



Analysis of structured e-Document formats used in Trans-European Systems

SC17DI06692 - D1.1 Survey on standardized e-Document formats



Document Metadata

Property	Value
Date	2014-05-15
Status	Accepted
Version	1.00
Authors	Oriol Bausà Peris – Invinet Lucas Colet – PwC EU Services Natacha Dewyngaert – PwC EU Services Stijn Goedertier – PwC EU Services Dusko Karaklajic – PwC EU Services Vianney le Clément de Saint Marcq – PwC EU Services
Reviewed by	Pieter Breyne – PwC EU Services
Approved by	Margarida Abecasis – European Commission Susanne Wigard – European Commission Vassilios Peristeras – European Commission

This study was prepared for the ISA Programme by:

PwC EU Services

Disclaimer:

The views expressed in this report are purely those of the authors and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

EXECUTIVE SUMMARY

This report presents the result of a study of twelve existing families of structured e-Document formats used for exchanging information between public administrations in Europe in connection to twelve so-called Trans-European Systems. The study was commissioned by the Interoperability Solutions for European Public Administrations (ISA) Programme¹ of the European Commission, in the context of its Action 2.15 on e-Documents.

Based on definitions in previous EU studies on electronic documents, we proposed the following definitions:

An **electronic document (e-Document)** is any document in electronic format containing structured data and possibly also unstructured data used in the context of an administrative process.

An **e-Document format** is a specification that lays down the syntax (structure) and semantics of a particular type of e-Documents.

Public administrations specify and typically use e-Documents for information exchange in the context of *message-based application integration*. In this study, we will focus on the use of the **structured** part of e-Document formats used in **message-based information exchanges** of Trans-European Systems.

The report is structured as follows. First, in Chapter 1 and 2 we introduce the study and describe a theoretical framework of analysis. In Chapter 3 we present the findings from applying the aforementioned analysis framework to twelve families of e-Document formats – the detailed analysis is included in Annex I. These families have been selected on the basis of scope criteria related to the usage in public sector, cross-border nature, and proven value of the e-Document formats. In Chapter 4, we formulate recommendations based on the good practices identified in the report.

Chapter 2 provides an analysis framework to analyse the families of e-Document formats used in Trans-European Systems. Its main purpose is to make sure that the analysis of e-Document formats is carried out in a consistent and harmonised manner, so that the analyses for each case study can be compared afterwards. The framework is composed of seven main elements, reflecting the following **research questions**:

1. **Descriptive metadata**: which e-Document formats already exist? Are they publicly available under an open licence? Are they described according to the vocabulary of the Asset Description Metadata Schema (ADMS) so that people can find them more easily?
2. **Context**: what is the context of the families of e-Document formats used in Trans-European Systems?

¹ ISA Programme, <http://ec.europa.eu/isa/>

3. **e-Document engineering method:** which e-Document engineering methods are used? Are these standard methods? Are e-Document formats based on shared libraries of core concepts?
4. **Conformance mechanisms:** which mechanisms do these e-Document formats use to guarantee conformance to the e-Document format?
5. **Security:** which security mechanisms are foreseen by the e-Document formats?
6. **Governance:** which roles, responsibilities, and decision-mechanisms are used to manage the lifecycle of these e-Document formats? Is the change management process formally documented and open to third-party change requests?
7. **Usage:** what is the actual usage and uptake of these e-Document formats?

Annex I provides a detailed analysis of twelve families of e-Document formats used in the Trans-European Systems that fulfil the scope criteria described in Section 1.4. The selected families of e-Document formats are depicted in the table below. Also systems like the Internal Market Information System (IMI) and Réseau permis de conduire/Driver Licence Network (RESPER) are relevant systems that could be analysed at a later point in time.

Selected families of e-Document formats

1. CEN/BII profiles used by e-Prior and PEPPOL
2. e-Document formats used by e-CODEX
3. Electronic Exchange of Social Security Information (EESSI)
4. European Criminal Records Information System (ECRIS)
5. European Register of Road Transport Undertaking (ERRU)
6. European Car and Driving Licence Information System (EUCARIS)
7. Tachograph Network (TACHOnet)
8. European Patients Smart open Services projects (epSOS)
9. Eurofiling: financial reporting based on XBRL used by the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) and proposed by XBRL Europe
10. Virtual Company Dossier (VCD) used by PEPPOL
11. Omnifarious Container for e-Documents (OCD) used by SPOCS
12. International Commission on Civil Status (ICCS)

The analysis of the families of e-Document formats was carried out in a structured and uniform way, following the aforementioned analysis framework. The information for the analysis of each family was collected through desk research and interviews with the concerned experts who were involved in the specification and maintenance of these e-Document formats.

Chapter 3 formulates the findings that can be concluded from a comparative analysis of the case studies. These include the following:

1. Descriptive metadata:

- There is insufficient publicly available information about the analysed e-Document formats;
- Most analysed e-Document formats are at best informally described, descriptive metadata is not available in machine-readable form expressed with the Asset Description Metadata Schema (ADMS);
- Half of the analysed e-Document formats are not available under an open licence;

2. Context:

- The analysed e-Document formats are all created for a single information exchange context;

3. e-Document engineering method:

- More than half of the cases analysed use standard e-Document engineering methods;
- Half of the cases analysed reuses standard libraries of data elements;
- Uptake of standard XML naming and design rules;
- XML and XSD are the dominant schema representation techniques;

4. Conformance:

- Application profiles facilitate the usage of e-Document formats in other information exchange contexts;
- Conformance testing and certification is important when on-boarding a large number of partners;
- Few e-Document formats come with a reference implementation;

5. Security:

- Most cases rely on security features such as standard digital signature formats and document containers applied end-to-end to the e-Documents themselves;

6. Governance:

- The majority of the analysed e-Document formats have a formal governance mechanism;
- The change management process is not always open;
- All e-Document formats are stored in an authoritative repository;

7. Usage

- e-Document formats are used in high-volume administrative processes.

Chapter 4 formulates **recommendations** based on the good practices identified in the case studies. These can be summarised as follows:

1. Rather than creating new e-Document formats from scratch, organisations should **consider using existing standard e-Document formats** – when available – and place these into their own geopolitical, legal, and administrative context. The latter can be done by defining *application profiles* of standard e-Document formats and build consensus on their usage within a particular information exchange context.
2. Organisations should **consider using a standard e-Document engineering method** that offers a methodology for requirement analysis and conceptual modelling, a standardised library of data types and elements, and conventions for syntax binding or schema production such as XML naming and design rules. Standard methods make it easier for public administrations to produce e-Document formats in a formal way, producing standard outcomes that could be re-used in other projects. Good e-Document formats do not only define a syntax binding or create a schema for the e-Document format, but also pay attention to information model requirements, definitions, and business rules.
3. Organisations should **consider using existing tools** that support standard methods to design new e-Document formats and create e-Document schemas.
4. In those information exchange contexts where there is a potential broad community of users to adopt the specifications, organisations should **consider providing an explicit document conformance testing procedure and testing artefacts** in addition to guidelines and textual specifications.
5. Organisations should **define a formal governance mechanism with roles, responsibilities, and decision-mechanisms to manage the lifecycle of the e-Document formats**. Additionally, they should define and operate clear lifecycle management processes for e-Document formats. Such processes include for example how updates to the e-Document format are published, or how external contributions and change requests are handled. Regarding the latter, organisations should consider a change management process that is open to third-party change requests. Openness is key as public administrations will be reluctant to use an e-Document format when they cannot provide input into the change management process.
6. **Owners of e-Document formats should make them available for use by other administrations** from other sectors and/or other countries. Hereby, they should be made aware of the importance of clear licensing arrangements that specify unambiguously under which conditions the metadata can be reused. To make reuse easier, it is also necessary to make accurate and accessible descriptions about e-Document formats available; preferably documented using the Asset Description Metadata Schema (ADMS).

Table of Contents

EXECUTIVE SUMMARY	2
1 INTRODUCTION	10
1.1 CONTEXT: DEFINING E-DOCUMENTS	10
1.2 LEARNING FROM TRANS-EUROPEAN SYSTEMS	11
1.3 OBJECTIVES AND RESEARCH QUESTIONS	12
1.4 SCOPE.....	13
1.5 SURVEY METHODOLOGY	14
1.6 GLOSSARY.....	14
2 ANALYSIS FRAMEWORK.....	18
2.1 DESCRIPTIVE METADATA	18
2.2 CONTEXT	18
2.3 E-DOCUMENT ENGINEERING METHOD	19
2.4 CONFORMANCE MECHANISMS	20
2.5 SECURITY MECHANISMS.....	20
2.6 GOVERNANCE MECHANISMS.....	21
2.7 USAGE	23
3 FINDINGS.....	24
3.1 DESCRIPTIVE METADATA	25
3.2 CONTEXT	26
3.3 E-DOCUMENT ENGINEERING METHOD	27
3.4 CONFORMANCE MECHANISMS	31
3.5 SECURITY.....	32
3.6 GOVERNANCE MECHANISMS.....	33
3.7 USAGE	35
4 RECOMMENDATIONS	36
4.1 USE STANDARD E-DOCUMENT FORMATS AND CREATE APPLICATION PROFILES.....	36
4.2 USE A STANDARD E-DOCUMENT ENGINEERING METHOD	36
4.3 USE EXISTING TOOLS FOR E-DOCUMENT ENGINEERING.....	37
4.4 PROVIDE DOCUMENT CONFORMANCE TESTING PROCEDURE AND MECHANISMS.....	39
4.5 FOLLOW GOOD PRACTICES FOR METADATA GOVERNANCE AND MANAGEMENT.....	40
4.6 MAKE E-DOCUMENTS AVAILABLE FOR REUSE	41
5 CONCLUSION	42
5.1 FINDINGS ON STRUCTURED E-DOCUMENT FORMATS USED IN TRANS-EUROPEAN SYSTEMS.....	42
5.2 RELEVANCE OF OUR RECOMMENDATIONS.....	43
5.3 FUTURE WORK.....	44
6 ACKNOWLEDGEMENTS	45
7 REFERENCES.....	46
ANNEX I. STRUCTURED E-DOCUMENT FORMATS USED IN TRANS-EUROPEAN SYSTEMS	53
I.1. CEN/BII PROFILES USED BY E-PRIOR AND PEPPOL	54
I.2. E-DOCUMENT FORMATS USED BY E-CODEX.....	64
I.3. ELECTRONIC EXCHANGE OF SOCIAL SECURITY INFORMATION (EESSI)	75
I.4. EUROPEAN CRIMINAL RECORDS INFORMATION SYSTEM (ECRIS).....	78
I.5. EUROPEAN REGISTER OF ROAD TRANSPORT UNDERTAKING (ERRU)	85

Analysis of structured e-Document formats used in Trans-European Systems

I.6.	EUROPEAN CAR AND DRIVING LICENCE INFORMATION SYSTEM (EUCARIS)	92
I.7.	TACHOGRAPH NETWORK (TACHONET)	105
I.8.	EUROPEAN PATIENTS SMART OPEN SERVICES PROJECTS (EPSOS)	112
I.9.	EUROFILING: FINANCIAL REPORTING BASED ON XBRL	121
I.10.	VIRTUAL COMPANY DOSSIER (VCD) USED BY PEPPOL	129
I.11.	OMNIFARIOUS CONTAINER FOR E-DOCUMENTS (OCD) USED BY SPOCS	137
I.12.	INTERNATIONAL COMMISSION ON CIVIL STATUS (ICCS).....	143
ANNEX II.	DESCRIBING FAMILIES OF E-DOCUMENT FORMATS WITH ADMS	149
ANNEX III.	LIST OF IDENTIFIED TRANS-EUROPEAN SYSTEMS	150

