au libre échange des biens sur le marché unique, ni constituer un goulet d'étranglement pour les activités quotidiennes des opérateurs économiques.* »

La condition nécessaire à la réalisation de cet objectif est de s'assurer que l'architecture EMCS visée (définie dans le document TESS [R9]) répond aux exigences de sécurité (c.-à-d. le « *Quoi* ») formulées dans la SEP et donc de spécifier les mesures de sécurité (c.-à-d. le « *Comment* ») qui doivent être mises en œuvre par le système EMCS.

Pour atteindre cet objectif, la SESS est élaborée en deux étapes :

- *La collecte des informations de base EMCS* (voir chapitre 3) en rapport avec l'architecture globale EMCS, les objectifs de sécurité EMCS, les domaines de sécurité EMCS, les canaux de communication EMCS de type métier, les canaux de communication EMCS de type infrastructure, et les exigences de sécurité EMCS. Ces informations proviennent de deux sources principales : la SEP [R3] et la TESS [R9] ;
- *La spécification des mesures de sécurité*, veillant à ce que les exigences stipulées dans la SEP soient respectées par l'architecture EMCS visée. Ce processus de spécification est axé sur trois principaux domaines (correspondant aux sections TESS II, III, et IV) :
 - Mesures de sécurité du domaine commun EMCS (voir chapitre 4) ;
 - Mesures de sécurité des services centraux EMCS (voir chapitre 5) ;
 - Mesures de sécurité de l'application standard d'accises (voir chapitre 6).

Il convient de noter que seules les spécifications de sécurité fournies dans le chapitre 4 sont de nature obligatoire pour les administrations des Etats Membres (MSA), puisqu'elles correspondent à la partie du système EMCS *qui doit être appliquée au niveau national* pour garantir l'interopérabilité entre les systèmes d'accises nationaux. Les autres chapitres n'imposent pas de contraintes spécifiques au domaine national.

Cependant, comme la sécurité globale de EMCS repose aussi sur la garantie que chaque MSA a bel et bien mis en œuvre les mesures de sécurité nécessaires au fonctionnement correct de son système national, un « *Guide de la sécurité pour le domaine national* » (*National Domain Security Guidance*) est fourni dans l'annexe B afin d'aider les MSA dans la mise en œuvre des mesures de sécurité EMCS au niveau national.

Il importe également de mentionner que l'élaboration du document SESS a été réalisée *en parallèle* à celle du document TESS, afin que les aspects liés à la sécurité puissent être pris en compte de manière précoce dans la conception du système EMCS et que la cohérence entre les deux documents puisse être assurée.

1.3.4. Structure du document

Le document SESS est composé de six chapitres principaux et de trois annexes, structurés comme suit :

- Chapitre 1 **Résumé.** Fournit au lecteur un tour d'horizon des objectifs et du contenu du document SESS.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

- Chapitre [2](#) **Références.** Fournit des renvois aux documents de référence, la liste des sigles utilisés dans le SESS (et non encore inclus dans le Glossaire terminologique [\[R1\]](#)), et des informations relatives aux normes de sécurité utilisées comme lignes directrices pour l'élaboration du document SESS.
- Chapitre [3](#) **Informations de base EMCS.** Fournit des informations de base en rapport avec l'architecture globale EMCS, les objectifs de sécurité EMCS, les domaines de sécurité EMCS, les canaux de communication EMCS de type métier, les canaux de communications EMCS de type infrastructure et les exigences de sécurité EMCS.
- Chapitre [4](#) **Mesures de sécurité du domaine commun EMCS.** Fournit les spécifications des mesures de sécurité à mettre en œuvre au niveau du domaine commun (services centraux exclus) afin de respecter les exigences de sécurité identifiées.
- Chapitre [5](#) **Mesures de sécurité des services centraux EMCS.** Fournit les spécifications des mesures de sécurité à mettre en œuvre au niveau des services centraux en vue de respecter les exigences en matière de sécurité.
- Chapitre [6](#) **Mesures de sécurité de l'application standard d'accises.** Fournit les spécifications des mesures de sécurité à mettre en œuvre au niveau de l'application standard d'accises pour répondre aux exigences identifiées en matière de sécurité.
- Annexe A **Matrice de Conformité.** Permet de valider que toutes les exigences de sécurité identifiées sont effectivement traitées dans la SESS. Est présentée sous la forme d'un tableau indiquant pour chaque exigence de sécurité générale (tel qu'indiqué dans la SEP [\[R3\]](#)) les mesures correspondantes à mettre en œuvre et fournit des renvois aux paragraphes où ces mesures de sécurité sont abordées plus en détail.
- Annexe B **Guide de la sécurité pour le domaine national.** Fournit des lignes directrices à l'intention des administrations des Etats membres pour la mise en œuvre des mesures de sécurité dans le domaine national.
- Annexe C **Sécurité du canal Web Service – Schéma d'authentification et d'autorisation.** Fournit des spécifications détaillées du schéma d'authentification et d'autorisation adopté pour accéder aux ressources des applications CEA de back office.
- Annexe D **Proposition pour le EMCS Common Domain PKI (CDPKI)**
Fournit la description de l'infrastructure à clé publique qui pourrait être mise en œuvre dans le Domaine Commun afin de répondre aux besoins spécifiques de contrôles cryptographiques.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
MANAGEMENT SUMMARY / KURZFASSUNG / RESUME	

1.3.5. Guide pour le lecteur

Le document SESS doit être lu en combinaison avec les documents suivants, lesquels contiennent des informations complémentaires aux spécifications :

- Le glossaire terminologique (GLT) [\[R1\]](#), lequel définit tous les concepts commerciaux utilisés dans EMCS ainsi que les termes du domaine IT utilisés dans le projet ESS ;
- La politique de sécurité pour les accises (Security Excise Policy ou SEP) [\[R3\]](#), laquelle définit la politique de sécurité dans EMCS ;
- Les spécifications techniques du système d'accises (Technical Excise System Specifications ou TESS) [\[R9\]](#), document fournissant les spécifications techniques de l'architecture EMCS, y compris les exigences en termes d'activité, d'application et d'infrastructure ;
- Les spécifications des opérations centrales (Central Operation Specifications ou COS) [\[R6\]](#), document définissant les fonctions des opérations centrales EMCS (EMCS/CO).

1.3.6. Changements apportés à ce document

Les changements apportés au présent document suivront les procédures de gestion des changements décrites dans les termes de collaboration EMCS [\[R2\]](#).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
REFERENCES	

2. References

2.1. Documents

Ref.	Identifier	Title	Version	Issued
[R1]	ECP1-ESS-GLT	Glossary of Terms (GLT)	1.01	14-Nov-04
[R2]	ECP1-ESS-TOC	EMCS Terms of Collaboration	0.05	13-May-04
[R3]	ECP1-ESS-SEP	EMCS Security Policy (SEP)	2.01	12-Nov-04
[R4]	ECP1-ESS-FESS	Functional Excise System Specifications	1.02	29-Apr-05
[R5]	ECP1-ESS-ACS	Acceptance and Certification Specifications	1.00	14-Oct-05
[R6]	ECP1-ESS-COS	Central Operation Specifications	1.00	14-Oct-05
[R7]	ECP1-ESS-FRS	Fallback and Recovery Specifications	1.02	29-Apr-05
[R8]	ECP1-ESS-PSS	Phasing and Scope Specifications	-	Under release
[R9]	ECP1-ESS-TESS	EMCS Technical Excise System Specifications (TESS)	1.00	25-Jan-06
[R10]	TMP-TEC-SEC	TEMPO: Security Approach - Technique	1.00	12/06/2001
[R11]	TMP-GDL-LAT	TEMPO: Logging and Audit Trails Procedures	0.1-EN	15/06/2006
[R12]	CCN-CSEC-POL	CCN/CSI General Security Policy	3.01	Under release
[R13]	TSS-SEC-POL	NCTS Security Policy	3.05	27-Jan-98
[R14]	POLSEC	EC Information Systems Security Policy	0.23	20-Dec-00
[R15]	3771	European Commission, DIGIT, Overview of the usage of the Information System Hosting Services of the Data Centre	3	25-Nov-05
[R16]	CCN-CSQP-DE111	CCN/TC Service Quality Plan for TAXUD/2005/DE/111-DE111		30-Apr-05
[R17]	CCN-CPRG-IAS	CCN Intranet Authentication Services – Programmer’s Guide	1.01	08-Dec-05
[R18]	CCN-CMPR-GW	CCN Gateway Management Procedures	14.00	04-May-04
[R19]	CCN-CSEC-TCPRO	CCN/TC Security Procedures	0.1	03-Jun-05
[R20]	CCN/CSI-PRG-AP/C-01-MARB	Application Programming Guide (C language)	11	11-Jul-00

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
REFERENCES	

Ref.	Identifier	Title	Version	Issued
[R21]	CCN-CREF-JCSI	jCSI Reference Manual (Java)	1.0	23/07/2004
[R22]	CCN/CSI-REF-HL/C-01-MARB	HL Reference Manual (C language)	15	19/06/2001
[R23]	CCN/CSI-REF-ComD/C-01-MARB	Common Definitions Reference Manual (C language)	15	19/06/2001
[R24]	CCN/CSI-REF-HL/COB-01-MARB	HL Reference Manual (COBOL language)	03	19/06/2001
[R25]	CCN/CSI-REF-ComD/COB-01 – MARB	Common Definitions Reference Manual (COBOL language)	03	19/06/2001
[R26]	CCN/CSI-REF-ERR-01-MARB	CSI Error Reason Codes Reference Manual	05	05/08/1998
[R27]	CCN/CSI-ACG-GEN-01-MARB	Application Configuration Guide	09	19/06/2001
[R28]	77/799/EEC	COUNCIL DIRECTIVE 77/799/EEC of 19 December 1977 concerning mutual assistance by the competent authorities of the Member States in the field of direct and indirect taxation http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&type_doc=Directive&an_doc=1977&nu_doc=0799&lg=EN		19-Dec-77
[R29]	92/12/EEC	COUNCIL DIRECTIVE 92/12/EEC of 25 February 1992 on the general arrangements for products subject to excise duty and on the holding, movement and monitoring of such products http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=en&numdoc=31992L0012		25-Feb-92
[R30]	1152/2003/EC	DECISION n°1152/2003/EC of the EUROPEAN PARLIAMENT and of the COUNCIL of 16 June 2003 of computerising the movement and surveillance of excisable products http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_162/l_16220030701en00050008.pdf		16-Jun-03
[R31]	1798/2003/EC	Council Regulation (EC) No		07-Oct-03

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
REFERENCES	

Ref.	Identifier	Title	Version	Issued
		1798/2003 of 7 October 2003 on administrative cooperation in the field of value added tax and repealing Regulation (EEC) No 218/92 http://europa.eu.int/scadplus/leg/en/lvb/131003.htm		
[R32]	2073/2004/EC	Regulation (EC) No 2073/2004 of the European Parliament and of the Council of 16 November 2004 on administrative cooperation in the field of excise duties http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Regulation&an_doc=2004&nu_doc=2073		16-Nov-04
[R33]	1999/93/EC	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_0132_0000119en00120020.pdf		13-Dec-99
[R34]	ISO/IEC 17799:2000	Information Security Management Systems (ISMS) – Specification with Guidance for Use		2000
[R35]	ISF	Information Security Forum (ISF) – Standard of Good Practice Ref. ISF_Standard_2005.pdf	4.1	Jan. 2005
[R36]		OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. Paris: OECD www.oecd.org		Jul. 2002
[R37]		European Interoperability Framework for Pan-European eGovernment Services - Framework.	4.2	Jan. 2004
[R38]	EuroPKI (2000-2004)	EuroPKI Certification Policy http://www.europki.org/ca/root/cps/en_cp.pdf	1.1	Jan. 2004
[R39]	FPKI	Federal Public Key Infrastructure (FPKI) Architecture Technical Overview http://www.cio.gov/fbca/documents/		Oct. 2005

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
REFERENCES	

Ref.	Identifier	Title	Version	Issued
		FPKIAtechnicalOverview.pdf		
[R40]	PKIX	Public-Key Infrastructure (X.509) http://www.ietf.org/html.charters/pkix-charter.html		16-Dec-05
[R41]	WS-Security	OASIS Web Services Security (WSS) - WS-Security 2004 http://www.oasis-open.org	1.0	06-Apr-04
[R42]	WS-Security	SOAP Message Security 1.0 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf	1.0	15-Mar-04
[R43]	WS-Security	Username Token Profile 1.0 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf	1.0	15-Mar-04
[R44]	SAL	Building an Encrypted and Searchable Audit Log – Palo Alto Research Center http://www.parc.com/research/publications/files/5059.pdf		09-Jan-04

Table 1: Reference Documents

2.2. Acronyms

Readers are referred to the EMCS Glossary of Terms (GLT) [\[R1\]](#) for project specific abbreviations and acronyms. Additional abbreviations and acronyms used in this document (but not included in the current GLT) are listed in [Table 2](#).

ACL	Access Control List
BCC	Business Communication Channel
BCP	Business Continuity Plan
Bridge CA/VA	Bridge Certification Authority / Validation Authority
CA	Certification Authority
CAD	Central Application Designer
CDIA	Central Directory Administrator
CDPKI	Common Domain Public Key Infrastructure
CEA	Central Excise Applications
CLFS	Common Logging Facilities Subsystem
CPR	Customer Premises Router
CRL	Certificate Revocation List

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
REFERENCES	

CRLDP	Certificate Revocation List Distribution Point
CSCA	Central Services Certificate Authority
CSP	Credential Service Provider
DDNEA	Design Documentation of the National Excise Application
DDS	Data Dissemination System
DMZ	De-Militarised Zone
ECN	EDI/CSI Node
EMCS/CO	EMCS Central Operation
EO	Economic Operator
ETA	Excise Test Application
EU	European Union
F/W	Firewall
GTA	Global Trust Authority
ICC	Infrastructure Communication Channel
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IMAP4	Internet Message Access Protocol (version 4)
ISDN	Integrated Services Digital Network
ISF	Information Security Forum
J2EE	Java 2 Enterprise Edition
LCMS	Local CCN Mail System
LLE	Link-Level Encryption
LDAP	Lightweight Directory Access Protocol
N/A	Not Applicable
NDCP	National Domain Connection Point
NCTS/CO	New Computerised Transit System / Central Operations
OCSP	Online Certificate Status Protocol
OSPF	Open Shortest Path First
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PoP	Point of Presence
POP3	Post Office Protocol (version 3)
PRF	Profile
QoS	Quality of Service
RA	Registration Authority
RAP	Remote API Proxy
RFC	Request for Comment
RIP	Routed Internet Protocol
RSK	(security) Risk
SAL	Secure Audit Log
SCVP	Simple Certification Verification Protocol
SEA	Standard Excise Application
SFI	Submitted for Information

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
REFERENCES	

SM	Security Measure
SMTP	Simple Mail Transport Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SR	Security Requirement
SRP	Secure Reverse Proxy
TSL	Trusted Status List
UC	Use Case
URI	Uniform Resource Identifier
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
WSSE	Web Service Security Element

Table 2: Abbreviations and Acronyms

2.3. Security Standards

The SESS has been written based on internationally recognised best practices in the field of Information Systems security. Mainly two documents constitute the basis for the SESS:

- The ISO/IEC 17799 Standard [\[R34\]](#);
- The Information Security Forum (ISF) practical guidance [\[R35\]](#).

Both standards are shortly described hereafter.

2.3.1. ISO/IEC 17799

ISO/IEC 17799 is a detailed security standard organised into ten major categories, each covering a specific security discipline:

- | | |
|--|---------------------------------------|
| 1. Security Policy | 6. Computer and Network Operations |
| 2. Security Organisation | 7. Access Control |
| 3. Asset Classification and Control | 8. System Development and Maintenance |
| 4. Personnel Security | 9. Business Continuity Planning |
| 5. Physical and Environmental Security | 10. Compliance |

The ISO/IEC 17799 has been widely used during the SEP elaboration [\[R3\]](#).

2.3.2. ISF Standard

The Information Security Forum (ISF) formalises the Information Security according to a framework divided into five main security building blocks ([Figure 1](#)):

1. **Security Management (SM)**: Keeping the business risks associated with information systems under control within an organisation requires clear direction and commitment from the top, the allocation of adequate resources, effective arrangements for promoting good information security practice throughout the organisation and the establishment of a secure environment.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
REFERENCES	

2. ***Critical Business Applications (CB)***: A critical business application requires a more stringent set of security measures than other applications. By understanding the business impact of a loss of confidentiality, integrity or availability of information, it is possible to establish the level of criticality of an application. This provides a sound basis for identifying business risks and determining the level of protection required to keep risks within acceptable limits.
3. ***Computer Installations (CI)***: Computer installations typically support critical business applications and safeguarding them is, therefore, a key priority. Since the same information security principles apply to any computer installation irrespective of where information is processed or on what scale or type of computer, a common standard of good practice for information security should be applied.
4. ***Networks (NW)***: Computer networks are complex. They have to link different systems together, are subject to constant change and often rely on services provided by external parties. Orchestrating the related technical and organisational issues requires sound management. Accordingly, this area covers the organisational arrangements for running a network, its design, resilience and documentation, and the management of relationships with service providers.
5. ***Systems Development (SD)***: Building security into systems during their development is more cost-effective and secure than grafting it on afterwards. It requires a coherent approach to systems development as a whole, and sound disciplines to be observed throughout the development cycle. Ensuring that information security is addressed at each stage of the cycle is of key importance

In short, Computer Installations and Networks provide the underlying infrastructure (or “*IT facilities*”) on which the Critical Business Applications run. Systems Development describes how new applications are created and Security Management addresses high-level direction and control.

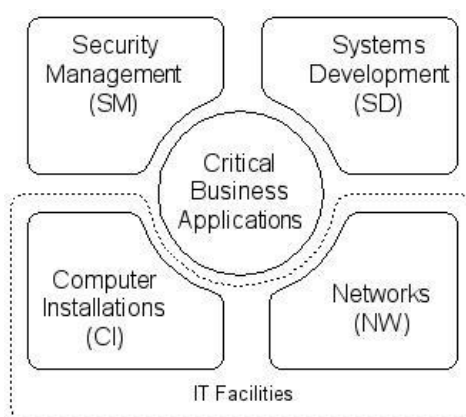


Figure 1: ISF Framework

It is interesting to notice in the ISF Standard (compared to the ISO/IEC 17799 Standard), that it provides a clear separation of the various responsibilities of the major IT security fields and therefore it provides an implicit guidance in “*who does what?*”:

- Managers in charge of security management,
- Developers and their team leaders producing secure software into the systems,

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
REFERENCES	

- System administrators installing and maintaining systems, and
- Network engineers in charge of the connectivity between the systems.

If one of these building blocks would be missing, the security architecture protecting the Critical Business Applications would be incomplete. To avoid gaps, it was therefore decided that the SESS Chapters [4](#), [5](#), [6](#) and [Appendix B](#) (i.e. where security measures are specified) would be structured following the ISF Standard.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

3. EMCS Background Information

3.1. Introduction

This section provides background information that allows selecting the appropriate security measures to be implemented by the EMCS Common Domain architecture (see §4), the EMCS Central Services Architecture (see §5), and the Standard Excise Application architecture (see §6), as well as those that are proposed to MSA to implement security of EMCS in the National Domain (see [Appendix B](#)).

Therefore, this Chapter focuses on the following items:

- EMCS Architecture Overview (see §3.2);
- EMCS Security Objectives (see §3.3);
- EMCS Security Domains (see §3.4);
- EMCS Business Communication Channels (see §3.5);
- EMCS Infrastructure Communication Channels (see §3.6);
- EMCS Security Requirements (see §3.7).

3.2. EMCS Architecture Overview

3.2.1. Domains and Applications

In line with the *Principle of Subsidiarity* (as explained in more detail in the TESS [\[R9\]](#)), the Excise Movement and Control System (EMCS) architecture is composed of three *Domains* with their related responsibility boundaries in the system implementation (see [Figure 2](#)). These domains are:

- The *Common Domain*, which encompasses the common infrastructure (i.e. CCN Network) and Central Services, which are made available and maintained by the European Commission to sustain the operation of the EMCS;
- The *National Domain*, which consists of the infrastructure of every MSA, including the hardware and software components implementing the National Excise Application⁴ (NEA), and the security and network distribution components that allow the National Domain to communicate with both the Common Domain and the External Domain;
- The *External Domain*, which includes all Economic Operators (EcOp) along with their system and network infrastructure used to exchange information with their MSA.

These domains impose specific requirements on the EMCS architecture and the decomposition of EMCS into *Applications* (as developed in the *TESS Section I* [\[R9\]](#)). In particular, any

⁴ The NEA consists of the integration of the (centrally developed) Standard Excise Application (SEA) to the Nationally Developed Excise Application (NDEA).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

constraints enforced on the National Domain are limited to the communication with the Common Domain. All other choices relating to nationally developed excise applications (referred to as NEA) are left up to each particular MSA.

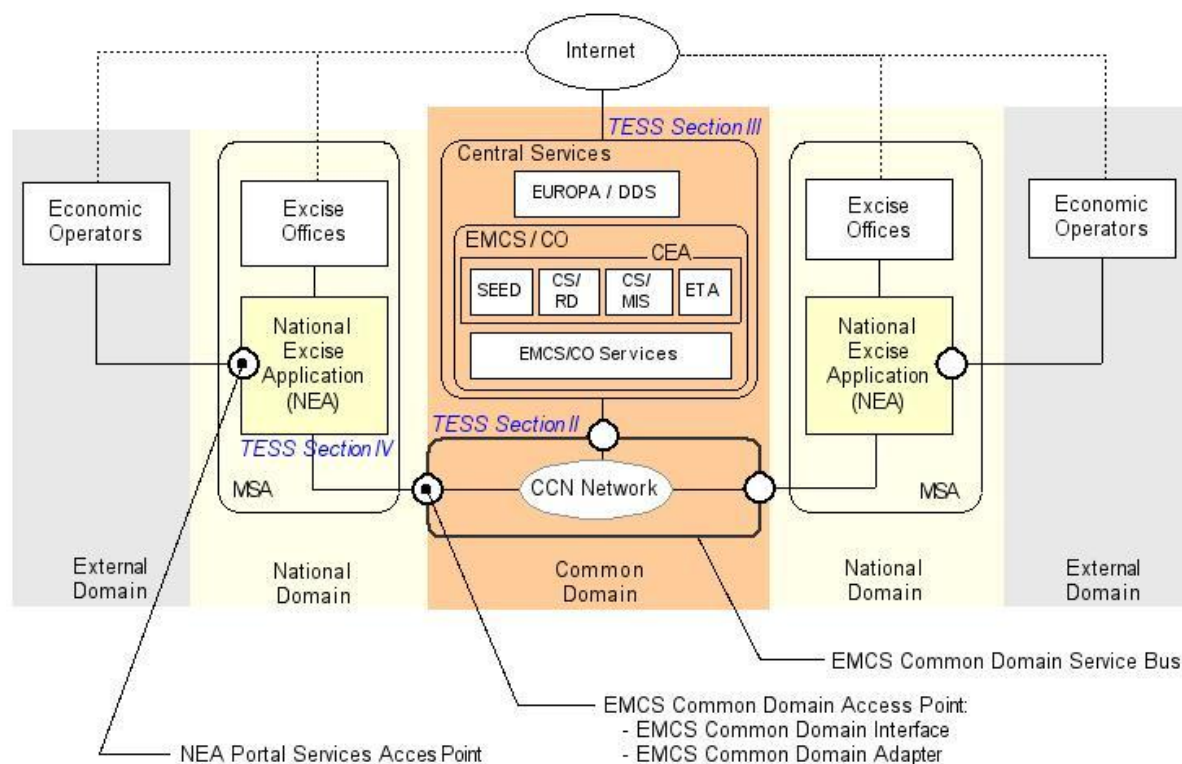


Figure 2: EMCS Overview

3.2.2. References to the Technical Excise Systems Specifications (TESS)

The SESS has been elaborated *in parallel* with the TESS [R9] so that security aspects could be considered at an early stage in the EMCS design and that consistency between both documents could be ensured. The TESS is articulated around three main topics:

- The specifications of the **EMCS Common Domain Architecture** (developed in the *TESS Section II*), which establishes the core architectural principles and design choices of the EMCS Common Domain components implemented by the **EMCS Common Domain Service Bus** (that provides the necessary functionality to support EMCS requirements in the Common Domain);
- The specifications of the **EMCS Central Services Architecture** (developed in the *TESS Section III*), which establishes the core architectural principles and design choices of the EMCS Central Excise Applications (CEA) that provide services made centrally available to MSAs and Economic Operators. Those services refer to:
 - **SEED**: The System for Exchange of Excise Data that provides management and dissemination services regarding information on the Economic Operators register. This is a vital part of the EMCS Central Services due to its dependency on the EMCS core business processes execution;

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

- **CS/RD**: The Central Services/Reference Data that provides management and dissemination services regarding common Reference Data;
- **CS/MIS**: The Central Services/Management Information System that provides the facilities to assist the monitoring and the reporting on the operations of EMCS. This is performed by collecting, distributing and publishing EMCS business and technical statistics (including availability statistics) and by providing information on movements (ARC follow-up);
- **ETA**: The Excise Test Application that is used for testing a NEA located at the MSA premises.

At MSA level, the interactions with the CEA are achieved through the CCN Network. At Economic Operators level, the interactions with the CEA are achieved through EUROPA / Data Dissemination System (DDS) via Internet.

The EMCS Central Operation Services (EMCS/CO) offered to MSAs are described in the Central Operation Specifications (COS) [\[R6\]](#).

- The specifications of the **Standard Excise Application (SEA) Architecture** (developed in the *TESS Section IV*), which aim at:
 - Providing MSA development teams with guidance and architecture on how NEA could be built and integrated;
 - Providing solutions for the implementation of the "Start-up Pack" (i.e. start-up solution addressed to MSA that did not yet implement their own national excise application). The Start-up Pack services would then allow Economic Operators to enforce the electronic continuity of documents flows.

3.3. EMCS Security Objectives

As already mentioned in *TESS Section I “General Introduction”* [\[R9\]](#), the specifications of the EMCS system shall comply with the Security Objectives as defined in the SEP [\[R3\]](#). To help in the readability of this document, those objectives are reminded hereafter. They are expressed in terms of availability, confidentiality and integrity of EMCS assets, and legitimate use of the EMCS.

3.3.1. Availability

[SO1]	Availability. Ensure the continuity of the EMCS system and its services to its users.
-----------------------	--

The EMCS system should never turn out to be responsible for a loss or an unacceptable delay in the transmission of data.

For the EMCS functions, which are considered as “business critical” (i.e. Submission and registration of AAD, Receipt of goods and discharge of movement guarantee, Update during the movement, Import of goods, Export of goods, Placement under customs procedures, and Risk assessment), this objective is translated in terms of 24h/24, 7d/7 availability requirement, which is not without implications in terms of security.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

In particular, this requirement highlights the need of adequate security measures to be implemented at infrastructure level (e.g. equipment redundancy – see §4.4.1.2), at application level (e.g. SEA broker object persistence – see §6), and at business level (e.g. establishment of a EMCS business continuity plan – §5.3.4), in addition to the native security offered by the CCN Network (which does not guaranty such availability rate for the time being as indicated in *TESS Section II, Chapter 7 [R9]*).

3.3.2. Confidentiality

[SO2]	Confidentiality. Minimise impact of damages to the EMCS Community, the Member State Administrations and the Economic Operators resulting from the unauthorised disclosure or loss of protected information.
-------	--

The EMCS target system shall also ensure the confidentiality of all EMCS data assets (as defined in the SEP [R3]). In particular, it shall ensure that:

- On the Economic Operators side: only the Economic Operators involved in an excise movement have access to the content of the e-AAD related to that movement;
- On the MSA side: only duly authorised MSA officials can access the content of an e-AAD (e.g. for control purposes).

3.3.3. Integrity

[SO3]	Integrity. Minimise impact of damages to the EMCS Community, the Member State Administrations and the Economic Operators resulting from improper modification of information.
-------	--

The EMCS target system shall ensure the integrity of data since the use of contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions, hence reducing the assurance of the EMCS system.

3.3.4. Legitimate Use of the System

[SO4]	Legitimate Use of the system.
-------	--------------------------------------

Security measures (referring to authentication, access control, and secure audit logs) shall be implemented so as to ensure that:

- Protected resources are not used by unauthorised persons or in unauthorised ways;
- Users and application activity can be traced back (history records).

Non-repudiation is implicitly included in the "Legitimate Use of the System" objective, which requires that "*users and application activity can be traced back (history record)*". This aspect is further developed in §10.2.3 and §8.5.2.2 "Secure Audit Logs (SAL)", which provides means to ensure that user/application activity log cannot be modified without this being detected. Cryptographically protected audit logs provide a legally valid proof of the system use (covering non-repudiation).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

3.4. EMCS Security Domains

According to the ISO/IEC 17799 standard [R34], a Security Domain refers to “an area of the same (or similar) security policy, requirements and measures, for example, network services, applications services, operations services, etc.” This means that a security incident in a single security domain should not be permitted to adversely impact the security of another security domain. Security domains have therefore their own protection profiles.

Based on this definition, it makes sense to consider that the *EMCS Security Domains* should follow the same responsibility domains decomposition as the one specified in the FESS (and further described in *TESS Section I, Chapter 2 [R9]*). Three main Security Domains can therefore be considered for EMCS: the *Common Domain*, the *National Domain* and the *External Domain*

As far as the Common Domain and National Domain are concerned, it is however to be noted that those domains are not totally disjoint. Indeed, as shown on [Figure 3](#), the CCN/CSI Security Policy [R12], due to the fact that Common Domain equipment is deployed at MSA premises, imposes a set of obligations on the National Domain.

Also the EMCS Security Policy (SEP) [R3] covers aspects, which relate to Common Domain Central Services but also to National Domain excise applications (NEA) that are subject to national security policies.

This overlapping between Common Domain and National Domain security policies is not an issue as long as the recommendations for the Common Domain do not contradict those for the National Domain, hence leading to potential inconsistencies in the implementation of the overall system security. To minimise the risk, Common Domain policies impacting National Domain systems (e.g. SEP) are submitted to MSAs for validation before their enforcement, which gives an opportunity to MSAs to address potential incompatibilities.

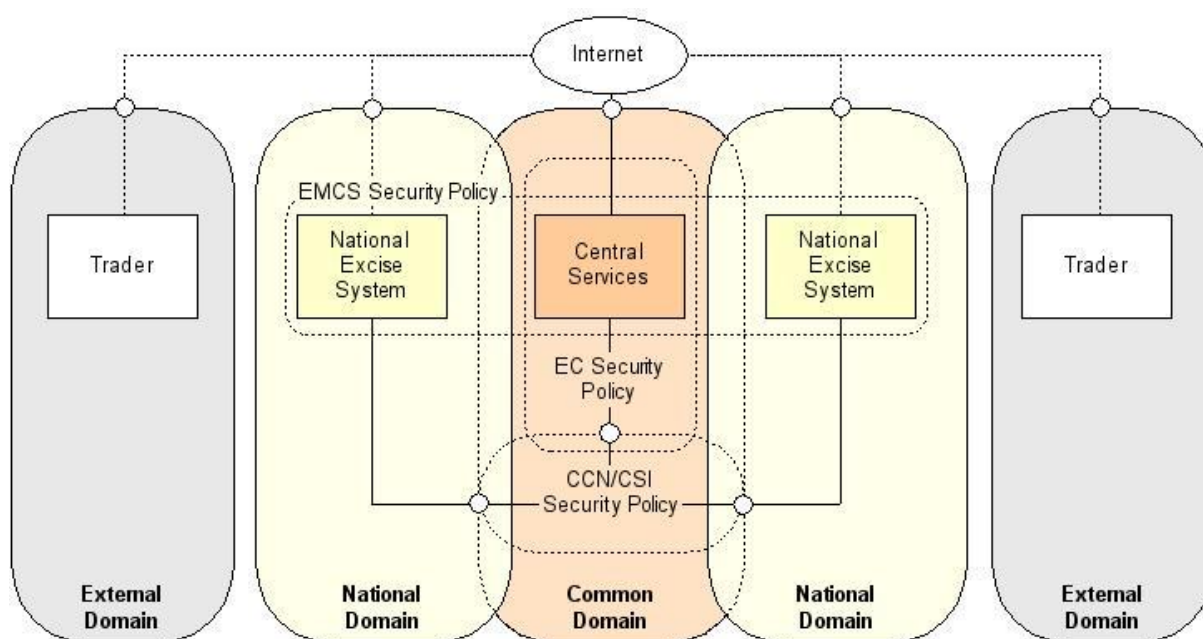


Figure 3: EMCS Security Domains

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

3.5. EMCS Business Communication Channels

Figure 4 shows the Business Communications Channels [BCC], which were identified during the EMCS Business Scenarios identification process.

These channels characterise the business relationships between the various EMCS actors, independently from the underlying IT infrastructure that makes those relationships possible. This is the reason why a single Business Communication Channel could rely on several Infrastructure Communication Channels (see §3.6).

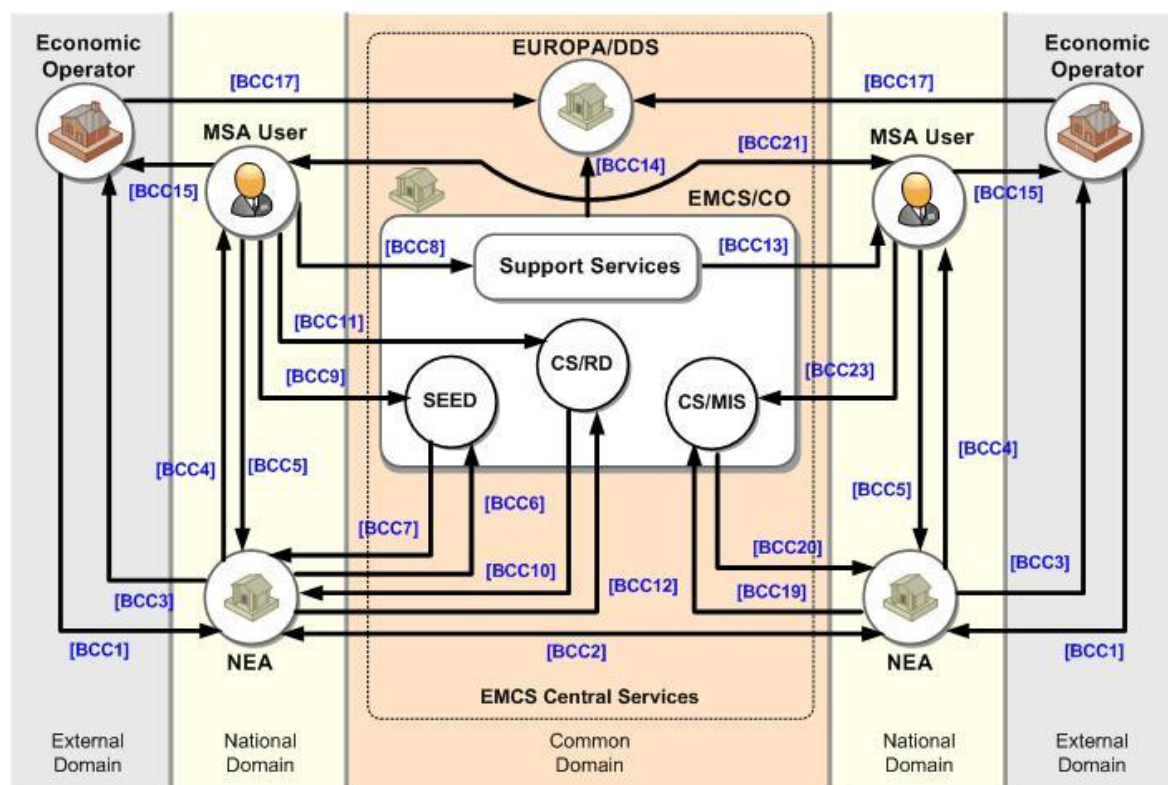


Figure 4: EMCS Business Communication Channels

These business communication channels are described in details in *TESS Section I, Chapter 4 [R9]*, along with their respective performance and availability requirements. They are summarised below:

- [BCC1] **Economic Operator to NEA**
This communication channel links the External Domain (e.g. Economic Operators) to the National Excise Application through the Internet (or eventually other networks, e.g. X.400). It requires a *permanent* class of availability [AR1], an *interactive* class of response time [PR1] since it supports critical business services, and *secure logging*.
- [BCC2] **NEA to NEA**
This is one of the most important communication channels to be considered in this document. It links all the National Excise Applications through the Common Domain. This communication channel is applicable in most EMCS

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

use cases relating to the core business involving system-to-system relationships. It requires a *high* class of availability [AR2], an *asynchronous* class of response time [PR2], a *guarantee of delivery* since it supports critical business exchanges, and *secure logging*.