List of Figures

FIGURE 1 – BPMN DIAGRAM: E-DOCUMENTS USED IN A TRADEMARK APPLICATION PROCESS	11
FIGURE 2 - CEN BII SCOPING USE CASE	54
FIGURE 3 - CONFORMANCE RELATIONS	58
FIGURE 4 - DOMAIN AND DOCUMENT MODEL [E-SENS, 2013]	65
FIGURE 5 - SCREENSHOT OF THE METADATA WORKBENCH	66
FIGURE 6 - FROM BUSINESS TO XML SCHEMAS [E-CODEX, 2012]	67
FIGURE 7 - BASIC WORKFLOW OF THE E-CODEX CENTRAL TRUST SERVICE.....	69
FIGURE 8 - E-CODEX HIGH-LEVEL ARCHITECTURE [E-CODEX, 2012]	70
FIGURE 9 - HIGH LEVEL STRUCTURE FOR CENTRALIZED ARCHITECTURE FOR ERRU (ERRU XML MESSAGING REFERENCE GUIDE)	89
FIGURE 10 - HIGH LEVEL STRUCTURE FOR PEER-TO-PEER ARCHITECTURE FOR ERRU (ERRU XML MESSAGING REFERENCE GUIDE)	89
FIGURE 11 - ARCHITECTURAL MODEL OF EUCARIS	98
FIGURE 12 - TACHONET GLOBAL ARCHITECTURE (TACHONET XML MESSAGING REFERENCE GUIDE) .	108
FIGURE 13 – EPSOS SEMANTIC SERVICES [EPSOS , 2014].....	114
FIGURE 14 - PEPPOL COMPONENTS	129
FIGURE 15 - OPENPEPPOL CHANGE MANAGEMENT	131

List of Tables

TABLE 1 - GLOSSARY	14
TABLE 2 - ANALYSIS FRAMEWORK: DESCRIPTIVE METADATA	18
TABLE 3 – ANALYSIS FRAMEWORK: CONTEXT	18
TABLE 4 – ANALYSIS FRAMEWORK: E-DOCUMENT ENGINEERING METHOD.....	19
TABLE 5 – IDENTIFIED E-DOCUMENT ENGINEERING METHODS MAINTAINED BY STANDARDISATION ORGANISATIONS	19
TABLE 6 – ANALYSIS FRAMEWORK: CONFORMANCE MECHANISMS	20
TABLE 7 - ANALYSIS FRAMEWORK: SECURITY MECHANISMS	20
TABLE 8 – ANALYSIS FRAMEWORK: METADATA GOVERNANCE	21
TABLE 9 - ANALYSIS FRAMEWORK: USAGE.....	23
TABLE 10 - FAMILIES OF E-DOCUMENT FORMATS INCLUDED IN THIS ANALYSIS	24
TABLE 11 – LIST OF IDENTIFIED REUSABLE E-DOCUMENT ENGINEERING TOOLS	38
TABLE 12 - FAMILIES OF E-DOCUMENT FORMATS INCLUDED IN THIS ANALYSIS	53
TABLE 13 - ANALYSIS OF CEN BII	60

TABLE 14 – ANALYSIS OF E-CODEX	72
TABLE 15 - ANALYSIS OF EUROPEAN CRIMINAL RECORDS INFORMATION SYSTEM (ECRIS)	82
TABLE 16 - ANALYSIS OF EUROPEAN REGISTER OF ROAD TRANSPORT UNDERTAKING (ERRU).....	89
TABLE 17 - ANALYSIS OF EUROPEAN CAR AND DRIVING LICENCE INFORMATION SYSTEM (EUCARIS)	101
TABLE 18 - ANALYSIS OF TACHOGRAPH NETWORK (TACHONET).....	109
TABLE 19 - ANALYSIS OF EUROPEAN PATIENTS – SMART OPEN SERVICES (EPSOS)	117
TABLE 20 - ANALYSIS OF FINANCIAL REPORTING BASED ON XBRL	126
TABLE 21 - ANALYSIS OF THE VIRTUAL COMPANY DOSSIER	133
TABLE 22 - ANALYSIS OF THE OMNIFARIOUS CONTAINER FOR E-DOCUMENTS	140
TABLE 23 - ANALYSIS OF INTERNATIONAL COMMISSION ON CIVIL STATUS (ICCS)	146
TABLE 24 – OVERVIEW OF E-DOCUMENT FORMATS DESCRIBED WITH ADMS.....	149
TABLE 25 – LIST OF IDENTIFIED TRANS-EUROPEAN SYSTEMS	150

1 INTRODUCTION

This report presents the results of a study of existing families of e-Document formats used for exchanging information with public administrations in Europe in different domains in connection to twelve so-called Trans European Systems. The study is commissioned by the Interoperability Solutions for European Public Administrations Programme (ISA programme)² of the European Commission, in the context of its Action 2.15 on e-Documents.

1.1 Context: defining e-Documents

In a previous EU study on electronic documents in the EU Member States [Graux, 2009]³ focusing specifically on the implementation of Article 8 of the Services Directive⁴, an electronic document (e-Document) is defined as follows: *any document in an electronic form regardless of the specific formats or solutions used [...] when completing procedures and formalities [..]*. In this study, we adopt this definition, but additionally require that an e-Document contains at least a portion of structured data that can be easily processed by a machine.

An **electronic document (e-Document)** is any document in electronic format containing structured data (and possibly also unstructured data) used in the context of an administrative process.

For the purpose of this study, we will focus on the use of the **structured** part of e-Document formats used in a **message-based information exchange**. Examples of e-Documents are requests for criminal records in the European Criminal Record Information System (ECRIS), the implementation of the European Payment Order (EPO)⁵ procedure by the e-CODEX Large-Scale Pilot, or the exchange of electronic orders and invoices following the guidelines of the UBL XML standard schemas specified in the PEPPOL profiles. In these examples, e-Documents are typically transmitted by a messaging system through a message channel to allow for message-based application integration. Participants that interact in the context of an administrative process exchange electronic documents to signal changes to the state of the process to each other or to provide evidence certifying the fulfilment of particular criteria in administrative processes. An example of this is displayed in Figure 1: this is a BPMN diagram representing the interactions between a Trademark Office and an Applicant who applies for a Trademark. The process – a simplified version of e-Filing process of the Community Trademark [OHIM, 2013] – is initiated through the submission of a Trademark Application which is an example of an electronic document.

² ISA Programme, <http://ec.europa.eu/isa/>

³ IDABC Programme (2009). Study on electronic documents and electronic delivery. <http://ec.europa.eu/idabc/en/document/7667/5644.html>

⁴ Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

⁵ European Payment Order, <http://ec.europa.eu/justice/civil/commercial/eu-procedures/>

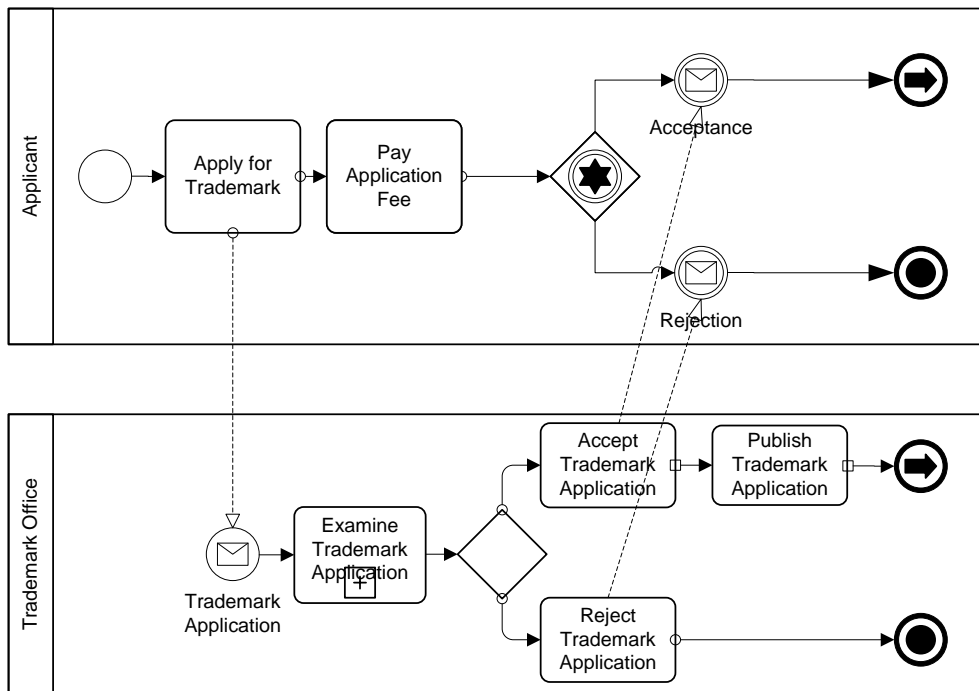


Figure 1 – BPMN diagram: e-Documents used in a Trademark Application process

Message-based application integration requires a consensus on the format of the e-Documents that are being exchanged. We define the concept 'e-Document format' as follows:

An **e-Document format** is a specification that lays down the syntax (structure) and semantics of a particular type of e-Documents.

e-Document formats are usually defined within the scope of projects addressing the needs of specific domains that define the business processes and collaborations among parties. They identify interactions that have to be fulfilled using e-Documents. Such e-Document formats are not defined in isolation: either they are based on existing e-Document standards or they are defined as a whole set of e-Documents using a custom-developed or tailored e-Document engineering method. These projects end up defining 'families of e-Document formats' that share a common library and are built using the same engineering method.

In this study we will focus on 'families of e-Document formats' as defined below.

A **family of e-Document formats** is a set of e-Document formats defined for a particular domain and created with the same engineering method and using a common library.

1.2 Learning from Trans-European Systems

In Europe, citizens and businesses increasingly live, work and conduct business across borders. Their increased mobility must be supported by cross-border public services, for example registering a trademark, registering a foreign branch, obtaining a licence to conduct business, or getting a birth certificate. In this

environment, public administrations must be capable of interacting efficiently and effectively across borders through the seamless **exchange of information**.

A study on the usage of e-Documents and e-Delivery in the EU Member States [Graux, 2009] reveals that EU Member States are already using e-Documents as a pattern of information exchange in their *national* e-Government systems. The study reveals that in most cases e-Document formats have been created for the **national context** only. Similarly, it can be observed from the study that in each domain of **administrative processes** (for example public procurement, social security, judicial procedures, transport, healthcare, financial reporting, tax declaration and collection, licensing, etc.) public administrations have created very different e-Document formats independently of other domains. This divergence stems from the lack of coordination, the lack of common legal definitions, lack of commonly agreed structural metadata, the multilingual challenge, etc. The lack of harmonisation in e-Document formats has resulted in **semantic interoperability barriers** that stand in the way of an efficient and effective delivery of public services across borders and sectors.

A first step towards better coordination is to take stock of the existing e-Document families that are being used in the context of cross-border and/or cross-sector information exchange between public administrations in so-called **Trans-European Systems** and to identify the engineering methodologies and libraries used to build them. This is the purpose of this study.

Trans-European Systems are operational solutions developed by the European Commission or other bodies (in some cases co-funded by Member States), that facilitate cross-border exchange of information and delivery of electronic public services between Public Administrations in support to the implementation and advancement of EU policies.

1.3 Objectives and research questions

The main **objectives** of this study, as commissioned by the ISA Programme, are:

- To identify existing families of e-Document formats, and to analyse their actual coverage, scope, real use and uptake;
- To identify engineering methodologies used to create electronic documents in these families of e-Document formats;
- To identify reuse of standards and shared libraries of core concepts;
- To describe the already available machine-readable formats in ADMS and to make the descriptions and links available in Joinup.

We have converted this into the following **research questions**:

1. **Descriptive metadata**: which e-Document formats already exist? Are they publicly available under an open licence? Are they described according to the vocabulary of the Asset Description Metadata Schema (ADMS) so that people can find them more easily?

2. **Context:** what is the context of the families of e-Document formats used in Trans-European Systems?
3. **E-Document engineering method:** which e-Document engineering methods are used? Are these standard methods? Are e-Document formats based on shared libraries of core concepts?
4. **Conformance mechanisms:** which mechanisms do these e-Document formats use to guarantee conformance to the e-Document format?
5. **Security:** which security mechanisms are foreseen by the e-Document formats?
6. **Governance:** which roles, responsibilities, and decision-mechanisms are used to manage the lifecycle of these e-Document formats? Is the change management process formally documented and open to third-party change requests?
7. **Usage:** what is the actual usage and uptake of these e-Document formats?

1.4 Scope

For this report, we will analyse *families* of e-Document formats, rather than individual e-Document formats. We have applied the following scope criteria to select them:

- **Cross-border setting:** The families of e-Document formats must be used in a cross-border setting, more specifically in the context of a Trans-European System. In 2009, the European Commission (DG MARKT) has commissioned a study that takes stock of the usage of e-Documents and e-Delivery in the EU Member States [Graux, 2009]⁶ focusing specifically on the implementation of Article 8 of the Services Directive⁷.
- **Structured e-Document formats:** For the purpose of this study, we will predominantly look at the use of the structured part of e-Document formats that can be easily processed by a machine.
- **Administrative procedures:** The families of e-Document formats must be used in the public sector for administration-to-administration (A2A), administration-to-business, or administration-to-citizen (A2C) communication;
- **Both coordinated by Member States or European Commission:** We aim to analyse both e-Document formats that originate from initiatives coordinated by Member States and initiatives coordinated by the European Commission.

⁶ IDABC Programme (2009). Strategic issues for the implementation of eGovernment services to Businesses (services sector). <http://ec.europa.eu/idabc/en/document/7667/5644.html>

⁷ Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

- **Proven value:** The families of e-Document formats must already be used to conduct a collaborative process; i.e. we will focus on those formats that have a proven value.

1.5 Survey methodology

The survey approach consisted of the following steps:

1. **Define an analysis framework for e-Document formats.** First, the key terminology is defined and an analysis framework is composed. The analysis framework outlines the approach, which is further referred to during the study. The framework is used to analyse and compare the identified families of e-Document formats based on different elements outlined in the framework. A glossary of terms is provided in Section 1.5. The analysis framework is outlined in Chapter 2.
2. **Identify, select, and analyse e-Document families.** We have identified families of e-Document formats used in Trans-European Systems through desk research. Annex III contains the full list of Trans-European Systems that were identified. From this list a total of 12 e-Document formats were selected, each meeting the scope defined in Section 1.4. The analysis is included in Annex I. The analysis is conducted on the basis of preparatory desk research and a validation interview with a project manager or enterprise architect of the corresponding Trans-European System.
3. **Summarize the findings.** Based on the survey conducted and the analysis of the e-Document families, the findings are summarized and an overall conclusion of the study is given in Chapter 3.
4. **Describe the identified e-Document formats with ADMS.** Describe the identified e-Document formats with the Asset Description Metadata Schema (ADMS). Such a machine-readable description of the e-Document families enables publication of these descriptions on many platforms such as Joinup.

1.6 Glossary

This section provides a number of common definitions used throughout the study.

Table 1 - Glossary

Term / Acronym	Description
ADMS	A common metadata vocabulary to describe standards, so-called interoperability assets, on the Web. ADMS is a W3C Working Group Note ⁸ .

⁸ W3C Working Group Note: <http://www.w3.org/TR/vocab-adms/>

Analysis of structured e-Document formats used in Trans-European Systems

ASiC	Associated Signature Containers
BPMN	Business Process Modelling Notation
CCTS	Core Components Technical Specification
Core Components	Core components are defined as context-free semantic building block for creating clear and meaningful data models, vocabularies, and information exchange packages [United Nations - Centre for Trade Facilitation and Electronic Business, 2009].
Core Vocabularies	Simplified, re-usable, and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral fashion [Interoperability solutions for European public administrations (ISA), 2011].
EDI	Electronic Data Interchange
e-Document	Any document in electronic format containing structured data and possibly also unstructured data used in the context of an administrative process.
e-Document format	An e-Document format is a specification that lays down the syntax (structure) and semantics of a particular type of e-Documents.
Family of e-Document formats	Set of e-Document formats defined for a particular domain and created with the same engineering method and using a common library.
Data model	A data model is a collection of entities, their properties and the relationships among them, which aims at formally representing a domain, a concept or a real-world thing
HL7	Health Level 7 Founded in 1987, Health Level Seven International (HL7) is a not-for-profit, ANSI-accredited standards developing organization dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information
Reference data	Reference data is small, discreet sets of values that are not updated as part of business transactions but are usually used to impose consistent classification. Reference data normally has a low update frequency. Reference data is relevant across more than one business systems belonging to different organisations and sectors.
Reference implementation	A reference implementation of a specification, to allow for interoperability testing. In the context of an e-Document format, a reference implementation refers to an application that is capable of consuming and producing an e-Document.

Analysis of structured e-Document formats used in Trans-European Systems

Interoperability	According the ISA Decision, interoperability means the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the <i>exchange of data</i> between their respective ICT systems.
Metadata	Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information. [National Information Standards Organization , 2004]
Metadata governance	Metadata governance comprises well-defined roles and responsibilities, cohesive policies and principles, and decision-making processes that define, govern and regulate the lifecycle of metadata.
Metadata management	We define metadata management as the good practice of adopting policies, processes, and systems to plan, perform, evaluate, and improve the use and re-use of data models and reference data.
Interoperability	According the ISA Decision, interoperability means the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the <i>exchange of data</i> between their respective ICT systems.
NDR	Naming and Design Rules
OCD	Omnifarious Container for e-Documents
Open data	"A piece of data or content is open if anyone is free to use, reuse, and redistribute it — subject only, at most, to the requirement to attribute and/or share-alike" [Open Knowledge Definition].
OASIS	OASIS (Organization for the Advancement of Structured Information Standards) is a non-profit consortium that drives the development, convergence and adoption of open standards for the global information society.
OWL	The Web Ontology Language
RDF	Resource Description Framework
SBDH	Standard Business Document Header
SKOS	Simple Knowledge Organization System – RDF Vocabulary for the representation of key reference data such as code lists,

Analysis of structured e-Document formats used in Trans-European Systems

	and taxonomies.
Trans European System	Solutions developed by the European Commission or other bodies (in some cases co-funded by Member States), that facilitate cross-border exchange of information and delivery of electronic public services between Public Administrations in support to the implementation and advancement of EU policies.
UMM	Unified Modelling Methodology
UML	Unified Modelling Language [Object Management Group, Inc., 2012].
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
URL	Uniform Resource Locator
VCD	Virtual Company Dossier
XBRL	XBRL stands for eXtensible Business Reporting Language. It is a language for the electronic communication of business information, providing major benefits in the preparation, analysis and communication of business information. Source: http://www.xbrl.org .
XBRL Taxonomies	XBRL Taxonomies are the reporting-area specific hierarchical dictionaries used by an XBRL community. They define the specific tags that are used for individual items of data (such as "net profit"), their attributes and their interrelationships. Different taxonomies will be required for different business reporting purposes. Some national jurisdictions may need their own reporting taxonomies to reflect local accounting and other reporting regulations. Many different organisations, including regulators, specific industries or even companies, may require taxonomies or taxonomy extensions to cover their own specific business reporting needs. Source: http://www.xbrl.org/Taxonomies .
XML	eXtensible Markup Language
XML Schema	An XML schema is a generic term used to identify the family of grammar based XML document structure validation languages to include the more formal W3C XML Schema Definition Language, ISO 8601 Document Type Definition, or Schematron [UN/CEFACT, 2009].
XSD	XML Schema Definition
XSLT	Extensible Stylesheet Language Transformations

2 ANALYSIS FRAMEWORK

This chapter outlines the theoretical framework used to analyse the identified families of e-Documents. Its purpose is to make sure that the analysis of e-Document formats is carried out in a consistent and harmonised manner, so that the case studies can be compared.

2.1 Descriptive metadata

We described the identified e-Document families according to the descriptive metadata elements outlined in Table 2.

Table 2 - Analysis framework: descriptive metadata

Descriptive metadata	Description
Licence	The licence under which the e-Document format can be used and re-distributed with or without modification.
Publisher	The organisation that makes the specifications available.
Publisher type	The type of publisher, according to the ADMS-AP controlled vocabulary for publisher type ⁹ .
Theme(s)	Classification of the activities of the exchanged information according to EuroVoc ¹⁰ .
Access URL	A landing page that gives access to the distribution of the e-Document formats.

2.2 Context

We described the context of e-Document families according to the categories listed in Table 3. The UN/CEFACT Core Component Technical Specification (CCTS) [UN/CEFACT, 2012] gives a more detailed definition of context for e-Documents; however we consider that categorisation too detailed for the purpose of this survey as it deals with individual e-Documents.

Table 3 – Analysis framework: context

Context category	Description
Administrative process context	A description of the activity of the administrative process.

⁹ Publisher type: https://joinup.ec.europa.eu/svn/adms/ADMS_v1.00/ADMS_SKOS_v1.00.html

¹⁰ EuroVoc: <http://eurovoc.europa.eu>

Geopolitical context	The influences related to geographical factors of the trading parties (e.g. region, nationality, etc.)
Legal context	The most relevant laws, regulations, and governmental policies that govern the context of information exchange.

2.3 e-Document engineering method

The e-Document engineering is described and analysed according to the four elements listed in Table 4.

Table 4 – Analysis framework: e-Document engineering method

e-Document engineering method	Description
Library of data elements	A library that is used to generate the e-Document definitions (e.g. a Core Component Library).
Naming and design rules	An architecture and set of rules to define, describe and use a representation language (e.g. XML) to consistently express information exchanges [UN/CEFACT, 2009].
e-Document engineering tools	The tools used for the design and implementation of data formats.
Representation techniques	Techniques such as UML, XML Schema and RDF Schema to represent an e-Document format.

International Standard Development Organizations have their own engineering methodologies and libraries to produce e-Document standards. Table 5 gives an overview.

Table 5 – Identified e-Document engineering methods maintained by standardisation organisations

Identified Engineering Methods
OASIS Universal Business Language (UBL)
UN/CEFACT Unified Modelling Methodology
ISO20022
XBRL Data Point Modelling
HL7 v3
NIEM e-Document formats by the National Information Exchange Model

2.4 Conformance mechanisms

The families of e-Documents are described and evaluated according to conformance mechanisms. An overview of the conformance mechanisms is given in Table 6.

Table 6 – Analysis framework: conformance mechanisms

Conformance mechanism	Description
Application profile	An application profile describes the use of metadata elements within a set of elements by means of rules and guidelines. The obligations and limitations are identified in the application profile. Additionally, it allows fulfilling the requirements of an application [Government On-Line Metadata Working Group, 2006].
Validation mechanisms	For each family of e-Documents, we will describe the main validation mechanisms used. A validation mechanism ensures that instance e-Documents comply with the structural and behavioural business rules of the information exchange context to which they pertain. It allows for more transparency and thus for better interoperability.
Conformance certification	A conformance certification is optional, if it is available. The certification ensures that interoperable e-Documents conform to a set of several requirements from applications.