- [BCC3] **NEA to Economic Operator**

This communication channel links the National Domain (NEA) to the External Domain (Economic Operator’s system) through the Internet. This communication channel is applicable in EMCS Core Business use cases (see FESS Section II [R4]) involving inter-domain system-to-user relationships. It requires a *permanent* class of availability [AR1], an *asynchronous* class of response time [PR2], and *secure logging*.

- [BCC4] **NEA to MSA User**

This communication channel links the NEA to MSA Users located in the National Domain (national Officials) through the national network. This communication channel is applicable to most EMCS use cases involving intra-domain system-to-user relationships. It requires an *office* class of availability [AR3], an *asynchronous* class of response time [PR2], and *secure logging*.

- [BCC5] **MSA User to NEA**

This communication channel makes accessible the National Excise Applications for the local MSA Users through the national network. This communication channel is applicable to most EMCS use cases involving intra-domain user-to-system relationships. It requires an *office* class of availability [AR3], an *interactive* class of response time [PR1] since it tightly links user interfaces and interactive applications, and *secure logging*.

- [BCC6] **NEA to SEED**

This communication channel mainly supports the submission of SEED updates by the MSAs. It requires a *high* class of availability [AR2], an *asynchronous* class of response time [PR2], a *guarantee of delivery* since it supports critical business exchanges with SEED, *strong authentication*, and *secure logging*.

- [BCC7] **SEED to NEA**

This communication channel mainly supports the dissemination of SEED data maintained centrally. It requires a *high* class of availability [AR2], an *asynchronous* class of response time [PR2], a *guarantee of delivery* since it supports critical business exchanges (in particular regarding SEED), and *secure logging*.

- [BCC8] **MSA Users to EMCS/CO Support Services**

This communication channel provides collaborative means of exchanges between MSA Users located in the MSAs and the Central Support Services provided by the EMCS/CO (see COS [R6]). It requires an *office* class of availability [AR3] and an *interactive* class of response time [PR1].

- [BCC9] **MSA Users to SEED**

This channel provides interactive exchanges between users in MSAs and

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

SEED. It requires an *office* class of availability [AR3], an *interactive* class of response time [PR1] since it tightly links user interfaces and interactive applications, and *strong authentication*.

- [BCC10] **EMCS CS/RD to NEA**

This communication channel mainly supports the dissemination of reference data maintained centrally. It requires an *office* class of availability [AR3], an *asynchronous* class of response time [PR2], and *secure logging*.

- [BCC11] **MSA Users to EMCS CS/RD**

This channel provides interactive exchanges between users in MSAs and the CS/RD services. It requires an *office* class of availability [AR3], an *interactive* class of response time [PR1] since it tightly links user interfaces and interactive applications, and *strong authentication*.

- [BCC12] **NEA to EMCS CS/RD**

This communication channel mainly supports the submission of Reference Data updates by the MSAs. It addresses the use cases described in *FESS Section III [R4]* and in particular the re-synchronisation of reference data (UC1.05) where NEAs request reference data (UC-105-110). It requires an *office* class of availability [AR3], an *asynchronous* class of response time [PR2], *strong authentication*, and *secure logging*.

- [BCC13] **EMCS/CO Support Services to MSA Users**

This communication channel provides collaborative means of exchanges between the Central Support Services provided by the EMCS/CO (see COS [\[R6\]](#)) and MSA Users located in the MSAs. It requires an *office* class of availability [AR3] and an *asynchronous* class of response time [PR2].

- [BCC14] **CEA to EUROPA/DDS**

This channel supports the information exchanges between CEA and EUROPA/DDS in order to provide a diverse set of publications and services, intended for public users. It requires a *scheduled* class of availability [AR4] and a *scheduled* class of response time [PR3].

- [BCC15] **MSA User to Economic Operator**

This communication channel links MSA Users located in the National Domain to MSA Users located in the External Domain (Economic Operators) through the Internet. This business channel has been deduced from the following requirements:

- Communication with Occasionally Registered Operator (ORO), which is required in some use cases (e.g. UC-206-410) where an MSA makes special arrangements to establish connection with ORO;
- Fallback Solution (FRS).

It is encountered in EMCS use cases involving inter-domain user-to-user relationships. It requires an *office* class of availability [AR3] and an *asynchronous* class of response time [PR2].

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

- [BCC17] **Economic Operator to EUROPA**

This channel provides interactive exchanges between users in the External Domain (Economic Operators) and the EUROPA web site. It addresses the use case UC1.30 (Consultation of registration information by economic operators). It requires a *high* class of availability [AR2] and an *interactive* class of response time [PR1] since it tightly links user interfaces and interactive applications.

- [BCC19] **NEA to CS/MIS**

This communication channel mainly supports the submission of logging, monitoring and statistical information captured by the NEA and transmitted to CS/MIS. It requires an *office* class of availability [AR3], a *scheduled* class of response time [PR3], *strong authentication*, and *secure logging*.

- [BCC20] **CS/MIS to NEA**

This communication channel mainly supports the dissemination of centrally consolidated statistics and monitoring information regarding availability of the infrastructure. It requires an *office* class of availability [AR3], a *scheduled* class of response time [PR3], and *secure logging*.

- [BCC21] **MSA User to Remote MSA User**

This communication channel provides collaborative means of exchanges between MSA Users. It allows users in the MSA to asynchronously communicate with people in the other MSA. It requires an *office* class of availability [AR3] and an *asynchronous* class of response time [PR2].

- [BCC23] **MSA User to CS/MIS**

This channel provides interactive exchanges between users in MSA and the CS/MIS services. It requires an *office* class of availability [AR3], an *interactive* class of response time [PR1] since it tightly links user interfaces and interactive applications, and *strong authentication*.

Note: In the case of [\[BCC8\]](#), [\[BCC9\]](#), [\[BCC11\]](#), [\[BCC13\]](#), and [\[BCC23\]](#), the term "MSA User" only includes the national Service Desk.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

3.6. EMCS Infrastructure Communication Channels

3.6.1. Introduction

The Infrastructure Communication Channels (ICC) characterise the technical links, which are made available to transport EMCS messages.

They are described in detail in *TESS Section I* [\[R9\]](#) and are summarised hereafter.

In short, three types of channels are considered ([Figure 5](#)):

- **CCN/CSI Channel** (see [§3.6.2](#)), which offer a secure and reliable communication channel for the asynchronous/synchronous exchange of messages;
- **CCN Intranet Channel** (see [§3.6.3](#)) used for HTTP/HTTPS (synchronous) exchanges and access to Web Services (e.g. those offered by Central Services applications as described in *TESS Section III* [\[R9\]](#));
- **CCN Mail 2 Channel** (see [§3.6.4](#)) offering standard SMTP-based e-mail exchanges (e.g. exchange between national officials).

The knowledge of those infrastructure channels is important from the security point of view. In particular, their compliance with regards to the EMCS security objectives (see [§3.3](#)) has been analysed carefully (see [Table 3](#) to [Table 5](#)) so as to be able to select the most appropriate channel(s) to answer EMCS security requirements (see [3.7](#)).

This analysis shows that the CCN Mail 2 channel does not offer today the level of reliability (in particular with regard to the EMCS availability requirements) that is required by EMCS to transport IE messages and that the CCN/CSI channel should be preferred to perform such operation. It also shows that the CCN Intranet could advantageously benefit from Public Key Infrastructure (PKI) related technologies to provide an acceptable level of security (in particular to provide secure interactive access to EMCS Central Services (see [§5.8](#))).

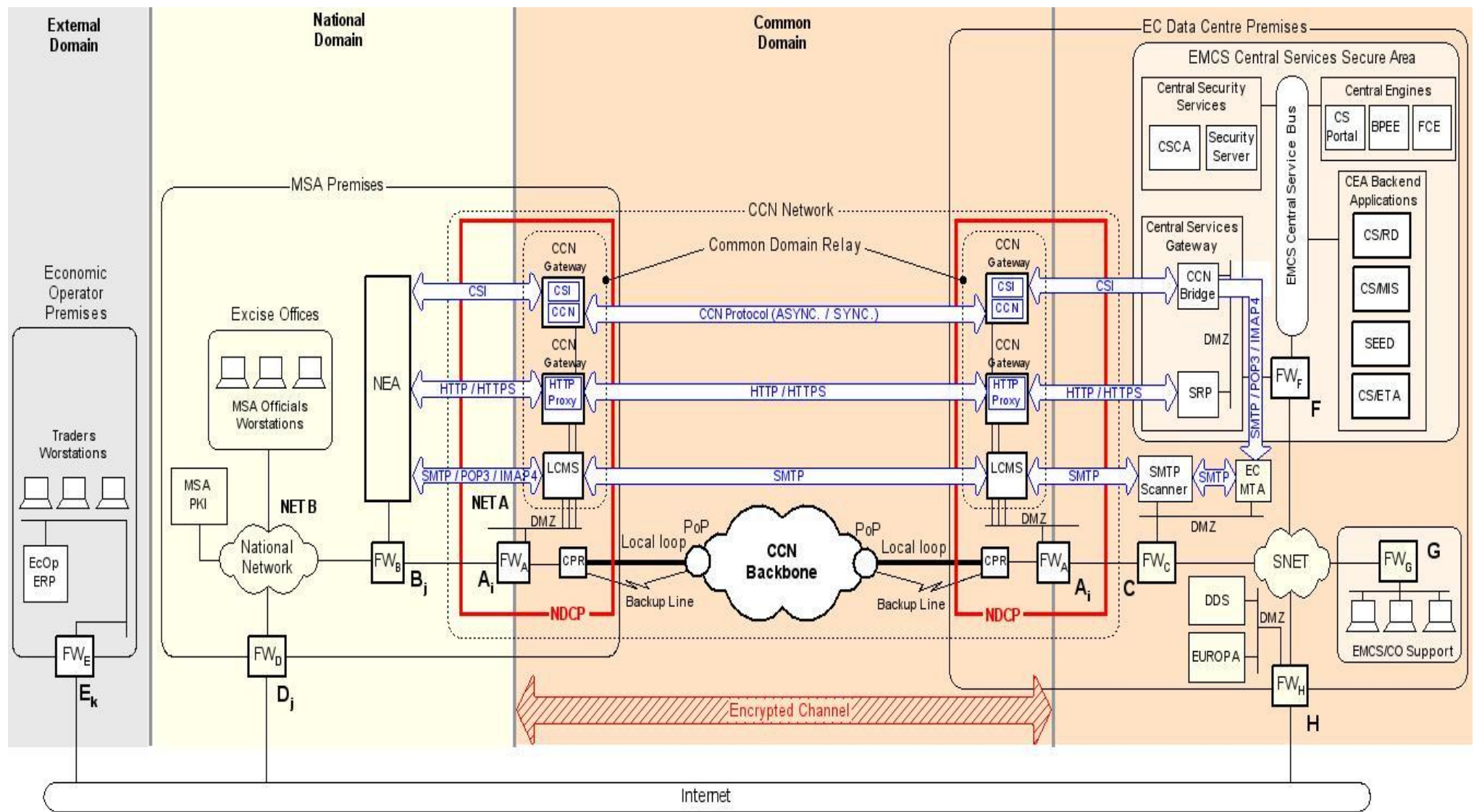


Figure 5: EMCS Infrastructure Channels - Overview

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

3.6.2. CCN/CSI Channel

3.6.2.1. Intended Usage

The CCN/CSI channel (see *TESS Section II, Chapter 3*) provides machine-to-machine communication in heterogeneous environments using both synchronous and asynchronous paradigms. CCN/CSI services are not intended for (human) interactive use and do not offer any user-interface.

CCN/CSI services offer the main communication channel to EMCS applications. More specifically National Excise Applications (NEA) must use the CCN/CSI *asynchronous* transmission mode to interact with other NEAs through the CCN Network (e.g. transmission of a locally validated e-ADD to the concerned NEAs at MSA of Destination).

According to the EMCS Business Communication Channels definition (see §3.5), CCN/CSI services are intended for the following usage:

- [\[BCC2\]](#)NEA to NEA
- [\[BCC6\]](#)NEA to SEED
- [\[BCC7\]](#)SEED to NEA
- [\[BCC10\]](#)EMCS CS/RD to NEA
- [\[BCC12\]](#)NEA to EMCS CS/RD
- [\[BCC19\]](#)NEA to CS/MIS
- [\[BCC20\]](#)CS/MIS to NEA

3.6.2.2. Description

The CCN/CSI channel topology (see [Figure 6](#)) provides a queue-based messaging model. Each queue offers persistent storage and allows applications to send and read messages. Messages are delivered in a reliable fashion between CCN gateways for processing by the target application.

This transmission mode significantly reduces the coupling between applications. Applications do not wait for immediate responses from other parts of the system before continuing, which makes the entire platform more tolerant to any application or system failure.

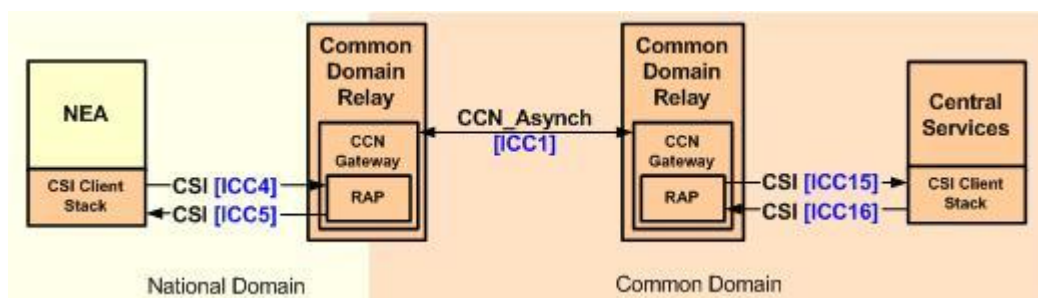


Figure 6: EMCS Infrastructure Communication Channel (CSI)

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

CSI-based applications interact with the Common Domain Relay using the Common Systems Interface (CSI), a programming interface provided by the CSI Client software, which is to be installed in the application platforms. CSI offers a simplified access to CCN services through the *Remote API Proxy (RAP)* located in the *CCN Gateway*.

3.6.2.3. Compliance with EMCS Security Objectives

The CCN/CSI channel compliance with regards to EMCS security objectives (see §3.5) is examined below (Table 3):

Security Objective	Channel Characteristic	Channel Compliance	
		Business critical data	Other data
Availability	Specific SLA arrangements are taken to ensure the availability of the CCN/CSI channel (see <i>TESS Section II, Chapter 3.3.3</i> for more details). Moreover equipment redundancy (e.g. doubling of NDCP equipment) is applied when needed to increase the system resilience.	Compliant	Compliant
Confidentiality.....	IPSec (168-bit 3DES) encryption ensures the confidentiality of data transiting the CCN backbone. Moreover CSI-based applications can request for data confidentiality in the QoS attribute of a message transmission. In this case, the message content is encrypted directly by the CSI stack, to ensure the confidentiality on the National Domain side (i.e. between the NEA and the local CCN Gateway).	Compliant	Compliant
Integrity	CSI-based applications can request for integrity checks in the QoS attribute of a message transmission, by applying a cryptographic hash function to the message contents.	Compliant	Compliant
Legitimate use.....	A set of audit logs on the CCN traffic that is exchanged via the CCN Gateways is maintained and consolidated centrally for audit and statistics purpose.	Not compliant (1)	Not compliant (1)
(1) Logs produced by the CCN Gateways are not linked to the EMCS business and consequently do not allow assessing the legitimate use of the EMCS system by Economic Operators and MSA Users. Additional security measures (e.g. Secure Audit Logs) have therefore to be implemented at NEA level. See §8.5 for more details.			

Table 3: CCN/CSI Channel - Compliance with EMCS Security Objectives

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

3.6.3. CCN Intranet Channel

3.6.3.1. Intended Usage

The CCN Intranet channel provides the CCN Community with a secure channel for the support of HTTP/S-based services and therefore offers a straightforward path for the deployment of Service-Oriented Architecture (SOA).

For EMCS this channel is mainly used to access Web Services (SOAP/HTTP/S) and Web Interface (HTML/HTTP/S), which are made available centrally to MSA applications and users (see *TESS Section III EMCS Central Services Architecture* for more information).

More precisely, according to the EMCS Business Communication Channels definition (see §3.5), CCN Intranet services are intended for the following usage:

- [\[BCC6\]](#)NEA to SEED
- [\[BCC8\]](#)MSA Users to EMCS/CO Support Services
- [\[BCC9\]](#)MSA Users to SEED
- [\[BCC12\]](#)NEA to EMCS CS/RD
- [\[BCC19\]](#)NEA to CS/MIS
- [\[BCC11\]](#)MSA Users to EMCS CS/RD
- [\[BCC23\]](#)MSA Users to CS/MIS

3.6.3.2. Description

CCN Intranet services are delivered through specialised servers, called CCN Gateways, deployed at every MSA site, and implementing AAA (Authentication, Authorisation and Accounting) and HTTP Proxy functions ([Figure 7](#)).

The CCN Intranet channel offers a straightforward path to the deployment of Web Services that can be used by client applications that need access to excise data such as Economic Operators details, the lists of Excise Offices and Excise Products.

The Web Services channel presents a synchronous interface based on SOAP (Simple Object Access Protocol) technology. The communication is provided by the HTTP/S protocol over the CCN Network. Applications interact with the HTTP Proxy running on their local CCN Gateway that routes the HTTP/S traffic to the requested destination.

When HTTPS is used the HTTP Proxy does not decrypt the communication and a point-to-point encrypted channel (e.g. NEA ↔ NEA, NEA ↔ CEA) can therefore be established over the CCN Network between the Applications Platforms.

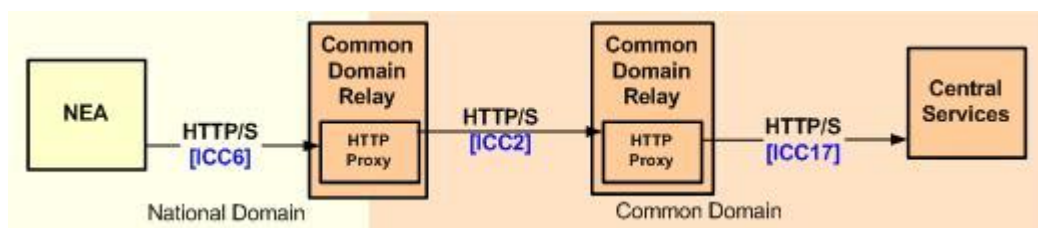


Figure 7: EMCS Infrastructure Communication Channel (Web Services)

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

3.6.3.3. Compliance with Security Objectives

The CCN Intranet channel compliance with regards to EMCS security objectives (see §3.3) is examined below ([Table 4](#)):

Security Objective	Channel Characteristic	Channel Compliance	
		Business critical data	Other data
Availability	Specific SLA arrangements are taken to ensure the availability of the CCN Intranet channel (see <i>TESS Section II, Chapter 3.3.3</i> for more details). Moreover equipment redundancy (e.g. doubling of NDCP equipment) is applied when needed to increase the system resilience.	Compliant	Compliant
Confidentiality....	IPSec (168-bit 3DES) encryption ensures the confidentiality of data transiting the CCN backbone. However, when the HTTPS protocol is used, the involved HTTP Proxies establish an SSL secure communication throughout the CCN Network (e.g. to allow the point-to-point communication between the NEA and the CEA) and therefore have no possibility to perform access controls at the NDCP level (e.g. no session ticket verification), which can be considered as a vulnerability affecting data confidentiality.	Not compliant (1)	Compliant
Integrity	When the HTTP protocol is used, the CCN Intranet channel does not provide any explicit support to ensure data integrity during transit. The IPSec (168-bit 3DES) encryption performed at NDCP level compensates this weakness, but this only concerns the integrity of data transiting the CCN Network (and not those transiting the MSA network on the National Domain side).	Not fully compliant (2)	Not fully compliant (2)
Legitimate use....	A set of audit logs on the HTTP traffic that is exchanged via the HTTP Proxies is maintained and consolidated centrally for audit and statistics purpose. But the HTTPS traffic is not logged with the same level of details since a point-to-point SSL secure communication is established between communicating parties (e.g. NEA ↔ NEA or NEA ↔ CEA).	Not compliant (3)	Not compliant (3)

(1) Additional security measures are needed at CEA level to provide the required level of confidentiality whatever the protocol used (HTTP or HTTPS). See §5.8.1 for more details.

(2) Compliance can however be obtained if an SSL v.3 point-to-point secure communication is established between the communicating parties (e.g. NEA ↔ NEA or NEA ↔ CEA) and/or if SOAP message-level integrity checks are used (see §5.8.2).

(3) Logs produced by the CCN Gateways are not linked to the EMCS business and consequently do not allow assessing the legitimate use of the EMCS system by Economic Operators and MSA Users. Additional security measures (e.g. Secure Audit Logs) have therefore to be implemented at NEA (see §8.5) and CEA (see §5.4.3.1) levels.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

Table 4: CCN Intranet Channel - Compliance with EMCS Security Objectives

3.6.4. CCN Mail 2 Channel

3.6.4.1. Intended Usage

The CCN Mail 2 channel provides the MSAs with a secure channel for the support of e-mail services over the CCN Network.

Concerning EMCS, the CCN Mail 2 channel is mainly used for the communication between MSA Users and for the transmission of automatic e-mail notifications generated by applications. More precisely, according to the EMCS Business Communication Channels definition (see §3.5), CCN Mail 2 services are intended for the following usage:

- [BCC8]MSA Users to EMCS/CO Support Services
- [BCC13]EMCS/CO Support Services to MSA Users
- [BCC21]MSA Users to Remote MSA Users

The CCN Mail 2 channel can also provide a simple fallback solution in case of unavailability of the CCN/CSI services (see §4.4.1.2.4).

3.6.4.2. Description

CCN Mail 2 services are delivered through specialised servers, called LCMS (for Local CCN Mail Server), deployed at every MSA site and implementing standard SMTP relaying functions as well as local functional mailboxes, which are made accessible to MSAs through standard protocols (i.e. POP3, IMAP4, and HTTP (webmail)).

Depending on MSA policy and technical environment, MSA users or NEA can interact either with their National MTA that routes the e-mail traffic to the LCMS, or directly to the LCMS, which in turn either gives access to the local resources (mailboxes) or relays the mail traffic to the right destination (e.g. Central Services) over the CCN backbone (Figure 8).

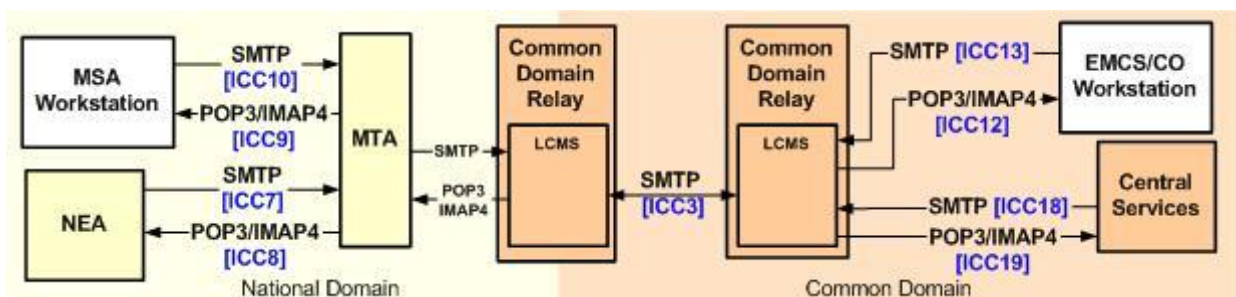


Figure 8: EMCS Infrastructure Communication Channels (Email-based Interface)

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

3.6.4.3. Compliance with EMCS Security Objectives

The CCN Mail 2 channel compliance with regards to EMCS security objectives (see §3.3) is examined below (Table 5):

Security Objective	Channel Characteristic	Channel Compliance	
		Business critical data	Other data
Availability	Specific SLA arrangements are taken to ensure the availability of the CCN Mail 2 channel (see <i>TESS Section II, Chapter 3.3.3</i> for more details). However the CCN/CSI Central Project does not provide redundancy of the LCMS equipment.	Not Compliant (1)	Compliant
Confidentiality.....	IPSec (168-bit 3DES) encryption ensures the confidentiality of data transiting the CCN backbone. However the access to the LCMS from the National Domain is not encrypted and end-to-end message-level confidentiality (through the use of S/MIME message encryption) is not supported.	Not Compliant (2)	Not Compliant (2)
Integrity	The CCN Mail 2 channel cannot guarantee that messages have not been modified during transit (unlike the CCN/CSI and SOAP message integrity checks).	Not Compliant (3)	Not Compliant (3)
Legitimate use.....	The CCN Mail 2 channel does not (yet) provide logging of e-mail traffic at Common Domain Relay level.	Not Compliant (4)	Not Compliant (4)
<p>(1) Due to the lack of redundancy, the use of the CCN Mail 2 should be considered as a fallback channel for EMCS messages transport (see §4.4.1.2.4).</p> <p>(2) Compliance could be obtained with the support of SSL at the LCMS level to secure POP3, IMAP4 and SMTP transport.</p> <p>(3) Support of digital signature to sign e-mail exchanged between the EMCS communicating parties could address this issue. This would require the communicating parties to make use of Public Key Infrastructure (PKI) services (e.g. for certificate management purposes) and, in some cases, trust relationships between existing PKIs to be established (as proposed in Appendix D, §10.3).</p> <p>(4) Additional security measures (e.g. Secure Audit Logs) have to be implemented at NEA (see Appendix B, §8.5) and CEA (see §5.4.3.1) levels.</p>			

Table 5: CCN Mail 2 Channel - Compliance with EMCS Security Objectives

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

3.7. EMCS Security Requirements

3.7.1. Introduction

The risk analysis performed within the SEP [\[R3\]](#) has helped defining a list of high-level security requirements to be met by the EMCS so as to eliminate (or at least to reduce) the identified security risks.

Note: The master risks list and related risk levels are provided in the SEP [\[R3\]](#).

Following the SESS scope (see §[1.1.1](#)), we were able to extract from this requirements list those involving technical measures (procedural measures being already addressed by the SEP).

The resulting subset of security requirements is provided in [Table 6](#). Each of them is described with its justification and the identifiers of the Business Communication Channels [BCCx] where those measures are applicable.

The next step will consist in specifying the Security Measures that meet those requirements. This is the scope of the Chapters [4](#), [5](#), and [6](#).

3.7.2. Security Requirements

To ensure the consistency between the SESS and the SEP, the codification adopted in [Table 6](#) to identify the selected Security Requirements [SRx] and their justification with regards to the assessed Security Risks [RSKx] uses the same labels and numbering as those used in the SEP.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

SEP Id.	Requirements Description	Justification	Applicable to the [BCC]
ISO Category #2: Security Organisation			
[SR2]	<p>Registration of Economic Operators</p> <p>Maintain the security of information processing facilities and information assets accessed by Economic Operators.</p>	<p>Eliminate (or at least reduce) the following risks:</p> <ul style="list-style-type: none"> • [RSK2] Illegitimate use of the EMCS system by Economic Operators • [RSK4] Illegitimate access to the EMCS system by Outsiders 	<p>[BCC15] [BCC5]</p>
ISO Category #5: Physical and Environmental Security			
[SR9]	<p>Secure Areas</p> <p>Prevent unauthorised physical access, damage and interference to business premises, to IT equipment (i.e. servers, routers, switches) and to information.</p>	<p>Eliminate (or at least reduce) the following risks:</p> <ul style="list-style-type: none"> • [RSK4] Illegitimate access to the EMCS system by Outsiders • [RSK10] Theft and/or Wilful Damage of Data and Facilities • [RSK23] Power failure • [RSK24] Air conditioning failure • [RSK25] Natural Disaster 	<p>[BCC2] [BCC6] [BCC7] [BCC10] [BCC12] [BCC14] [BCC19] [BCC20]</p>
[SR10]	<p>Equipment Security</p> <p>Prevent loss, damage or compromise of physical assets (e.g. telecom equipment) and interruption to business activities (e.g. power cut, over power).</p>	<p>Eliminate (or at least reduce) the following risks:</p> <ul style="list-style-type: none"> • [RSK4] Illegitimate access to the EMCS system by Outsiders • [RSK10] Theft and/or Wilful Damage of Data and Facilities • [RSK17] Failure in Outsourced Operations • [RSK18] Hardware Maintenance Error • [RSK19] Software Maintenance Error • [RSK20] Technical failure of host • [RSK21] Technical failure of storage device • [RSK22] Technical failure of print facilities • [RSK23] Power failure • [RSK24] Air conditioning failure • [RSK25] Natural Disaster 	<p>[BCC2] [BCC6] [BCC7] [BCC10] [BCC12] [BCC14] [BCC19] [BCC20]</p>

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

SEP Id.	Requirements Description	Justification	Applicable to the [BCC]
ISO Category #6: Operations Management			
[SR13]	Protection against Malicious Software Protect the integrity of software and information from damage by malicious software.	Eliminate (or at least reduce) the following risks: <ul style="list-style-type: none"> [RSK9] Introduction of Damaging or Disruptive Software 	All Business Channels
[SR14]	Back-up and Media Handling Prevent damage to assets and interruptions to business activities.	Eliminate (or at least reduce) the following risks: <ul style="list-style-type: none"> [RSK9] Introduction of Damaging or Disruptive Software [RSK10] Theft and/or Wilful Damage of Data and Facilities [RSK11] Errors in using the EMCS application [RSK17] Failure in Outsourced Operations [RSK18] Hardware Maintenance Error [RSK19] Software Maintenance Error [RSK20] Technical failure of host [RSK21] Technical failure of storage device 	[BCC2] [BCC6] [BCC7] [BCC10] [BCC12] [BCC14] [BCC19] [BCC20]
ISO Category #7: Access Control			
[SR15]	Access Control Policy Define general guidance for access to information. Recommended measures.	Eliminate (or at least reduce) the following risks: <ul style="list-style-type: none"> [RSK1] Illegitimate use of the EMCS system by MSA officials [RSK2] Illegitimate use of the EMCS system by Economic Operators [RSK3] Illegitimate use of the EMCS system by Contracted Service Providers [RSK4] Illegitimate access to the EMCS system by Outsiders [RSK5] Repudiation [RSK11] Errors in using the EMCS application 	All Business Channels

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

SEP Id.	Requirements Description	Justification	Applicable to the [BCC]
[SR16]	<p>User Access Management</p> <p>Ensure that access rights to information systems are appropriately authorised, allocated and maintained.</p>	<p>Eliminate (or at least reduce) the following risks:</p> <ul style="list-style-type: none"> • [RSK1] Illegitimate use of the EMCS system by MSA officials • [RSK2] Illegitimate use of the EMCS system by Economic Operators • [RSK3] Illegitimate use of the EMCS system by Contracted Service Providers • [RSK4] Illegitimate access to the EMCS system by Outsiders • [RSK5] Repudiation • [RSK11] Errors in using the EMCS application 	<p>[BCC1] [BCC5] [BCC8] [BCC9] [BCC11] [BCC17] [BCC23]</p>
[SR17]	<p>Network Access Control</p> <p>Ensure the protection of networked services.</p>	<p>Eliminate (or at least reduce) the following risks:</p> <ul style="list-style-type: none"> • [RSK1] Illegitimate use of the EMCS system by MSA officials • [RSK2] Illegitimate use of the EMCS system by Economic Operators • [RSK3] Illegitimate use of the EMCS system by Contracted Service Providers • [RSK4] Illegitimate access to the EMCS system by Outsiders • [RSK7] Eavesdropping • [RSK9] Introduction of Damaging or Disruptive Software 	<p>All Business Channels</p>
[SR18]	<p>Application Access Control</p> <p>Prevent unauthorised access to information handled by the EMCS application.</p>	<p>Eliminate (or at least reduce) the following risks:</p> <ul style="list-style-type: none"> • [RSK1] Illegitimate use of the EMCS system by MSA officials • [RSK2] Illegitimate use of the EMCS system by Economic Operators • [RSK3] Illegitimate use of the EMCS system by Contracted Service Providers • [RSK4] Illegitimate access to the EMCS system by Outsiders 	<p>[BCC1] [BCC2] [BCC5] [BCC6] [BCC7] [BCC9] [BCC10] [BCC11] [BCC12] [BCC14] [BCC17] [BCC19] [BCC20] [BCC23]</p>

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS BACKGROUND INFORMATION	

SEP Id.	Requirements Description	Justification	Applicable to the [BCC]
		<ul style="list-style-type: none"> • [RSK5] Repudiation • [RSK11] Errors in using the EMCS application 	
ISO Category #8: System Development and Maintenance			
[SR20]	Application Security Prevent loss, modifications or misuse of user data in the system.	Eliminate (or at least reduce) the following risks: <ul style="list-style-type: none"> • [RSK1] Illegitimate use of the EMCS system by MSA officials • [RSK2] Illegitimate use of the EMCS system by Economic Operators • [RSK3] Illegitimate use of the EMCS system by Contracted Service Providers • [RSK4] Illegitimate access to the EMCS system by Outsiders • [RSK8] Unauthorised Software Changes • [RSK9] Introduction of Damaging or Disruptive Software • [RSK14] Software Programming Errors (business critical functions) • [RSK15] Software Programming Errors (other functions) • [RSK19] Software Maintenance Error 	[BCC2] [BCC6] [BCC7] [BCC10] [BCC12] [BCC14] [BCC19] [BCC20]
[SR21]	Privacy and Cryptographic Controls Protect the privacy of users and guaranty the confidentiality, authenticity or integrity of information (see also Appendix D for more details).	Eliminate (or at least reduce) the following risks: <ul style="list-style-type: none"> • [RSK5] Repudiation • [RSK7] Eavesdropping • [RSK16] Accidental misrouting 	All Business Channels
[SR22]	Software Maintenance Maintain the security of application system software.	Eliminate (or at least reduce) the following risks: <ul style="list-style-type: none"> • [RSK14] Software Programming Errors (business critical functions) • [RSK15] Software Programming Errors (other functions) 	[BCC2] [BCC6] [BCC7] [BCC10] [BCC12] [BCC14] [BCC19] [BCC20]

Table 6: Security Requirements

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4. EMCS Common Domain Security Measures

4.1. Introduction

This Chapter provides the specifications of security measures that *must* be implemented by the EMCS Common Domain Architecture (Central Services excluded) so as to meet the applicable requirements expressed in §3.7.

It therefore focuses on the security of the Business Communications Channels (see §3.5), which make use of the CCN/CSI, CCN Intranet, and CCN Mail II infrastructure channels (see §3.6).

Common Domain Central Services security is covered at the Chapter 5.

The structure adopted in this Chapter follows the ISF Standard [R35] and considers four main topics⁵:

- Security Management (see §4.2);
- EMCS Common Domain Infrastructure (see §4.3);
- CCN Network Security (see §4.4);
- Systems Development (see §4.5).

Note: Refer to *TESS Section II* [R9] for the technical specifications of the EMCS Common Domain Architecture.

4.2. Security Management

ISF building block (see §2.3.2): *Security Management*

4.2.1. Management Commitment

Measure principle..... Top management’s direction on information security should be established, and commitment demonstrated.

Status Implemented.

Description See below.

The regulations 77/799/EEC [R28], 1152/2003/EC [R30], 1798/2003/EC [R31], 2073/2004/EC [R32] provide management direction on how excise information exchanges between MSAs, and between MSAs and the Commission shall be established, which implicitly includes information security aspects.

Moreover [R31] indicates that: “*the Commission and the Member States are to ensure that the existing or new communication and information exchange systems, which are necessary to provide for the exchanges of information, are operational. The Commission will be responsible for whatever development of the common communication network/common system*

⁵ The ISF building block (see §2.3.2) related to “*Critical Business Applications*” is developed in §5.4.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

interface (CCN/CSI) is necessary to permit the exchange of this information between Member States.”

4.2.2. Security Policy

Measure principle.....	A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the organisation information and systems.
Status	Implemented.
Description	See below.

The management of the Common Domain security (Central Services excluded) is under the responsibility of the CCN/CSI Central Project Team (DG TAXUD) and governed by the CCN/CSI General Security Policy [\[R12\]](#), which covers the protection of CCN/CSI assets including:

- [CCN1] CCN/CSI Transport and Communication Services
 - CCN/CSI services
 - CCN Intranet services
 - CCN Mail 2 services

- [CCN2] CCN/CSI Operations and Support Services
 - Hardware and System maintenance
 - Corrective and evolutive software maintenance
 - System Monitoring
 - Production of statistics
 - User Management and application support

- [CCN3] CCN/CSI Communication Equipment
 - Common Domain Relay gateways (CCN Gateways, LCMS)
 - Network distribution components (router, IDB, switch)
 - Routing/Security device (encryption box)

- [CCN4] CCN Backbone
 - Local loops (e.g. leased lines to local POP, ISDN dial-up lines, etc.)
 - Fully meshed inter-sites communication links

- [CCN5] Application Data
 - Data exchanged by applications using CCN/CSI transport and communication services (typically NEA ↔ NEA interactions)

- [CCN6] CCN Directory
 - CCN Users repository
 - CCN Configuration data

- [CCN7] CCN/CSI Software
 - CCN Software running on the CCN Gateways

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

- CSI software running on CCN Gateways and Application Platforms
- Other specific software

[CCN8]

Reputation

- EC Internal
- To the Member State Administrations using CCN/CSI transport and communication services
- To the public domain

4.2.3. Security Coordination

Measure principle..... Arrangements should be made to co-ordinate information security activity in business units/departments.

Status Implemented.

Description See below.

The EMCS security in the Common Domain (Central Services excluded) is coordinated by the **CCN/TC** (Figure 9), which is in charge of the daily operation of the CCN/CSI network infrastructure and related services. Key security roles are:

- CCN/TC Directory Administrator (CDIA), responsible for the central management of the CCN Directory;
- Central Application Designer (CAD), responsible for the design of a given DG TAXUD application running over the CCN/CSI system.

The CCN/TC has a direct relationship with:

- The **EMCS/CO**, entity to be set-up (see §5.3.3), which is in charge of the daily operation of EMCS Central Services and provides support to national EMCS support entities established in the MSAs.
- The National CCN Support entities established in the MSAs.

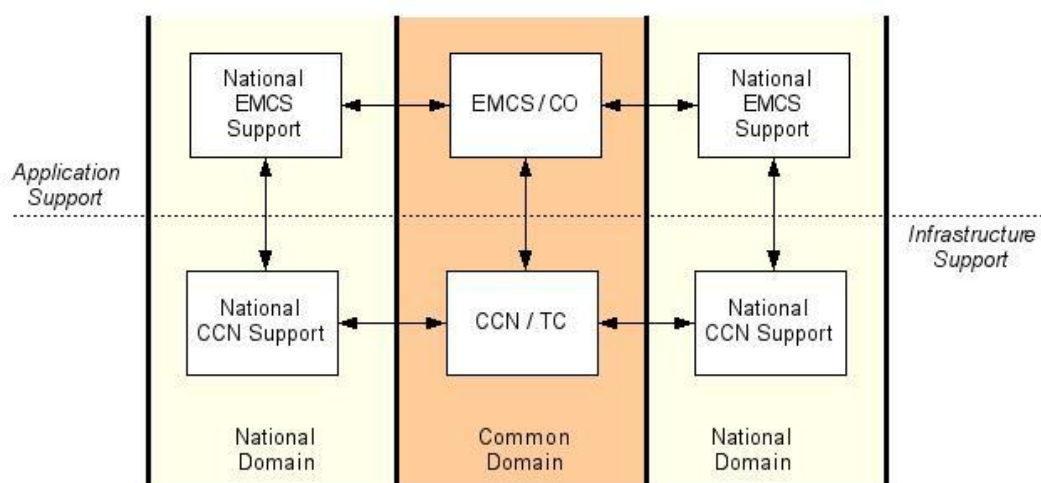


Figure 9: Responsibility Model

Note: Refer to [\[R18\]](#) for the detailed description of the CCN/TC role and responsibilities in the daily administration of the CCN Network and related services.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4.2.4. Business Continuity

Measure principle.....	Documented standards/procedures should be established for developing business continuity plans and for maintaining business continuity arrangements throughout the organisation.
Status	To be implemented.
Description	See below.

The establishment of a CCN Business Continuity Plan (BCP) for CCN/CSI services is currently under consideration by the CCN/CSI Central Project.

Either the CCN BCP will increase the minimum availability of the CCN/CSI services to reach the availability requirements stated in the TESS (see *TESS Section I [R9]*), or it will be necessary to increase the EMCS resilience by implementing:

- Equipment redundancy at CCN level (see *TESS Section II, §7.4*);
- Data flow regulation capabilities (see *TESS Section II, §6.2*).

4.2.5. Security Audit/Review and Monitoring

Measure principle.....	The information security status of critical IT environments should be subject to thorough, independent and regular security audits/review. The information security condition should be monitored periodically and reported to top management.
Status	Partially implemented.
Description	See below.

A regular reporting of information security condition is made by the CCN/TC to the CCN/CSI Central Project Team. However the CCN/CSI infrastructure security is not regularly audited (particularly IT systems installed at MSA premises), which makes difficult to assess the “real” security condition of the Common Domain infrastructure on which the EMCS is intended to rely.

4.2.6. Public Key Infrastructure (PKI)

Measure principle.....	Any Public Key Infrastructure (PKI) used by the application shall be protected by “hardening” the underlying operating system(s) and restricting access to Certification Authorities (CA)
Status	Under investigation.
Description	See below.

Refer to [Appendix D](#) that provides a proposal for the EMCS Common Domain Public Key Infrastructure (CDPKI) implementation.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4.3. EMCS Common Domain Infrastructure

ISF building block (see §2.3.2): *Computer Installations*

4.3.1. Installation Management

4.3.1.1. Roles and Responsibilities

Measure principle.....	An owner should be identified for the computer installation, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Status	Implemented.
Description	See below.

The European Commission (DG TAXUD) is the owner of the Common Domain equipment installed at every NDCP (with the exception of the CPR, which is leased to the network carrier).

MSA obligations with regard to Common Domain equipment installed at the NDCP are described in [\[R18\]](#).

4.3.1.2. Asset Management

Measure principle.....	Essential information about hardware and software (e.g. version numbers, physical locations, etc.) should be recorded in inventories, and software licensing requirements met.
Status	Implemented.
Description	See below.

The CCN/TC is responsible for the establishment and maintenance of the inventory of all CCN/CSI assets (see §4.2.2) under the control of DG TAXUD.

4.3.2. Environment

4.3.2.1. Physical Security

Measure principle.....	Physical security perimeter shall be implemented to protect critical computer installations. Physical access to the security perimeter shall be restricted to authorised individuals.
Status	Implemented.
Description	See below.

[\[R19\]](#) provides the description of the security measures applied by the CCN/TC to ensure the physical security of the Common Domain equipment hosted by the CCN/TC (i.e. CCN Gateways, LCMS, central CCN Directory server, CCN/TC Portal, central monitoring platform, central development site, central backup site, CCN/TC members workstations).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

Those measures conform to ISF best practices [\[R35\]](#) and refer to the implementation of physical security perimeter, physical entry controls, and isolation of delivery and loading areas from computer area.

Refer also to Appendix B §[8.3.2.1](#), which covers aspects related to the Common Domain equipment that is hosted at the MSA premises.

4.3.2.2. Equipment Sitting and Protection

Measure principle.....	Computer equipment and facilities should be protected against fire, flood, environmental, and other natural hazards.
Status	Implemented.
Description	See below.

[\[R19\]](#) provides the description of the security measures applied by the CCN/TC for equipment protection. Those measures conform to ISF best practices [\[R35\]](#) and provide a satisfactory level of protection of the Common Domain equipment hosted by the CCN/TC.

4.3.2.3. Power Supplies

Measure principle.....	Critical computer equipment and facilities should be protected against power outages.
Status	Implemented.
Description	See below.

[\[R19\]](#) provides the description of the security measures applied by the CCN/TC to prevent services provided by the computer installation from being disrupted by loss of power.

Those measures conform to ISF best practices [\[R35\]](#) and provide a satisfactory level of protection of the Common Domain equipment hosted by the CCN/TC.

4.3.2.4. Equipment Maintenance

Measure principle.....	Server equipment shall be correctly maintained to enable its continued availability and integrity.
Status	Implemented.
Description	See below.

The European Commission (DG TAXUD) has established contractual agreements (covering hardware maintenance aspects) with the providers of Common Domain equipment installed at every NDCP (e.g. CCN Gateways, LCMS, NDCP Firewall).

The co-ordination of the hardware maintenance activity is performed by the CCN/TC, which acts as unique contact point for all hardware providers.

As part of the business continuity management activity, the CCN/TC has defined a set of procedures [\[R18\]](#) destined to minimise the impact on the system availability of both preventive and corrective maintenance activities performed on Common Domain equipment.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4.3.3. System Operation

4.3.3.1. Backup

Measure principle.....	Back-ups of essential information and software used by the computer installation should be taken on a regular basis, according to a defined cycle.
Status	Implemented.
Description	See below.

The Local System Administrator in the MSA is responsible for performing backups of the CCN Gateways and LCMS equipment. Therefore, backup procedures/systems already in place in the MSA can be applied to the backup of the CCN Gateways and LCMS.

[R18] provides the description of the backup policy, which is currently in use at the CCN/TC, and that is proposed to any MSA that has not yet defined its own backup procedures. It also provides the description of the backup activation procedure, the tape format characteristics, and the restore procedure.

4.3.3.2. Incident and Change Management

Measure principle.....	All incidents of any type should be recorded, reviewed and resolved using an incident management process. Changes to any part of the computer installation should be tested, reviewed and applied using a change management process.
Status	Implemented.
Description	See below.

The CCN/TC has implemented an incident management process [R16] supported by specialised software tools aiming at identifying and resolving incidents effectively, minimising their impact on the system availability, and reducing the risk of similar incidents occurring.

The CCN/TC ensures that changes on Common Domain software owned by the DG TAXUD are applied correctly and do not compromise the security of the installation.

4.3.3.3. Media Handling

Measure principle.....	Information held on data storage media (including magnetic tapes, disks, printed results, and stationery) should be protected against corruption, loss or disclosure and additional security controls applied to media containing sensitive information.
Status	Implemented.
Description	See below.

The CCN/TC ensures that data storage media (including magnetic tapes, hard disks, and printed documentation) is handled in accordance with documented standards/procedures [R19]. Moreover, the CCN/TC ensures that sensitive media (e.g. full system backup tapes) are stored in a physically secure location (i.e. locked, fireproof safe) outside CCN/TC premises.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4.3.3.4. Protection against Malicious Software

Measure principle.....	Virus protection arrangements should be established and maintained organisation-wide.
Status	To be implemented.
Description	See below.

According to the risk valuation performed in the SEP [R3], there is a high probability for malicious software to be introduced in the EMCS infrastructure, in particular due to the usage of e-mail ([BCC4] [BCC8] [BCC13] [BCC15] [BCC21]), which is recognised as the most important vector of virus propagation.

It is therefore important to mention that the CCN Network infrastructure does not provide today any protection against malicious software, considering (until a very recent past) that it is the MSA responsibility to ensure that the data prepared by national systems are “clean” before being sent over the CCN Backbone. The CCN/CSI Central Project has however recently decided to deploy anti-virus protection at every NDCP level. The CCN Network full coverage should be completed before the end of 2006.

In any case, considering the high impact on the EMCS business and reputation if malicious code (virus) would be introduced in the CEA backend systems, security best practices recommend that at least a second protection barrier should be implemented. This latter point is further developed in §5.5.3.4.

4.3.3.5. Patch Management

Measure principle.....	There should be a strategy for patch management that should be supported by a management framework and a documented patch management process.
Status	Implemented.
Description	See below.

The CCN/TC has established a patch management process [R16] [R18] related to software installed at NDCPs so as to address potential vulnerabilities quickly and effectively and to reduce the likelihood of a serious incident occurring and important impact on the CCN Network availability arising.

4.3.4. Access Control

4.3.4.1. Access control Arrangements

Measure principle.....	Access control arrangements should be established to restrict access by all types of user/applications to approved system capabilities of the computer installation.
Status	Implemented.
Description	See below.

The access control policy is governed by the CCN/CSI General Security Policy [R12]. The background principle indicated by the policy is that user/application access control is performed at the *originator* Common Domain Relay level and that no further check is performed at the destination Common Domain Relay level.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

The choice to implement additional access controls at destination application level (e.g. at SEED level) therefore depends on the application owner policy. As a general rule, any message routed through the CCN/CSI channel or the CCN Intranet channel should be considered as coming from a trusted (i.e. authenticated and authorised) source.

Access controls are applied to distinguish legitimate MSA users/applications from those that are not. They rely on *registration* (see §4.3.4.2), *authorisation* (see §4.3.4.3), and *authentication* (see §4.3.4.4) security services, which are described hereafter.

4.3.4.2. Registration

Measure principle.....	All users shall be registered before they are granted access privileges.
Status	Implemented.
Description	See below.

The registration of users authorised to use CCN Network services and applications, also known as *CCN Users*, is a national activity, which is under the sole responsibility of every MSA. This follows the basic principle that the MSA is supposed to be the most appropriate authority (better than any other entity, e.g. central entity) to know if a user’s request to access CCN Network services and applications is legitimate or not.

This means that every MSA shall appoint a local CCN System Administrator who takes in charge:

- The registration of (human) users following the MSA internal policy (see §4.3.4.2 and the guidance provided in Appendix B, §8.2.4);
- The administration of access privileges (see §4.3.4.3).

Once duly authorised by the CCN/TC, the local CCN System Administrator has access to a web-based user management tool embedded in the CCN Gateway software package, called ADM2G, which allows performing the following tasks:

- The creation, modification, removal of user accounts. Those accounts are either used by applications or MSA Users authorised to access Common Domain Relay services (CCN/CSI, CCN Intranet, CCN Mail 2);
- Password reset;
- Allocation of CCN Profiles defining user access rights to applications (e.g. SEED) that are made available through the CCN network (see §4.3.4.3).

CCN User account information is stored in a local X.500 directory running on the local CCN Gateway and is not replicated in any way at central location so that the CCN Users’ information remains purely local to the MSA to which the CCN User is attached ([Figure 10](#)).

Note: The CCN User account information that is stored in the local CCN Directory allows accessing resources through the CCN/CSI and the CCN Intranet channels *only*. The CCN Mail 2 system has its own user (LDAP) directory and considers the user’s e-mail address as its unique identifier.

Therefore an MSA User who is intended to access resources through the three channels has to get registered twice: as CCN User in the local CCN Directory and as CCN Mail 2 user in the

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

LCMS LDAP directory (which obviously is not ideal from the security viewpoint). This confirms the choice that only CCN/CSI and CCN Intranet channels should be used by EMCS as far as IE exchanges are concerned (see also §3.6 for more information).

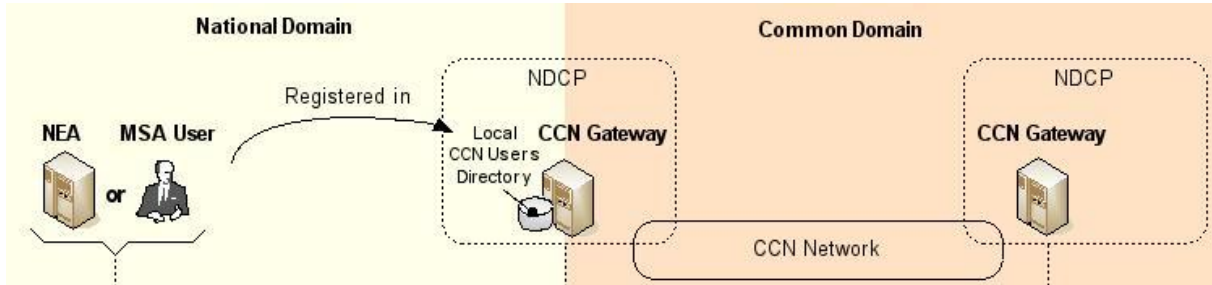


Figure 10: Access Control – Registration

4.3.4.3. Authorisation

Measure principle.....	All users/applications of the computer installation shall be assigned specific privileges to allow them to access particular information or systems.
Status	Implemented.
Description	See below.

All applications and users must be **authorised** to access resources made available through the CCN Network. According to the CCN/CSI General Security Policy [R12], this authorisation must be checked each time they connect to the Common Domain Relay. Therefore only authorised applications and users can exchange messages through the CCN network.

The access privileges take the form of Access Control Lists (ACL), which contain a set of “**profiles**” (PRF). These profiles are defined by Central Project teams (according to business needs) and created centrally by the CCN/TC under the control of the Central Security Officer (Security Officer of the Common Domain).

Local CCN System Administrators are then granted the right to allocate those (centrally created) profiles to national applications and users (using the ADM2G) following to the security policy defined for each concerned application.

4.3.4.4. Authentication

Measure principle.....	All users shall be authenticated by using UserIDs and passwords or by strong authentication (e.g. smartcards) before they can gain access to target systems.
Status	Implemented.
Description	See below.

The authentication scheme that is used to access an application resource (e.g. SEED), which is made available through the CCN Network, depends on the infrastructure channel (i.e. CCN/CSI, CCN Intranet, CCN Mail 2 – see §3.6) that is used to access that resource.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4.3.4.4.1. CCN/CSI Authentication

CSI-based applications use the confidentiality and integrity checking services offered through the GSS API (which is included in the CSI stack) to authenticate to the Remote API Proxy (RAP) running on the local CCN Gateway. The authentication phase involves a unique user ID and password that is securely transmitted through a CSI message-level encrypted channel (between the NEA and the local CCN Gateway) and verified against the local CCN Directory (running on the local CCN Gateway).

This ensures that only authorised CSI-based applications can access the EMCS resources made available through the CCN Network.

4.3.4.4.2. CCN Intranet Authentication

HTTP clients authenticate to the CCN Intranet services using a Username/Password based mechanism that offers both human and programmatic interfaces⁶ [R17].

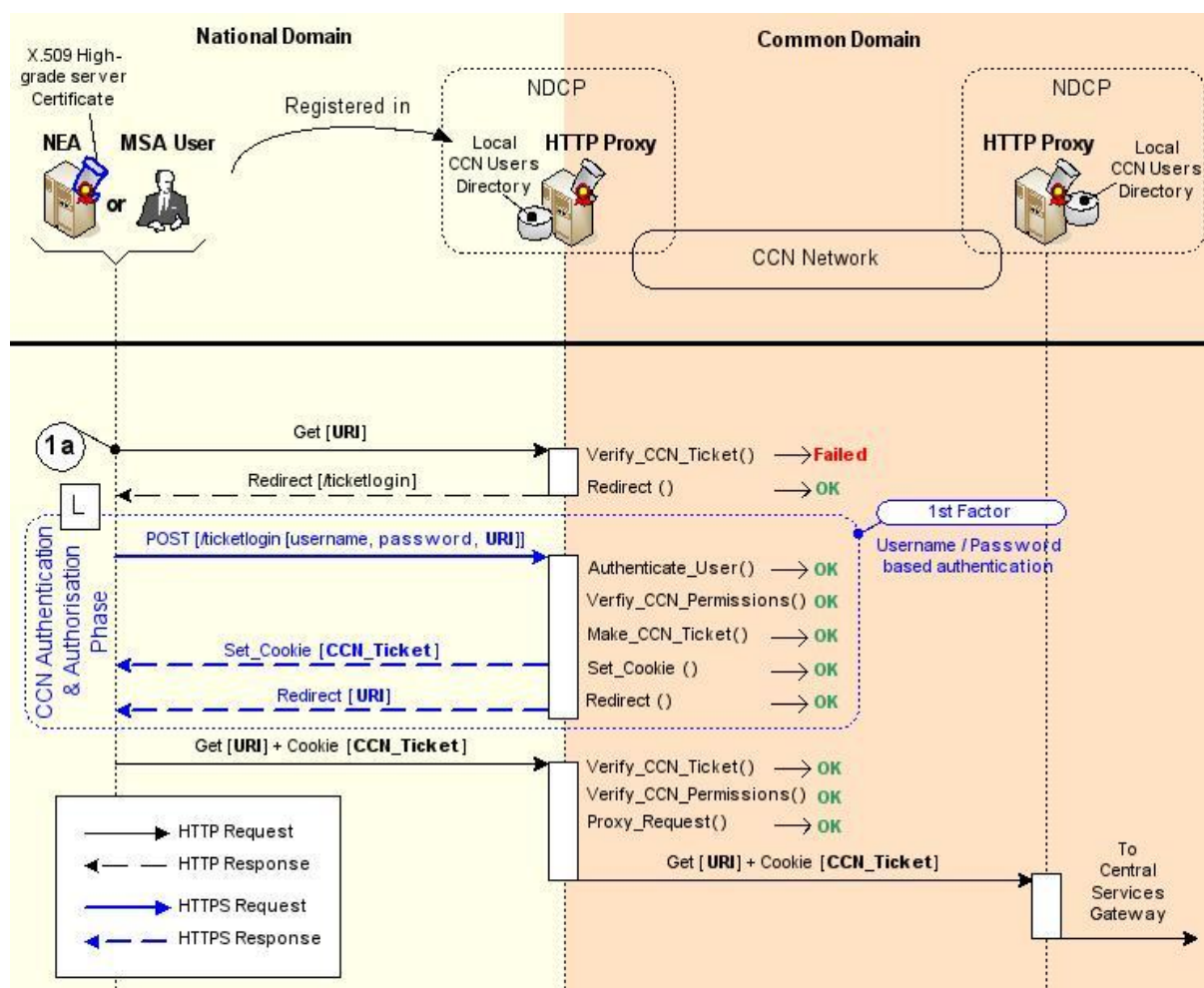


Figure 11: CCN Intranet Authentication

⁶ CCN Intranet Authentication Services – Programmer’s Guide [R17]: The purpose of the document is to describe the authentication system implemented in the framework of the action “Improvement of the User Management Services”. The document has been written with a development perspective; it contains the basic knowledge needed to develop a web-application using the server authentication mechanisms and calling the front-office user management intranet services to extract the information that was formerly given in the CCN_Ticket cookie.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

The authentication scheme that is applied is illustrated on [Figure 11](#). It involves the following main functions at HTTP Proxy level:

1. Verify if incoming HTTP request to *URI* is authenticated by checking the content of the CCN session ticket (CCN_Ticket). If CCN_Ticket is not present or incorrectly built, return HTTP response 301 (moved) to direct towards login phase;
2. Login phase: authenticate user/application and verify permissions. If verification fails, return HTTPS response 403 (forbidden).
3. If everything is OK, then make the CCN_Ticket session ticket, request the client to set a cookie including CCN_Ticket information, and return HTTPS response 301 (moved) to redirect the client toward the *URI* initially requested.

The HTTP client (i.e. NEA or MSA User) then issues the same HTTP request to *URI* but this time with a valid CCN_Ticket. The HTTP Proxy verifies the client request and, if everything is OK, forwards the HTTP request to the remote HTTP Proxy through the CCN Network.

4.3.4.4.3. CCN Mail 2 Authentication

Users / applications provide a user ID and password before gaining access to the CCN Mail 2 services (i.e. both for accessing functional mailboxes defined on the LCMS or for sending e-mail through the CCN Network). However, this cannot be used to guarantee the identity of the user / application.

It is also to be noted that the exchanges occurring during the authentication phase are not encrypted.

4.4. CCN Network Security

ISF building block (see §2.3.2):*Networks*

The *Common Communication Network (CCN)* is a closed, secured network that is provided by the Common Domain to facilitate intra-community exchange of information ([Figure 12](#)).

EMCS is designed to use the CCN Network infrastructure and dependent services, which are of three types:

- Message-based synchronous/asynchronous communication through the CCN/CSI Channel (see §3.6.2);
- HTTP/HTTPS (synchronous) access to Web Services (e.g. those offered by Central Services applications as described in *TESS Section III [R9]*) through the CCN Intranet Channel (see §3.6.3);
- Standard SMTP-based e-mail exchanges (e.g. exchange between national officials) through the CCN Mail 2 Channel (see §3.6.4).

National Domain Connection Points

Access to the CCN Network is implemented through *National Domain Connection Points (NDCP)* located at the MSA premises. Each NDCP is designed to provide gateways and

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

security services and is connected to the CCN Backbone (full-mesh IP VPN) through a local loop.

The local loop is made of a leased line connecting the NDCP CPR (Customer Premises Router) to the CCN Backbone local Point of Presence (PoP). Local loop redundancy is ensured by the means of a backup line (e.g. ISDN).

Moreover, MSA Organisational Units (located in the National Domain) connect to the NDCP through a national firewall (F/W) that may provide additional measures to protect the National Domains from unwanted accesses coming from the Common Domain.

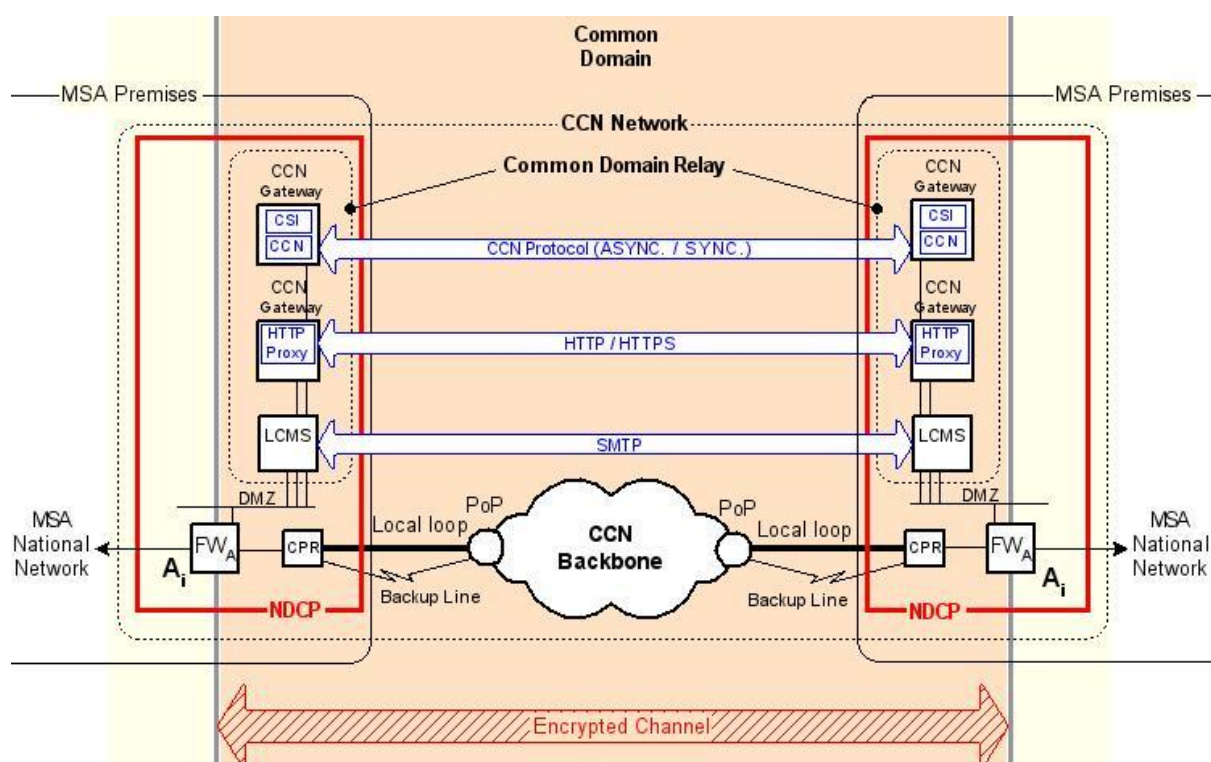


Figure 12: CCN Network

Common Domain Relay

The Common Domain Relay is the logical entity located on the DMZ created inside the NDCP and that is composed of the following physical devices:

- **CCN Gateways**, which is a pair of specialised equipment deployed at every MSA site offering both CCN/CSI Services and CCN Intranet Services;
- **Local CCN Mail System (LCMS)**, which is the specialised equipment deployed at every MSA site offering CCN Mail 2 services.

Other equipment may be added on the DMZ as part of the Common Domain Relay entity, according to business needs.

Note: The Common Domain Relay as well as the related services (CCN/CSI, CCN Intranet, CCN Mail 2) are described in detail in the *TESS Section I, Chapter 3 [R9]*.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4.4.1. Network Management

4.4.1.1. Roles and Responsibilities

Measure principle.....	An “owner” should be identified for the network, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Status	Implemented.
Description	See below.

The overall responsibility for the CCN Network activity is assigned to the European Commission (DG TAXUD), which has established contractually a relationship subject to Service Level Agreement (SLA) with an external contractor (i.e. the network carrier) ensuring:

- The proper operation of the CCN backbone;
- The maintenance of the network (CPR) and security devices (Firewall) deployed at every NDCP;
- The help desk and network support services.

4.4.1.2. Network Resilience

Measure principle.....	The network should be powered by a robust, reliable hardware and software, supported by alternative or duplicate facilities.
Status	To be implemented (except § 4.4.1.2.1).
Description	See below.

4.4.1.2.1. Protection of CCN Exchanges

The CCN exchanges protection mechanisms can be summarised as follows:

- All messages transiting over the CCN backbone, except acknowledgement messages, are acknowledged. The messages IE908 (CCN Confirm on Delivery Acknowledgement) and IE909 (CCN Confirm on Arrival Acknowledgement) are used to validate the arrival or the delivery of the messages. Refer to *TESS Section II, Chapter 3.3 [R9]* for more details;
- CCN/CSI provides all MSAs with the guarantee that in the event of a failure of their NEA or when their NEA is deliberately taken off-line due to maintenance activities, all messages received by CCN/CSI are held until the NEA comes back on-line (the only limitation being the available disk space on the CCN Gateway which is about 3 GB);
- The confidentiality of message content is preserved during its transit over the CCN Backbone by means of IPSec (168-bit 3DES) encryption (see §[4.4.2.3](#));
- Corrupt or bogus messages are not delivered;
- Messages are labelled with at least their country of origin.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

However, it should be noted that the CCN protocol does not provide:

- A “real” non-repudiation service (i.e. cryptographically protected); CCN however provides a log of all exchanges occurring on the CCN backbone (this log does not include message content, only information about the interchange itself);
- Protection against message replay;
- Intrusion Detection System (IDS) at the NDCP level.

4.4.1.2.2. NDCP Equipment Redundancy

The CCN/CSI Central Project is able to provide every NDCP involved in the EMCS business with the necessary equipment redundancy at all levels (i.e. firewall, gateways, routers, local loop to the CCN backbone, etc.) so as to provide on the field a higher availability rate than the one committed in the CCN/CSI Service Level Agreement (see *TESS Section I, Chapter 3.3.3 [R9]*).

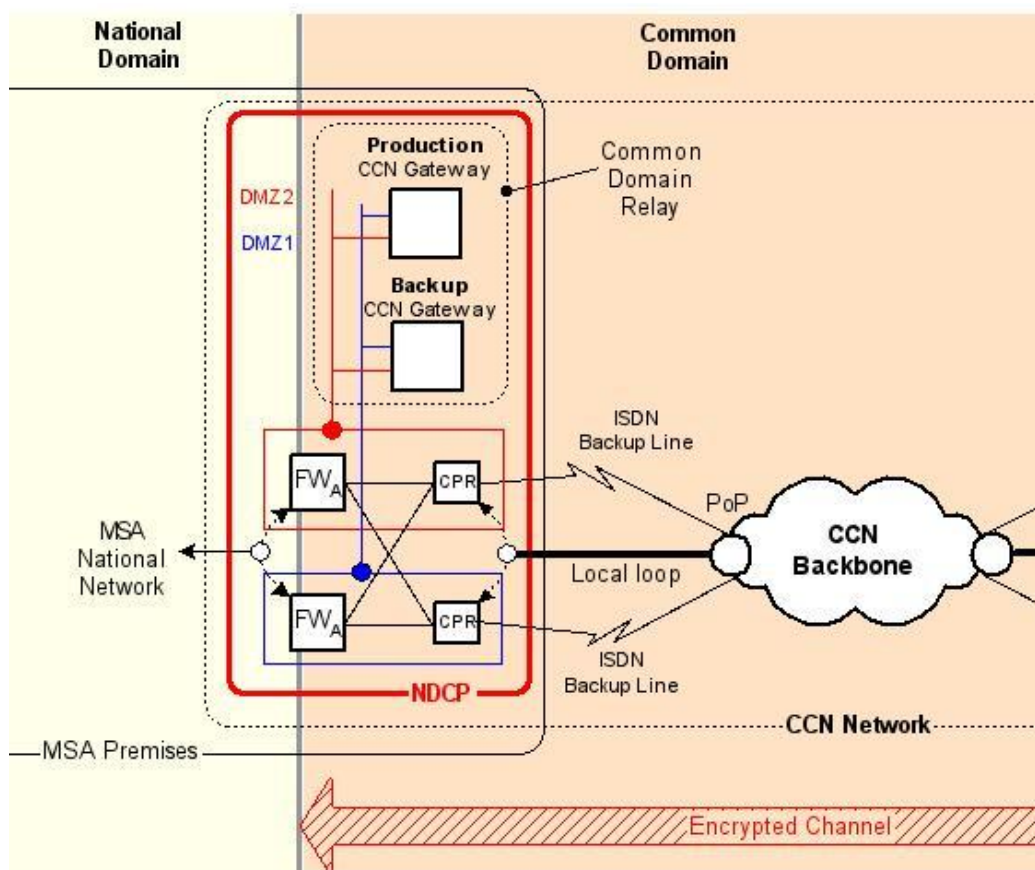


Figure 13: CCN Network Resilience – Equipment Redundancy

By default, the equipment redundancy illustrated on [Figure 13](#) (i.e. doubling of firewalls, CPR, and backup ISDN lines) shall be applied to every MSA site involved in the EMCS business. Moreover, there shall be a process for dealing with vulnerabilities in firewalls, which should include:

- Monitoring vulnerabilities in firewalls, such as running firewall checking software and reviewing third party warnings;
- Issuing instructions to the CCN/TC on the action to be taken if a firewall fails;
- Re-routing traffic automatically to an alternative firewall;

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

- Testing patches for firewalls and applying them in a timely manner;

Note: This equipment redundancy should not apply to the LCMS which usage is considered as less critical (than the CCN Gateways) with regards to the EMCS business.