2.5 Security mechanisms

Table 7 - Analysis framework: security mechanisms

Security mechanism	Description
Authentication Mechanisms	Proving that a document is coming from a claimed sender. <ul style="list-style-type: none"> • Digital Signatures of the hash of the document, to increase efficiency.
Integrity Mechanisms	Ensuring that the content of a document is not modified by a malicious party. <ul style="list-style-type: none"> • Parity bits and CRC (Cyclic Redundancy Check), as basic integrity checks. • One-way hash, such as SHA1, SHA2, SHA3 or MD5. The hash of a document act as its unique fingerprint. • MAC (Message Authentication Code)- a hash function "enriched" with a secret key to prevent an attacker of modifying a simple hash when attached to a document.

Confidentiality Mechanisms	<p>Encryption:</p> <ul style="list-style-type: none"> • Symmetric keys, using the symmetric ciphers such as AES, 3DES or RC4. • Asymmetric keys, using public key cryptography, such as RSA or ECC (Elliptic Curve Cryptography). • Hybrid, using symmetric cryptography for document encryption and asymmetric cryptography to protect symmetric keys. • Digital Signatures, using different levels of assurance, e.g., Fully Qualified Signature or Advanced Signature
Non-repudiation Mechanisms	<p>Ensuring that a signer cannot deny that she/he has signed a document.</p> <ul style="list-style-type: none"> • Digital Signatures, supported by a PKI (Public Key Infrastructure).

2.6 Governance mechanisms

Governance mechanisms allow the regulation of changes made to e-Document formats, including the libraries and methodologies via which they are created. Tailoring TOGAF's definition of governance in the context of this study, we argue that governance is about ensuring that the management of e-Document formats is conducted properly, i.e. following a set of guiding principles and practices, and in accordance with an organization's strategic objectives. In this vein, governance comprises well-defined roles and responsibilities, cohesive policies and principles, and decision-making processes that define, govern and regulate the lifecycle of e-Document formats.

In order for the public administrations to implement e-Document formats, the openness of the change management is a key evaluation criterion in the Common Assessment Method of Standards and Specifications [IDABC - CAMSS, 2012]. Openness is important to allow reuse in different information exchange contexts: public administrations will be reluctant to reuse an e-Document format when they cannot provide input into the change management process.

Table 8 gives an overview of the aspects according to which we will analyse the governance of e-Document formats.

Table 8 – Analysis framework: metadata Governance

Metadata Governance	Description
Goals	What are the long-term goals of cross-border/sector governance, management and reuse of common metadata?
Change management	Organisational roles: What are the roles responsible for metadata governance and what is their mandate? Is information on the terms and policies for the establishment

(openness)	<p>and operation of the organisation publicly available?</p> <p>Decision making process: How open is the management process regarding the taking decisions on the lifecycle of metadata, e.g. on updating a definition, releasing a new version or deprecating an existing one?</p> <p>Documentation: Is the change management process formally described and openly available? Are the e-Document formats openly available?</p>
Enforcement policy	<p>Sharing: which governance model is used to encourage/ensure sharing of metadata?</p> <ul style="list-style-type: none"> • Legal requirement: sharing is enforced by law; it is an official requirement; • Voluntary: sharing is not enforced, but encouraged on a voluntary basis. <p>Reuse: which governance model is used to encourage/ensure reuse of metadata?</p> <ul style="list-style-type: none"> • Legal requirement: reuse is enforced by law; it is an official requirement; • Comply-or-explain: reuse is not enforced by law, but public administration have to comply with the use of a particular specification or standard for metadata, or if they do not comply, explain publicly why they do not; • Oversight board: reuse is encouraged via project review committees; • Voluntary: reuse is encouraged via information campaigns.
Authoritative source	<p>Is there an authoritative source, e.g. a repository or a file server, on which the metadata is housed?</p>
Licensing framework	<p>Under which licensing framework are metadata shared and reused?</p> <ul style="list-style-type: none"> • No explicit licence; • Class 1: Traditional, proprietary licence; • Class 2: Free to use and redistribute, no modifications allowed; • Class 3: Free to use, redistribute, and modify via copy left licence (e.g. CeCILL); • Class 4: Free to use, redistribute, and modify via non-copy left licence (e.g. Academic Free Licence).
Quality controls	<p>What is the quality management process for metadata?</p>

Metadata Schema	<ul style="list-style-type: none"> • Vocabulary: Is there a common vocabulary in place, such as ADMS, for documenting metadata? • Identifiers scheme: Are there common guidelines and design patterns for creating identifiers for the metadata? • Schema documentation: Is there schema documentation in place, which explains commonly agreed definitions about the meaning of the data? • Multilingualism: Are different languages supported for the metadata properties and/or values?
------------------------	--

2.7 Usage

In order to measure the usage of e-Documents in the Trans-European Systems, metrics are collected on the purposes of the use of e-Documents in specific situations. The metrics should also assess how much of the exchanged e-Documents are conform to the standards of the identified families.

These metrics – where available – are collected by means of interviews and desk research.

Table 9 - Analysis framework: usage

Usage	Description
#formats	Total number of e-Document formats.
#implementations	Total number of known implementations in production-grade software, not counting individual instances of the software.
#transactions	Number of e-Document exchanges annually.

3 FINDINGS

This section formulates a number of general findings based on a comparative analysis of the twelve case studies on e-Document formats used in Trans-European Systems analysed in detail in Annex I. The analysis was conducted on the basis of preparatory desk research and a validation interview with a project manager or enterprise architect of the corresponding Trans-European System.

The selection of the twelve Trans-European Systems is based on the scope criteria described in Section 1.4. It should be noted that this selection is only a *sample* within the population of Trans-European Systems that use e-Document formats. Annex III contains an indicative list of seventy systems identified in the context of ISA Action 2.14 [Kurt Salmon, 2013]. Also systems like the Internal Market Information System (IMI) and Réseau permis de conduire/Driver Licence Network (RESPER) are relevant systems that could be analysed at a later point in time.

Table 10 - Families of e-Document formats included in this analysis

Identified families of e-Document formats
1. CEN Business Interoperability Interfaces on public procurement in Europe (CEN/BII) used by e-Prior and PEPPOL
2. e-Justice Communication via Online Data Exchange (e-CODEX)
3. Electronic Exchange of Social Security Information (EESSI)
4. European Criminal Records Information System (ECRIS)
5. European Register of Road Transport Undertaking (ERRU)
6. European Car and Driving Licence Information System (EUCARIS)
7. Tachograph Network (TACHOnet)
8. European Patients - Smart open Services (epSOS)
9. Eurofiling: financial reporting based on XBRL used by the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) and proposed by XBRL Europe
10. Virtual Company Dossier (VCD) used by PEPPOL
11. Omnifarious Container for e-Documents (OCD) used by SPOCS
12. International Commission on Civil Status (ICCS)

3.1 Descriptive metadata

There is insufficient publicly available information about the analysed e-Document formats

We noticed that there is often insufficient publicly available information about the e-Document format for third-parties to consider reusing them – fully or only one particular aspect. In particular, the following is missing:

- **Lack of introductory descriptions:** Performing the analysis as outsiders, we noticed that there is often insufficient information available for people that are not familiar with a trans-European system to identify what the e-Document formats are about and whether there is anything – e.g. a method, a definition, a set of reference data – that can be reused. For example, although all the large-scale pilots such as epSOS, e-CODEX, and SPOCS make their deliverables publicly available, these deliverables do not necessarily provide an understandable introduction about the usage of e-Document formats to a reader that is an outsider to the project.
- **Lack of availability:** Many e-Document formats cannot be retrieved online; and are at best retrievable upon request with a given contact point. This lack of availability creates a significant barrier to the reuse of these specifications.

Supporting cases: ECRIS, ERRU, EUCARIS, TACHOnet, and the epSOS' MVC lack publicly available information.

Counter-example: CEN/BII, e-CODEX had sufficient information publicly available.

Most analysed e-Document formats are at best informally described, descriptive metadata is not available in machine-readable form expressed with the Asset Description Metadata Schema (ADMS)

Only two (e-CODEX¹¹ and ICCS) out of twelve analysed families of e-Documents have a description of their e-Document formats that follows the Asset Description Metadata Standard (ADMS). Creating a machine-readable description of e-Document families achieves that these descriptions are created once and can be published on many platforms that can read the ADMS RDF format.

Half of the analysed e-Document formats are not available under an open licence

Six out of twelve analysed families of e-Document formats were not available under an open licence. Licences to reuse e-Document formats may not be known (e.g. ICCS), creating a juridical blur in the way it is possible to reuse them in other

¹¹ e-CODEX catalogue of interoperability solutions

<https://joinup.ec.europa.eu/catalogue/repository/e-codex-catalogue-interoperability-solutions>

platforms. Some European Commission projects have not published their formats under a specific license. Others make their specifications available using licences such as the EU Public Licence, (e.g. e-CODEX, VCD, etc.).

Significance of this finding: A licence provides to the users and re-users information about what exactly they can do with the e-Document format. Interoperability is difficult, if no explicit licence is provided. A user does not know what can be done with the e-Document format – the default legal position is that nothing can be done without contacting the owner on a case-by-case basis.

Supporting cases: CEN BII, e-CODEX, OCD, VCD, Eurofiling, and epSOS formats are available under an explicit licence.

Counter-evidence: EUCARIS, TACHOnet, ERRU, ECRIS and ICCS formats are not distributed under a licence.

3.2 Context

The analysed e-Document formats are all created for a single information exchange context

Trans-European Systems have their own specific administrative, geopolitical and legal context. This context drives the definition of the semantics, which allows conveying very specific and precise information on the topics to be exchanged. However, when designing e-Document formats, little attention is paid to their possible cross-sector reuse.

Significance of this finding: When e-Document formats are created for a specific context of information exchange, there is a risk to create context-specific silos of information. To alleviate this, there should be a formal process to look for reutilization of existing data elements in generic contexts that could ease the development and enhance the overall interoperability. An effort should be made to align concepts with other sectors, avoiding the creation of context-specific silos of information when referring to common data elements.

Supporting cases: e-CODEX, EESSI, ECRIS, ERRU, EUCARIS, TACHOnet, epSOS, Eurofiling, VCD, OCD and ICCS

3.3 e-Document engineering method

More than half of the cases analysed use standard e-Document engineering methods

Seven out of twelve analysed families of e-Document formats define e-Document formats by following a standard e-Document engineering method developed and maintained by a standards body. The use of standard methods allows for the reuse of common tools. In some case, we nonetheless witnessed that no common tools were used. Two situations seem to exist:

- **Manual schema creation:** when there are few documents to define and they are not complex, the main task is defining the actual syntax of e-Document formats, and this activity is performed in an artisanal way, even hand coding the schemas from scratch, without following any methodological approach. This is for example the case for the e-Document formats created by ECRIS, TACHOnet and ICCS.
- **Custom-designed tools:** when there are more documents and they could be complex, there is a tendency on developing proprietary tools that risk not to be further maintained when the project is over. Even for the tools developed with open-source licenses, if there is not a sustainability model for this tool's maintenance, they may end up being not used and abandoned. An example for a custom-made tool (that is however also used in other contexts) is the Metadata Workbench used by e-CODEX.

Significance of this finding: The use of standard e-Document engineering methods would make it easier for public administrations to produce their e-Document formats in a formal way, producing standard outcomes that could be reused in other projects. At present, a lot of time is spent on defining the framework for producing the e-Document formats.

Supporting cases: CEN/BII, e-CODEX, epSOS, Eurofiling, VCD and OCD have standard e-Document engineering methods.

Counter examples: ECRIS, TACHOnet, EUCARIS, ERRU, ICCS do not use standard e-Document engineering methods.

Half of the cases analysed reuses standard libraries of data elements for syntax binding

Already six families of e-Document formats are systematically reusing the concepts and elements from common libraries of data elements:

- e-CODEX reuses the Core Component Library from UN/CEFACT;
- CEN/BII and VCD reuse the UBL Common Aggregate Components library from OASIS;
- epSOS reuses the health library provided by HL7; or
- Eurofiling reuses the financial library provided by the XBRL standard.

ERRU and TACHOnet are both exchanging information about drivers across Europe, the platforms and systems they use are similar (sTESTA, HTTPS, Digital Certificates, etc.), the national source databases may be the same, but XML message fields are different, for example, in one, they use "familyName" and in the other "Surname".

Significance of this finding: Using common libraries has several benefits:

- 1) A standard catalogue or dictionary of terms ensures not forgetting important elements in your e-Document;
- 2) Provides exact semantics of the concepts; and
- 3) A potential for interoperability with other projects. The usage of common data elements in different context-specific projects could lead to better cross-sector interoperability.

There are different aspects of reuse that have to be highlighted. The Core Component Library is a library of concepts, of abstract Core Components from where the actual Business Entities can be inferred, but not directly reused, while the UBL and the ISA Core Vocabularies are two sets of actual Business Information Entities that can be reused.

With the first approach, the inference method from the Core Component Library to the actual XSD Schema is loose and this implies that two different implementations of the same CCL could be non-interoperable.

On the contrary, reusing the Core Vocabularies or UBL Business Information Entities will result in interoperable schemas. Nevertheless, reusability also creates issues as it makes the schemas larger and, in some cases, there is a need for customization with an application profile to get usable schemas.

Supporting cases:

- **CEN/BII:** has syntax bindings for both the UN/CEFACT CCL and UBL;
- **e-CODEX:** uses the UN/CEFACT CCL to build e-Documents;
- **VCD:** Reused concepts from the UBL Library;
- **OCD:** Reused concepts from the VCD and ISA Core Vocabularies;
- **epSOS:** Reused the HL7 CDA Library; and
- **Eurofiling:** Reused the XBRL standard.

Counter-evidence: ECRIS, ERRU, EUCARIS, TACHOnet, and ICCS do not reuse common libraries.

Uptake of standard XML naming and design rules

Five of the twelve analysed families of e-Document formats use standard XML naming and design rules.

Significance of this finding: The structure (or syntax) of the e-Documents is a key factor to enable interoperability. XML Naming and Design Rules are sets of technical rules used to create XSD Schemas. For instance,

- Rules on the naming of the XML tags, stating that they must be written in English or in upper camel case,
- Rules on data types, specifying the metadata for each allowed data type,
- Rules on the architecture of the schema, defining which schemas should be imported and so on.

Software tools like eDoCreator, Crane UBL Generator or GEFEG.FX that allow automation of schema production are based on standard XML Naming and Design Rules.

The use of standard XML naming and design rules has among others the following benefits:

- Creating e-Document formats following known patterns eases the work for the developers when implementing these e-Documents in their systems.
- The usage of standard XML naming and design rules promotes the creation of tools to automate the schema production task.
- The use of a standard XML naming and design rules facilitates the standardisation of the new e-Document format. Using standard XML naming and design rules allows standardization initiatives to adopt the produced XSD schema artefacts. An example of this is what happened with the Spanish CODICE e-Document formats. The Spanish Ministry of Economics developed a national standard for electronic tendering e-Documents called CODICE. The documents produced in that project followed the UBL Naming and Design Rules. After a harmonisation process, the documents developed for electronic tendering ended up being adopted as new e-Document types in the UBL 2.1 standard package.

Supporting cases: CEN/BII, e-CODEX, epSOS, VCD, OCD use or recommend standard XML naming and design rules

Counter-evidence: ECRIS, ERRU, EUCARIS, TACHOnet and ICCS.

XML and XSD are the dominant schema representation techniques

Within the scope of our research we have found no e-Document formats specified using for example RDF Schema or EDI. Old technologies such as EDI are not implemented in modern projects, even though they are still widely used in some industries.

RDF and OWL are not used to define e-Documents. These technologies are used for flexible data integration. Some projects like the PEPPOL and SPOCS have used OWL/RDF to create the knowledge for mapping criteria and evidences in a pan-European context, but it is not used to create the metadata of the VCD or OCD documents.

The majority of the assessed projects are relying on XML for the creation of e-Documents. And they are using XSD Schema for definition of the structure and for syntactical validation.

There is a small set of projects that start using Schematron to implement business rules as validation artefacts to allow testing conformance of e-Document instances.

Significance of this finding: The e-Document engineering method can be focused on the XML and XSD technologies, and take into account the newer technical methods to validate against business rules using Schematron.

Supporting cases: e-CODEX, EESSI, ECRIS, ERRU, EUCARIS, TACHOnet, epSOS, Eurofiling, VCD, OCD, and ICCS have e-Document formats defined as an XML Schema.

Counter-evidence: CEN BII is not using XML or XSD to represent the e-Documents, as it promotes the reuse of existing schemas by OASIS and UN/CEFACT. They use HTML and Word to define the transaction models that will be bound to specific syntaxes and Schematron to describe the intended behaviour of the documents.

3.4 Conformance mechanisms

Application profiles facilitate the usage of e-Document formats in other information exchange contexts

The e-Document formats used in the context of the PEPPOL and epSOS large-scale pilots seem to indicate that some e-Document formats maintained by standardisation organisations can be reused in different information exchange contexts. Both projects have created their own application profiles that add further context-specific restrictions to the information exchange.

In the case of PEPPOL, their application profiles have already been further refined in national contexts such as Norway or Sweden, where the usage is rapidly increasing.

CEN BII has defined only application profiles, and finally has bound them to UBL and UN/CEFACT. The idea behind CEN BII is to guide on how to use a syntax standard instead of defining a new one.

Significance of this finding: The definition of syntaxes is not enough. Especially when reusing generic standardised formats, the e-Document engineering method has to also focus on defining application profiles to demonstrate and specify in more detail how the e-Document formats have to be used, fostering uptake and usage on the target audience.

Supporting cases:

- CEN/BII: defines profiles to be used with UBL or UN/CEFACT in electronic public procurement.
- epSOS: defines application profiles of the HL7 CDA standards.
- Eurofiling: defines application profiles for the XBRL standard.

Conformance testing and certification is important when on-boarding a large number of partners

Experience from the PEPPOL case study shows that the use of conformance testing is particularly relevant when a large number of partners must be on-boarded. Even when two systems that exchange information claim conformance to a particular e-Document format, it may happen that they are not interoperable due to misunderstandings or different implementation decisions. Therefore, conformance testing is a key success factor for the deployment of projects involving heterogeneous and multiple parties.

Significance of this finding: Creating validation artefacts enable implementers to ensure they are implementing the e-Document format in the way that it was designed for. The e-Document engineering method should take this activity into account.

It would be also relevant to promote the creation of conformance certificates in order to ensure compliance to the e-Document standards.

Supporting cases: PEPPOL and epSOS have created validation artefacts in order to facilitate conformance testing within their user communities.

Few e-Document formats come with a reference implementation capable of producing and/or consuming e-Documents in that format. (This may be because they have been created to achieve interoperability between existing systems.)

In only three cases, we have found a reference implementation capable of producing and/or consuming e-Documents in that format. In the case of epSOS, OpenNCP provides a feature capable of rendering epSOS CDA documents (patient summary and ePrescription documents) into HTML for validation. In the case of Eurofiling, there is an open source tool called Openfiling¹² that is able to produce and consume the specific XBRL formats. SPOCS provides modules that allow the creation, verification and extraction of OCD containers both in ZIP and PDF formats.

Significance of this finding: A reference implementation can be used for testing the implementation of the e-Document formats in software. It can be used to foster interoperability beyond available conformance tests.

Supporting case: Eurofiling, epSOS, SPOCS OCD

Counter-evidence: no reference implementation was found for the e-Document formats for CEN/BII, e-CODEX, EESSI, ECRIS, ERRU, EUCARIS, TACHOnet, PEPPOL VCD and ICCS.

3.5 Security

Most cases rely on security features such as standard digital signature formats and document containers applied end-to-end to the e-Documents themselves.

The analysis of the existing e-Document formats and associated schemes shows that security is taken into account in all identified projects. The extent to which security is addressed highly depends on the type of information in scope. For instance, if the e-Documents are dealing with legal (e-CODEX), personal (epSOS) or business critical (CEN/BII) information, security requirements are specified in more detail, which is in accordance with the risks associated with the exchanged information.

Authentication, integrity and non-repudiation are achieved primarily using digital signatures in all identified projects. Interoperability between the analysed security mechanisms is achieved in two ways:

1. Using specific software modules to transform party-specific digital signature formats, like e.g. the "connectors" in e-CODEX project. It relies on the "Trust-OK" token to achieve authenticity and integrity in the document exchange process.

¹² <http://www.openfiling.info/>

2. Relying on widely accepted digital signature formats, such as XAdES (and PAdES for PDF), as in the case of Eurofiling and the Omnifarious Container for e-Documents

The first approach may seem easier to implement and manage from a technical point of view; however it raises some practical and legal concerns. The second approach is more generic, and it is supported by a European legal framework. Relying on the standard digital signature formats and associated containers, targeted in the scope of eIDAS standardisations and regulation process, interoperability can be achieved on much larger scale, also reaching high security levels, such as qualified digital signatures. For more details how interoperability of security in trusted services is addressed in Large Scale Pilots (LSPs), the reader is referred to ENISA study on Trust Service Providers [ENISA, 2013]. Where possible, consider using widely accepted digital signature formats in end-to-end communication, such as PAdES and XAdES.

3.6 Governance mechanisms

The majority of the analysed e-Document formats have a formal governance mechanism.

The definition and maintenance of e-Document formats, and in particular in the context of a Trans-European System where numerous stakeholders are involved, requires defining a formal governance mechanism. Eight out of eleven cases have put in place a formal governance mechanism. They generally used a two-level model of governance composed of a "group of experts", discussing and initiating changes, and a "steering committee", managing change proposals.

Significance of this finding: Trans-European projects with multiple systems and processes need a formal governance mechanism with a system of decision rights, executed according to agreed-upon models which describe who can take what actions with which information, when, under what circumstances, and using which methods.

Supporting cases: CEN BII, ECRIS, ERRU, EUCARIS, TACHOnet, epSOS, Eurofiling, and ICCS have a formal governance mechanism for their e-Document formats.

Counter-evidence: e-CODEX, VCD, OCD have a governance mechanism which is not formalised for their e-Document formats.

Unknown: EESSI.

The change management process is not always open.

The analysis demonstrates that the change management process is formally defined but most of the time this is not an open one. The change is limited to the experts, who initiate the change, and a committee, who manages the change, involved in the project.

Indeed, in some case the governance mechanism is not formalised and not public. Thus the change management process is not open to outsiders, and the experts may not be users.

This could also be explained because some of the projects are at the level of implementation. It would be open once the production stage will be reached.

Significance of this finding: An open change management process improves the quality (accurate definition, etc.) and also the creation or the deprecation of the metadata. With an open approach, more users can be involved in the metadata lifecycle and by giving them more decision power it will encourage them to implement the solution. Moreover it will also give a better assurance on how the metadata will evolve.

Supporting cases: CEN BII and Eurofiling have an open change management process.

Counter-evidence: e-CODEX, ECRIS, ERRU, TACHOnet, OCD, VCD have no open change management process.

All e-Document formats are stored in an authoritative repository.

Our study shows that all e-Document formats are stored in centralized access points (file server, repository, etc.), which serve as an authoritative source. These access points are not necessarily all publicly accessible.

Significance of this finding: In the context of projects where numerous e-Document formats are produced, a centralized repository has several benefits:

- **Decreased risk:** with an authoritative source, all edits and manipulations to core documents are housed and stored centrally. This model allows for access controls, detailed audit trails, and enables team members to access consistent documents.
- **Documents consistency:** projects can achieve consistent document management and distribution to all its stakeholders. Upon entry into the authoritative repository, the documents can be cleaned up, validated, and readied for distribution.
- **Specification quality:** A centralized approach enables the establishment of standards across the project.
- **Operational efficiency:** when an authoritative source controls document formats centrally, projects can more easily eliminate manual processing.