4.4.1.2.3. Central Backup Site

If for some reasons the fallback to the local backup CCN Gateway is not possible (e.g. backup gateway out of order, no backup gateway available locally), data flows shall be redirected to a Central Backup Site. The Central Backup Site is maintained by the CCN/TC and consists of a pool of machines that can be dynamically configured to take over the CCN/CSI service in case of unavailability of a production CCN Gateway at a local site.

The redirection of data flows towards the Central Backup Site is achieved by modifying the routing tables of the local security device (Firewall) deployed at every local site. It is therefore completely transparent at the National Excise Application level. The only drawback of such fallback solution (i.e. compared to the use of a local CCN backup Gateway) is that the CSI link between the national Application Platform and the central Backup gateway is established over a low-speed link (i.e. the CCN Network), hence decreasing the performance level of the communication.

4.4.1.2.4. CCN Mail 2 Fallback

The CCN Mail 2 channel (see §3.6.4) can also provide a simple fallback solution in case of unavailability of other services. Indeed, if the access to CCN/CSI services is not possible whereas e-mail services remain available, CCN Mail 2 could be used to ensure the business continuity of the following channels:

- [\[BCC2\]](#)NEA to NEA
- [\[BCC6\]](#)NEA to SEED
- [\[BCC7\]](#)SEED to NEA
- [\[BCC10\]](#)EMCS CS/RD to NEA
- [\[BCC12\]](#)NEA to EMCS CS/RD
- [\[BCC19\]](#)NEA to CS/MIS
- [\[BCC20\]](#)CS/MIS to NEA

Note: Given the current situation of CCN Mail 2 development, it is clear that using it as a fallback channel will decrease the level of security.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4.4.2. Traffic Management

4.4.2.1. Network Routing Control (Enforced Path)

Measure principle.....	Networks shall have routing controls to ensure that computer connections and information flows do not breach the access control policy.
Status	Implemented.
Description	See below.

Any user or application using CCN/CSI services, CCN Intranet services, or CCN Mail 2 services must have only one access path to the CCN network. This access path must run through the **Common Domain Relay** (see [Figure 12](#)). There must be no possibility for a user or an application to gain access to the CCN network without going through the Common Domain Relay.

4.4.2.2. Firewalls

Measure principle.....	Network traffic should be routed through a firewall, prior to being allowed access to the network.
Status	Implemented.
Description	See below.

Based on the EMCS background information provided in §3, and according to the principle of “*network segregation*”, which is systematically applied to perform network access control [\[SR17\]](#), it is possible to represent the entry points where controls need to be enforced ([Figure 12](#)), also referred to as “**Controlled Access Points (CAP)**”. Each CAP characterises the location where a firewall shall be implemented.

[Table 7](#) provides the list of CAP related to the Common Domain (Central Services excluded).

CAP	Responsibility	Description
A _i (1)	Common Domain (CCN Network)	Protection against unwanted accesses coming from the National Domain.
		Protection against unwanted accesses coming from the Common Domain (SNET network).
(1)	i ∈ [1, 37] CCN/CSI interconnects national customs and taxation administrations at 35 sites in 29 countries (i.e. all the members of the EU + Romania, Bulgaria, Switzerland and Norway) + 1 site at EC Data Centre + 1 site at CCN/TC.	

Table 7: Controlled Access Points – CCN Network

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4.4.2.3. Network Encryption

Measure principle.....	Network encryption shall be applied to protect the confidentiality of sensitive or critical information during transit over networks.
Status	Implemented.
Description	See below.

The CCN network infrastructure provides the necessary security protection for unauthorised disclosure, loss or alteration of information by use of IPSec (168-bit 3DES) encryption for all types of traffic (i.e. CCN, HTTP, SMTP), which is adequate for EMCS applications.

The IPSec encryption is achieved by the security device (firewall), labelled “FW_A” on [Figure 12](#), which is deployed at every NDCP.

4.4.2.4. External Access

Measure principle.....	All external connections to the network should be individually identified, verified, recorded, and approved by the network owner.
Status	Implemented.
Description	See below.

According to CCN/CSI General Security Policy [\[R12\]](#), external accesses to the CCN Network are prohibited.

4.4.3. Network Operations

4.4.3.1. Network Monitoring

Measure principle.....	Key network activities should be monitored.
Status	Implemented.
Description	See below.

To ensure the operational efficiency of the whole CCN information system, the CCN/TC applies a proactive approach to the management of incidents. The objective is to detect as early as possible the minor incidents that could impede the CCN/CSI service, so that they do not turn into blocking problems.

To reach this goal the CCN/TC uses an open source Linux-based solution, called *Big Brother*, which implements system and network monitoring facilities.

In the current implementation, *Big Brother* is “embedded” in the CCN Gateway standard package and therefore provides CCN administrators with near real-time monitoring facilities (through a web-based interface) of local resources of the Common Domain Relay including:

- app..... Monitoring of predefined list of processes
- cda..... Monitoring of the Cache Directory Access
- clfs Monitoring of the Common Logging Facilities Subsystem
- cpu..... Monitoring of the CPU usage
- disk Monitoring of the disk space usage
- mem..... Monitoring of the memory

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

- mqm..... Monitoring of MQSeries processes
- ping..... Monitoring of the network connectivity
- proc Monitoring of active processes
- que..... Monitoring of the application queues
- sched..... Monitoring of the scheduler
- sts Monitoring of the statistics generation
- trigger Monitoring of the trigger monitor
- tuxedo..... Monitoring of the Tuxedo transactional monitor
- usr..... Monitoring of the validity of local users
- ldap..... Monitoring of the LDAP directory (Netscape Directory Service)

A consolidated view of all local *Big Brother* instances is also provided by a central monitoring platform located at the CCN/TC, which performs a polling of all CCN/CSI critical resources and provides the central support team with a global view of the whole CCN/CSI infrastructure.

Alarms issued by the local instances are sent to the central monitoring platform for further processing by the support team.

4.4.3.2. Event Logging

Measure principle.....	Logs of all key events within the computer installation should be maintained (preferably using automated tools), reviewed periodically and protected against unauthorised change.
Status	Implemented.
Description	See below.

The CCN/TC implements a logging system called “*Common Logging Facilities Subsystem (CLFS)*”, which ensures the individual accountability of messages crossing the CCN Network. It is to be noted that this logging system concerns the CCN/CSI and CCN Intranet channels *only*. Messages sent over the CCN Mail 2 channel are not logged (but this is not an issue for EMCS as IE messages are not to be sent over this channel).

4.4.3.3. Remote Maintenance

Measure principle.....	Remote maintenance of network should be restricted to authorised individuals, confined to individual sessions, and subject to review.
Status	Implemented.
Description	See below.

The procedures related to the remote maintenance of Common Domain equipment (in particular the remote access to CCN Gateways) installed at MSA premises are described in [\[R18\]](#).

Access to CCN gateways by the CCN/TC administrators is only authorised via the CCN network. Access by other means such as a modem is authorised only after explicit MSA authorisation, only for maintenance purposes, and only for the duration of the intervention. Moreover, these CCN/TC administrators can only perform the tasks that belong to their profile. For instance, they cannot access systems of the MSA network.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4.5. Systems Development

ISF building block (see §2.3.2): *Systems Development*

4.5.1. Roles and Responsibilities

Measure principle..... An individual/organisation with overall responsibility for the development activity, together with business, shall be appointed to manage system development activities, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Status Implemented.

Description See below.

As a general rule, national systems development activities are carried out by MSAs. The specific part of national systems that interface the Common Domain infrastructure follows common specifications (most of the times elaborated by central project teams of the European Commission) agreed by all MSAs.

4.5.2. System Design and Build

Measure principle..... System build activity (including coding and package customisation) shall be carried out in accordance with industry good practice, performed by individuals provided with adequate skills/tools and inspected to identify unauthorised modifications or changes which may compromise security measures.

Status Implemented.

Description See below.

4.5.2.1. CSI-based Application Development

Due to the “proprietary” nature of CSI-based application development, the CCN/CSI Central Project has produced a set of manuals and guidelines, which are made available to development teams. The definitions of data structures, data types and constants can be found in language specific documents:

- jCSI Reference Manual (Java) for the Java language [\[R21\]](#);
- HL Reference Manual (C language) and Common Definitions Reference Manual (C language) for the C language [\[R22\]](#);
- HL Reference Manual (COBOL language) and Common Definitions Reference Manual (COBOL language) for the COBOL language [\[R24\]](#);
- Error codes are available in CSI Error Reason Codes Reference Manual [\[R26\]](#).

The actual configuration procedures and parameters applicable to a CSI-based application are defined in [\[R27\]](#). These parameters have to be collected in a set of pre-defined forms to be filled by various MSAs and DG TAXUD representatives in order to configure the support by CCN/CSI of the communication paradigms (e.g. asynchronous) used by the CSI-based application.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS COMMON DOMAIN SECURITY MEASURES	

4.5.2.2. HTTP-based Application Development

The CCN/CSI Central Project does not provide manuals with regards to the development of applications using the CCN Intranet channel as development teams are intended to follow Web-based applications development best practices. The only document that is made available is the CCN Intranet Authentication Services Programmer’s Guide [\[R17\]](#), which describes the programmatic interface offered by the HTTP Proxy (running on the local CCN Gateway) to automate the authentication and authorisation services in a machine-to-machine communication context.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5. EMCS Central Services Security Measures

5.1. Introduction

This Chapter provides the specifications of security measures that *must* be implemented by the EMCS Central Services Architecture to meet the applicable requirements expressed in §3.7. It therefore focuses on the security of the Business Communications Channels involving interaction with CEA backend systems through the Central Services Security Components (see §5.2).

Note: Refer to *TESS Section II [R9]* for the technical specifications of the EMCS Common Domain Architecture.

The structure adopted in this Chapter follows the ISF Standard [R35] and considers five main topics:

- Security Management (see §5.3);
- CEA Security (see §5.4);
- EMCS Central Services Infrastructure (see §5.5);
- SNET Network Security (see §5.6);
- Systems Development (see §5.7).

Moreover (still in relation with CEA Security), the specifications of the CEA Access Control (when accessed through the CCN Intranet channel), which is an important aspect of the EMCS Central Services security, are provided in §5.8.

Note: The security measures described in this Chapter are of a compulsory nature. Providing that they do not contradict the EC Security Policy guidance [R14], all of them have therefore to be implemented at the EC Data Centre under the responsibility of the Central Information Security Officer (CISO).

5.2. Central Services Security Components

[Figure 14](#) provides an overview of the Central Services security architecture. The main components of this architecture (i.e. Central Services Gateway and Central Security Services) are described hereafter.

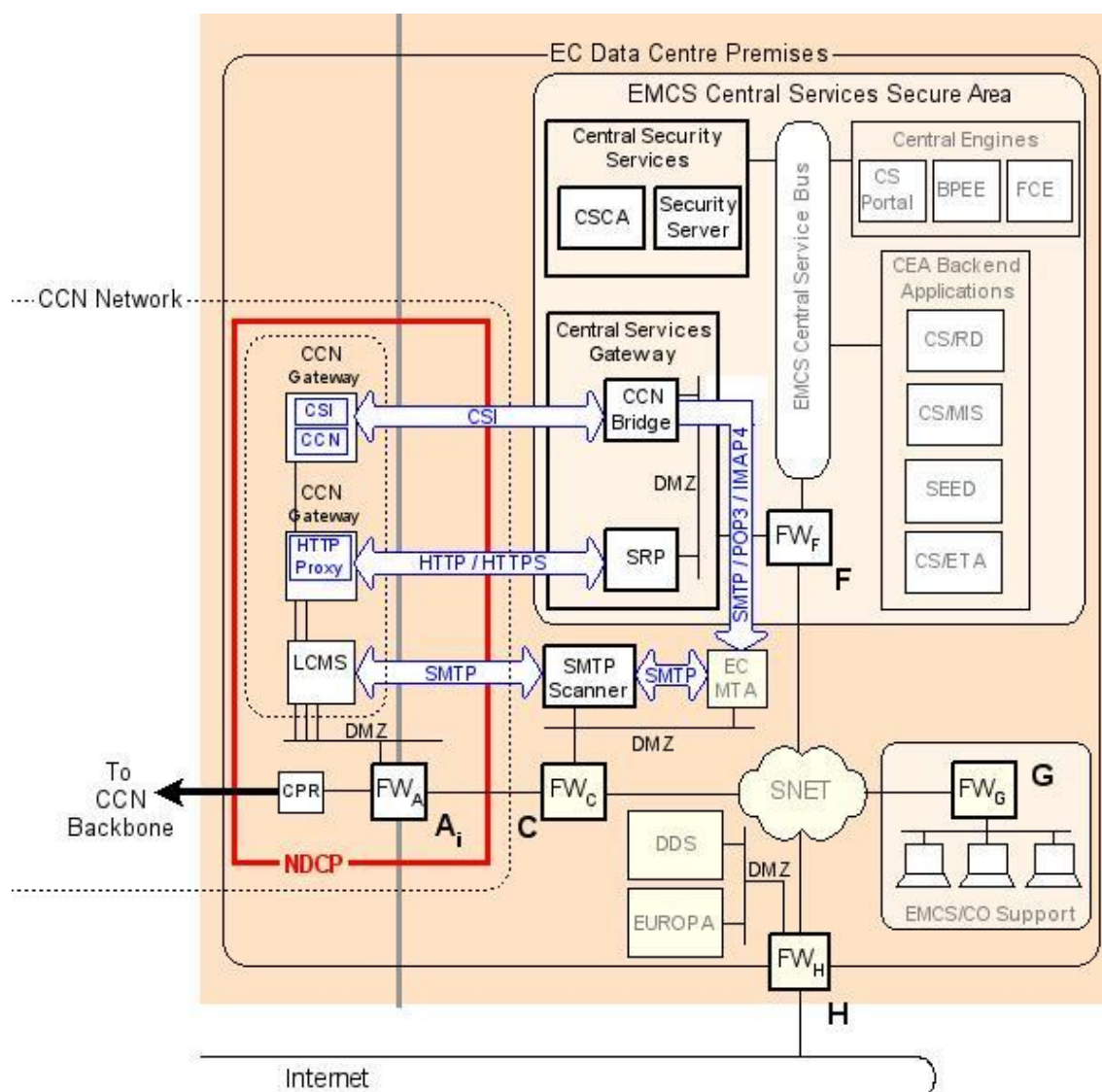


Figure 14: Central Services Security Components – Overview

5.2.1. Central Services Gateway

The *Central Services Gateway* is the single point of contact of the EMCS Central Services infrastructure (see *TESS Section III §3.3 [R9]*). Consequently, it plays a key role in the access control to CEA (see §5.4.2.2). It includes:

- The *CCN Bridge*, which manages the asynchronous exchanges with Common Domain Relay (i.e. CSI, SMTP and POP3). It addresses in particular the CSI-based applications access control (see §4.3.4);
- The *Secure Reverse Proxy*, which manages HTTP/S exchanges relayed by the Common Domain Relay. It addresses in particular the Web-based applications access control (see §5.8).

The Central Services Gateway takes place in a DMZ and discharges the rest of the infrastructure from an important part of the security aspects regarding the external accesses, establishing a so-called *Implicit Trusted Zone*. In this zone, the various services can proceed securely by only dealing with functional requirements, keeping to the Central Services Gateways the responsibility of the access control.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5.2.2. Central Security Services

The Central Services Gateway (see §5.2.1) controls exchanges with external communicating parties, but it is not built to implement all security aspects (particularly those related to CEA users management and key management). Therefore there is a need for complementary components that provides additional security services:

- **Security Server**, which provides mechanisms to secure data exchange between consumers and producers of services such as: authorisation, authentication, and data encryption (see §5.2.2.1);
- **EMCS CSCA**, which provides EMCS Common Domain X.509 certificates management services (see §5.2.2.2).

5.2.2.1. Security Server

The EMCS Central Services Architecture (see *TESS Section III [R9]*) is based on a key element called **EMCS Central Services Bus**. It provides value added services (offered by BEA AquaLogic™) that are used to ease the development and the deployment of EMCS central applications. Part of processing, including security is deported from applications to these services.

BEA AquaLogic Enterprise Security™ is an application security infrastructure solution that uses a service-oriented approach to enable applications to leverage shared security services offered by the so-called “*security server*”.

The security server provides:

- Authentication service;
- Rules-based authorisation;
- Identity assertion;
- Credential and role mapping;
- Auditing;
- Web-based administrative console;
- Support for heterogeneous infrastructure.

5.2.2.2. EMCS Central Services CA (CSCA)

The “*Central Services CA*” or “*CSCA*” (see [Figure 33](#)) provides certificates management services to Central Services applications and authorised users (e.g. EC officials). In particular, it issues X.509 high-grade server certificates to Central Services applications, which use the credentials contained in the respective certificates to establish point-to-point SSL v.3 secure communications with remote systems (e.g. NEAs).

The CSCA includes the following components:

- One or more back-end systems running Certificate Services and providing certificate enrolment, revocation and other certificate management services;
- Directory service that provides account management, policy distribution, and certificate publication services.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

Note: The CSCA is not intended to deliver certificates to NEA or MSA Users. But MSAs that are not able to obtain certificates from a national Certification Authority could temporarily receive certificates from the CSCA following the procedures defined in the CSCA Certificate Practice Statement (CPS).

5.2.2.2.1. CSCA Options

Four options can be considered with regard to the entity, which could play the role of trusted certification authority for the EMCS Central Services. Indeed the CSCA could be:

- Option 0: A Certification Authority attached to an EC accepted authority, such as EuroPKI⁷ [R38] (provided that the EMCS CSCA would accept to follow the EuroPKI Top Level certification policy);
- Option 1: A Certification Authority attached to a Common Domain accepted authority. As such authority does not exist today, this represents a value proposal addressed to the CCN/CSI Central Project for e.g. the deployment of a “*cross-project*” Certification Authority (NCTS, EMCS, AFIS, etc.) on the CCN/CSI network;
- Option 2: A Certification Authority attached to a third-party Certification Authority (e.g. GlobalSign CA), which is accredited by the EC Security Office, and with which the EC has established a contractual relationship;
- Option 3: an EMCS self-signed Certification Authority.

Note: Another option (avoiding the establishment of the CSCA) would consist in using the services of an existing national CA for the EMCS Central Services.

⁷ The EuroPKI Top Level Certification Authority is a no-profit organisation established to create and develop a pan-European public-key infrastructure (PKI). It has its roots in the PKI established by the ICE-TEL project and further developed by the ICE-CAR one. Both these projects were funded by the European Commission under the Telematics for Research programme. The Root CA of ICE-CAR project is hosted by Politecnico di Torino.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5.3. Security Management

ISF building block (see §2.3.2):*Security Management*

5.3.1. Management Commitment

Measure principle.....	Top management’s direction on information security should be established, and commitment demonstrated.
Status	Implemented.
Description	See below.

The decision n°1152/2003/EC of the European Parliament and of the Council of 16 June 2003 of computerising the movement and surveillance of excisable products [\[R30\]](#) provides the legal basis for the implementation of an Excise Movement Control System (EMCS).

Moreover, the Regulation (EC) No 2073/2004 of the European Parliament and of the Council of 16 November 2004 on administrative cooperation in the field of excise duties [\[R32\]](#) stipulates in the CHAPTER VII CONDITIONS GOVERNING THE EXCHANGE OF INFORMATION, Article 33 that the “[...] Commission shall communicate without delay to the competent authority of each Member State any information which it receives and which it is able to provide”, which justifies the Commission’s commitment for **EMCS Central Services** to be made available to Member State Administrations.

5.3.2. Security Policy

Measure principle.....	A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the organisation information and systems.
Status	Implemented.
Description	See below.

The general security of Central Services is governed by the EC Security Policy [\[R14\]](#). It covers all aspects with regard to security organisation, asset classification and control, personnel security, physical and environmental security, and access control. Specific aspects related to EMCS (and not already covered by [\[R14\]](#)) are governed by the SEP [\[R3\]](#).

5.3.3. Security Coordination

Measure principle.....	Arrangements should be made to co-ordinate information security activity in business units/departments.
Status	To be implemented.
Description	See below.

The EMCS Central Operations (EMCS/CO) services are the services proposed by the Excise Computerisation Project (ECP) to provide the MSAs with operational and technical support during EMCS implementation and operation. The EMCS/CO services include the **Central Service Desk**, the **Technical Centre** and the **Central services**.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

Its role also consists in managing the Central Services applications (i.e. CS/RD, SEED, CS/MIS, CS/ETA), including the coordination of information security activity in cooperation with the EC Data Centre (which is the entity in charge of Central Services hosting) and the Central Project Team.

Note: Refer to the Central Operation Specifications (COS) [\[R6\]](#) for more details about the services offered by the EMCS/CO.

5.3.4. Business Continuity

Measure principle.....	Documented standards/procedures should be established for developing business continuity plans and for maintaining business continuity arrangements throughout the organisation.
Status	To be implemented.
Description	See below.

A Business Continuity Plan (BCP) must be developed to counter interruptions to EMCS Central Services activities and to protect critical business procedures from the effects of major failure or natural disaster. The definition of a Disaster (or fallback) Recovery Plan (DRP) is one of the aspects covered by the BCP.

This document has to define a list of critical assets (hardware, software, networking, etc.) that would need to be re-established in order to recover normal business processing, should a disaster occur.

This document assists in reducing the disruption and the recovery time to the level defined by the EMCS Central Services availability objectives through a combination of preventive and recovery control information.

The “*EMCS Central Services Business Continuity Plan*” must specify:

- Conditions for its invocation.
- The critical timescale associated with the Central Services applications (i.e. CS/RD, SEED, CS/MIS and CS/ETA).
- A schedule of key tasks to be carried out.
- Procedures in sufficient detail so that they can be followed by individuals who do not normally carry them out.
- Information security measures applied during the recovery process.

It must also include:

- Responsibilities for carrying out tasks and activities, including deputies.
- Procedures to be followed in completing key tasks and activities, including emergency, fallback and resumption procedures.
- Procedures to be followed by business users (e.g. MSA users).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5.3.5. Security Audit/Review and Monitoring

Measure principle.....	The information security status of critical IT environments should be subject to thorough, independent and regular security audits/review. The information security condition should be monitored periodically and reported to top management.
Status	To be implemented.
Description	See below.

The COS [\[R6\]](#) defines the functions of the EMCS Central Operation (EMCS/CO), including its role in the EMCS monitoring. As EMCS Central Services are hosted by the EC Data Centre (LU), a procedure shall be established between both entities to ensure that every incident detected by the EC Data Centre support is reported to the EMCS/CO for further analysis.

Moreover, to provide the EMCS Central Project Team (and indirectly MSAs) with an independent assessment of the security conditions of the EMCS Central Services, security audits/reviews shall be performed periodically for critical environments, including CEA applications, computer installations, networks, and systems development activities.

5.4. CEA Security

ISF building block (see [§2.3.2](#)): *Critical Business Applications*

5.4.1. Application Management

5.4.1.1. Roles and Responsibilities

Measure principle.....	An owner should be identified for the application, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Status	Implemented.
Description	See below.

The European Commission (DG TAXUD) is the owner of the Central Services infrastructure and applications, provides a sound management structure for entities running or using them and gives responsible individuals a vested interest in their protection.

5.4.2. User Environment

5.4.2.1. Registration

Measure principle.....	All users shall be registered before they are granted access privileges.
Status	To be implemented.
Description	See below.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

Refer to the *COS, Chapter 6.2.9 “User Administration Procedures’* [\[R6\]](#) for the description of the method of accessing the EMCS/CO Central Service Desk for declaring a new user or a change in user access definition.

5.4.2.2. Access Control

Measure principle.....	Access to the application and associated information should be restricted to authorised users/applications and enforced accordingly.
Status	To be implemented.
Description	See below.

5.4.2.2.1. CEA Access Control (CCN/CSI Channel)

The access to the CEA through the CCN/CSI channel is subject to the controls mechanisms described in §[4.3.4](#). It requires that the CCN Bridge (see §[5.2.1](#)) be authenticated to and authorised by the local CCN Gateway to access the CCN/CSI resources (e.g. read and/or write to the CCN queues dedicated to EMCS Central Services applications).

The CCN Bridge also interacts with the Security Server to verify if the NEA that issues (request) messages through the CCN/CSI channel (but also through the CCN Intranet channel in fallback mode), has the required privileges to access CEA backend applications.

5.4.2.2.2. CEA Access Control (CCN Intranet Channel)

Due to their relative complexity, aspects related to the CEA security when accessed through the CCN Intranet channel are subject to an extensive development provided in §[5.8](#).

5.4.3. System Management

CEA applications typically run on one or more computers and make use of one or more networks. To make this possible, the EC Data Centre provides services covering:

- Service agreements;
- Resilience of the application;
- External connections security;
- Backup of essential information and software (using Storage Area Network (SAM) facilities).

Refer to [\[R15\]](#) for more details.

5.4.3.1. Event Logging and Accounting

Measure principle.....	Logs of all key events within the computer installation should be maintained (preferably using automated tools), reviewed periodically and protected against unauthorised change.
Status	To be implemented.
Description	See below.

The Event logging and accounting functions shall be taken in charge by the Central Services Gateway (i.e. by the CCN Bridge for information exchanged through the CCN/CSI and CCN mail 2 channels, and by the SRP for information exchanged through the CCN Intranet channel) due to its role as single entry point to the Central Services.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

The Central Services Gateway must keep a log of exchanged information, in order to relate an error to the information that has been exchanged, and to solve any disputes regarding exchanged information. This log must at least contain:

- Timestamp showing at which date and time the IE message has been sent or has been received;
- The parameters of the transport of the message (e.g. CSI header, CCN reports and queue name for CCN/CSI).

According to [\[R11\]](#) the retention period of log files is defined as follows:

- Firewall.....Three (3) years
- E-mailThree (3) years
- Other systems (e.g. CCN Gateway, Application Platforms):
 - Sensitive (or ‘Moderate’).....Six (6) months
 - CriticalFive (5) years
 - Strategic.....Ten (10) years

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5.5. EMCS Central Services Infrastructure

ISF building block (see §2.3.2): *Computer Installations*

The EMCS Central Services infrastructure management is under the responsibility of the EC Data Centre and governed by the EC Security Policy [R14] (POLSEC).

5.5.1. Installation Management

5.5.1.1. Roles and Responsibilities

Measure principle.....	An owner should be identified for the computer installation, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Status	Implemented.
Description	See below.

The European Commission (DG TAXUD) is the owner of the EMCS Central Services infrastructure, achieves accountability for the computer installation, and provides a sound management structure for the staff operating it.

5.5.2. Environment

5.5.2.1. Physical Security

Measure principle.....	Physical security perimeter shall be implemented to protect critical computer installations. Physical access to the security perimeter shall be restricted to authorised individuals.
Status	To be implemented.
Description	See below.

[R15] provides the description of the security measures applied by the EC Data Centre to restrict physical access to computer installation. Those measures conform to best practices and will provide a satisfactory level of protection of the Common Domain equipment (i.e. the NDCP equipment and the EMCS Central Services equipment) hosted by the EC Data Centre (Figure 14). In particular those measures refer to:

- Installation of the Common Domain equipment in a safe location (i.e. in a area with low risk of fire, flood, explosion, civil unrest, damage from neighbouring activities or natural disasters);
- Implementation of physical entry controls;
- Isolation of delivery and loading areas from IT equipment area.

The physical access to the EC Data Centre site, including all its security components must be strictly limited to individuals mandated by the EMCS Central Project and duly authorised by the EC Security Directorate.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5.5.2.2. Equipment Sitting and Protection

Measure principle.....	Computer equipment and facilities should be protected against fire, flood, environmental, and other natural hazards.
Status	To be implemented.
Description	See below.

[R15] provides the description of the security measures applied by the EC Data Centre for equipment protection. Those measures conform to best practices and will provide a satisfactory level of protection of the EMCS Central Services equipment hosted by the EC Data Centre.

5.5.2.3. Power Supplies

Measure principle.....	Critical computer equipment and facilities should be protected against power outages.
Status	To be implemented.
Description	See below.

[R15] provides the description of the security measures applied by the EC Data Centre to prevent services provided by the computer installation from being disrupted by loss of power. Those measures conform to best practices and provide a satisfactory level of protection of the EMCS Central Services equipment hosted by the EC Data Centre.

5.5.2.4. Equipment Maintenance

Measure principle.....	Server equipment shall be correctly maintained to enable its continued availability and integrity.
Status	To be implemented.
Description	See below.

The EC Directorate General for Informatics (DIGIT) shall establish contractual agreements (covering hardware maintenance aspects) with the providers of the Central Services equipment installed at the EC Data Centre.

The co-ordination of the hardware maintenance activity shall be performed by the EMCS/CO, which shall take the necessary actions to minimise the impact on the Central Services availability of both preventive and corrective maintenance activities performed on Central Services equipment.

5.5.3. System Operation

5.5.3.1. Backup

Measure principle.....	Back-ups of essential information and software used by the computer installation should be taken on a regular basis, according to a defined cycle.
Status	Implemented.
Description	See below.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

According to [R15], the EC Data Centre applies a sound backup policy ensuring that, in the event of emergency, essential information and software required by the installation can be restored within critical timescales.

5.5.3.2. Incident and Change Management

Measure principle.....	All incidents of any type should be recorded, reviewed and resolved using an incident management process. Changes to any part of the computer installation should be tested, reviewed and applied using a change management process.
Status	To be implemented
Description	See below.

According to [R6], the EMCS/CO shall implement an incident management process supported by specialised software tools aiming at identifying and resolving incidents effectively, minimising their impact on the system availability, and reducing the risk of similar incidents occurring. Interrelation with the EC Data Centre incident management process shall be established.

The EMCS/CO shall also ensure that changes on Central Services software (owned by the DG TAXUD) are applied correctly and do not compromise the security of the installation.

5.5.3.3. Media Handling

Measure principle.....	Information held on data storage media (including magnetic tapes, disks, printed results, and stationery) should be protected against corruption, loss or disclosure and additional security controls applied to media containing sensitive information.
Status	Implemented
Description	See below.

According to [R15], the EC Data Centre ensures that data storage media (including magnetic tapes, hard disks, and printed documentation) is handled in accordance with documented standards/procedures.

5.5.3.4. Protection against Malicious Software

Measure principle.....	Virus protection arrangements should be established and maintained organisation-wide.
Status	To be implemented
Description	See below.

As mentioned in §4.3.3.4, a second protection barrier shall be implemented to protect Central Services applications against malicious software. This is achieved by:

- Routing all SMTP traffic coming from the CCN Mail 2 channel to the EC SMTP Scanner (Figure 15), as imposed by the EC Security Policy [R12]. The EC SMTP Scanner is configured to detect malicious code (viruses, worms, trojans, etc.) that may be contained in e-mail messages, to provide an alert when a suspected code is identified, and to disinfect, delete, or quarantine malicious code when identified. If

nothing is detected, the EC SMTP Scanner redirects the incoming SMTP traffic to an EC internal MTA. The CCN Bridge is then able to access incoming e-mail messages stored on the EC MTA using standard protocols (POP3, IMAP4).

- Implementing a security device (FW_F on [Figure 15](#)), acting as unique entry point to Central Services platforms and providing anti-virus protection, intrusion detection, and HTTP content filtering capabilities (see §5.5.3.5).

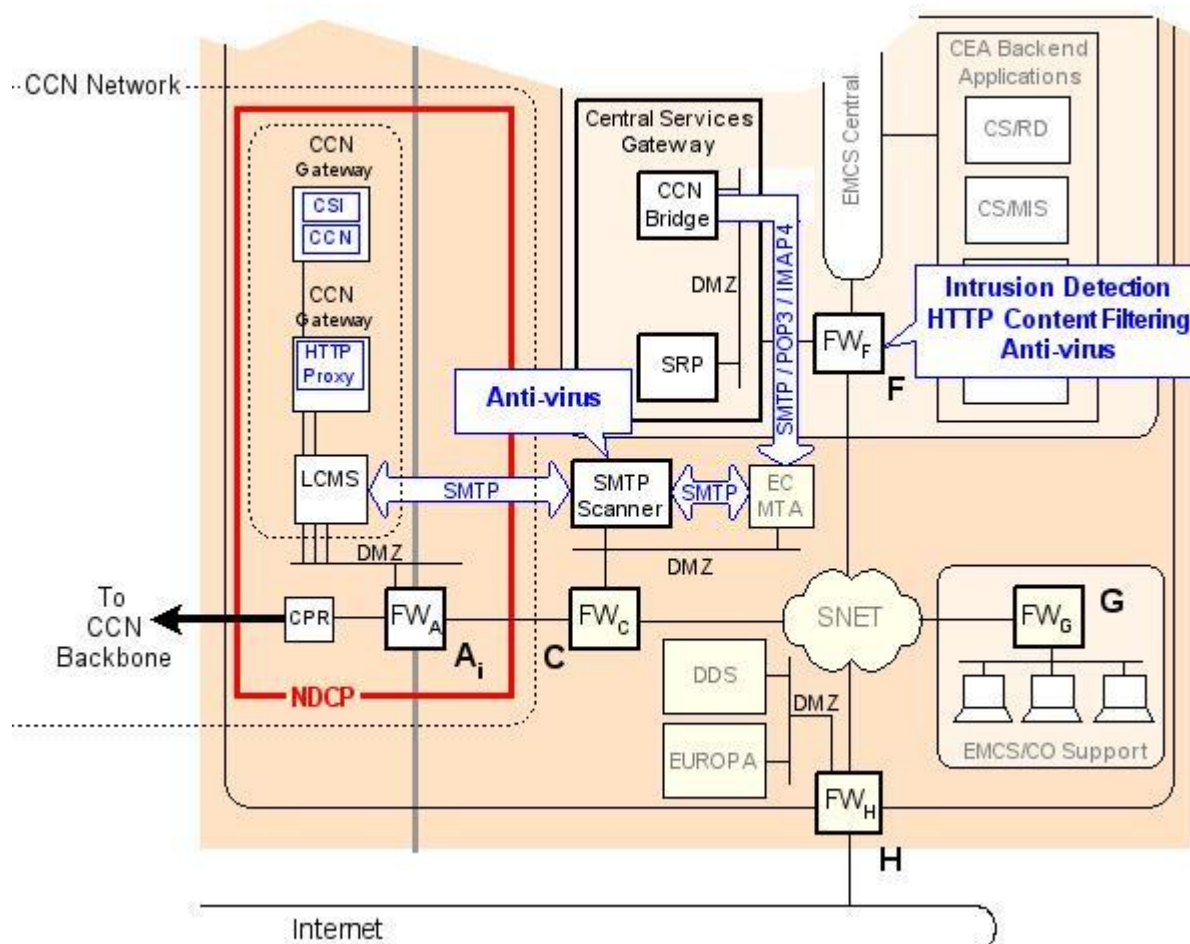


Figure 15: CEA Security - Protection against Malicious software

5.5.3.5. Intrusion Detection

Measure principle.....	Intrusion detection mechanisms should be applied to critical systems and networks.
Status	To be implemented
Description	See below.

FW_F equipment ([Figure 15](#)) shall also provide intrusion prevention and detection capabilities. The Intrusion Detection System (IDS) ensures that the EMCS/CO support team is informed when an attack mounted from an external network (e.g. from SNET) is detected, and may take further actions. The IDS is also configured to allow FW_F to block access from an attacker network address and to provide web content filtering.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5.5.3.6. Patch Management

Measure principle.....	There should be a strategy for patch management that should be supported by a management framework and a documented patch management process.
Status	To be implemented.
Description	See below.

The EC Data Centre has already established a patch management process related to the EC-supported Operating System software so as to address potential vulnerabilities quickly and effectively and to reduce the likelihood of a serious incident occurring.

The EMCS/CO shall establish a similar process but focusing on the EMCS Central Services specific software that will not be supported by the EC Data Centre.

5.6. SNET Network Security

ISF building block (see §2.3.2): *Networks*

This part mainly refers to security of the EC private network, called *SNET*, supporting the CEA interoperability with the CCN Network and the Internet (as far as information published on the Europa is concerned).

5.6.1. Network Management

5.6.1.1. Roles and Responsibilities

Measure principle.....	An owner should be identified for the network, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Status	Implemented.
Description	See below.

The overall responsibility for the SNET activity is assigned to the European Commission (DIGIT), which ensures operation and support of the SNET backbone.

5.6.2. Traffic Management

5.6.2.1. Network Routing Control (Enforced Path)

Measure principle.....	Networks shall have routing controls to ensure that computer connections and information flows do not breach the access control policy.
Status	To be implemented.
Description	See below.

As shown on [Figure 14](#), CEA backend applications can be accessed either by NEAs or MSA Users through the CCN Network or by EC Officials through the SNET network (EC private network).

Direct access to CEA backend systems from the Internet shall not be permitted.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5.6.2.2. Firewalls

Measure principle.....	Network traffic should be routed through a firewall, prior to being allowed access to the network.
Status	Partially implemented.
Description	See below.

To protect against unwanted accesses, a Firewall (FW_F) ensures the protection of the CEA backend systems. FW_F is the unique entry point to the EMCS Central Services Secure Area.

Moreover FW_F is configured in such a way that direct connection to CEA backend systems is not permitted and must be routed instead to the Central Services Gateway (see §5.2.1) that will perform additional security measures (pertaining to authentication and authorisation).

[Table 8](#) provides the list of CAPs related to the Common Domain Central Services and which correspond to the locations where firewalls shall be implemented.

CAP	Responsibility	Description
C	Common Domain (SNET)	Protection against unwanted accesses coming from the CCN/CSI network.
F	Common Domain (Central Services)	Protection against unwanted accesses coming from the CCN Network and the SNET network.
G	Common Domain (EMCS-CO)	Protection against unwanted accesses coming from the SNET network.
H	Common Domain (SNET)	Protection against unwanted accesses coming from the outside world (e.g. Internet).

Table 8: Controlled Access Points – Central Services

5.6.2.3. Network Encryption

Measure principle.....	Network encryption shall be applied to protect the confidentiality of sensitive or critical information during transit over networks.
Status	To be implemented.
Description	See below.

The confidentiality of data shall be protected during transit over SNET. It requires the FW_A ↔ FW_F link (see [Figure 15](#)) to be encrypted e.g. using 168-bit 3DES encryption. If FW_A and FW_F are located in the same physical security perimeter (or dedicated VLAN) at the EC Data Centre then network encryption between both devices is not needed.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5.7. Systems Development

ISF building block (see §2.3.2): *Systems Development*

In this paragraph focus is placed on the security specifications of Web-enabled development, as this type of development will be applied to the building of CEA Backend Applications.

Other aspects with regards to systems development best practices are developed in the section [6.2](#).

5.7.1. Web-enabled Development

Measure principle.....	Specialised technical controls should be applied to the development of web-enabled applications.
Status	To be implemented.
Description	See below.

The following security measures shall be implemented to ensure that the increased risks associated with the development of (web-enabled) CEA Backend Applications are minimised:

- The build process shall ensure that the SRP is:
 - Located in a “Demilitarised Zone” (DMZ) – an area that is isolated from the Internet and other internal networks by firewalls;
 - Run on dedicated computer(s);
 - Run with “least privileges” (e.g. excluding the use of high-level privileges, such as “root” for Unix systems or “Administrator” for Windows NT systems);
 - Prevented from initiating network connections to the Internet;
 - Reviewed to ensure that all unnecessary software, network services or applications have been removed;
 - Configured to log activity on the systems.
- The build process shall ensure that connection between the SRP and the CEA back-end systems is:
 - Protected by firewalls;
 - Restricted to those services that are required by the application;
 - Restricted to code generated by web server applications, rather than by client applications;
 - Supported by mutual (two-way SSL) authentication⁸;

⁸ SSL can be either one-way or two-way:

- In one-way SSL, the identity of the server is confirmed through the presentation of a certificate to the client and communication between client and server is encrypted;
- In two-way SSL, both the client and server are required to present a certificate during an exchange that precedes the establishment of a secure SSL connection.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

- Based on documented application programming interfaces (APIs).
- User accounts that are used by the SRP to make connections to the CEA back-end systems shall be built to run with “least privilege”;
- The build process shall ensure that information used by the CEA applications under development are protected against corruption or disclosure by performing data input validation at the server, and not only on the client application;
- The build process shall ensure that the CEA Applications are:
 - Stored on a separate partition/disk from the operation system;
 - Protected by setting file permissions;
 - Updated and reviewed by authorised individuals only.
- Sensitive data in transit shall be protected against disclosure by using SSL 128-bit encryption;
- CEA Application (HTTP-) sessions shall be protected against being hijacked or cloned by ensuring SessionIDs cannot be easily predicted (See CEA Ticket generation - §5.8.1.2);
- CEA Applications shall be configured to log activity.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5.8. CEA Access Control (CCN Intranet Channel)

ISF building block (see §2.3.2): *Critical Business Applications*

Web Services invoked to access Central Excise Application functions (CS/RD, CS/MIS, and SEED), also referred to as “*CEA Web Services*”, can be secured on two levels: transport and message.

- HTTP Transport-level security (see §5.8.1): concerns the use of the Secure Socket Layer (SSL) to secure the HTTP transport between the communicating parties (i.e. MSA Users and/or NEA) and the CEA Web Services;
- (Optionally) SOAP message-level security (see §5.8.2): concerns the security of the actual content of the SOAP message exchanged between the communicating parties. A specific OASIS specification called “*WS-Security*” [R41] addresses such message-level security.

5.8.1. HTTP Session-level Security

5.8.1.1. Topology

The topology of the Web Services channel is represented in [Figure 16](#). On the National Domain side, the invocation of CEA Web Services can be made in two different ways:

- Case 1: Through a non-encrypted channel (i.e. at least as far as the NEA/MSA User ↔ Local CCN Gateway communication link is concerned) using the HTTP protocol;
- Case 2: Through an end-to-end SSL-encrypted using the HTTPS protocol. In this case the SSL encrypted channel is established between the NEA (or the MSA User’s workstation) and the Central Services Gateway’s SRP (Secure Reverse Proxy), which is part of the Central Services Gateway.

At this stage, it is important to mention that the HTTP Proxy (running on the CCN Gateway) behaves differently whether the protocol in use is HTTP or HTTPS:

- If the HTTP protocol is used, then the HTTP Proxy acts as a “*real*” proxy. It intercepts every incoming HTTP request from the NEA (or MSA user); it performs security controls regarding CCN Intranet authentication⁹ and authorisation (through the Apache handler called `TicketAccess.pm`); and it forwards the request to the remote HTTP Proxy, which in turn forwards the request to the right destination.
- If the HTTPS protocol is used, a point-to-point secure communication between the NEA (or MSA User) and the Central Services Gateway is established. This means that the HTTP Proxy forwards every incoming HTTPS request (even non-authenticated) performed on TCP Port 8443 (or 8444) without performing any further security controls with regard to CCN Intranet authentication and authorisation.

⁹ As logon time the HTTPS protocol is used between the NEA (or MSA User) and the local HTTP Proxy to ensure the confidentiality of user’s credentials during the transport. Then the HTTP Proxy switches back from HTTPS to HTTP.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

Does this mean that it is not possible to rely on the CCN Intranet “native” security if HTTPS is used? Not completely. But to do so, additional security measures will have to be implemented at the Central Services Gateway level, in particular to force the CCN Intranet controls to be applied whatever the supporting protocol (HTTP or HTTPS). This is the scope of the specifications developed at the paragraphs [5.8.1.2](#) “Authentication” and [5.8.1.3](#) “Authorisation”.

Note: Refer also the [Appendix C](#), which provides the detailed specifications of the authentication (and authorisation) scheme implemented by the EMCS to allow NEA (or MSA Users) ↔ CEA secure interactions.

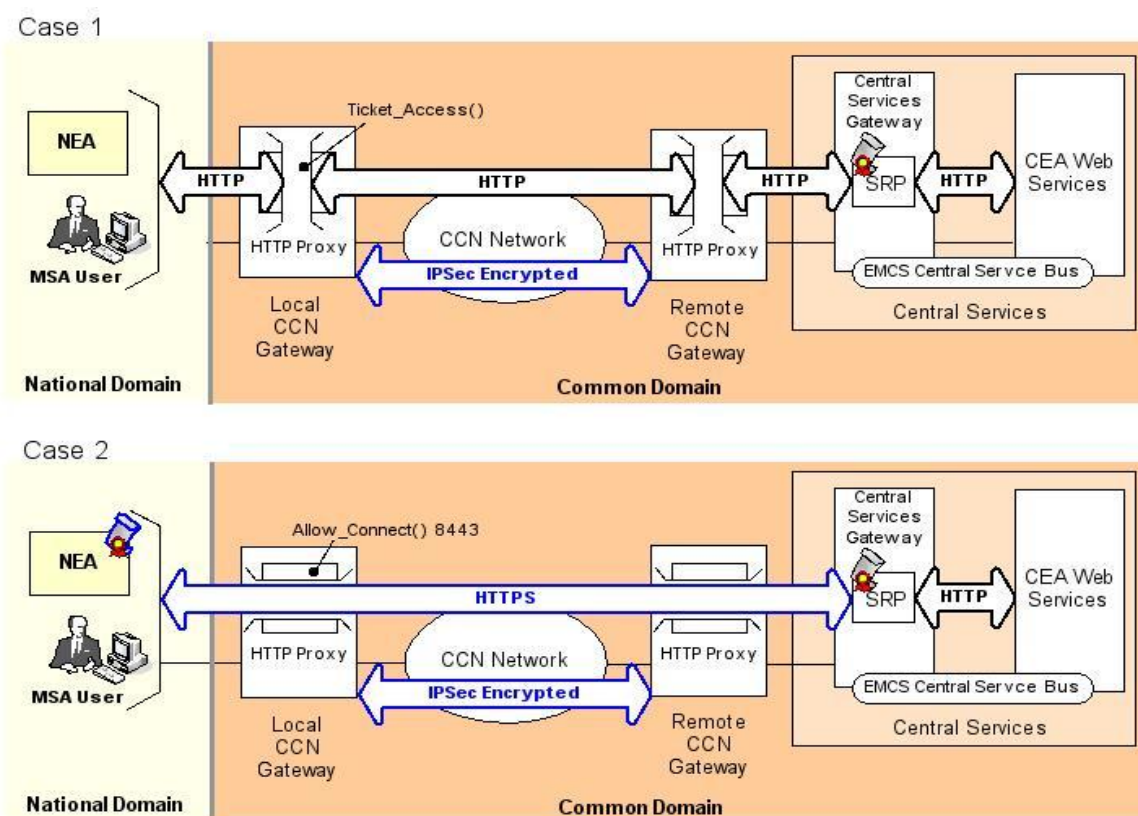


Figure 16: HTTP Session-level Security – Topology

5.8.1.2. Authentication

As said previously, the use of the HTTPS protocol over the CCN Network bypasses the local form-based authentication to the CCN Intranet (which is basically invoked when the target resource is accessed through HTTP) and consequently there is a need to compensate this lack of security by implementing additional controls at SRP levels.

The proposed way to implement this is illustrated on [Figure 17](#). It relies on the following principles:

1. Any incoming request to CEA services transported through the CCN Intranet channel, *must* first be authenticated and authorised by the CCN Intranet before being routed to the SRP, whatever the protocol in use (HTTP or HTTPS) and the client type (NEA or MSA User), so as to benefit from the CCN Intranet *built-in* security (and comply with the CCN/CSI General Security Policy [\[R12\]](#));

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

2. Once authenticated to the CCN Intranet, then a second authentication phase is initiated by the SRP. The second authentication depends on the client type:
 - If the client is an NEA, it involves a 2-way SSL v.3 (Certificate-based) mutual authentication between the NEA and the SRP;
 - If the client is an MSA user, it involves a login/password-based form authentication initiated by the SRP following the CEA services password policy.

In both cases (NEA or MSA user) the second authentication involves the creation of an assertion (e.g. session ticket, WSSE security token) that will be used for subsequent exchanges access control. The DDNEA will refine technological choices at this level.

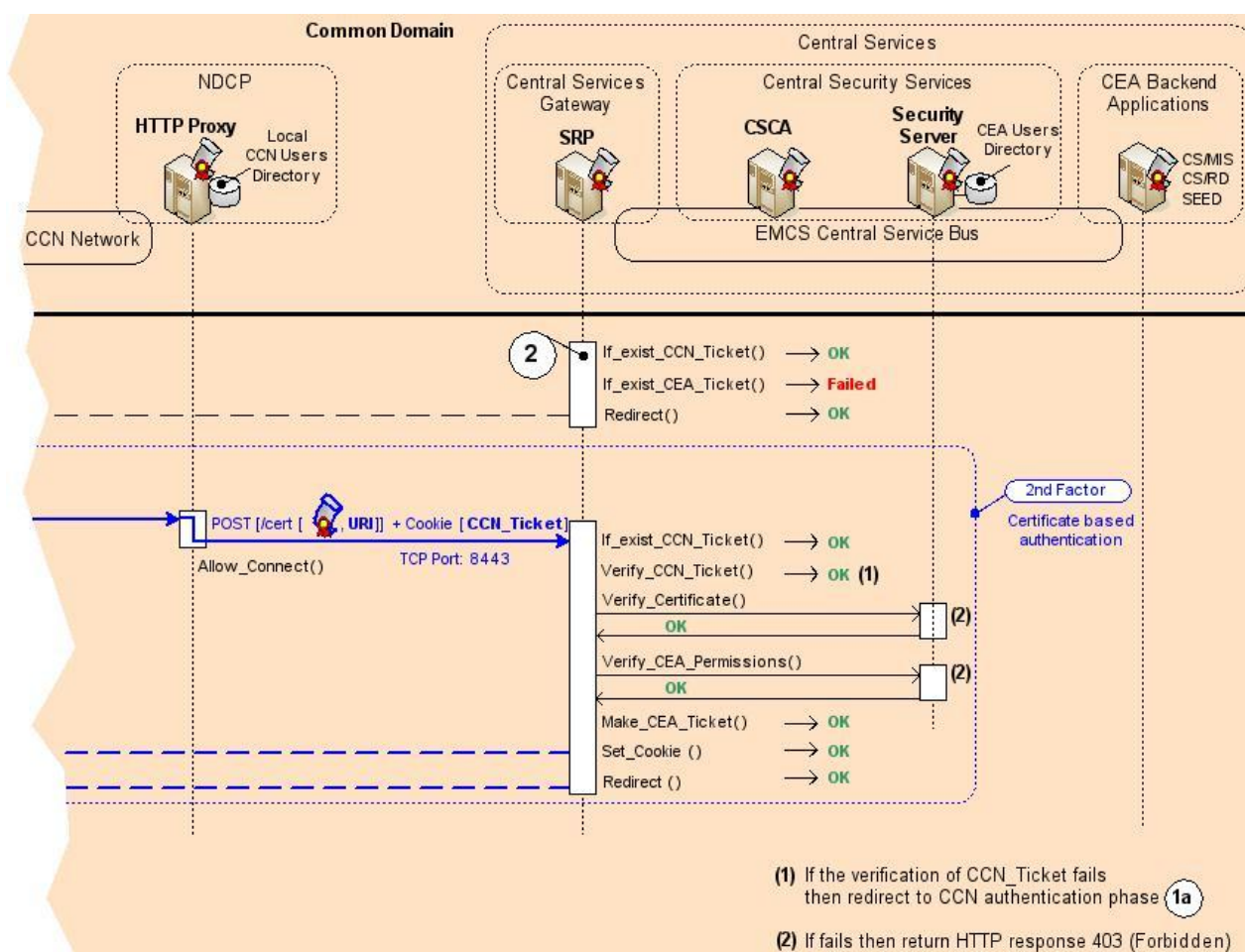


Figure 17: NEA to CEA authentication – Certificate-based

The NEA ↔ CEA (basically SRP) certificate-based authentication involves the capability to verify the validity of the client certificate, which relies on the services offered by the Security Server (see §5.2.2.1).

The implementation of the two-way SSL v.3 certificate-based authentication mechanism between the NEA and the SRP requires that:

1. The NEA has received from its MSA an X.509 high-grade server certificate signed by a CA accredited by the MSA. The certificate type – soft or token based – remains under MSA responsibility;

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

2. The NEA certificate is registered in the Trusted Status List (TSL) managed by the Security Server (to allow performing the certificate verification process);
3. The NEA is built to programmatically send an X.509 Certificate to the Central Services Gateway (see §5.4).

Note: If, on the National Domain side, the NEA is located behind a reverse proxy, then the X.509 high-grade server certificate should be installed on the national reverse proxy instead of the platform running the NEA. Note also that the NEA does not only access CEA Web services, it also implements exchanges with other NEA [BCC2], MSA users [BCC4] [BCC5] and Economic Operators [BCC1] [BCC3].

5.8.1.3. Authorisation

Figure 18 illustrates the mechanism implemented to perform CEA authorisations. It involves interactions with the Central Services Security Server (see §5.2.2.1) in two ways:

- At SRP level, to verify the MSA User or NEA permissions for accessing a CEA backend-end application (e.g. SEED, CS/MIS);
- At CEA Backend application level, to verify the MSA User or NEA permissions for accessing a particular function within the application (“fine” access control).

Those access privileges are stored in the CEA users directory (e.g. LDAP directory) running on the Security Server and are securely protected.

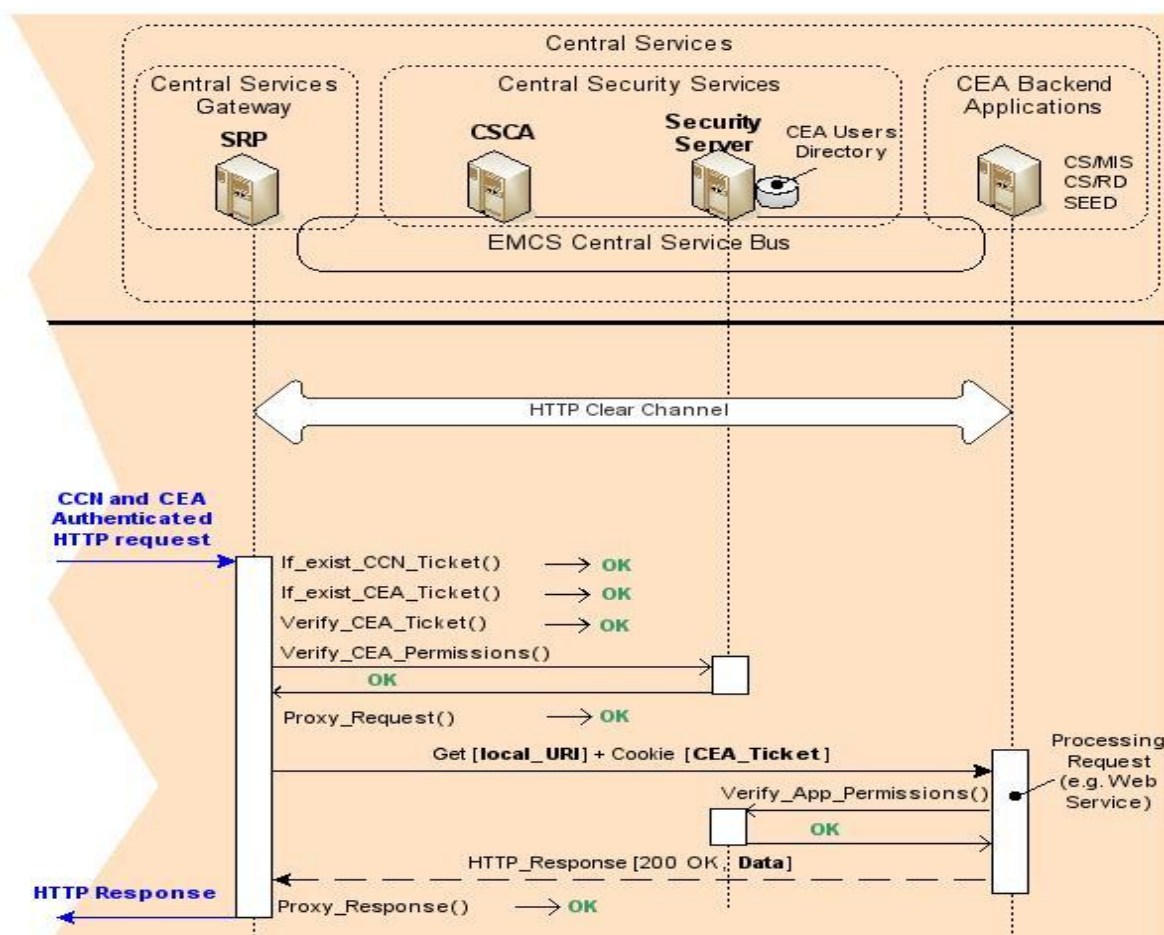


Figure 18: CEA Authorisations

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

5.8.2. SOAP Message-level Security

WS-Security offers “message-level” security, which supplements “transport level” security (see §5.8.1) by addressing its weaknesses:

- HTTPS Transport level security is “*point-to-point*” – SSL encrypts the connection between the NEA (or MSA User) client and the SRP. This means that the SRP is able to retrieve the (SOAP) message in clear before forwarding it to the right CEA back-end application (e.g. SEED). In contrast, message-level security offers “*end-to-end*” security – *WS-Security* ensures the *integrity* of a SOAP message. That is, the SOAP message is not available in clear text to any intermediary component, so it is not possible to alter the message content in any way during its transit from the NEA to the end destination CEA;
- SSL is a full encryption protocol; where as, in message-level security with XML Encryption it is possible to protect the *confidentiality* of a SOAP message by encrypting only those specific parts of the SOAP message that contain confidential information;
- With HTTP Transport level security, the originator of the request (NEA) is no longer known to the receiver (e.g. SEED) due to the fact that HTTP request is proxied during its transit. In contrast, with message-level security it is possible to authenticate the identity of the sender (NEA) through the use of *XML Digital Signatures*.

To support the WS-Security standard, CEA back-end applications shall comply with the OASIS WS-Security standard [R41], [R42], and [R43]. WS-Security is defined in the OASIS standard specification as “*a standard set of SOAP extensions that can be used when building secure Web services to implement integrity and confidentiality ...(and) provides three main mechanisms: security token propagation, message integrity, message confidentiality.*”

Note: So far, message-level security has not been explicitly expressed as a requirement for EMCS. This is the reason why it is presented here as an “optional” feature. So, the NEA should not do any specific checks at this level.

5.8.3. CEA Web Services Addressing Scheme

Every CEA Web Service is located by its *URI* (Uniform Resource Identifier). The proposed *URI* addressing scheme is described below:

```
URI ::= <Protocol>://<WebCEA>:<Port>/<AppPath>/<WebService>
```

Where:

- <Protocol> is the protocol used (i.e. HTTP or HTTPS);
- <WebCEA> is the CEA domain qualified name;
- <Port> is the TCP port number to be used to access the resource;
- <AppPath> is the logical path to reach the CEA application (e.g. SEED);
- <WebService> is the name of the web service relative to <AppPath>.

Example:

```
https://cea.taxud.ccncsi.int:8443/seed/webservices1.jws
```


DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
EMCS CENTRAL SERVICES SECURITY MEASURES	

Figure 19 illustrates in which way the proposed addressing can be used for accessing CEA Web Services (and more specifically the <AppPath> rewriting mechanism performed by the SRP to reach CEA Backend applications in a transparent manner for clients (MSA User and NEA).

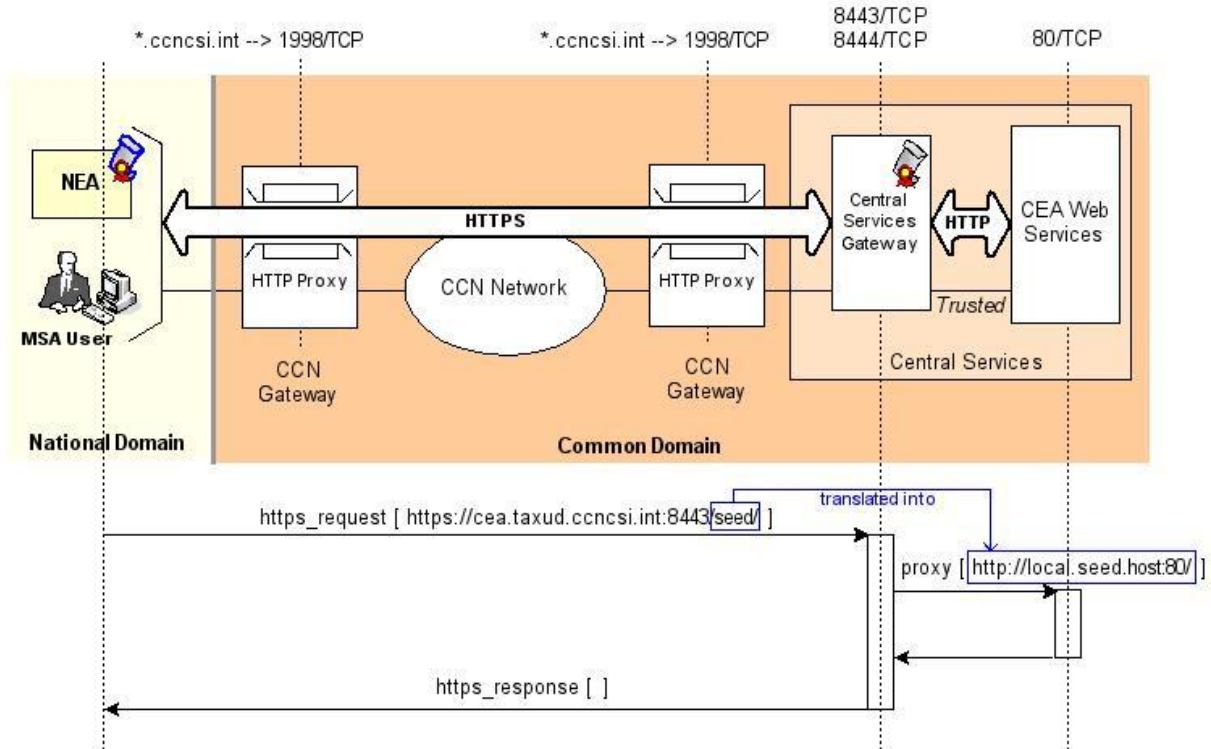


Figure 19: CEA Web Services Addressing – HTTPS Transport

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
STANDARD EXCISE APPLICATION (SEA) SECURITY MEASURES	

6. Standard Excise Application (SEA) Security Measures

6.1. Introduction

The centrally developed Standard Excise Application (SEA) as specified in *TESS Section IV [R9]* and its nationally developed counterpart, referred to as NDEA, form the National Excise Application (NEA).

In this Chapter, focus is placed on the SEA only, and more precisely on its main component called *Service Broker*, which technical specification is provided in the *TESS Section IV, Chapter 3*. The objective is to examine in which way the general design principles, which help in the creation of secure systems, can ensure that information security is addressed at each stage of the SEA development cycle (see §6.2).

Note: As far as NDEA security is concerned, refer to the security guidance provided in [Appendix B](#), knowing that the security implementation in the National Domain remains the sole responsibility of the MSA.

[Figure 20](#) shows the central role of the SEA Service Broker, which regulates the business process flows (including the coordination protocol in the Common Domain).

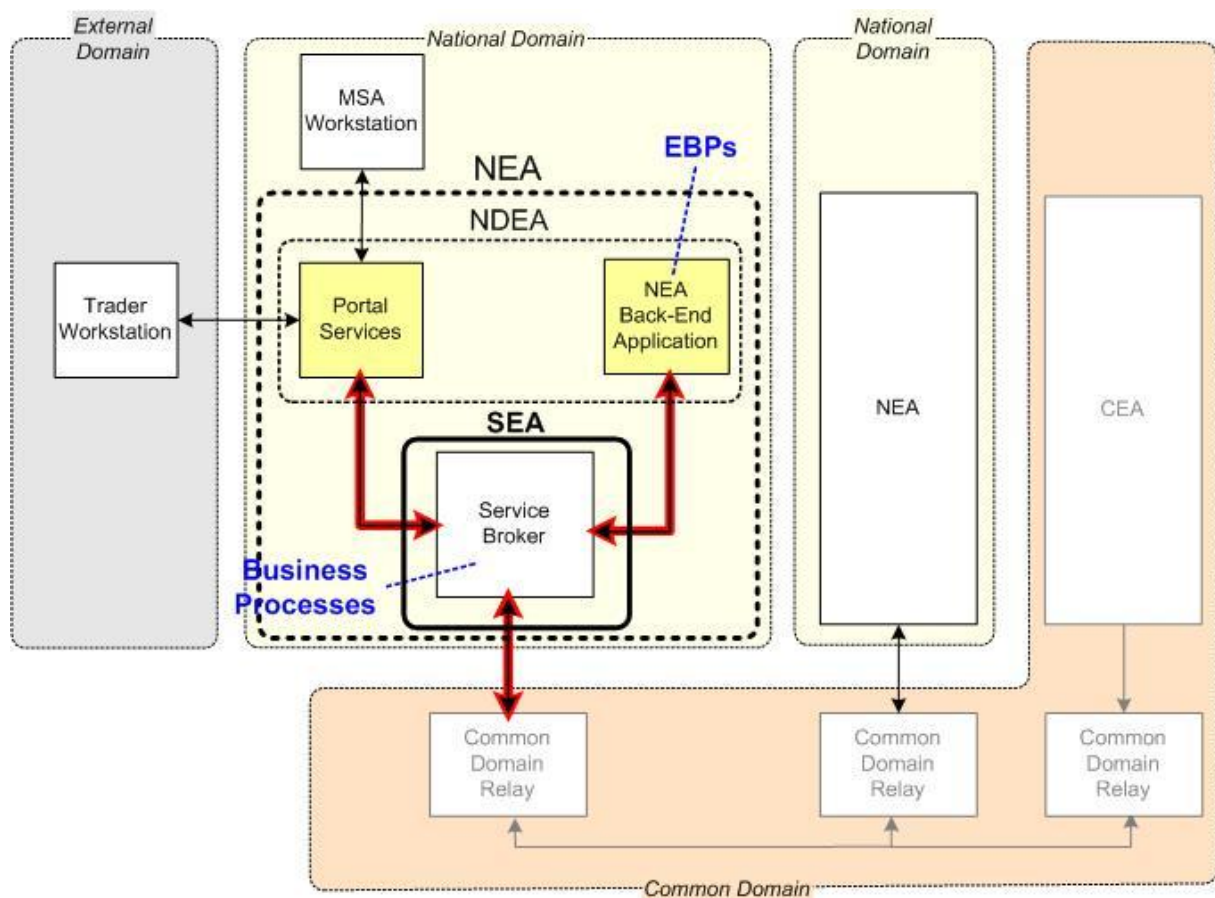


Figure 20: Standard Excise Application Architecture

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
STANDARD EXCISE APPLICATION (SEA) SECURITY MEASURES	

6.2. Security Measures

ISF building block (see §2.3.2): *Systems Development*

6.2.1. Development Management

6.2.1.1. Roles and Responsibilities

Measure principle.....	An individual/organisation with overall responsibility for the development activity, together with business, shall be appointed to manage system development activities, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Status	To be implemented.
Description	See below.

The decision to have the SEA developed or not by the Commission has to be taken by the involved parties, i.e. the Central Project Team (CPT) and the MSAs. To help in this decision process, the TESS proposes the possible architecture for the SEA.

6.2.1.2. Development Methodology

Measure principle.....	Development activities should be carried out in accordance with a documented system development methodology.
Status	To be implemented.
Description	See below.

Development activities shall be carried out in line with the security requirements of the Tempo methodology [R10] and following the guidance provided by the ISF [R35].

6.2.1.3. Quality Assurance

Measure principle.....	Quality assurance of key security activities should be performed during the development lifecycle.
Status	To be implemented.
Description	See below.

During the SEA development, quality assurance of key security activities must include:

- Assessing development risks (i.e. those related to running a *central* development project, which would typically include risks associated with business requirements, benefits, technology, technical performance, costing and timescale);
- Ensuring that security requirements have been defined adequately;
- Ensuring that security measures agreed during SESS elaboration process (e.g. policies, methods, procedures, security mechanisms schemes intended to protect the confidentiality, integrity or availability of information and legitimate use of the system) have been developed;
- Determining if security requirements are being met effectively.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
STANDARD EXCISE APPLICATION (SEA) SECURITY MEASURES	

Quality assurance of key security activities shall be:

- Performed at an early stage of the development process;
- Reviewed at the key stages during the development lifecycle;
- Documented.

6.2.1.4. Development Environments

Measure principle.....	System development activities should be performed in specialised development environments, isolated from the production environment, and protected against disruption and disclosure of information.
Status	To be implemented.
Description	See below.

The SEA development environment shall be protected by:

- Preventing development staff from making unauthorised changes to the production environment (e.g. by using access control software);
- Applying strict version control over system development software;
- Employing anti-virus software to reduce the threat of viruses;
- Preventing malicious code from being downloaded into development environments (e.g. by the use of filtering or blocking techniques).

The SEA development environment shall be isolated from the production environment and acceptance testing separated from development activity.

6.2.2. Requirements Definition

TESS Section IV [R9] describes the architecture of the SEA based on the Standard Transit Application model (see *TESS Appendix B [R9]*). [Figure 21](#) depicts the various elements of the Service Broker and in particular:

- **Enhanced EDI/CSI Node (ECN)** regulating the flow of EMCS message exchanges between the various involved domains (External Domain, National Domain and Common Domain), addressing the interfaces of the Service Broker;
- **Application Bus** that consists of a Message-oriented Middleware (MoM) that allows exchanges between parties to be persistent, guaranteeing that the transaction is finally successfully achieved even if incidents occur.

The Service Broker shall rely on the security provisions offered by:

- The CCN/CSI security services for the exchanges with the Common Domain Relay;
- The Portal Services with respect to connection with the External Domain;
- The LAN connection with the Portal Services and the NEA back-end services will be considered as safe (trusted);
- The BEA Tuxedo¹⁰ security features.

¹⁰ The BEA Tuxedo product is mentioned because this tool is already used by the Commission.