In the opposite situation, specification documents are sometimes shared with stakeholders via the experts involved in the "group of experts". This model could introduce problems of consistency and quality in the specification documents provided because it depends on an expert who may share the wrong specification documents and thus may reduce efficiency. If the documentation is not available, there is a huge risk of non-conformance. Furthermore, later projects will not be able to lean on experience of the development of these formats, or only with difficulties. No evidence of this situation was encountered

Supporting cases: CEN/BII, e-CODEX, ECRIS, ERRU, EUCARIS, TACHOnet, epSOS Eurofiling, VCD, OCD, and ICCS.

Unknown: EESSI.

3.7 Usage

e-Document formats are used in high-volume administrative processes.

The actual amount of implementations of e-Document formats in production-grade software is prominent for five out of eleven e-Document families. When disclosed, the number of e-Document formats exchanges amounts from tens of thousands of requests to one million on an annual basis. For ECRIS, we noted that over the past few years, the amount of enquiries has increased significantly, with the on-boarding of more partners.

Significance of this finding: the volumes of e-Documents processed indicate that the exchange of e-Document can be an efficient and effective pattern of information exchange with public administrations.

Supporting cases: ECRIS, ERRU, EUCARIS, TACHOnet and Eurofiling

Counter-evidence: no information on the number of e-Document formats exchanges for CEN/BII, e-CODEX, EESSI, epSOS, PEPPOL, SPOCS and ICCS was available.

4 RECOMMENDATIONS

This section includes recommendations regarding e-Document engineering, governance, conformance checking, and reuse based on the good practices identified in the analysed case studies.

4.1 Use standard e-Document formats and create application profiles

Rather than creating new e-Document formats from scratch, organisations should consider using existing standard e-Document formats – when available – and place them into their particular geopolitical, legal, and administrative context. The latter can be done by defining *application profiles* of standard e-Document formats.

The mechanism of application profiles is demonstrated by the CEN/BII profiles used by e-Prior and PEPPOL (see the case study in Annex I.1). The CEN CWA 16558 BII Architecture specification¹³ describes the generic method applied for the development and specification of profiles. Similarly, our analysis of epSOS (see Annex I.8) indicates that for each document type epSOS has defined a specific profile (CDA document template), derived from known CDA templates.

Rationale: Where available, the use of application profiles of standard e-Document formats lowers the implementation costs through the use of standard specifications. This is especially the case for message-based information exchange with numerous parties: rather than starting the development of an e-Document format and systems to process them from scratch, existing standards and tools can be maximally used reducing development costs. The use of standards may also help reducing maintenance cost of the specification, as funding the lifecycle management of a profile is likely to cost less than funding the maintenance of an ad-hoc specification. Finally, the reuse of standard e-Document formats also has positive network effects as it reduces the amount of interoperability conflicts in a large ecosystem of information exchange partners and facilitates the mesh-up of data that originates from e-Documents.

4.2 Use a standard e-Document engineering method

Use a standard e-Document engineering method such as these methods developed by UN/CEFACT, OASIS, CEN/BII, Health Level 7, and XBRL international. These e-Document engineering methods offer a methodology for requirement analysis and conceptual modelling, a standardised library of data types and elements, and conventions for syntax binding or schema production such as XML naming and design rules.

The use of standard e-Document engineering methods is demonstrated in the following case studies.

¹³ CEN CWA 16558 BII Architecture specification
<http://www.cenbii.eu/deliverables/cen-bii-2/cwa-16558-bii-architecture/>

- UN/CEFACT e-Document engineering method (used by e-CODEX);
- CEN BII e-Document engineering method (used by ePRIOR and PEPOL);
- HL7 method for healthcare (used by eSOS); and the
- XBRL method for business reporting (used by the eurofiling project).

Other case studies seem to indicate that considerable effort was spent on defining an ad-hoc e-Document engineering method used for producing the e-Document formats.

Rationale: The use of a standard e-Document engineering method, library of data elements, and XML naming and design rules makes it easier for public administrations to produce e-Document formats in such a formal way, producing standard outcomes that could be re-used in other projects. This has several **benefits:**

- **Speeds up the process to create e-Document formats:** A methodology depicts a systematic approach to build the XML Schemas and validation artefacts, reducing the uncertainty of the production process and speeding up the overall project.
- **Enhances documentation:** Every step is documented in a formal way. Project teams have to provide clear definition of goals and rationales for elements and components. Documentation from goals to the final implementation eases the understanding both for business and technical people.
- **Lowers the risk and decreases the cost:** The use of a standard e-Document engineering methods allows for the creation of tools to support the XML Schema production.
- **Facilitates maintenance and governance:** A clear method specifies the maintenance process of the artefacts and can provide guidance on long-term sustainability and governance.

4.3 Use existing tools for e-Document engineering

Use existing tools to design new e-Document formats and create e-Document schemas.

In the case studies, we have seen examples of the use of existing open-source and commercial tools, as summarised in Table 11. Conversely, it seems a bad practice to manually create e-Document formats or design one's own tools for designing e-Document formats and creating e-Document schemas.

Rationale: Tools reduce the production time and the risk of adding errors in the production phase. Hence, the overall production cost is drastically lowered.

Table 11 – List of identified reusable e-Document engineering tools

Tool	Key functionality	Type of licence	Owner/ Vendor	Reusability
Metadata Workbench (used by e-CODEX)	MWB is an integrated tool, in which the Core Components can be specified and that allows the derivation of BIEs and the specification of Business Documents.	Available on request		Generally reusable
GEFEG.FX (used by CEN/BII)	Information Modelling, Schema creation GEFEG.FX is a commercial tool for schema development and schema requirement management.	Commercial		Generally reusable
eDoCreator (used by SPOCS, PEPPOL)	The iSurf eDoCreator is an on-line tool that provides the CCTS-based document schemas.	Commercial	iSurf	Generally reusable
Enterprise Architect (used by INSPIRE)	This tool supports modelling, visualization and design platform based on the UML standard.	Commercial	SparxSystems	Generally reusable
Shapechange (used by INSPIRE)	Java tool that takes application schemas constructed according to ISO 19109 from a UML model and derives implementation representations.	Available under the GNU General Public Licence.	Tool was originally written by interactive instruments GmbH, and expanded by The MITRE Corporation.	Possible to reuse with some adoption
Crane Software GC-to- UBL NDR script (used by CEN/BII)	Crane's Genericcode to UBL NDR script implements the UBL Naming and Design Rules 2.1 XSD schemas and OASIS CVA (context/value association) files from an input OASIS genericcode expression of a compatible UBL NDR 2.1 spreadsheet	Available under the Modified BSD Licence	Cranesoftwrights	Generally reusable
Altova XML Spy (used by ECRIS, ICCS)	XML Editor	Commercial licence	Altova	Generally reusable

4.4 Provide document conformance testing procedure and mechanisms

For those projects where there is a potential broad community of users to adopt the specifications, providing an explicit document conformance testing procedure and testing artefacts besides the guidelines and textual specifications has to be considered.

The testing can be at two different levels:

- Document instance level to ensure a document instance follows the e-Document format specifications.
- System capability conformance to ensure an IT system is able to submit an e-Document instance following the e-Document format and to receive any type of document that fulfils the e-Document format specification.

At least, the document instance level testing artefacts and mechanisms should be provided with the e-Document format specifications in order to ease the work for the implementers, helping them understanding the format and allowing to shorten the learning curve and the development time.

Most of the e-Document formats provide XML Schema language mechanisms that allow the testing of the structure of the e-Document instances. It would be a step forward with a great interest to add to these structural validation mechanisms, additional systems to allow testing the business rules associated with the document instances. There are different artefacts that allow checking the validity of business rules of e-Document instances such as XSLT or Schematron. For these projects with a real large set of potential users, it would be a major achievement to provide a **reference implementation** against which others could test their implementation.

There is an on-going CEN Workshop¹⁴ that has been set to define a General eBusiness Interoperability Test Bed that has the potential to solve the settlement of this system capability conformance.

Rationale: Even with well documented e-Document formats, we have seen that different groups of implementers can end up with non-interoperable solutions. This can be due to their need to support additional requirements, or because they use them inconsistently. These inconsistencies can be minimized if the e-Document format specification is accompanied with sample e-Document instances illustrating common use cases, which can better demonstrate how the e-Document instances are supposed to be used in different situations.

Adding to the sample e-Document instances tools and artefacts that can help testing the structure and business rules of the e-Document instances would allow the implementers to setup testing frameworks that would ease their development and deployment work.

¹⁴ <http://www.cen.eu/work/areas/ict/ebusiness/pages/ws-gitb.aspx>

4.5 Follow good practices for metadata governance and management

Organisations should define a formal governance mechanism with roles, responsibilities, and decision-mechanisms to manage the lifecycle of the e-Document formats. Additionally, they should define and operate clear lifecycle management processes for e-Document formats. Such processes include for example how updates to the e-Document format are published, or how external contributions and change requests are handled. Regarding the latter, organisations should consider a change management process that is open to third-party change requests.

The reader is referred to deliverable *D4.2 Methodology and tools for Metadata Governance and Management for EU Institutions and Member States* which includes a generic specification for metadata governance and management. An important principle is the separation of data models from reference data. For example, UBL 2.0 expresses code list values in separate files using the genericcode format, instead of binding those values inside the document schemas.¹⁵

Rationale: A formal governance mechanism and lifecycle management processes indicates how decisions about e-Document formats are taken and implemented. A formal governance mechanism is an essential coordination mechanism, especially when involving a large number of stakeholders with different nationalities and backgrounds. Openness is a key element in this: public administrations will be reluctant to use an e-Document format when they cannot provide input into the change management process.

The separation of data models and reference data can be motivated because they have different life cycles. These differences are linked to the different needs for stability versus flexibility. Separating data models and reference data allows for independent updates of one or the other.

Data models are strongly linked to the interoperability of applications and therefore changes in a data model have a direct effect on the applications that are based on it. In many cases, software systems will need to be rebuilt importing the new model and upgrading the functionality before they can interoperate with others. In practice, changes in data models will be relatively infrequent (less than annual) and changes will be accompanied by a strongly managed implementation plan aligned with a software upgrade cycle.

Reference data is usually more loosely linked to the basic functionality of applications. Changing or adding a code in a code list will not have a disruptive effect on the existing functionality. These types of changes may also occur with a higher frequency (one or more times per year) than model changes, and are usually easier to propagate through a network.

¹⁵ <https://www.oasis-open.org/committees/ubl/faq.php>

4.6 Make e-Documents available for reuse

Owners of e-Document formats should make them available for reuse by administrations from other sectors and/or other countries. Hereby, they should be made aware of the importance of clear licensing arrangements that specify unambiguously under which conditions the metadata can be reused.

The process involves the following steps:

1. Choose an open licence such as the ISA Open Metadata Licence¹⁶ or a Creative Commons¹⁷ licence. EU Institutions often use the European Union Public Licence or the EU legal notice.
2. Make the e-Document formats publicly available for download on the web under the licence chosen above.
3. Rigorously document the e-Document formats and make the documentation publicly available on the web.
4. Describe the e-Document formats with ADMS and publish it on the Joinup¹⁸ platform. The e-Document formats analysed in this report have been described with ADMS and published on Joinup, as described in Annex II.

Rationale: The sharing and reuse of e-Document formats in a cross-border and cross-sector context contributes to enable positive network effects of interoperability. By publishing the e-Document formats with an open licence, other public administration are sure that they have the right to reuse them. If no licence is in place, users will hesitate to use the e-Document format, since it is effectively not clear to them if they can do so and under which conditions. Additionally, Good documentation is essential to enable others to understand and reuse the e-Document formats.