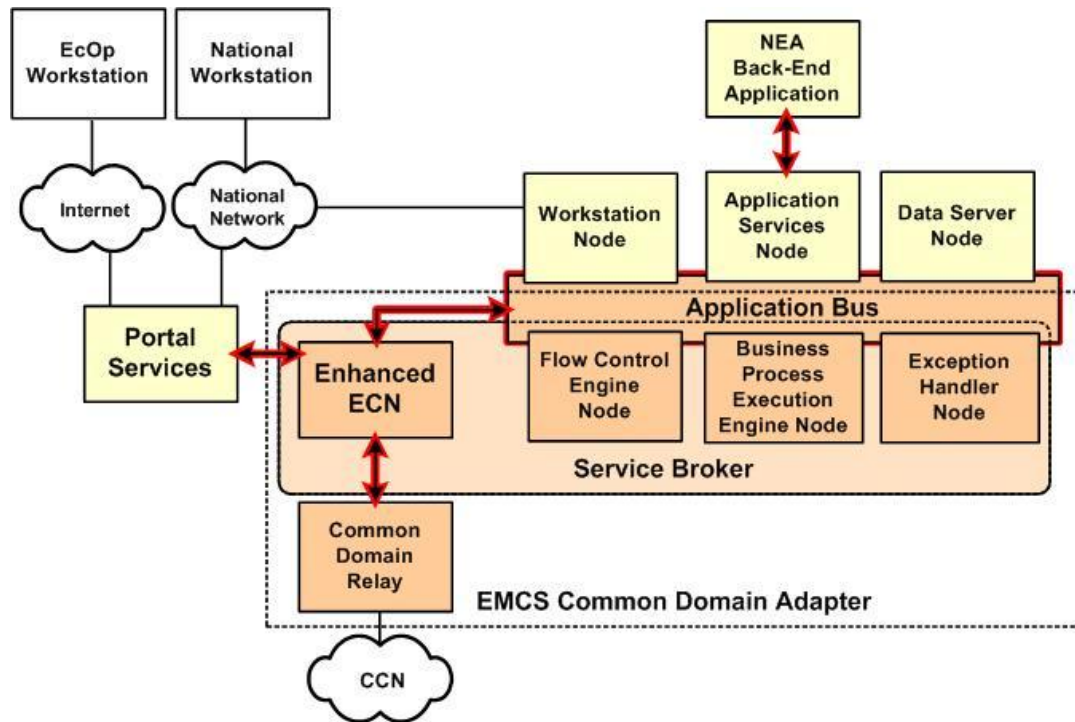


Figure 21: Service Broker Technical Architecture

6.2.2.1. Confidentiality Requirements

Measure principle.....	The business impact of unauthorised disclosure of information associated with the system under development should be assessed.
Status	To be implemented.
Description	See below.

Confidentiality is the ability to keep communications secret from parties other than the intended recipient. It is achieved by encrypting all data.

BEA Tuxedo security includes encryption to ensure data privacy when deploying applications across networks. Two levels of encryption are supported:

- Network-level encryption using proprietary Link-Level Encryption (LLE);
- Session-level encryption using the Secure Sockets Layer (SSL) protocol and public key encryption.

6.2.2.2. Integrity Requirements

Measure principle.....	The business impact of the accidental corruption or deliberate manipulation of business information stored in or processed by the system under development should be assessed.
Status	To be implemented.
Description	See below.

- Integrity is a guarantee that the data being transferred has not been modified in transit.

BEA Tuxedo security includes end-to-end digital signing. This capability is built upon the PKCS-7 standard, which is one of a set of Public-Key Cryptography Standards (PKCS)

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
STANDARD EXCISE APPLICATION (SEA) SECURITY MEASURES	

developed by RSA Laboratories in cooperation with several other leading communications companies.

Message-based digital signature ensures data integrity by having the sending party bind proof of its identity to a specific message buffer.

6.2.2.3. Availability Requirements

Measure principle.....	The business impact of business information stored in or processed by the system under development being unavailable for any length of time should be assessed.
Status	To be implemented.
Description	See below.

The Service Broker is the central piece of the architecture, which must ensure reliability and availability by implementing prevention, detection and compensation measures. In case of failures, the system must keep the application running in the following ways:

- Ensures no single point of failure by providing replicated server groups that can continue when something breaks.
- Restores the running application to good condition after failures occur.

BEA Tuxedo ensures constant access to applications. System components are constantly monitored for application, transaction, network, and hardware failures. When a failure occurs, BEA Tuxedo logically removes that component from the system, manages any necessary recovery procedures, and re-routes messages and transactions to surviving systems. This occurs transparently to the end user and without disruption in service.

6.2.2.4. Logging and Auditing

Measure principle.....	Logs of all key events within the computer installation should be maintained (preferably using automated tools), reviewed periodically and protected against unauthorised change.
Status	To be implemented.
Description	See below.

The Service Broker must keep a log of exchanged information. ECN provides the logging of incoming and outgoing messages, translation and validation results and system events. This log must contain:

- The content of the messages that have been exchanged (either sent or received);
- Timestamp showing at which date and time the IE message has been sent or has been received;
- The result of the message processing, including all detected errors.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
STANDARD EXCISE APPLICATION (SEA) SECURITY MEASURES	

6.2.3. Design and Build

6.2.3.1. Design

Measure principle.....	Information security requirements for the system under development should be considered when designing the system.
Status	To be implemented.
Description	See below.

The SEA design phase shall:

- Consider the full range of security measures;
- Identify specific security measures required by particular business processes supported by the system under development (e.g. encryption of sensitive data);
- Document security controls that do not fully meet requirements;
- Specify a system architecture that can support the technical specifications (TESS);
- Include design reviews, to ensure that security measures are in place.

The SEA shall be designed to:

- Provide “defence in depth”, to avoid relying on one line of defence or one type of security control;
- Assume input from external systems is insecure as it might be an “attack”;
- Repeat any client validation at the server;
- Employ secure defaults in software configuration;
- Ensure key components “fail securely” (e.g. when an application fails it does not disclose any information that would not be disclosed ordinarily and that the information still cannot be tampered with);
- Run with “least privilege”, so that applications do not run with high-level privileges (e.g. “root” in Unix systems or “Administrator” in Windows NT systems).

Before SEA coding or acquisition work begins, system designs should be documented, verified to ensure that they meet security requirements, reviewed by a specialist in information security and signed-off by the organisation in charge of the system(s) under development.

6.2.3.2. Application Controls

Measure principle.....	The full range of application controls should be considered when designing the system under development.
Status	To be implemented.
Description	See below.

The system design phase shall include an assessment of possible application controls. This assessment should include security controls associated with the validation of:

- Information entered (e.g. range checks, making key fields mandatory, control balances);
- Automated processes (e.g. record counts and/or hash, session, batch or balancing totals);

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
STANDARD EXCISE APPLICATION (SEA) SECURITY MEASURES	

- Information integrity, i.e. the completeness, accuracy and validity of information (e.g. Economic Operators registration information, lists of codes);
- Information output (e.g. reconciling control counts to ensure all data is processed or using plausibility checks to ensure output is reasonable);
- Changes to information (e.g. inspection of the contents of records before and after they have been changed).

6.2.3.3. System Build

Measure principle.....	System build activities (including coding and package customisation) should be carried out in accordance with industry good practice, performed by individuals provided with adequate skills/tools and inspected to identify unauthorised modifications or changes which may compromise security measures.
Status	To be implemented.
Description	See below.

System build activities (such as programming, creating web pages, customising packages or defining data structures) shall be carried out in accordance with documented standards/procedures.

Those standards/procedures shall at least specify:

- Approved methods of building systems;
- Mechanisms for ensuring systems comply with good practices for system build;
- Secure methods of making changes to the base code of software packages;
- Review and sign-off processes (including those for package customisation).

6.2.4. Testing

6.2.4.1. Testing Process

Measure principle.....	All elements of a system (i.e. application software packages, system software, hardware and services) should be tested before the system is promoted to the live environment.
Status	To be implemented.
Description	See below.

The Acceptance and Certification Specifications (ACS) [\[R5\]](#) defines the testing process to be followed for the technical Conformance Testing of National Excise Applications (NEA), including the SEA.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
STANDARD EXCISE APPLICATION (SEA) SECURITY MEASURES	

6.2.5. Deployment

6.2.5.1. System Deployment Criteria

Measure principle..... Rigorous criteria should be met before new systems are deployed into the production environment.

Status To be implemented.

Description See below.

- The Acceptance and Certification Specifications (ACS) [\[R5\]](#) defines the conformance criteria for the deployment into production environment. It has to be proven that these pre-requisites have been tested successfully, including:
 - All the mandatory test scenarios specified in the ACS are successfully completed;
 - All critical errors have been fixed and satisfactorily re-tested;
 - All major errors have either been fixed and satisfactorily re-tested or the ECWP has agreed to accept a work-around and a plan to defer their correction;
 - A plan has been proposed for fixing the remaining minor errors.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX A: COMPLIANCE MATRIX	

7. Appendix A: Compliance Matrix

To make sure that all identified Security Requirements are covered by the SESS, the following table takes the form of a compliance matrix ([Table 9](#)) indicating for each requirement the general security measures [SMx] to be implemented (as indicated by the SEP [\[R3\]](#)) and providing pointers to the sections of this document where those security measures are further specified.

The additional security measures that are specified in the SESS, but which are not already explicitly mentioned in the SEP, are labelled [*ASM_x*] (for Additional Security Measure) in the matrix. Those additional security measures will be integrated to the SEP later in the project according to the change management procedures defined in the EMCS Terms of Collaboration [\[R2\]](#).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX A: COMPLIANCE MATRIX	

SEP Id.	Requirements Description	General Security Measures recommended by the SEP	Cross Reference in SESS Document			
			CD (§4)	CS (§5)	SEA (§6)	ND (§8)
ISO Category #2: Security Organisation						
[SR2]	Registration of Economic Operators Maintain the security of information processing facilities and information assets accessed by Economic Operators. <u>Justification:</u> Eliminate (or at least reduce) the following risks: [RSK2] Illegitimate use of the EMCS system by Economic Operators [RSK4] Illegitimate access to the EMCS system by Outsiders					
		[SM5] Perform Identity Proofing	N/A	N/A	N/A	§8.3.4.2
		[SM6] Define and implement access control policy for Economic Operators	N/A	N/A	N/A	§8.2.4
ISO Category #5: Physical and Environmental Security						
[SR9]	Secure Areas Prevent unauthorised physical access, damage and interference to business premises, to IT equipment (i.e. servers, routers, switches) and to information. <u>Justification:</u> Eliminate (or at least reduce) the following risks: [RSK4] Illegitimate access to the EMCS system by Outsiders [RSK10] Theft and/or Wilful Damage of Data and Facilities [RSK23] Power failure [RSK24] Air conditioning failure [RSK25] Natural Disaster					
		[SM18] Implement physical security perimeter	§4.3.2.1	§5.5.2.1	N/A	§8.3.2.1
		[SM19] Implement physical entry controls	§4.3.2.1	§5.5.2.1	N/A	§8.3.2.1
		[SM20] Isolate delivery and loading areas	§4.3.2.1	§5.5.2.1	N/A	§8.3.2.1
[SR10]	Equipment Security Prevent loss, damage or compromise of physical assets (e.g. telecom equipment) and interruption to business activities (e.g. power cut, over power). <u>Justification:</u> Eliminate (or at least reduce) the following risks:					
		[SM21] Provide equipment sitting and protection	§4.3.2.2	§5.5.2.2	N/A	§8.3.2.2

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX A: COMPLIANCE MATRIX	

SEP Id.	Requirements Description	General Security Measures recommended by the SEP	Cross Reference in SESS Document			
			CD (§4)	CS (§5)	SEA (§6)	ND (§8)
	[RSK4] Illegitimate access to the EMCS system by Outsiders	[SM22] Provide uninterruptible power supply	§4.3.2.3	§5.5.2.3	N/A	§8.3.2.3
	[RSK10] Theft and/or Wilful Damage of Data and Facilities	[SM23] Perform equipment maintenance	§4.3.2.4	§5.5.2.4	N/A	§8.3.2.4
	[RSK17] Failure in Outsourced Operations	[SM24] Provide security of equipment off-premises	N/A	N/A	N/A	§8.3.2.5
	[RSK18] Hardware Maintenance Error	[SM25] Secure disposal or re-use of equipment	N/A	N/A	N/A	§8.3.2.6
	[RSK19] Software Maintenance Error					
	[RSK20] Technical failure of host					
	[RSK21] Technical failure of storage device					
	[RSK22] Technical failure of print facilities					
	[RSK23] Power failure					
	[RSK24] Air conditioning failure					
	[RSK25] Natural Disaster					
ISO Category #6: Operations Management						
[SR13]	Protection against Malicious Software Protect the integrity of software and information from damage by malicious software. <u>Justification:</u> Eliminate (or at least reduce) the following risks:					
	[RSK9] Introduction of Damaging or Disruptive Software	[SM33] Implement controls against malicious software	§4.3.3.4	§5.5.3.4	N/A	§8.3.3.4
		<i>[ASM1] Patch Management</i>	§4.3.3.5	§5.5.3.6		§8.3.3.5
[SR14]	Back-up and Media Handling Prevent damage to assets and interruptions to business activities. <u>Justification:</u> Eliminate (or at least reduce) the following risks:					
		[SM34] Perform information back-up	§4.3.3.1	§5.5.3.1	N/A	§8.3.3.1

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX A: COMPLIANCE MATRIX	

SEP Id.	Requirements Description	General Security Measures recommended by the SEP	Cross Reference in SESS Document			
			CD (§4)	CS (§5)	SEA (§6)	ND (§8)
	[RSK9] Introduction of Damaging or Disruptive Software	[SM35] Produce operator logs	§4.3.3.2	§5.5.3.2	N/A	§8.3.3.2
	[RSK10] Theft and/or Wilful Damage of Data and Facilities	[SM36] Perform fault logging				
	[RSK11] Errors in using the EMCS application	[SM37] Manage removable computer media	§4.3.3.3	§5.5.3.3	N/A	§8.3.3.3
	[RSK17] Failure in Outsourced Operations	[SM38] Provide security of system documentation				
	[RSK18] Hardware Maintenance Error	<i>[ASM2] MSA Officials Workstation Security</i>				§8.3.3.6
	[RSK19] Software Maintenance Error					
	[RSK20] Technical failure of host					
	[RSK21] Technical failure of storage device					
ISO Category #7: Access Control						
[SR15]	Access Control Policy Define general guidance for access to information. <u>Justification:</u> Eliminate (or at least reduce) the following risks:					
	[RSK1] Illegitimate use of the EMCS system by MSA officials	[SM39] Define and implement access control policy	§4.3.4.1	§5.4.2.2	N/A	§8.2.4
	[RSK2] Illegitimate use of the EMCS system by Economic Operators					
	[RSK3] Illegitimate use of the EMCS system by Contracted Service Providers					
	[RSK4] Illegitimate access to the EMCS system by Outsiders					
	[RSK5] Repudiation					
	[RSK11] Errors in using the EMCS application					

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX A: COMPLIANCE MATRIX	

SEP Id.	Requirements Description	General Security Measures recommended by the SEP	Cross Reference in SESS Document			
			CD (§4)	CS (§5)	SEA (§6)	ND (§8)
[SR16]	User Access Management: Ensure that access rights to information systems are appropriately authorised, allocated and maintained. <u>Justification:</u> Eliminate (or at least reduce) the following risks:					
	[RSK1] Illegitimate use of the EMCS system by MSA officials	[SM40] Perform user registration	§4.3.4.2	§5.4.2.1	N/A	§8.3.4
	[RSK2] Illegitimate use of the EMCS system by Economic Operators	[SM41] Manage privileges	§4.3.4.3		N/A	
	[RSK3] Illegitimate use of the EMCS system by Contracted Service Providers	[SM42] Manage users tokens and electronic credentials	§4.3.4.3		N/A	
	[RSK4] Illegitimate access to the EMCS system by Outsiders	[SM43] Perform user identification and authentication	§4.3.4.4	§5.4.2.2 §5.8	N/A	§8.5.2.1
	[RSK5] Repudiation	[SM44] Perform review of user access rights	Following ISF Best Practices [R35]			
	[RSK11] Errors in using the EMCS application					
[SR17]	Network Access Control: Ensure the protection of networked services. <u>Justification:</u> Eliminate (or at least reduce) the following risks:					
	[RSK1] Illegitimate use of the EMCS system by MSA officials	[SM45] Implement segregation in networks	§4.4.2.2	§5.6.2.2	N/A	§8.4.2.2
	[RSK2] Illegitimate use of the EMCS system by Economic Operators	[SM46] Implement node authentication	Following ISF Best Practices [R35]			
	[RSK3] Illegitimate use of the EMCS system by Contracted Service Providers	[SM47] Perform network connection control				
	[RSK4] Illegitimate access to the EMCS system by Outsiders	[SM48] Perform network routing control	§4.4.2.1	§5.6.2.1	N/A	§8.4.2.1
	[RSK7] Eavesdropping					
[RSK9] Introduction of Damaging or Disruptive Software						

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX A: COMPLIANCE MATRIX	

SEP Id.	Requirements Description	General Security Measures recommended by the SEP	Cross Reference in SESS Document			
			CD (§4)	CS (§5)	SEA (§6)	ND (§8)
[SR18]	<p>Application Access Control: Prevent unauthorised access to information handled by the EMCS application.</p> <p><u>Justification:</u> Eliminate (or at least reduce) the following risks:</p> <p>[RSK1] Illegitimate use of the EMCS system by MSA officials</p> <p>[RSK2] Illegitimate use of the EMCS system by Economic Operators</p> <p>[RSK3] Illegitimate use of the EMCS system by Contracted Service Providers</p> <p>[RSK4] Illegitimate access to the EMCS system by Outsiders</p> <p>[RSK5] Repudiation</p> <p>[RSK11] Errors in using the EMCS application</p>					
		[SM49] Implement information access restriction	N/A	§5.4.2.2 §5.8	N/A	§8.5.2.1
		[SM50] Implement event logging facilities	§4.4.3.2	§5.4.3.1	§6.2.2.4	§8.5.2.2
ISO Category #8: System Development and Maintenance						
[SR20]	<p>Application Security: Prevent loss, modification or misuse of user data in the system.</p> <p><u>Justification:</u> Eliminate (or at least reduce) the following risks:</p> <p>[RSK1] Illegitimate use of the EMCS system by MSA officials</p> <p>[RSK2] Illegitimate use of the EMCS system by Economic Operators</p> <p>[RSK3] Illegitimate use of the EMCS system by Contracted Service Providers</p> <p>[RSK4] Illegitimate access to the EMCS system by Outsiders</p> <p>[RSK8] Unauthorised Software Changes</p>					
		<i>[ASM3] Roles and Responsibilities</i>			§6.2.1.1	
		<i>[ASM4] Development Methodology</i>			§6.2.1.2	
		<i>[ASM5] Quality Assurance</i>			§6.2.1.3	
		<i>[ASM6] Development Environments</i>			§6.2.1.4	
		<i>[ASM7] Requirements Definition</i>			§6.2.2	
		[SM52] Source Code Mastering	N/A	§5.7.1	§6.2.3	§8.5.1

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX A: COMPLIANCE MATRIX	

SEP Id.	Requirements Description	General Security Measures recommended by the SEP	Cross Reference in SESS Document			
			CD (§4)	CS (§5)	SEA (§6)	ND (§8)
	[RSK9] Introduction of Damaging or Disruptive Software	[SM53] Perform input data validation	N/A			
	[RSK14] Software Programming Errors (business critical functions)	[SM54] Perform control of internal processing	N/A			
	[RSK15] Software Programming Errors (other functions)	[SM55] Perform output data validation	N/A			
	[RSK19] Software Maintenance Error	[ASM8]Testing			§6.2.4	
		[ASM9]Deployment			§6.2.5	
[SR21]	Privacy and Cryptographic Controls: Protect the privacy of users and guaranty the confidentiality, authenticity or integrity of information (see §10.2 for more details). <u>Justification:</u> Eliminate (or at least reduce) the following risks:					
	[RSK5] Repudiation	[SM56] Define and implement EO Privacy Policy	N/A	N/A	N/A	§8.2.5
	[RSK7] Eavesdropping	[SM57] Provide network encryption	§4.4.2.3	§5.6.2.3	N/A	§8.4.2.3
	[RSK16] Accidental misrouting	[SM58] Use digital signature	§10.3	§5.8.2	N/A	N/A
		[SM59] Perform key management		§5.2.2.2	N/A	N/A
[SR22]	Software Maintenance: Maintain the security of application system software. <u>Justification:</u> Eliminate (or at least reduce) the following risks:					
	[RSK14] Software Programming Errors (business critical functions)	[SM60] Define and implement change control procedures	Following ISF Best Practices [R35] . Patch management aspects are however considered in §4.3.3.5 , §5.5.3.6 , and §8.3.3.5 .			
	[RSK15] Software Programming Errors (other functions)	[SM61] Impose restrictions on changes to software packages				
		[SM62] Perform technical reviews				
		[SM63] Protect software against covert channel and Trojan code				
		[SM64] Control outsourced software development				

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX A: COMPLIANCE MATRIX	

Table 9: EMCS Security Compliance Matrix

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

8. Appendix B: National Domain Security Guidance

8.1. Introduction

The security measures proposed hereafter should be compared with existing or planned safeguards in the Member State Administrations for the security area being considered. Those that are not in place, and are applicable, should be implemented. According to the ISF Standard [R35] (see §2.3.2) four main areas are considered: Security Management (see §8.2), EMCS National Domain Infrastructure (see §8.3), MSA Network Security (see §8.4), and NEA Development (see §8.5).

Note: 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 out of scope of this guidance.

8.2. Security Management

ISF building block (see §2.3.2): *Security Management*

8.2.1. Security Policy

Measure principle.....	A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the organisation information and systems.
Type	Mandatory.
Description	See below.

MSAs must comply with the guidance expressed in the EMCS Security Policy (SEP) [R3] and the CCN/CSI General Security Policy [R12] as far as NEA (either SEA or NDEA) is concerned. And each MSA must communicate (on a yearly basis) to the Central Project Management its EMCS Security Compliance Certificate as defined in [R3].

NEA security might also be subject to MSA internal policy and procedures. But this aspect remains a national matter, which is out of the scope of this guidance.

8.2.2. Security Organisation

Measure principle.....	Arrangements should be made to co-ordinate information security activity in business units/departments.
Type	Mandatory.
Description	See below.

In the National Domain, the EMCS security is managed through two main entities: the National EMCS Support and the National CCN Support. The National CCN Support is already in place in all MSA. The National EMCS Support has still to be set-up by each MSA participating to EMCS so as to provide for support services to local entities involved in the development of the National Excise System, MSA users, and Economic Operators.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

Note: The setting-up of the National EMCS Support is a national matter, which remains under the sole responsibility of every MSA.

8.2.3. Issuance of the EMCS Security Compliance Certificate & EMCS Security Measures Questionnaire

Measure principle.....	Arrangements shall be made to issue the EMCS Security Compliance Certificate and EMCS Security Measures Questionnaire
Type	Mandatory.
Description	See below.

As stipulated in the SEP [\[R3\]](#), each MSA *must* communicate its EMCS Security Compliance Certificate to the EMCS Central Project Management. In order to demonstrate compliance, the Compliance Certificate must be accompanied by a completed EMCS Security Measures Questionnaire (see 11.2 'EMCS Security Measures Questionnaire'). Lastly, an updated 'EMCS Security Measures Questionnaire' must be communicated to the Central Project Management every year.

The EMCS Security Compliance Certificate must be issued every three years or at every major milestone of the project, by a qualified organisation chosen by the MSA (but can also be an MSA internal organisational unit that is independent of the EMCS project team). This certificate can take the form of an official letter (see 11.1 Sample 'EMCS Security Compliance Certificate') and should stipulate the following:

- Confirmation by the representative of the certifying organisation that a compliance review was conducted of the EMCS project at the MSA.
- The review measured the degree of compliance of the EMCS project of the MSA to the security measures indicated in Section 8 of the EMCS Security Policy (SEP) and further specified in Appendix B of the Security Excise System Specifications (SESS) which are applicable the MSA environment.
 - Where security measures have been implemented, they are considered operationally effective.
 - Where security measures have not been implemented, the MSA has identified the risks and an appropriate action plan to manage these risks has been developed.
- The completed 'EMCS Security Measures Questionnaire' (as specified in Appendix E of the SESS) that accompanies the certificate indicates the most up-to-date implementation status of the MSA security measures.

The MSA should note that although it is only obliged to implement 'Mandatory' security measures, it is expected that 'Recommended' security measures will be implemented on a best-effort basis.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

8.2.4. Access Control Policy

Measure principle.....	Business requirements for access control shall be defined and documented, and access shall be restricted to what is defined in the access control policy. That policy shall address authentication and authorisation issues and shall be applicable to all users (including Economic Operators).
Type	Mandatory.
Description	See below.

Specification items to be considered by every MSA for the development of an Access Control Policy are listed hereafter ([Table 10](#)). The objective of this policy is to provide guidance for the reduction of the security risks identified in [\[R3\]](#), in particular:

- Illegitimate use of the EMCS system by MSA officials;
- Illegitimate use of the EMCS system by Economic Operators;
- Illegitimate use of the EMCS system by Contracted Service Providers;
- Illegitimate access to the EMCS system by Outsiders;
- Repudiation;
- Errors in using the EMCS application.

ISO Category #1: Security Policy	
Publication of Policy	The NISO [R3] must notify users, via both active (e.g. e-mail) and passive (e.g. web link) communications, of the MSA information protection policies. Communications should occur at least annually and/or whenever changes to the policy are made.
Publication of Advisories	Security advisories must be posted by NISO in a manner that ensures that all users (mainly MSA officials) who may be affected have access to these documents.
ISO Category #4: Personnel Security	
Periodic review of (physical) access rights	Physical access to all NEA-related facilities (e.g. servers, computer rooms) must be controlled with appropriate responsibility assigned for periodic inspection and review of security policies.
Security definition in third parties contracts	Data confidentiality, integrity, and availability controls will be specifically defined in contracts with third parties involved in the EMCS business (e.g. NEA development, exploitation, and maintenance). Controls will cover all appropriate physical, personnel, and logical information protection. In addition, controls will take into account all prevailing statutory and regulatory requirements.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

Include security concepts in job definition and resourcing	Security roles and responsibilities, as laid down in the MSA information security policy, shall be documented in job definitions. Guidance with regard to roles and responsibilities is provided in [R3] and [R12] .
Personnel screening and policy	Verification checks on permanent staff, contractors, and temporary staff shall be carried out at the time of job applications.
Confidentiality agreements	MSA officials shall sign a confidentiality agreement as part of their initial terms and conditions of employment.
Terms and conditions of employment	The terms and conditions of employment shall state the MSA Official responsibility for information security.
Reporting security incidents	Security incidents shall be reported through appropriate management channels as quickly as possible.
Reporting security weaknesses	Users of the EMCS system shall be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services.
ISO Category #7: Access Control	
Info access restriction according to the “Need To Know” principle	EMCS users (MSA officials, Economic Operators, contracted service providers) must be restricted to the information required to complete the assigned/contracted work.
Access rights review when user function changes	Network and application access levels must be reassessed for appropriateness when job functions change (e.g. transfers) or during MSA organisational changes (e.g., creation or merger of units, departments, etc.).
Limit privileged account to those who need it	Limit privileged access (e.g., admin, sysop, command line, root, etc.) to only those people who require it for their job function.
Report access abuse	Report in an immediate and urgent manner any attempt at unauthorised use of identification codes and passwords to the assigned security personnel, and, as appropriate, organisational management.
Audit of privileges	Auditing of private and/or confidential file and directory access must occur on a periodic basis.
Economic Operators must be uniquely registered	This point is further developed at section 8.3.4.2 .
NISO approval for remote access	All dial-in access and access via untrusted networks (e.g., ISPs, cable, application service providers, DSL connections, etc.) to national EMCS resources must use MSA approved access methods (e.g., Remote Access Server (RAS), SecureID, etc.).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

Justify need for Remote Access	Users must have a justifiable business case for remote access to national EMCS resources in order to be authorised for remote access by the NISO. Remote access includes all connections to NEA information system outside of MSA firewalls (e.g. controlled access points B and D on Figure 22).
Non-Official / Official access restrictions	Non-Official personnel (e.g. vendors, consultants, and contractors) must have at least the same access restrictions to which an MSA Official is subject.

Table 10: Access Control Policy

8.2.5. Economic Operators Privacy Policy

Measure principle.....	Responsibility for managing information privacy should be established and security controls for handling personally identifiable information applied.
Type	Recommended.
Description	See below.

The Privacy Policy applicable to Economic Operators shall be published on the MSA Portal, which is made available to Economic Operators to access NEA services.

The Privacy Policy aims at preventing information about individuals being used in an inappropriate manner, and ensuring compliance with legal and regulatory requirements for information privacy.

Therefore, there should be in the MSA documented standards/procedures for dealing with information privacy, which should cover:

- Acceptable use of personally identifiable information;
- The rights of individuals about whom personally identifiable information is held;
- Privacy assessment, awareness and compliance programmes;
- Legal and regulatory requirements for privacy.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

8.3. EMCS National Domain Infrastructure

ISF building block (see §2.3.2): *Computer Installation*

8.3.1. Installation Management

8.3.1.1. Roles and Responsibilities

Measure principle.....	An owner should be identified for the computer installation, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Type	Mandatory.
Description	See below.

8.3.1.1.1. NDCP Equipment

The European Commission (DG TAXUD) is the owner of the Common Domain equipment installed at every NDCP (with the exception of the CPR, which is leased to the network carrier). MSA obligations with regard to Common Domain equipment installed at the NDCP are described in [\[R18\]](#).

8.3.1.1.2. NEA Equipment

The MSA is the owner of the application platform hosting the NEA and is responsible for its operation and maintenance.

8.3.1.2. Asset Management

Measure principle.....	Essential information about hardware and software (e.g. version numbers, physical locations, etc.) should be recorded in inventories, and software licensing requirements met.
Type	Recommended.
Description	See below.

There should be documented procedures for asset management, which should cover:

- Acquisition of software/hardware;
- Software licensing;
- Recording of assets in an inventory (or equivalent);
- Archiving of information.

When acquiring hardware/software:

- They should be selected from a list of approved suppliers;
- Security requirements should be considered;
- High priority should be given to reliability in the selection process;
- Contractual terms should be agreed with suppliers.

8.3.2. Environment

The following guidance applies to the environmental security of the computing devices participating to EMCS.

8.3.2.1. Physical Security

Measure principle..... Physical security perimeter shall be implemented to protect critical computer installations. Physical access to the security perimeter shall be restricted to authorised individuals.

Type Mandatory.

Description See below.

The National Domain responsibility, as far as physical security is concerned, does not only cover National Domain equipment (i.e. application platforms running the NEA, network equipment, firewalls and other security equipment) but also the NDCP equipment (i.e. CCN Gateways, LCMS, firewall, encryption boxes, router, etc.), which are installed at the MSA premises.

[Figure 22](#) describes the National Domain network topology and indicates areas where physical security applies. The NDCP physical security perimeter corresponds to the part of the MSA Computer Room housing the Common Domain equipment. This part may be shared by or physically separated from other MSA IT equipment depending on national policies.

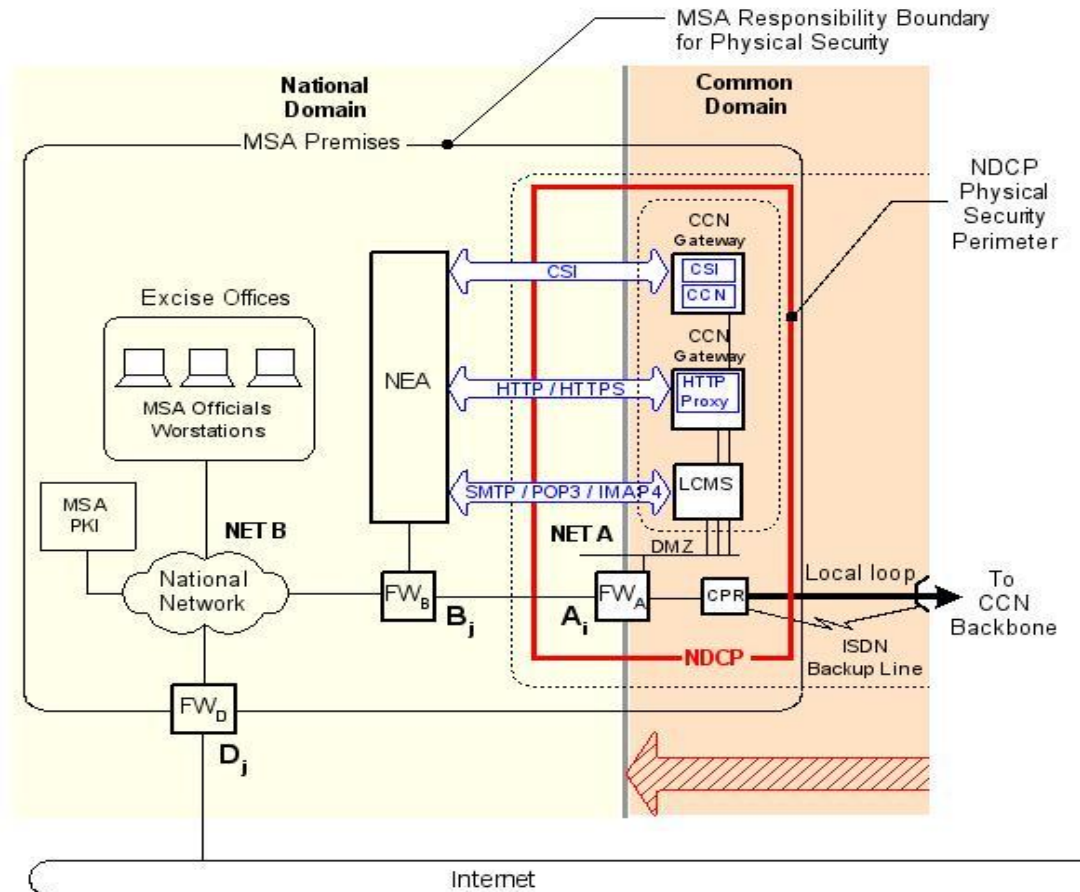


Figure 22: National Domain – Physical Security

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

[R18] provides the description of the procedures to be applied by the MSA to ensure the physical security of the NDCP equipment. Those procedures refer to implementation of physical security perimeter, physical entry controls, and isolation of delivery and loading areas from computer area.

8.3.2.2. Equipment Sitting and Protection

Measure principle.....	Computer equipment and facilities should be protected against fire, flood, environmental, and other natural hazards.
Type	Mandatory.
Description	See below.

Computer installations housing the NEA and NDCP equipment shall be located safely i.e. in an area with low risk of fire, flood, explosion, civil unrest, damage from neighbouring activities or natural disasters.

In particular, rooms housing the NEA and NDCP equipment shall be:

- Free from intrinsic fire hazards (such as paper or chemicals);
- Fitted with fire detection and suppression systems;
- Protected against the spread of fire.

8.3.2.3. Power Supplies

Measure principle.....	Critical computer equipment and facilities should be protected against power outages.
Type	Mandatory.
Description	See below.

The power supply to NEA and NDCP equipment shall be protected by:

- Fitting uninterruptible power supply (UPS) devices;
- Providing back-up generators (supplied with adequate fuel) in case of extended power failure;
- Installing emergency lighting in case of main power failure;
- Sitting emergency power-off switches near emergency exits to facilitate rapid power-down in case of an emergency;

8.3.2.4. Equipment Maintenance

Measure principle.....	Server equipment shall be correctly maintained to enable its continued availability and integrity.
Type	Mandatory.
Description	See below.

The MSA shall established contractual agreements (covering hardware maintenance aspects) with the providers of the NEA equipment installed at the MSA premises (maintenance of NDCP equipment being already covered by the European Commission (see §4.3.2.4)).

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

8.3.2.5. Provide security of equipment off-premises

Measure principle..... Use of equipment for information processing outside the organisation’s premises shall be subject to strict controls.

Type Mandatory.

Description See below.

Any use of equipment for information processing outside the MSA premises shall require authorisation by management. Once proper authorisation has been obtained, the physical security of the equipment and of the data it contains shall be ensured.

8.3.2.6. Secure disposal or re-use of equipment

Measure principle..... Information shall be erased from equipment prior to disposal or re-use.

Type Mandatory.

Description None.