The reuse of an e-Document format by other public administrations can also provide valuable feedback, helping the initial public administration in improving the e-Document format.

¹⁶ <https://joinup.ec.europa.eu/category/licence/isa-open-metadata-licence-v11>

¹⁷ <http://creativecommons.org/>

¹⁸ <http://joinup.ec.europa.eu/>

5 CONCLUSION

The goal of this study was to analyse families of e-Document formats used in Trans-European Systems, to identify a number of best practices and formulate recommendations. To this end, we sketched the context in which public administrations typically use e-Documents and provided an introduction to the research questions of the study (Chapter 1). We created a framework of analysis (Chapter 2) in accordance with these research questions. We presented the findings (Chapter 3) from applying the aforementioned analysis framework to twelve families of e-Document formats – the detailed analysis is included in Annex I. We also created ADMS-conform descriptions of the analysed e-Document formats and published them on Joinup (Annex II). Finally, in Chapter 4 we formulated a number of recommendations for e-Documents.

5.1 Findings on structured e-Document formats used in Trans-European Systems

The analysis of the twelve families of e-Document formats revealed that there is a considerable amount of heterogeneity. Our findings, structured in accordance with the research questions formulated in Section 1.3, can be summarised as follows:

Descriptive metadata: It proved not easy to create accurate and informative descriptions about the analysed e-Document formats using *only* the information that is publicly available. This lack of descriptive metadata combined with missing licensing information, is a barrier to the reuse and thus uptake of e-Document formats.

Context: Although e-Document formats of Trans-European Systems are created for *cross-border* information exchange, they are currently not designed to function in a *cross-sector* setting, i.e. by *different* Trans-European Systems.

e-Document engineering method: In our analysis, standard e-Document engineering methods and standard libraries of data elements are being used in at least half of the analysed cases; however all different. This can be explained because different domains such as public procurement, e-Health, or financial reporting benefited from already existing standardisation efforts by UN/CEFACT, OASIS, CEN, HL7, and XBRL international. The CEN/BII profiles demonstrate that semantic interoperability can be achieved even when different syntax bindings, i.e. e-Document formats by UN/CEFACT and OASIS UBL, are being used.

Conformance mechanism: For conformance testing, all analysed e-Document formats rely on an e-Document validation mechanism based on an XML Schema language such as XSD or Schematron. In addition to this, some cases such as PEPPOL or epsOS work with application profiles that add further restrictions to the use of an e-Document format in a particular administrative process or transaction. Some systems also define reference implementations to better test interoperability, beyond the mere conformance to the specification of the e-Document format. Only in cases where a large number of partners need to be interconnected (e.g. PEPPOL), an explicit conformance testing procedure was used.

Security: Authentication, integrity and non-repudiation are achieved primarily using digital signatures in all identified projects. For this it is important to rely on the standard digital signature formats and associated containers targeted in the scope of eIDAS standardisations and regulation process as it allows achieving interoperability of security mechanisms on much larger scale, also reaching high security levels, such as qualified digital signatures. For more details how interoperability of security in trusted services is addressed in Large Scale Pilots (LSPs), the reader is referred to ENISA study on Trust Service Providers [ENISA, 2013]. Where possible, consider using widely accepted digital signature formats in end-to-end communication, such as PAdES and XAdES.

Governance mechanism: Most analysed cases have a formal governance mechanism with roles, responsibilities, and decision-mechanisms to manage the lifecycle of the e-Document formats. Fewer also maintain a change management process that is open to third-party change requests. Openness is important to allow reuse in different information exchange contexts: public administrations will be reluctant to reuse an e-Document format when they cannot provide input into the change management process.

Usage: For five out of twelve cases, we have found evidence that the e-Document formats are already being used in production-grade systems. For these systems, the number of exchanged e-Documents ranges from tens of thousands of requests to one million on an annual basis. This fact alone demonstrates that the exchange of e-Documents is a working pattern of information exchange in cross-border interactions with public administrations.

5.2 Relevance of our recommendations

It is the intention of this study that the best practices identified from the case studies and the subsequent recommendations given in Chapter 4 can serve as guiding principles for organisations that are using or starting to use e-Document formats. The underlying motivation is to foster the harmonisation in e-Document formats and thus contribute to the efficient and effective delivery of public services across borders and sectors. The recommendations can be summarised as follows:

1. Rather than creating new e-Document formats from scratch, organisations should consider using existing standard e-Document formats – when available – and place these into their own geopolitical, legal, and administrative context. The latter can be done by defining *application profiles* of standard e-Document formats and build consensus on their usage within a particular information exchange context.
2. Organisations should consider using a *standard* e-Document engineering method that offers a methodology for requirement analysis and conceptual modelling, a standardised library of data types and elements, and conventions for syntax binding or schema production such as XML naming and design rules. Standard methods make it easier for public administrations to produce e-Document formats in a formal way, producing standard outcomes that could be re-used in other projects. Good e-Document formats do not only define a syntax binding or create a schema for the e-Document

format, but also pay attention to information model requirements, definitions, and business rules.

3. Organisations should consider using *existing tools* that support standard methods to design new e-Document formats and create e-Document schemas. In the case studies, we have seen examples of the use of existing open-source and commercial tools, as summarised in Table 11.
4. In those information exchange contexts where there is a potential broad community of users to adopt the specifications, organisations should consider providing an explicit document conformance testing procedure and testing artefacts in addition to guidelines and textual specifications.
5. Organisations should define a formal governance mechanism with roles, responsibilities, and decision-mechanisms to manage the lifecycle of the e-Document formats. Additionally, they should define and operate clear lifecycle management processes for e-Document formats. Such processes include for example how updates to the e-Document format are published, or how external contributions and change requests are handled. Regarding the latter, organisations should consider a change management process that is open to third-party change requests. Openness is key as public administrations will be reluctant to use an e-Document format when they cannot provide input into the change management process.
6. Owners of e-Document formats should make them available for reuse by administrations from other sectors and/or other countries. Hereby, they should be made aware of the importance of clear licensing arrangements that specify unambiguously under which conditions the metadata can be reused. To make reuse easier, it is also necessary to make accurate and accessible descriptions about e-Documents formats available; preferably documented using the Asset Description Metadata Schema (ADMS).

5.3 Future work

As a follow-up to this work, we will investigate and pilot the use of standard e-Document engineering methods in combination with standard libraries of such as the Core Vocabularies of the ISA Programme. This work will be reported in deliverable 'D1.2 Recommendations for public administrations on e-Document engineering methods'.

6 ACKNOWLEDGEMENTS

Specific acknowledgement is due to:

Person	Organisation / Trans-European System
Luisa Guedes	European Commission DG MOVE / ERRU / TACHOnet
Jaime Lopez Loosvelt	European Commission DG JUSTICE / ECRIS
Kornelis Drijfhout (eTendering) Jaap van der Marel (Secretariat)	CEN/BII
Cristian Tatu-Caravan (technical project manager) Silvia Kersemakers (project manager)	European Commission DG EMP / EESSI
Ignacio Boixo (Eurofiling Community Coordinator)	Eurofiling
Sjaak Kempe	EUCARIS
Giancarlo De Stefano Anders Kingstedt Sven Rasmussen	PEPPOL Consortium
Muriel Foulonneau Ana Branco Joseph Grech Fergal Marrinan	SPOCS Consortium
Marcello Melgara Anna Adelöf Giorgio Cangioli Juergen Wehnert Gottfried Heider Rainer Hoerbe Fredrik Linden	epSOS Consortium
Fineke Beukema Ronald Smit E.J. Steigenga A.O.H. Wauters Carsten Schmidt	e-CODEX Consortium
Dimitris Alexandrou Paul Polydoros	ICCS

7 REFERENCES

- Eurofiling Minutes*. (2014, January 23). Retrieved January 30, 2014
- CEBS. (2005, June 7). *European banking supervisors support the adoption of digital reporting*. Retrieved January 30, 2014, from <http://www.eba.europa.eu/-/european-banking-supervisors-support-the-adoption-of-digital-reporting>
- CEN/WS XBRL. (2013). *Improving transparency in financial and business reporting - Harmonisation topics - Part 1: European data point methodology for supervisory report*.
- CIEC. (2013). *Information note*. Strasbourg: CIEC.
- CIEC-ICCS. (1999). *Civil Status and Perinatal Death in ICCS Member States*. Strasbourg: CIEC - Secrétariat Général.
- COREP. (2005). *Leveraging XBRL on Banking Supervision*. Tokyo.
- COREP. (2006, January 13). *Guidelines on a common reporting framework (COREP)*. Retrieved January 30, 2014, from <http://www.eba.europa.eu/-/guidelines-on-common-reporting-200-1>
- Council of the European Union. (2009). Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA. *Official Journal L 093*, 33-48.
- Directorate General: Energy & Transport. (2011, 01 17). Tachonet Project: XML Messaging Reference Guide.
- EBA. (2013). *COREP/FINREP XBRL Taxonomy v2.0.0*. EBA.
- EBA. (2013). *Implementing Technical Standard on Supervisory Reporting (COREP, COREP Large Exposures and FINREP)*. Retrieved January 27, 2014, from European Banking Authority: <http://www.eba.europa.eu/regulation-and-policy/supervisory-reporting/implementing-technical-standard-on-supervisory-reporting-corep-corep-large-exposures-and-finrep->
- ECN. (2013, 10 21). *European Competition Network*. Retrieved 12 24, 2013, from European Commission: competition: <http://ec.europa.eu/competition/ecn/>
- ECN. (n.d.). *Joint Statement of the Council and the Commission on the Functioning of the Network of Competition Authorities*. Retrieved 12 23, 2013, from European Commission: competition: http://ec.europa.eu/competition/ecn/joint_statement_en.pdf
- e-CODEX. (2011). *D7.1 Governance and Guidelines Definition*. European Commission.

- e-CODEX. (2012). *D4.2: Concept for Implementation of WP4*. European Commission.
- e-CODEX. (2012). *D6.3 Concept for Implementation of WP6*. European Commission.
- e-CODEX. (2012). *D7.3 High Level Architecture Definition*. European Commission.
- e-CODEX. (2012). *e-Justice Communication via Online Data Exchange*. European Commission.
- e-CODEX. (2012). *Realizing cross-border e-Justice in Europe - Factsheet 4: e-Signature and e-Identity*.
- e-CODEX. (2013). *D3.10 Selection of possible pilots (update of D3.1)*. European Commission.
- e-CODEX. (2013). *D4.3: Developed Modules and Building Blocks*. European Commission.
- e-CODEX. (2013). *Work Package 4 - e-Signature and e-Identity*. Retrieved January 27, 2014, from e-CODEX: <http://www.e-codex.eu/about-the-project/work-overview/work-package-4.html>
- EESSI. (2013). *Electronic Exchange of Social Security Information*. Retrieved 12 24, 2013, from European Commission: Employment, Social Affairs & Inclusion: <http://ec.europa.eu/social/main.jsp?catId=869>
- EIOPA. (2013). *Solvency II*. Retrieved January 29, 2014, from EIOPA: <https://eiopa.europa.eu/en/fixed-width/activities/insurance/solvency-ii/index.html>
- EIOPA. (2014, January). *Data modelling and XBRL taxonomy design*. Retrieved January 30, 2014, from EIOPA: <https://eiopa.europa.eu/publications/eu-wide-reporting-formats/index.html>
- ENISA. (2013, December). *Trusted e-ID Infrastructures and services in the EU - Recommendations for Trusted Provision of e-Government services*. Retrieved from <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/trusted-egov>
- epSOS . (2014, January). *epSOS Architecture and Design - EED DESIGN 2.0 – Interoperability Specification version 1.0*.
- epSOS. (2013). *Auditing*. Retrieved January 16, 2014, from epSOS: <http://www.epsos.eu/technical-background/systems-standards/auditing.html>
- epSOS. (2013). *Glossary*. Retrieved January 23, 2014, from epSOS: http://www.epsos.eu/faq-glossary/glossary.html?no_cache=1