The MSA shall make sure that information is erased from NEA equipment prior to disposal or re-use.

8.3.3. System Operation

8.3.3.1. Backup

Measure principle..... Back-ups of essential information and software used by the computer installation should be taken on a regular basis, according to a defined cycle.

Type Mandatory.

Description See below.

The Local System Administrator in the MSA is responsible for performing backups of the CCN Gateways and LCMS equipment. Therefore, backup procedures/systems already existing in the MSA can be applied to the backup of the CCN Gateways and LCMS.

[\[R18\]](#) provides the description of the backup policy, which is currently in use at the CCN/TC, and that is proposed to any MSA that has not yet defined its own backup procedures. It also provides the description of the backup activation procedure, the tape format characteristics, and the restore procedure.

8.3.3.2. Incident and Change Management

Measure principle..... All incidents of any type should be recorded, reviewed and resolved using an incident management process. Changes to any part of the computer installation should be tested, reviewed and applied using a change management process.

Type Recommended

Description See below.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

8.3.3.2.1. Incident Management

All incidents that affect the installation (including third party attack, internal party attack, internal misuse/abuse, malfunctions, loss of power/communications services, overloads and mistakes by users or computer staff) should be dealt with in accordance with an incident management process. Incidents should be:

- Reported to a single point of contact, such as a help desk, telephone hot line or individual IT specialist;
- Documented, typically using an automated incident management system;
- Categorised by type (e.g. malfunctions, malicious attack or internal abuse/misuse of systems);
- Prioritised according to their impact/urgency.

Patterns of incidents should be reviewed to identify potential security breaches and minimise the chances of similar incidents disrupting the installation in the future.

8.3.3.2.2. Change Management

The change management process should be documented and include:

- Approving and testing changes to ensure that they do not compromise security;
- Performing and signing-off changes to ensure they are made correctly and securely;
- Reviewing completed changes to ensure that no unauthorised changes have been made.

8.3.3.3. Media Handling

Measure principle..... Information held on data storage media (including magnetic tapes, disks, printed results, and stationery) should be protected against corruption, loss or disclosure and additional security controls applied to media containing sensitive information.

Type Mandatory.

Description See below.

The MSA shall ensure that data storage media (including magnetic tapes, hard disks, and printed documentation) is handled in accordance with documented standards/procedures.

8.3.3.4. Protection Against Malicious Software

Measure principle..... Virus protection arrangements should be established and maintained organisation-wide.

Type Mandatory.

Description See below.

There shall be in the MSA documented standards/procedures for providing protection against viruses, which shall specify:

- Methods for configuring virus protection software;
- Update mechanisms and frequencies for virus protection software;

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

- A process for dealing with virus attacks.
 - The risk of virus infection should be reduced by:
 - Evaluating virus protection software prior to purchase;
 - Installing virus protection software on servers, mail gateways, and workstations, including laptop computers and handheld computing devices (e.g. PDAs);
 - Updating virus definitions used by virus protection software whenever a new version is released;
 - Distributing virus protection updates to key servers automatically and within a critical timescale;
 - Implementing emergency procedures for dealing with virus incidents;
 - Monitoring external media sources for intelligence of new virus threats;
 - Making third parties aware of MSA's virus protection standards/procedures.

8.3.3.5. Patch Management

Measure principle.....	There should be a strategy for patch management that should be supported by a management framework and a documented patch management process.
Type	Recommended
Description	See below.

A patch management process should be established by the MSA and should:

- Determine methods of obtaining patches;
- Specify methods of validating patches (e.g. ensuring that the patch is from an authorised source);
- Identify vulnerabilities that are applicable to the installation;
- Assess the business impact of implementing patches (or not implementing a particular patch);
- Ensure all patches are tested against known criteria;
- Describe detailed deployment methods for patches (e.g. software distribution tools) report on the status of patch deployment across the installation;
- Include methods of dealing with a patch failure be documented and approved.

8.3.3.6. MSA Officials Workstation Security

Measure principle.....	Workstations connected to systems within the computer installation should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.
Type	Mandatory.
Description	See below.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

The following specification items apply to workstation security:

- MSA officials must authenticate to their workstation before being granted access to the network resources and applications.
- Workstation must be locked following expiration of an inactivity timer to prevent unauthorised access.
- Workstations must be correctly configured and maintained (security patches, anti-virus library) to optimise anti-virus protection.
- If the workstation is connected to a public network (e.g. internet) and to the Common Domain, it provides a potential route for security breaches. To prevent this vulnerability, network isolation devices such as firewalls (i.e. FW_D and FW_B on [Figure 22](#)) must be implemented to guarantee the segregation of networks and network routing control.

Workstations will be procured in accordance with MSA procurement policy.

8.3.4. Access Control

8.3.4.1. Registration of MSA Users

Measure principle.....	MSA users shall be registered before they are granted access privileges.
Type	Mandatory.
Description	See below.

The registration of MSA Users is the process through which an authorised MSA Official gets registered in the local CCN Directory as “CCN User” so as to be able to use EMCS applications made available through the CCN Network. Refer to §[4.3.4.2](#) and §[4.3.4.3](#) for more details.

8.3.4.2. Registration of Economic Operators

Measure principle.....	Economic Operators shall be registered before they are granted access privileges.
Type	Mandatory.
Description	See below.

The registration of Economic Operators (EO) is the process through which an EO gets registered in the national SEED directory by its ruling administration.

This registration process is let to the MSA responsibility and varies from one MSA to another. In most cases, the MSA performs some verification work requiring an EO representative to present proof of his real-world’s identity (such as birth certificate, passport) as well as a certified copy of the company legal status.

However, the deployment of National Excise Applications (either centrally or nationally developed) in the MSA and therefore the gradual introduction of the electronic-based exchanges between EO and MSA may have an impact on the way EO will be registered.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

The main change that is anticipated concerns the fact that electronic credentials will have to get delivered to the users of the system (whatever their type: human user or machine) to ensure their unicity during the electronic authentication phase.

The specification items to be considered for the electronic credentials delivery process are listed hereafter:

- A Registration Authority (RA) and a Credential Service Provider (CSP) must be present in one way or another to complete the registration process. Those entities can either be MSA internal organisational units or external relying parties (e.g. PKI services provider).
- Two additional processes must be implemented:
 - **Identity Proofing:** this is the process of ensuring that an EO identity is actually a real person, with correctly associated attributes (perhaps only a name). Increasing levels of assurance require increasing effort to establish the identity of the subscribing EO. The entity that does the identity proofing is the Registration Authority (RA).
 - **Credentials delivery:** the Credential Service Providers (CSP) provides the subscribing EO a token to be used in an authentication protocol and issues credentials as needed to bind that token to the EO identity, or to bind the EO identity to some other useful attribute (e.g. company name).

8.4. MSA Network Security

ISF building block (see §2.3.2):*Networks*

8.4.1. Network Management

8.4.1.1. Roles and Responsibilities

Measure principle.....	An owner shall be identified for the network, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Type	Mandatory.
Description	See below.

The MSA is responsible for the proper running and maintenance of the MSA Network so as to comply with the availability requirements of the EMCS systems.

If required, the MSA will adapt the existing network infrastructure so as to support the NEA according to the present security specifications.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

8.4.2. Traffic Management

8.4.2.1. Network Routing Control (Enforced Path)

Measure principle.....	Networks shall have routing controls to ensure that computer connections and information flows do not breach the access control policy.
Type	Recommended.
Description	See below.

Network devices shall be restricted to use by authorised network staff using access controls that support individual accountability, and protected from unauthorised access.

Routers (i.e. network devices that perform routing) shall be configured to prevent unauthorised or incorrect updates by:

- Verifying the source of routing updates, for example by using software tools such as OSPF (Open Shortest Path First) or RIP (Routed Internet Protocol);
- Verifying the destination of routing updates (e.g. by transmitting updates only to specific routers);
- Protecting the exchange of routing information (e.g. by using password);
- Encrypting the routing information being exchanged.

8.4.2.2. Firewalls

Measure principle.....	Network traffic should be routed through a firewall, prior to being allowed access to the network.
Type	Mandatory.
Description	See below.

[Table 11](#) provides the list of CAP related to the National (and also External Domains), where firewalls shall be implemented.

CAP	Responsibility	Description
B_j (2)	National Domain	Protection against unwanted accesses coming from the CCN/CSI network.
D	National Domain	Protection against unwanted accesses coming from the outside world (e.g. Internet).
E_k (3)	External Domain	Protection against unwanted accesses coming from the outside world (e.g. Internet).
(2)	$j \in [1, 35]$ (35 sites in 29 countries).	
(3)	$k \in [1, \infty[$ (Number of Economic Operators per MSA depends on the MSA importance in the Excise business, but could be potentially very high e.g. more than 30 000 for France).	

Table 11: Controlled Access Points – National Domain and External Domain

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

8.4.2.3. Network Encryption

Measure principle.....	Network encryption should be applied to protect the confidentiality of sensitive or critical information during transit over networks.
Type	Recommended.
Description	See below.

Network encryption, although recommended, is not imposed on the MSA network.

8.5. NEA Development (NDEA)

ISF building block (see §2.3.2): *System Development*

The development of applications (e.g. NDEA) in the National Domain is an internal matter under the MSA’s responsibility. Compliance with FESS contents is however required. It is recommended that the MSAs follow the best practices indicated by the ISF Standard [R35] to achieve these goals.

8.5.1. Development Management

Producing robust NDEA systems, on which the MSA organisation can depend, requires a sound approach to systems development, including:

- Organisation of systems development staff,
- Methodology used in developing systems,
- Quality assurance, and
- Security of development environments.

It is recommended that the MSAs follow the best practices indicated by the ISF and ISO Guidance to achieve these goals.

8.5.2. Requirements Definition

A thorough understanding of business requirements (including those for the confidentiality, integrity and availability of information) is essential for NDEA to fulfil their intended purpose. Accordingly, MSA have to make the necessary arrangements for:

- Specifying business requirements,
- Determining security requirements, and
- Conducting risk assessments.

Among those aspects, two of them are of a particular relevance: Application Access Control and Secure Audit Log (SAL). There are shortly presented below.

8.5.2.1. Application Access Control

Specification items to be considered on the NDEA side to implement access control facilities are listed hereafter:

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

- It must be made impossible to log into the NDEA while bypassing the identification and authentication procedures by the use of, for example stored passwords, “back” button, URL manipulation, cookies.
- On the NDEA side, the identification and authentication procedures are mandated steps for every session initiated by a requestor.
- Access restrictions (e.g. based on user profile) must be defined to prevent unauthorised access to information handled by the NDEA.
- It should not be allowed to forward information to Economic Operators (e.g. e-AAD) by unsecured e-mail.

8.5.2.2. Secure Audit Logs (SAL)

The implementation of Secure Audit Logs (SAL) at NEA level is a recommendation (not a mandatory requirement). The decision to implement it (or not) remains under MSA responsibility.

According to the SEA architecture (see *TESS Section IV [R9]*), MSA Users and Economic Operators access the NEA services through a single entry point, the *Portal Services* (see [Figure 23](#)).

Consequently, this entry point is the best place to record the exchanges between the consumers and the provider (NEA) of the EMCS Services.

The recorded information should be protected in order to prevent accidental or deliberate modifications. This is achieved by using *Secure Audit Logs (SAL)*.

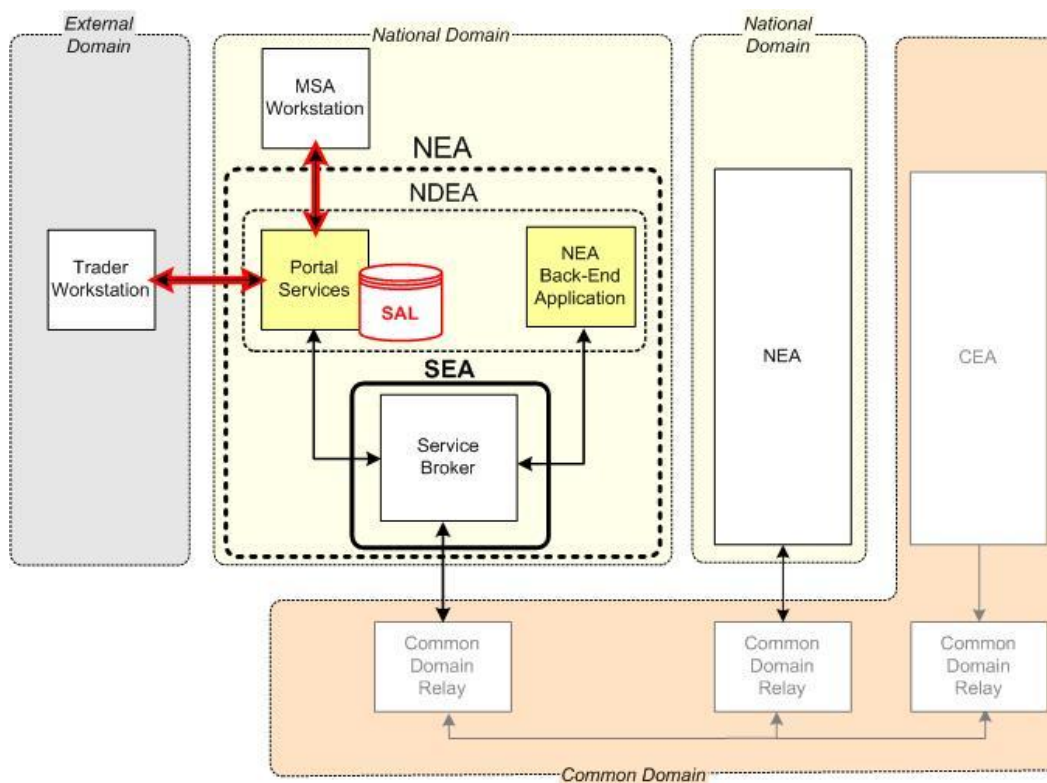


Figure 23: Secure Audit Logs (SAL)

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX B: NATIONAL DOMAIN SECURITY GUIDANCE	

SAL must provide strong cryptographic assurances that data stored by the logging facility before a system compromise cannot be modified after the compromise without detection.

To achieve that, the system should establish a small “secret” at log creation time and stored somewhere safe on a separate trusted computer.

The secret stored on the computer is the head of a hash chain, changing via a cryptographic one-way function every time an entry is written to the log. This secret is used to compute a cryptographic message authentication code (MAC) for the log each time an entry is added, and optionally to encrypt the log as well.

If the system is compromised, the attacker has no way to recover the secrets used to create the MACs or decryption keys for entries in the log, which have already been completed.

The attacker could eventually delete the log entirely, but could not modify it without detection. Later, the administrator can use the original secret to recreate the hash chain and check whether the logs are still intact. To keep an attacker from interfering with this process, this should happen on a separate, secure machine.

MACs may also be sent to another machine as they’re written; then they can serve as commitments to log entries. The MACs of each submitted draft e-AAD, for instance, could be sent to an auditing agency. Later, it is possible to prove the message match the MACs the system sent out. But otherwise, the auditor would have no way of knowing what the messages were. The system is protected from accusations of fraud, and the Economic Operator’s privacy (see §8.2.5) is protected.

Moreover, significant improvement would consist of the use public key cryptography. Using the symmetric techniques just described before, any entity that wishes to verify a log must possess the secret used to create the MACs. This secret gives the entity the ability to falsify log entries as well, which could be a major drawback in applications. Public key cryptography allows signatures to be created with one key and verified with a different one. Such signatures can be used in place of MACs to allow verification of a log without the ability to modify it, as well as allowing publication of the initial key used to create the log, since only the public key is needed for verification.

In order to prevent deletion, it is also useful to include measures for storing the log entry using media, which cannot be rewritten.

Note: Refer to [\[R44\]](#) for more information on how to build an encrypted and searchable audit log.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX C: WEB SERVICE CHANNEL SECURITY – AUTHENTICATION AND AUTHORISATION SCHEME	

9. Appendix C: Web Service Channel Security – Authentication and Authorisation Scheme

The authentication and authorisation scheme specifications that are provided below should serve as an input to the detailed design phase.

It shows how a two-factor based authentication can be implemented to access CEA backend applications resource in full compliance with the current CCN implementation and policy.

[Table 12](#) provides information about the sequences illustrated in the diagrams provided hereafter ([Figure 25](#) to [Figure 28](#)). Those diagrams should be read together. They have been split in 4 parts for a better readability.

Sequence	Description
L	CCN Access Control Phase: <ul style="list-style-type: none"> • 1st factor (UserID/Password-based) authentication; • Authorisation.
M	CEA Access Control Phase: <ul style="list-style-type: none"> • 2nd Factor (Certificate-based) authentication; • Authorisation.
S to T	Standard exchange of an authenticated and authorised HTTP request
U to V	Standard exchange of an authenticated and authorised HTTPS request

Table 12: Authentication and Authorisation Scheme – Sequences

The convention adopted in these diagrams to differentiate HTTPS exchanges from HTTP exchanges is shown below ([Figure 24](#)):

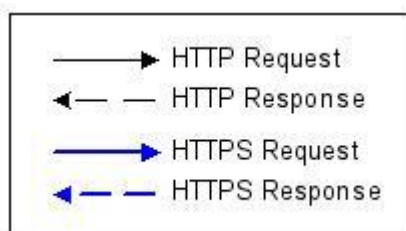


Figure 24: Arrows conventions

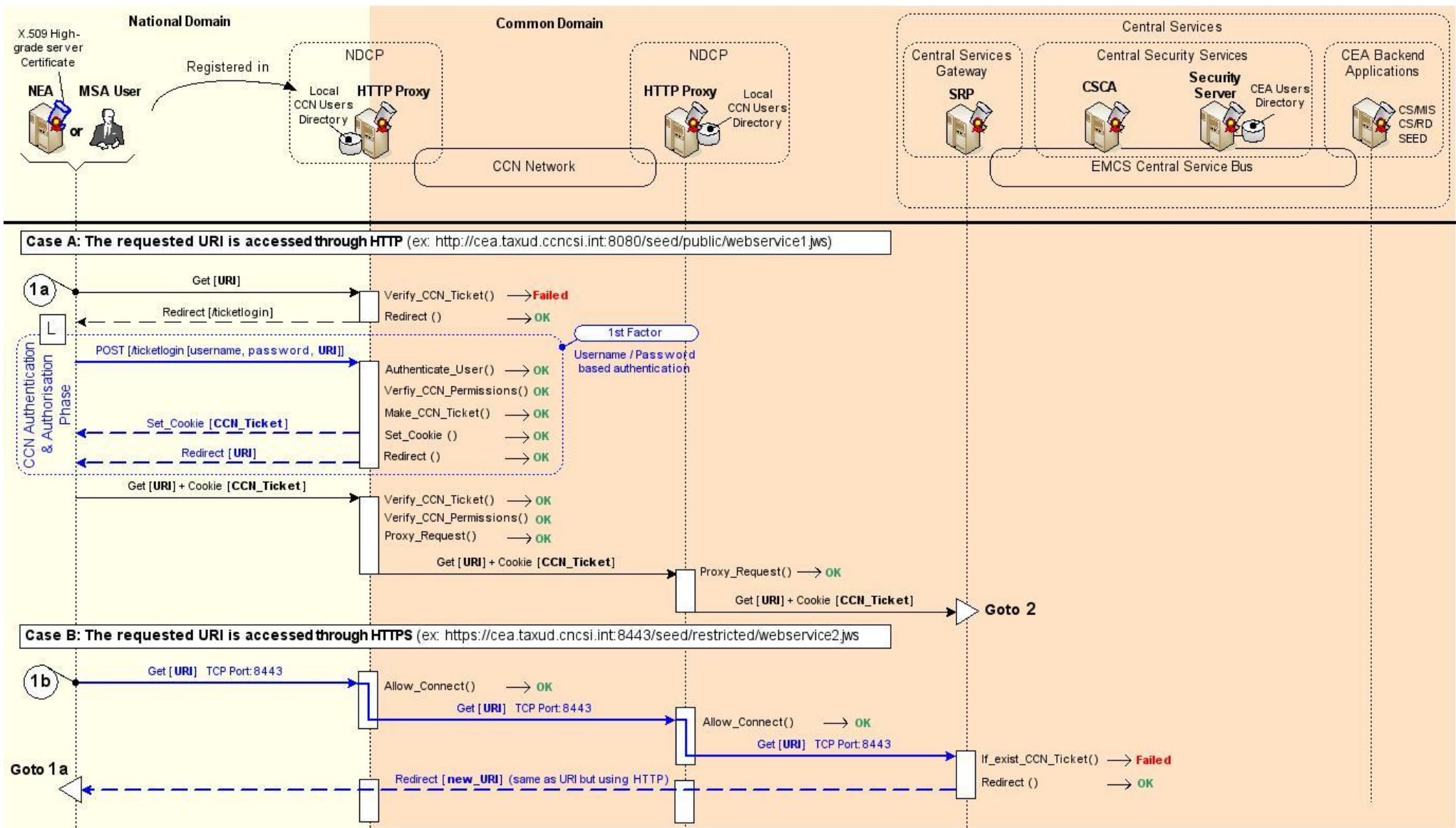


Figure 25: Web Service Channel Security – Authentication and Authorisation (Part 1)

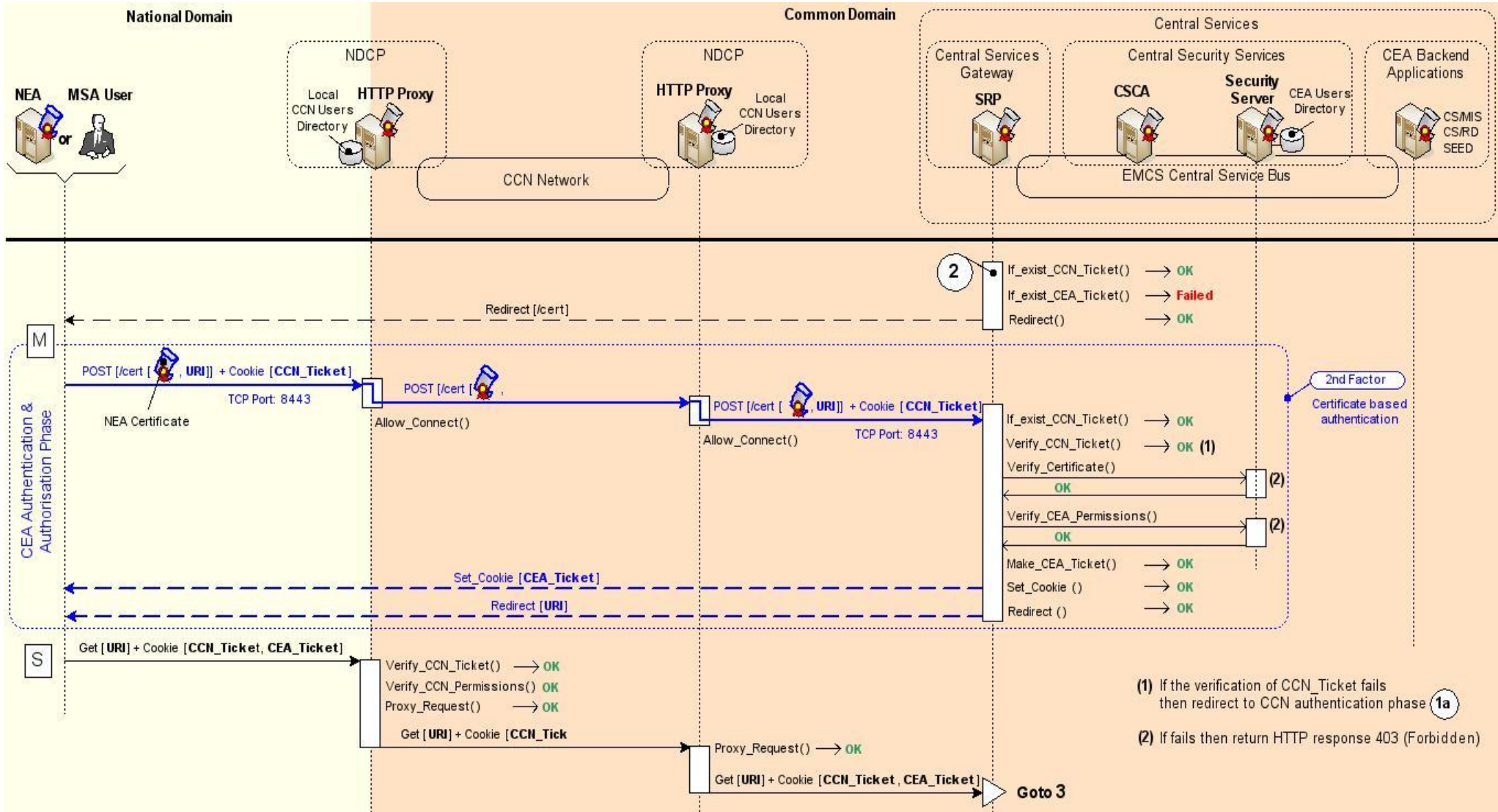


Figure 26: Web Service Channel Security – Authentication and Authorisation (Part 2)

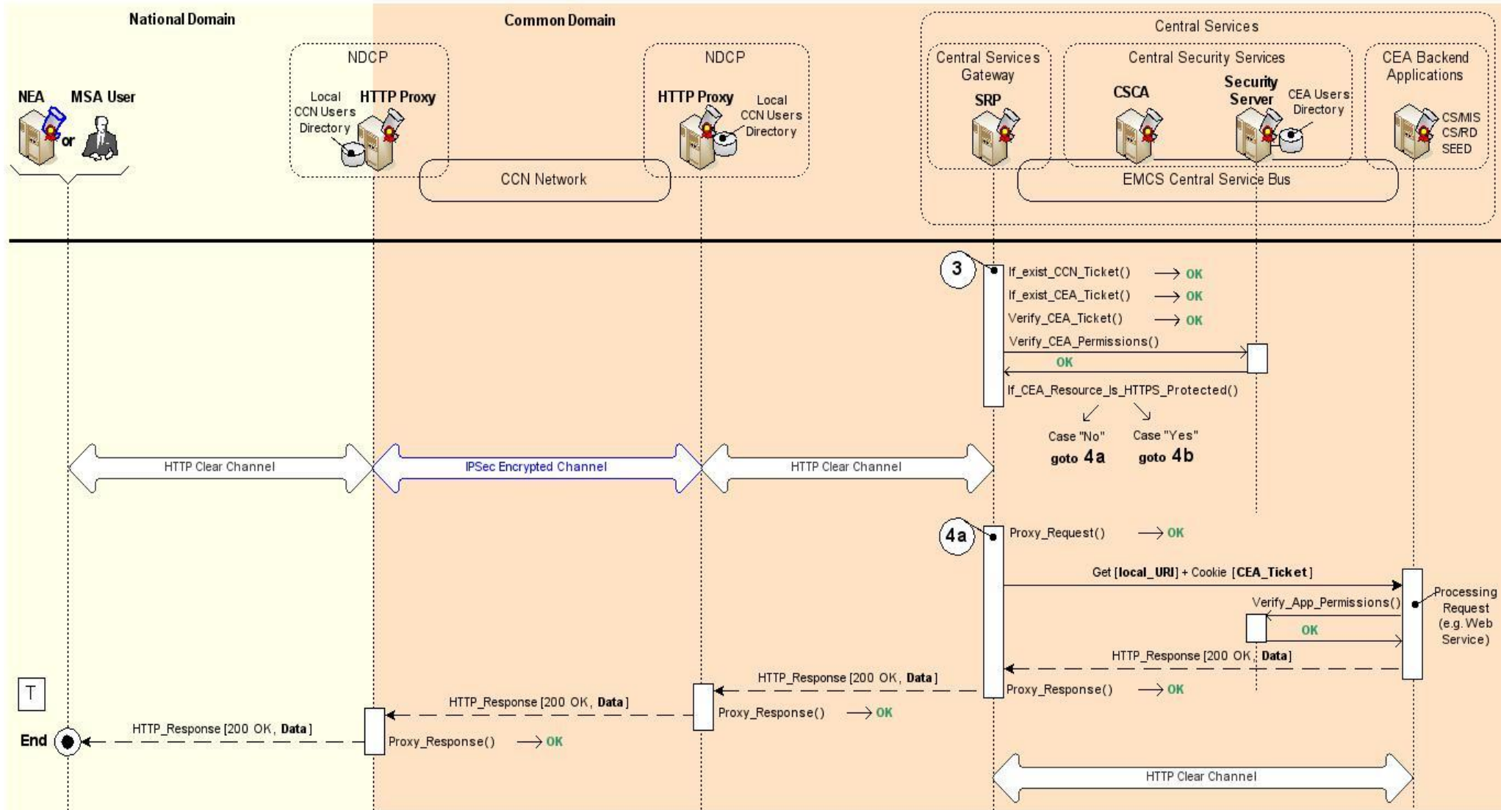


Figure 27: Web Service Channel Security – Authentication and Authorisation (Part 3)

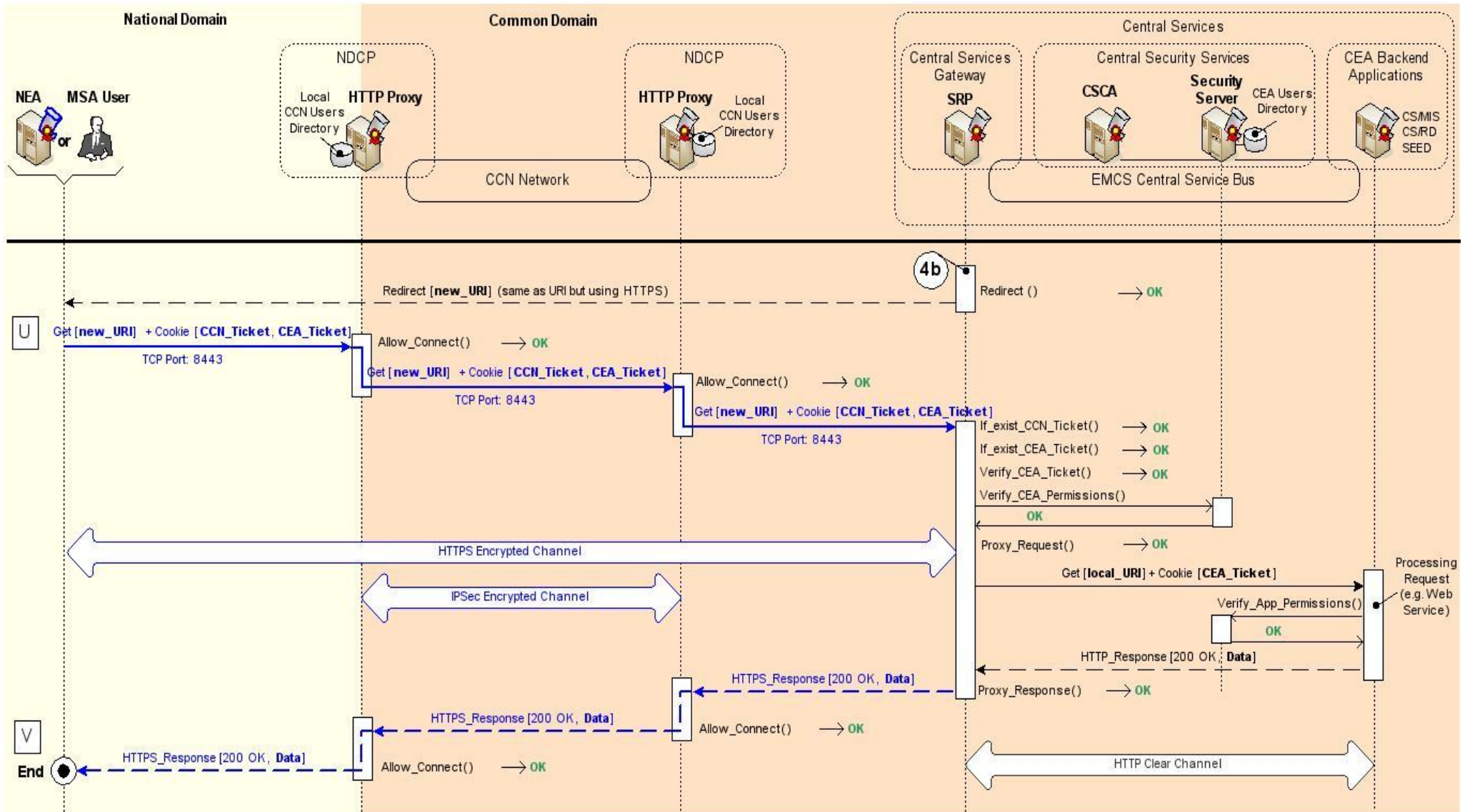


Figure 28: Web Service Channel Security – Authentication and Authorisation (Part 4)

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

10. Appendix D: Proposal for the EMCS Common Domain PKI (CDPKI)

10.1. Introduction

The activities carried out during the elaboration of the FESS [\[R4\]](#) and the TESS [\[R9\]](#) allowed to precise the cryptographic controls requirements that *should* be met by the EMCS target system. These requirements are gathered under the label [\[SR21\]](#) in the SEP and are further detailed in §[10.2](#).

Those requirements are usually well served by a Public Key Infrastructure (PKI). This is the reason why a description of the infrastructure that *could* be implemented to meet those requirements is proposed hereafter (see §[10.3](#)). This infrastructure is called “*EMCS Common Domain PKI (CDPKI)*”.

Note: MSA representatives must confirm those requirements through an appropriate ad-hoc working group before it can be decided to go further in the EMCS CDPKI implementation. In the meantime, the EMCS CDPKI will remain at the state of *proposal* without any impact on the EMCS master project plan.

10.2. Cryptographic Controls Requirements

10.2.1. Strong Authentication [\[SR21.1\]](#)

Strong authentication (i.e. 2-factor based), which is required to securely authenticate MSA Users and NEA applications accessing CEA services (SEED, CS/RD, CS/MIS) through the HTTP channel – the CCN/CSI channel being used by applications *only* and considered as secure enough with regards to the authentication mechanism already in place (see §[4.3.4.4.1](#)).

The business channels concerned by the strong authentication requirement are:

- [\[BCC6\]](#) NEA to SEED
- [\[BCC12\]](#) NEA to EMCS CS/RD
- [\[BCC19\]](#) NEA to CS/MIS
- [\[BCC9\]](#) MSA Users to SEED
- [\[BCC11\]](#) MSA Users to EMCS CS/RD
- [\[BCC23\]](#) MSA Users to CS/MIS

Measures implementing strong authentication should consider the usage of username/password (1st factor) to access the CCN network services and the usage of X.509 Certificates (2nd factor) by both NEA and MSA users to transparently and securely access CEA services.

Note: Similar requirement may be encountered by MSAs wishing to securely authenticate Economic Operators accessing the NEA. This issue remains however a national matter, which is out of the scope of the SESS. There are also examples of successful implementation of certificate-based authentication mechanisms in the e-Customs area.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

10.2.2. Shared Identity between National and Common Domains [SR21.2]

An MSA Official who has already received an X.509 certificate from its administration to access national services could use this same certificate to access EMCS Central Services (and not a second certificate delivered by an accredited EC certification authority).

This means that a trust relationship has to be established between MSA PKIs and the EMCS Common Domain PKI (CDPKI) as proposed in §10.3.4.

The business channels concerned by the cross-organisational unique identity requirement are:

- [\[BCC6\]](#)NEA to SEED
- [\[BCC12\]](#)NEA to EMCS CS/RD
- [\[BCC19\]](#)NEA to CS/MIS
- [\[BCC9\]](#)MSA Users to SEED
- [\[BCC11\]](#)MSA Users to EMCS CS/RD
- [\[BCC23\]](#)MSA Users to CS/MIS

10.2.3. Secure Audit Logs (SAL) [SR21.3]

To provide a legally valid proof of an illegitimate use of the system by EMCS users or applications, every NEA should produce audit logs that are protected in order to prevent accidental or deliberate modifications. This protection is obtained by the cryptographic assurance that data stored by the logging facility before a system compromise cannot be modified after the compromise without detection. This is achieved by the implementation of Secure Audit Logs (SAL). Although being a national matter, technical options regarding the production of these logs will be considered in Appendix B §8.5.

The business channels concerned by the secure audit log requirement are:

- [\[BCC1\]](#)Economic Operator to NEA
- [\[BCC2\]](#)NEA to NEA
- [\[BCC3\]](#)NEA to Economic Operator
- [\[BCC4\]](#)NEA to MSA User
- [\[BCC5\]](#)MSA User to NEA
- [\[BCC6\]](#)NEA to SEED
- [\[BCC7\]](#)SEED to NEA
- [\[BCC10\]](#)EMCS CD/RD to NEA
- [\[BCC12\]](#)NEA to EMCS CS/RD
- [\[BCC19\]](#)NEA to CS/MIS
- [\[BCC20\]](#)CS/MIS to NEA

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

10.2.4. Excise Movement Authenticity [SR21.4]

Although not explicitly mentioned in the FESS [R4], there might be a need for MSAs to get the assurance that an excise movement agreed upon between two Economic Operators (i.e. the consignor and the consignee) will not lead to a fake movement.

A way to address this issue could consist in obtaining from the Economic Operators involved in an excise movement a document informing about the nature of the agreed movement (e.g. product, volumes, place of dispatch, place of destination, etc.) that would be digitally signed by both operators (Figure 29).

This document would be attached to the draft e-AAD (or might form part of the draft e-AAD, or be referenced by it) submitted by the consignor and checked by the MSA at Dispatch prior to the delivery of a valid e-AAD.

The verification of both consignor and consignee digital signatures could be achieved automatically by the NEA.

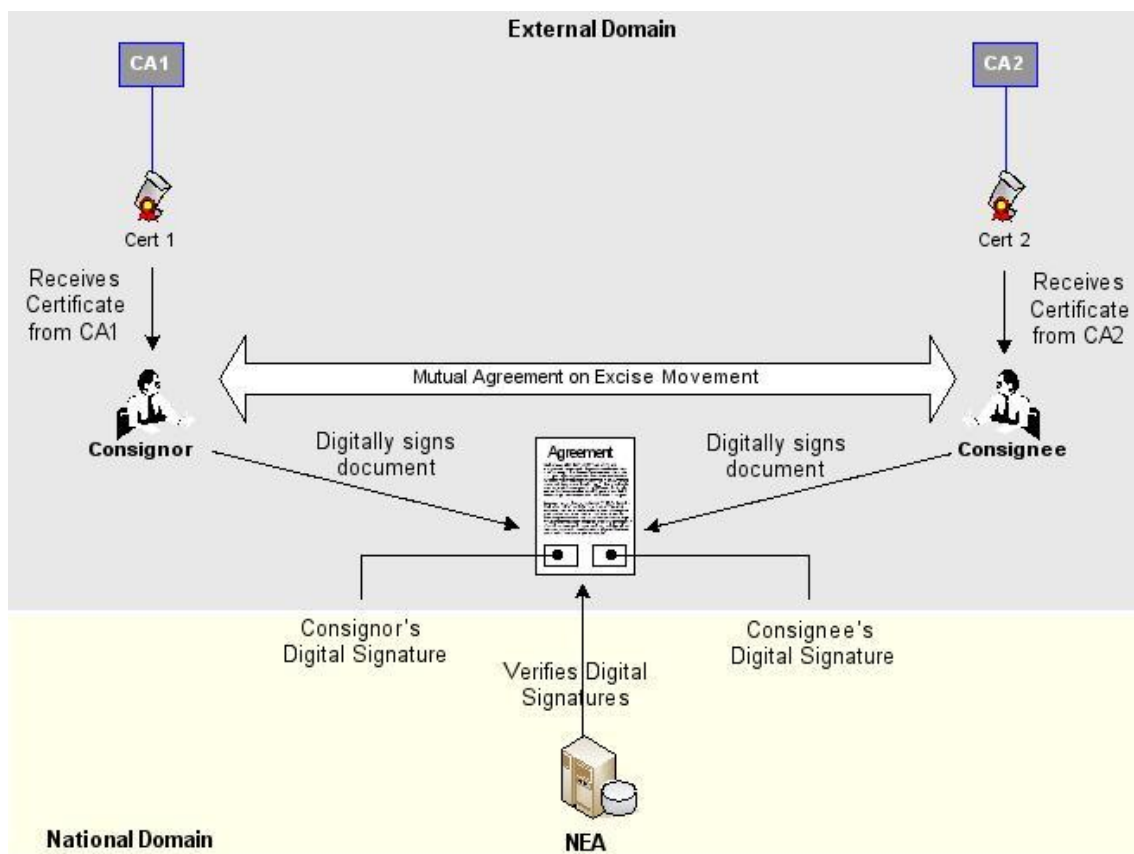


Figure 29: Excise Movement Authenticity - Digital Signature

There are also other use cases where digital signature could apply to assess the authenticity of the excise movement. For instance, the digital signature could be applied:

- By the Consignor to the draft e-AAD before submitting it to the NEA for validation;
- By the Consignee to the Report of Receipt to confirm that he has received the goods;
- By the (MSA of dispatch) NEA to ensure message-level integrity during its transit through the Common Domain.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

The business channels concerned by the excise movement authenticity requirement are:

- [\[BCC1\]](#)Economic Operator to NEA
- [\[BCC2\]](#)NEA to NEA
- [\[BCC3\]](#)NEA to Economic Operator
- [\[BCC15\]](#)MSA User to Economic Operator

Note: The mutually signed agreement between the Consignor and the Consignee might not be necessarily needed, since every data of the agreement should be present in the e-AAD. And if the Consignee is not involved in the consignment, he has to immediately indicate this fact to his competent authority, which can make the needed arrangement. In this case the Consignor (guarantor) is responsible for the consignment. Regarding those facts, it might be enough if only the Consignor digitally signs the e-AAD, hence allowing the consignment to get verified immediately.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

10.3. EMCS Common Domain PKI (CDPKI)

ISF building block (see §2.3.2):*Security Management*

10.3.1. Problem Statement

Many MSAs are deploying or are using existing governmental Public Key Infrastructure (PKI) to support internal business processes, implement virtual private networks, and secure corporate assets. In addition, some MSAs have also established a business partnership with external parties (e.g. Economic Operators). If MSAs wish to exploit their electronic capability for business-to-business applications e.g. to transparently access EMCS Central Services, *$n \times (n-1)$ trust relationships between national PKIs will be required.*

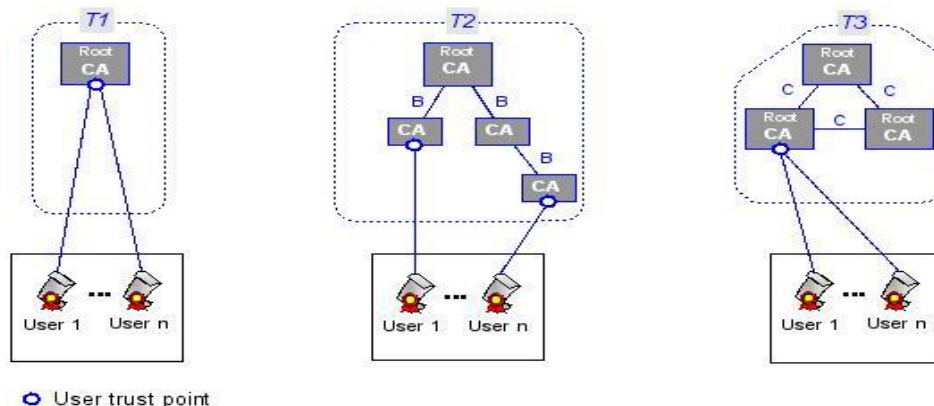
However, national domain PKIs may implement different architectures, security policies, and cryptographic suite, which make the interoperability between those PKIs almost impossible considering the high number of PKIs communities to interconnect. Therefore a flexible mechanism is needed to link these PKIs.

Within a PKI, a normalised data structure called *X.509 certificate* is used to bind a specific identity to a specific public key and information on how the public key can be used (e.g. SSL server certificate, e-mail signer certificate, etc.). *Certification Authorities (CA)* are trusted entities that issue certificates to users within a PKI and provide status information about the certificates the CA has issued.

Today, PKI architectures encountered in the MSAs (and Economic Operators) fall into one of the three configurations illustrated at the [Figure 30](#):

- A single CA (T1), or
- A hierarchy of CAs (T2), or
- A mesh of CAs (T3).

Each of the configurations is determined by fundamental attributes of the PKI: the number of CAs in the PKI, the links between CAs in a hierarchy of CAs (links labelled “B” on the figure), where users of the PKI place their trust (known as *user trust point*¹¹), and the trust relationships between CAs within a multi-CA PKI (links labelled “C” on the figure).



¹¹ The user trust point corresponds to the CA that effectively signed the user certificate.

Figure 30: PKI Architecture Types

To allow interoperability between MSAs, isolated CAs shall be combined to form larger PKIs. The two basic ways to achieve this is using superior-subordinate relationships, or peer-to-peer relationships (Figure 31). In theory, any organisational structure can be realised using either of the two methods.

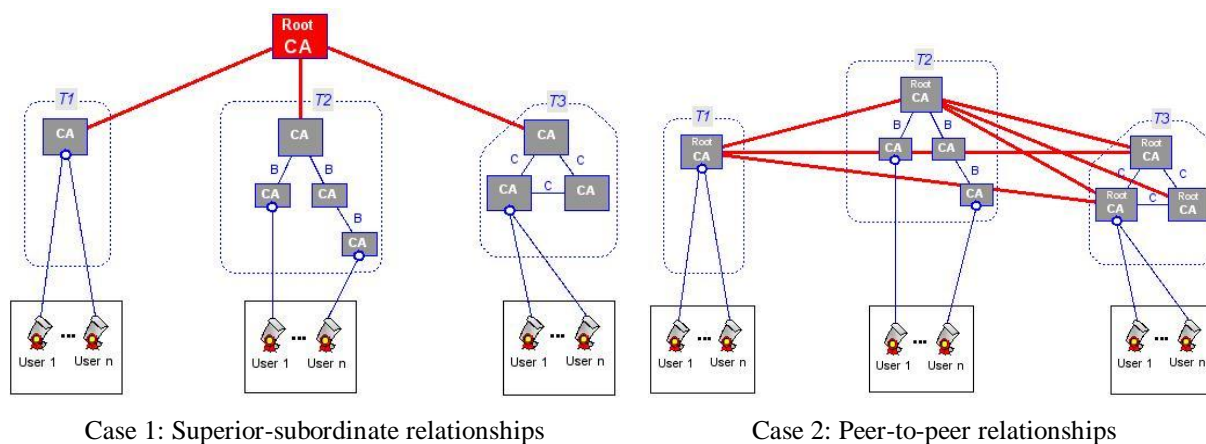


Figure 31: CA Combinations

In practice, however, there are technical and political issues encountered when architecting organisational PKIs. Each method has its strengths and weaknesses. For large, more complex organisations such as the one encountered within EMCS, none of those methods can provide a satisfactory result.

Indeed, in a PKI constructed with superior-subordinate relationships (Case 1) provides a good scalability and easy to develop certification paths (unidirectional) but presents some drawbacks resulting from the reliance on a single trust point; the compromise of a “root” CA, everyone’s trust point, results in a compromise of the entire PKI.

Worse yet, there are no straightforward recovery techniques. The nature of a hierarchical PKI is that all trust is concentrated in the “root” CA and failure of that trust point is catastrophic. Another drawback is that agreement on a single “root” CA may be politically impractical because all MSAs must adjust their trust points.

PKI constructed with a peer-to-peer relationship (Case 2) presents the advantage of being very resilient (no single point of failure): CAs issue certificates to each other and since the CAs have peer-to-peer relationships, they cannot impose conditions governing the types of certificates other CAs can issue.

Moreover, mesh PKI can easily incorporate a new community of users; any one of the CAs in the mesh simply establishes a trust relationship with that community’s CA. But mesh PKIs presents some drawbacks resulting from the bi-directional trust model: certification path development is more complex than in a hierarchy. This makes path discovery more difficult since there are multiple choices.

Users in a mesh PKI must also determine which application a certificate may be used for (e.g. access to SEED database) based on the contents of the certificates rather than the CA’s location in the PKI. This requires larger and more complex certificates and more complicated certificate path processing.

DG TAXUD – EXCISE COMPUTERISATION PROJECT	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

To address the shortcomings of the two basic PKI architectures presented above while answering the requirements expressed in §10.2, we propose to implement a *Bridge Certification and Validation Authority (Bridge CA/VA)* architecture as part of the Common Domain Public Key Infrastructure services (CDPKI). An overview of the CDPKI architecture is provided in the §10.3.2.

10.3.2. Architecture

10.3.2.1. Basic Principle

According to §10.3.1, a key component of the EMCS CDPKI is the *Bridge Certification and Validation Authority (Bridge CA/VA)*.

The Bridge CA/VA architecture is designed to link PKIs that implement different architectures such as the ones encountered in the MSAs.

Unlike a mesh PKI, the Bridge CA/VA does not issue certificates directly to users. In addition the Bridge CA/VA will not be used as a trust point by the users of the PKI, unlike the “root” CA in a hierarchy.

The Bridge CA/VA establishes peer-to-peer trust relationships with the different user communities participating to EMCS, which elevates political issues between organisations and *allows the MSAs to keep their natural trust points*.

These relationships are combined to form a “bridge of trust”, enabling users from the different MSAs to interact with each other through the BCA with a specified level of trust.

So, if a MSA decides to implement a trust domain in the form of a hierarchical PKI, the Bridge CA/VA will establish a relationship with the PKI’s “root” CA.

If an MSA decides to implement a trust domain by creating a mesh PKI, the Bridge CA/VA only needs to establish a relationship with one of the PKI’s CAs.

In either case, the CA of the PKI that enters into a trust relationship with the Bridge CA/VA is termed a *Principal CA* (Figure 32).

A PKI created with a Bridge CA/VA is often called a “*hub-and-spoke*” PKI¹². The Bridge CA/VA links the national PKIs at a single, known hub that could be hosted and managed centrally as part of the EMCS Central Services.

Note: The proposed architecture should be further consolidated based on existing implementations / studies (e.g. the IDA Bridge/Gateway CA Feasibility Study available at <http://ec.europa.eu/idabc/servlets/Doc?id=17267>) before being submitted to MSAs for approval.

¹² Refer also to [R39] for reference documentation about the Bridge CA implementation performed within the framework of the US Federal Public Key Infrastructure (FPMI).

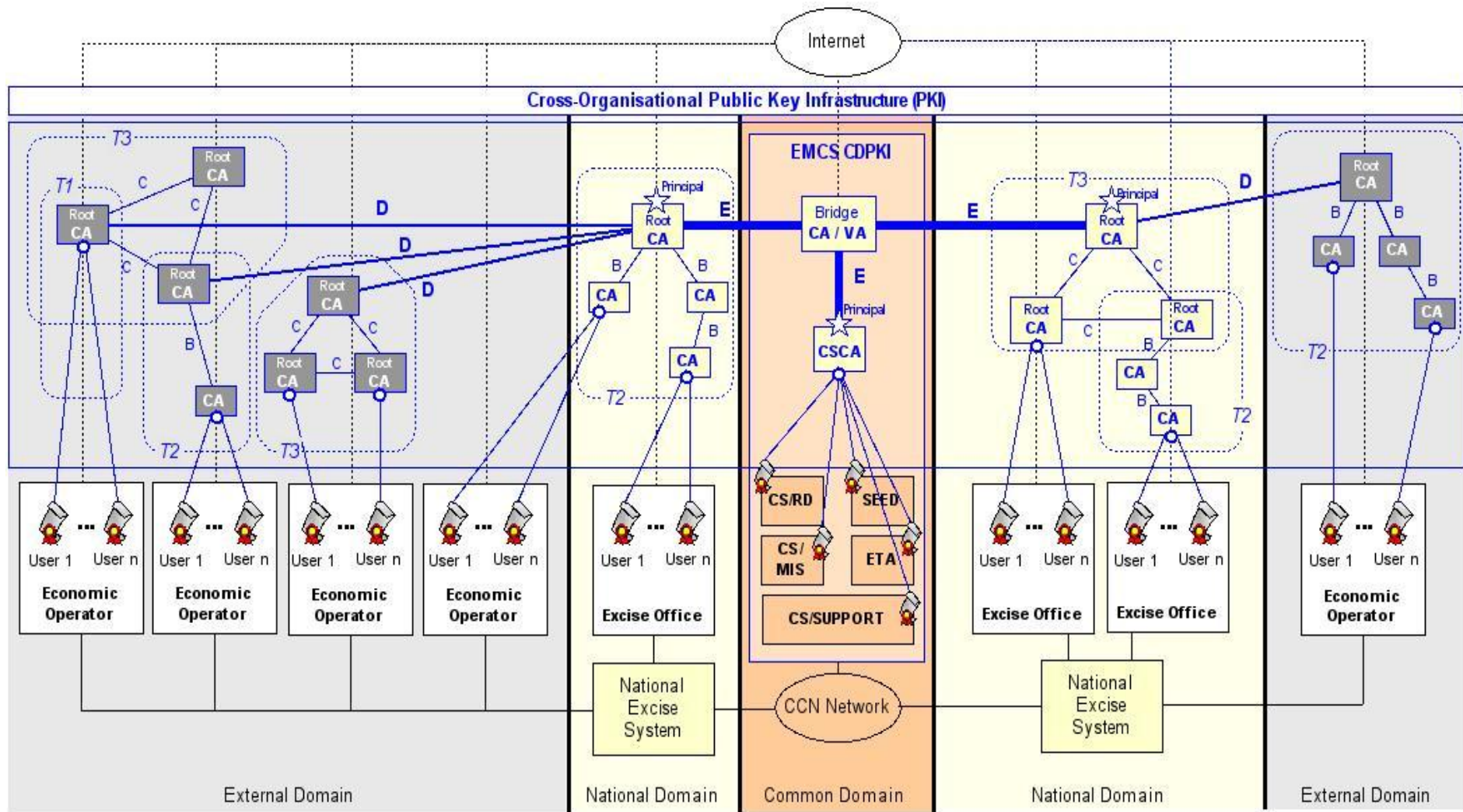


Figure 32: EMCS Common Domain PKI (CDPKI) – Overview

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

10.3.2.2. Links between CAs

In addition to the three configurations illustrated at the [Figure 30](#), each MSA has to establish a trust relationship with the PKIs (when available) of the Economic Operators involved in the EMCS business (links labelled “D” on the [Figure 32](#)).

In some Member States, national federations of Economic Operators have already established trust relationships between individual operator’s PKIs within multi-CA PKI.

In this case, the MSA only needs to establish a trust relationship with the exiting federated multi-CA PKI (and not with every individual one).

The same Bridge CA/VA architecture principles can obviously be applied at national level to achieve such inter-relationships between the national PKI and Economic Operator’s PKIs.

Finally, each MSA Principal CA (links labelled “E” on the [Figure 32](#)) has to establish a trust relationship with the CDPKI Bridge CA/VA to achieve EU-wide interoperability.

10.3.3. Bridge CA/VA

10.3.3.1. Objective

The CDPKI Bridge CA aims at:

- Bridging multiple *existing* national PKIs;
- Reducing the number of trust relationships required between national CAs to allow the interoperability between national PKIs;
- Equating the different PKI policies enforced in the MSAs.

The drawback of Bridge CA implementation is that it puts some complexity on client applications. More precisely it imposes:

- Rules on CA repositories (or requires client applications to understand multiple CA repositories);
- Rules on access to CA repositories (as each CA has its own Certificate Practice Statement (CPS) which implies different rules on accessing repositories and keys management);
- Clients applications to support multiple certificate validation mechanisms, including:
 - Consultation of Certificate Revocation Lists (CRL);
 - Access to CRL Distribution Points (CRLDP);
 - Support of the Online Certificate Status Protocol (OCSP).

To reduce the complexity on client side, the CDPKI architecture includes another central component called “Bridge Validation Authority (Bridge VA)”, which offers:

- Ability to deal with multiple CAs and Directories;
- Flexible search mechanisms (e.g. when looking for certificates);
- Support for multiple certificate validation mechanisms:
 - OCSP (simple OCSP, Global Trust Authority (GTA), Identrus, etc.);

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

- CRL, CRLDP.
- Ability to enforce Bridge CA policies;
- A flexible way to handle local policies;
- Better performance (on the client application side) in the certificate validation process.

Figure 33 describes the role of the Bridge CA/VA components in the certificate validation process once a trust relationship has been established between a national PKI and the CDPKI Bridge CA.

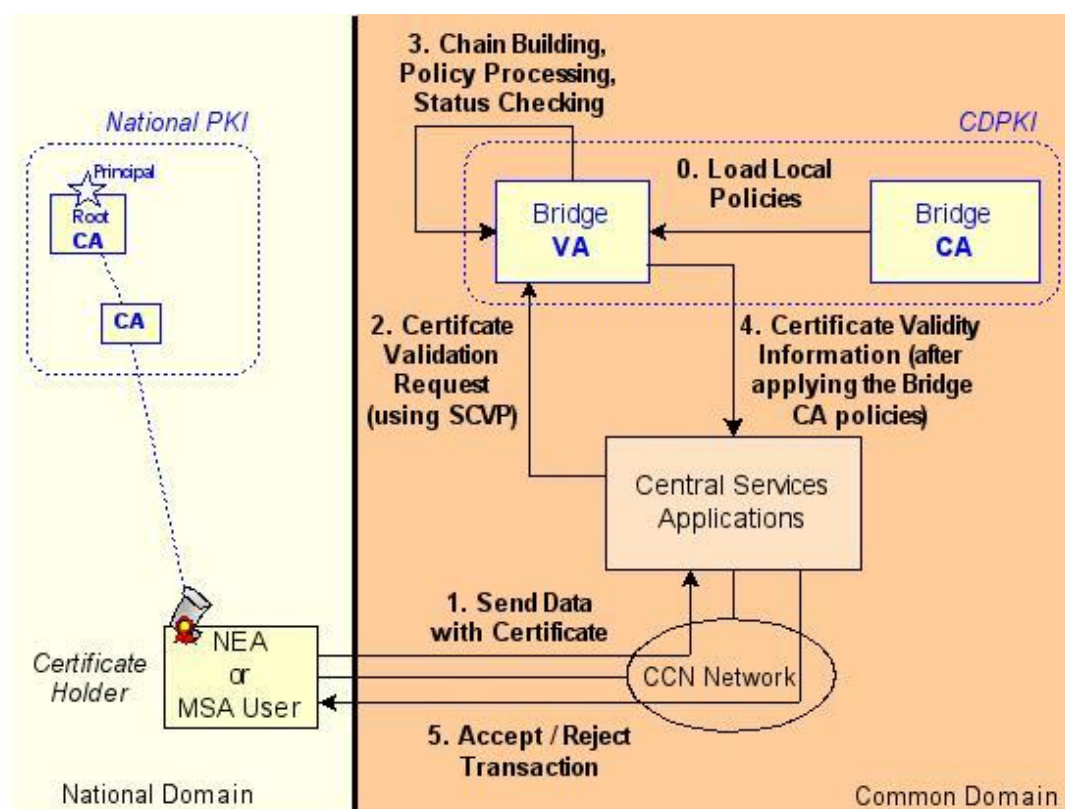


Figure 33: EMCS Common Domain PKI (CDPKI) – Bridge CA/VA

10.3.4. Trust Relationship Establishment

Cross-certification procedures and criteria are needed to establish a trust-relationship between a national PKI Principal CA and the EMCS CDPKI Bridge CA.

To make this process as straightforward as possible, a request to cross certify with the CDPKI Bridge shall trigger a 5-phase process designed to achieve a mutually reliable trust relationship (Figure 34).

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

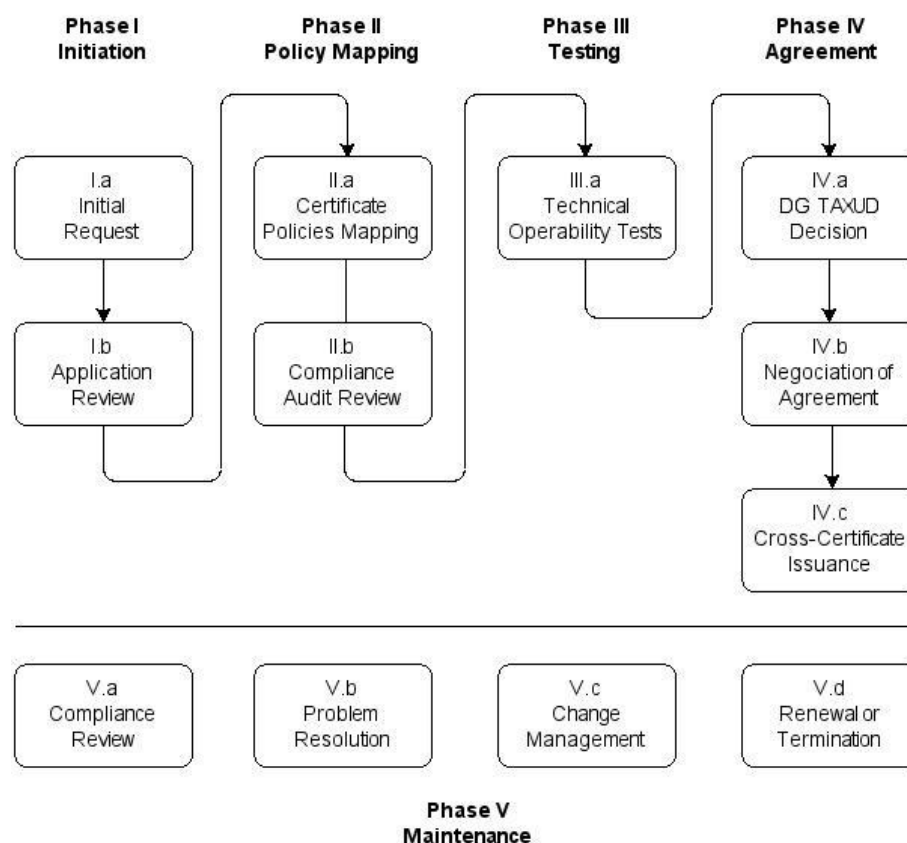


Figure 34: Trust Relationship Establishment Process

Phase I – Initiation

- a) **Initial Request.** To prepare and submit the required information to cross-certify with the EMCS CDPKI Policy;
- b) **Application Review.** To establish the MSA PKI suitability for cross certification and to decide whether to continue with the process.

Phase II – Certificate Policy Mapping

- a) **Mapping of Certificate Policies.** To examine the MSA PKI's Certificate Policy(ies) and to establish their equivalency with the EMCS CDPKI Bridge CA;

Note: Adherence to the PKIX Framework [R40]. Applicant MSA Certificate Policies must follow a current or recent version of the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647 or RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Presenting Certificate Policies in this format expedites the comparison with the CDPKI Bridge CA and applicant MSAs Certificate Policies by category and element for consistency.

- b) **Compliance Audit Review.** Demonstrate that the MSA Principal CA is operated in accordance with its Certificate Policy and Certificate Practice Statement. The applicant

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

MSA PKI must deliver a summary of the Principal CA compliance audit report to the policy authority as part of its cross-certification application.

Phase III – Testing

- a) **Technical Interoperability Tests.** It considered at this time that DG TAXUD has designated a Test CDPKI Bridge CA (e.g. located at the EC Data Centre). The Test CDPKI Bridge CA is used for the purpose of:
 - o Identifying and resolving incompatibilities between the PKI technologies of the CDPKI Bridge CA and the PKI products used in the applicant MSA;
 - o Minimising the risk of introducing incompatibilities with CAs already available in the Production CDPKI Bridge CA.

Phase IV – Agreement

- a) **CDPKI Authority Decision.** To decide whether to enter into a cross-certification agreement with the applicant MSA;
- b) **Negotiation of Agreement.** To negotiate the terms and conditions of the cross-certification Memorandum of Agreement (MoA);
- c) **Cross-certificates Issuance.** Granting the CDPKI Operational Authority (probably the EC Data Centre) and the applicant MSA PKI cross-certificates.

Phase V – Maintenance

It is important to ensure that, once in place and for its duration, the cross-certification arrangement continues to guarantee the agreed upon level of trust between the two parties involved. Each cross-certification is governed by the specific agreement (MoA) entered into Phase IV.

The maintenance phase provides mechanisms both for managing the relationship between cross-certified CAs, as required for the proper operation of the arrangement, and for terminating the arrangement if either party contravenes its terms and conditions or at the desire of either party. The elements of this phase are not sequential and they will depend on circumstances.

- a) **Compliance Review.** To determine if the affiliated MSA PKI is operating in compliance with its stated policies and practices;
- b) **Problem Resolution.** To report and correct problems the parties may encounter during the effective period of cross-certification agreement;
- c) **Change Management.** To manage changes to the CDPKI Bridge CA of affiliate PKI associated with a particular cross-certification agreement and to decide what actions to take as a result of implementing such changes;
- d) **Renewal or Termination.** To decide either to renew or terminate an existing cross-certification arrangement, and to specify the process for either renewal or termination of the cross-certification.

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

10.3.5. Technical Operability Tests

Technical interoperability testing is used to ensure technical interoperability between the EMCS CDPKI Bridge CA and the applicant MSA Principal CA. The objective is to determine whether there can be a successful exchange of cross-certificates and a directory of interoperability or not. The EMCS CDPKI Bridge CA will not issue cross-certificates before successful completion of interoperability tests. The EMCS CDPKI Bridge CA operational authority (most probably the EC Data Centre) operates the Test CDPKI Bridge CA on behalf of DG TAXUD. It is configured to be a duplicate of the Production CDPKI Bridge CA. The applicant MSA CA technical personnel will also be required to work with the EMCS CDPKI Bridge CA operational authority to complete the technical interoperability testing.

In preparing a *Technical Interoperability Report*, the CDPKI Bridge CA operational authority describes the results of the tests and provides it to the EMCS CDPKI Authority.

As a minimum, the technical interoperability test will demonstrate:

- Network connectivity is achieved using all required protocols;
- The directories of the CDPKI Bridge CA and the applicant MSA Principal CA are interoperable;
- The cross-certificate is correctly constructed by the CDPKI Bridge CA, and exchanged and recognised by the applicant MSA Principal CA;
- The cross-certificate is correctly constructed by the applicant MSA Principal CA, exchanged with the CDPKI Bridge CA, and recognised by the CDPKI Bridge CA;
- A test transaction, using a test subscriber of the applicant MSA PKI, can be successfully validated;
- The ability to share revocation information between the CDPKI Bridge CA and the applicant MSA PKI.

The report will also include a description of deficiencies identified during the test. Deficiencies may include technical interoperability deficiencies and potential performance issues that were not specifically identified by the test criteria. The report will also include the anticipated consequences of the deficiencies and a recommendation by the CDPKI operational authority.

10.3.6. Certificate Management

10.3.6.1. X.509 Certificates

According to the directive 1999/93/EC [\[R33\]](#), the legal value of documents exchanged under electronic format could only be recognised if the link between the person with power of signature and the electronic document is legally valid.

The use of X.509 digital certificates answer this requirement by providing electronic credentials that are associated with a public key and a private key and that an organisation uses to authenticate users/applications and to ensure data integrity. Digital certificates are created on servers running Certificate Services and stored on clients and in a directory such as LDAP Directory.

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX D: PROPOSAL FOR THE EMCS COMMON DOMAIN PKI (CDPKI)	

10.3.6.2. Certificate Services

Certificate Services are the part of the core operation system that allows the EMCS business to act as its own *Certification Authority (CA)*, and to issue and manage digital certificates.

Certificate Services include tools to manage issued certificates, publish CA certificates and *Certificate Revocation Lists (CRLs)*, configure CAs, import and export certificates and keys.

Note: In the EMCS context, the archived private keys recovery service is not needed since data are stored unencrypted in databases.

10.3.6.3. Certificate Authority (CA)

Servers on which Certificate Services have been configured to issue, validate, and manage certificates. Standard implementation supports multiple levels of a CA hierarchy and a cross-certified trust network. This includes offline and online CAs.

10.3.6.4. Certificate Revocation List (CRL)

This is the list of certificates that the EMCS CA considers no longer usable. Certificates have a specified lifetime, but CAs can reduce this lifetime by a process known as “*certificate revocation*”. Publishers can use any kind of directory service, including X.500, LDAP, or directories in a specific operating system, including Active Directory, to store CRLs. Publishers can also publish CRLs on Web servers.

10.3.6.5. Certificate Policy (CP) and Certificate Practice Statements (CPS)

CP and CPS documents outline how a CA and its certificates are to be used, the degree of trust that can be placed in these certificates, legal liabilities if the trust is broken, and so on. These documents can also define or impact PKI designs, operations, and usage, including how a CA is configured, how client requests are processed, and guidelines and procedures for revoking certificates.

10.3.6.6. Certificate and CRL Repositories

The Certificate and CRL Repositories are directory services (preferably LDAP-based) or other locations where certificates are stored and published.

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX E: EMCS SECURITY COMPLIANCE CERTIFICATE	

11. Appendix E: EMCS Security Compliance Certificate

11.1. Sample 'EMCS Security Compliance Certificate'

Subject: EMCS Security Compliance Certificate

Issued on: <date1> (mm-dd-yy)

Valid until: <date 1 + 1 year>

Dear <EMCS CPT Manager>,

With this certificate, I confirm to you that a compliance review was conducted by my organisation¹³ of the EMCS project at <Member State Administration>. As the representative of this organisation, I hereby certify that:

- *The review conducted by my organisation measured the degree of compliance of the EMCS project at <Member State Administration> to the security measures indicated in Section 8 of the EMCS Security Policy (SEP) and further specified in the Appendix B of the Security Excise System Specifications (SESS) which are applicable to its environment.*
 - *Where security measures¹⁴ have been implemented, they are considered operationally effective.*
 - *Where security measures have not been implemented, the <Member State Administration> has identified the risks and an appropriate action plan to manage these risks has been developed.*
- *The completed "EMCS Security Measures Questionnaire" (as specified in Appendix E of the SESS) that accompanies this certificate indicates the most up-to-date (as at <Insert date here>) implementation status of <Member State Administration> security measures.*

Yours sincerely,

<Representative of Certifying Organisation> (and signature)


¹³ The EMCS Security Compliance Certificate must be issued every three years by a qualified organisation chosen by the MSA (but can also be an MSA internal organisational unit that is independent of the EMCS project team).

¹⁴ Although the MSA is only obliged to implement "Mandatory" security measures, it is expected that "Recommended" security measures will be implemented on a best-effort basis.

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2
APPENDIX E: EMCS SECURITY COMPLIANCE CERTIFICATE	

11.2. 'EMCS Security Measures Questionnaire'

The EMCS Security Measures Questionnaire should accompany the EMCS Security Compliance Certificate (see 8.2.3) to be submitted annually by the MSA. Its purpose is for the MSA to demonstrate compliance to the EMCS Security Measures, facilitate benchmarking and promote transparency amongst EMCS stakeholders. The questionnaire must indicate the most up-to-date implementation status of the MSA security measures.

EMCS Security Measures Questionnaire	 I:\Common\SEC\TES Security\EMCS\Securi
--------------------------------------	--

EMCS SYSTEM SPECIFICATION	REF: ECP1-ESS-SESS
SECURITY EXCISE SYSTEM SPECIFICATIONS (SESS)	VERSION: 2.2

End of Document