- epSOS. (2013). *Identification and Authentication*. Retrieved January 07, 2014, from epSOS: <http://www.epsos.eu/technical-background/identification-authentication.html>
- epSOS. (2013). *Patient Service, Order Service*. Retrieved January 16, 2014, from epSOS: <http://www.epsos.eu/technical-background/systems-standards/patient-service-order-service.html>
- epSOS. (2013). *Reference Implementation*. Retrieved January 16, 2014, from epSOS: <http://www.epsos.eu/technical-background/reference-implementation.html>
- epSOS. (2013). *Requirements*. Retrieved January 16, 2014, from epSOS: <http://www.epsos.eu/technical-background/security-aspects/requirements.html>
- e-SENS. (2013, August 27). *Electronic Simple European Networked Services - D6.1 Executable ICT Baseline Architecture*.
- e-SENS. (2013, October 24). *e-SENS WP62*. Poznan, Poland.
- ETSI. (2011). *Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)*. Sophia Antipolis: European Telecommunications Standards Institute.
- EUCARIS. (2013). *EUCARIS - Technology*. Retrieved 12 24, 2013, from EUCARIS: <https://www.eucaris.net/technology>
- EUCARIS. (2013). *Use of EUCARIS*. Retrieved 12 23, 2013, from European Car and Driving License Information System: <https://www.eucaris.net/use-of-eucaris>
- EUR-Lex. (2009, April 06). *Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA*. Retrieved January 17, 2014, from EUR-Lex: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009D0316:EN:NOT>
- Eurofiling. (2007). *COREP - FINREP Taxonomies*. COREP - FINREP Groups.
- Eurofiling Initiative. (2009). *FINREP Taxonomy Documentation*. Retrieved January 27, 2014, from Eurofiling Initiative: http://www.eurofiling.info/finrepTaxonomy/finrep_taxonomy_documentation.shtml
- Eurofiling Initiative. (2010). *COREP Taxonomy Documentation*. Retrieved January 27, 2014, from Eurofiling Initiative: http://www.eurofiling.info/corepTaxonomy/corep_taxonomy_documentation.shtml
- Eurofiling Initiative. (2011). *Legal Notice*. Retrieved January 27, 2014, from Eurofiling Initiative: <http://www.eurofiling.info/legal.shtml>

Eurofiling Initiative. (2013). *Acknowledgements*. Retrieved January 20, 2014, from Eurofiling Initiative: <http://www.eurofiling.info/corepTaxonomy/acknowledgments.shtml>

Eurofiling, about us. (n.d.). Retrieved January 30, 2014, from http://www.eurofiling.info/about_us/about_us.shtml

European Commission . (2010). Commission Regulation (EU) No 1213/2010 of 16 December 2010 establishing common rules concerning the interconnection of national electronic registers on road transport undertakings Text with EEA relevance . *Official Journal of the European Commission*, 21-29.

European Commission - Mobility and Transport. (n.d.). *European Register of Road Transport Undertakings (ERRU)*. Retrieved 12 23, 2013, from European Commission - Mobility and Transport: http://ec.europa.eu/transport/modes/road/access/erru_en.htm

European Commission. (2000). *Communication from the Commission to the Council and the European Parliament: Mutual Recognition of Final Decisions in Criminal Matters*. Brussels: Commission of the European Communities.

European Commission. (2010). *Evaluation of the 2004 action plan for electronic public procurement*. Brussels: European Commission.

European Commission. (2011, December 12). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions. *Open data - An engine for innovation, growth and transparent governance*. Brussels, Belgium.

European Commission. (2013). *e-CODEX (e-Justice Communication via Online Data Exchange)*. Retrieved January 10, 2014, from European Commission: http://ec.europa.eu/justice/criminal/european-e-justice/e-codex/index_en.htm

European Commission. (2013). *ECRIS (European Criminal Records Information System)*. Retrieved January 17, 2014, from European Commission: http://ec.europa.eu/justice/criminal/european-e-justice/ecris/index_en.htm

European Commission. (2013). *European procedures - Justice*. Retrieved January 09, 2014, from European Commission: <http://ec.europa.eu/justice/civil/commercial/eu-procedures/>

European Commission. (2013). *ISA Work Programme Fourth Revision 2014 - Annex to Section I: Part 1: Detailed description of actions*. European Commission.

European Commission. (2013). *Official documents - Employment, Social Affairs & Inclusion - European Commission*. Retrieved December 17, 2013, from European Commission: <http://ec.europa.eu/social/main.jsp?catId=868&langId=en>

- Fabian Büttner, U. B. (2013). *Model-driven Standardization of Public Authority Data Interchange*.
- FINREP. (2005, December 16). *Guidelines establishing a standardised financial reporting framework (FINREP)*. Retrieved January 30, 2014, from CEBS: <http://www.eba.europa.eu/-/cebs-harmonises-reporting-framework-for-european-financial-groups>
- FSMA. (n.d.). *Financial reporting framework - FINREP*. Retrieved January 27, 2014, from FSMA: http://www.fsma.be/en/Supervision/finbem/bo/Article/imp/Supervisory%20Disclosure%20under%20Basel%20II/laws_regulations/finrep.aspx
- General Secretariat of the Council. (2010). *ECRIS Technical Specifications - Detailed Technical Specifications*. Brussels: European Commission - DG Justice.
- General Secretariat of the Council. (2010). *ECRIS Technical Specifications - Inception Report*. Brussels: European Commission – DG Justice.
- General Secretariat of the Council. (2010). *ECRIS Technical Specifications - Security Analysis*. Brussels: Council of the European Union.
- Government On-Line Metadata Working Group. (2006). *Records Management Application Profile*. Canada: Government of Canada.
- Graux, H. (2009). *Study on electronic documents and electronic delivery for the purpose of the impementation of Art. 8 of the Services Directive*. Brussels: Timelex.
- Hohpe, G., & Woolf, B. (2003). *Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions*. Addison-Wesley.
- IDABC - CAMSS. (2012, June 4). *CAMSS Assessment Criteria*. Retrieved November 27, 2013, from IDABC - CAMSS: https://webgate.ec.europa.eu/fpfis/mwikis/idabc-camss/index.php/CAMSS_Assessment_Criteria
- Interoperability solutions for European public administrations (ISA). (2011, May 5). *eGovernment Core Vocabularies: The SEMIC.EU approach*. Brussels, Belgium: European Commission.
- ISA. (2010). *European Interoperability Framework (EIF) for European public services*. Brussels: European Commission.
- ISA. (2013, January 04). *ICCS-CIEC Civil Status Forms*. Retrieved December 09, 2013, from Joinup: <https://joinup.ec.europa.eu/catalogue/repository/iccs-ciec-civil-status-forms>
- Jones, O. (2013, December 10). *EBA Taxonomy and DPM Architect*. Retrieved January 30, 2014, from

<http://www.eurofiling.info/201312/presentations/20131210TaxonomyOwenJones.pptx>

Kurt Salmon. (2013). *Assessment of TESSs supporting EU policies*.

LeBlanc, P., & Smith, B. L. (2002). *A Workshop on Managing Horizontal Issues*. Retrieved 12 24, 2013, from *Managing Horizontal Issues*: <http://www.thinkwell.ca/groupwork/managingHorizontalIssues/documents/MHIWkshopOutlinev2.pdf>

Ministry of Justice, Estonia. (2012). *D4.2: Concept for Implementation of WP4*. EC.

National Information Standards Organization . (2004). *Understanding Metadata*.

Object Management Group, Inc. (2012, October). *Unified Modeling Language™ (UML®)*. Retrieved November 20, 2013, from Object Management Group: <http://www.omg.org/spec/UML/>

OHIM. (2013). *Community Trademark Registration Process*. Retrieved December 15, 2013, from <https://oami.europa.eu/ohimportal/en/registration-process>

Open Knowledge Definition. (n.d.). *Open Definition*. Retrieved 11 20, 2013, from Open Definition: <http://opendefinition.org/>

PEPPOL. (2013). *Virtual Company Dossier*. Retrieved November 22, 2013, from PEPPOL | Pan-European Public Procurement Online: http://www.peppol.eu/peppol_components/virtual-company-dossier

Portal Administración Electrónica. (2013). *Technical standards for interoperability* . Retrieved December 09, 2013, from Portal Administración Electrónica: http://administracionelectronica.gob.es/pae_Home/pae_Organizacion/pae_DGM APIAE.html?idioma=en

Publications Office. (2009, April 07). *Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA*. Retrieved January 07, 2014, from EUR-Lex - Access to European Union law: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009D0316:en:HTML>

RDW. (2008). *EUCARIS Overview*.

Roy, D. (n.d.). *National Information Exchange Model (NIEM): Technical Introduction to NIEM*.

SPOCS. (2012). *eDocuments - Specification*. Retrieved December 16, 2013, from eDocuments: <http://joinup.ec.europa.eu/site/spocs/eDocuments/specification.html>

- UBITECH. (2013). *The ICCS-CIEC Data Exchange Platform*. Retrieved January 29, 2014, from UBITECH: <http://www.ubitech.eu/?q=node/107>
- UN/CEFACT. (2004). *Standard Business Document Header - Technical Specification*. European Commission.
- UN/CEFACT. (2008). *UML Profile for Core Components (UPCC)*.
- UN/CEFACT. (2009). *Core Components Technical Specification - Version 3.0*.
- UN/CEFACT. (2009). *XML Naming and Design Rules Technical Specification - Version 3.0*.
- UN/CEFACT. (2012). *Core Components Business Document Assembly - Technical Specification - Version 1.0*.
- UN/CEFACT. (2012, June 27). *Core Components Business Document Assembly Technical Specification*.
- United Nations - Centre for Trade Facilitation and Electronic Business. (2009). *Core Components Technical Specification - Version 3.0*.
- WikiXBRL. (n.d.). Retrieved January 30, 2014, from http://wikixbrl.info/index.php?title=XBRL_Industry_Solutions
- XBRL Europe. (2013). *xEBR Taxonomy*. Retrieved January 29, 2014, from XBRL Europe: <http://www.xbrleurope.org/working-groups/xebr-wg/xebr-taxonomy>
- XBRL Specification*. (n.d.). Retrieved January 30, 2014, from <http://xbrl.org/TheStandard>

Annex I. STRUCTURED E-DOCUMENT FORMATS USED IN TRANS-EUROPEAN SYSTEMS

In this annex, a detailed analysis of twelve families of e-Document formats used in Trans-European Systems is provided. The analysis was conducted on the basis of preparatory desk research and a validation interview with a project manager or enterprise architect of the corresponding Trans-European System.

The selection of the twelve Trans-European Systems is based on the scope criteria described in Section 1.4. It should be noted that this selection is only a *sample* within the population of Trans-European Systems that use e-Document formats. Annex III contains an indicative list of seventy systems identified in the context of ISA Action 2.14 [Kurt Salmon, 2013]. In this list also systems like the Internal Market Information System (IMI) and Réseau permis de conduire/Driver Licence Network (RESPER) are relevant systems that could be analysed at a later point in time.

Table 12 - Families of e-Document formats included in this analysis

Identified families of e-Document formats
1. CEN/BII profiles used by e-Prior and PEPPOL
2. e-Document formats used by e-CODEX
3. Electronic Exchange of Social Security Information (EESSI)
4. European Criminal Records Information System (ECRIS)
5. European Register of Road Transport Undertaking (ERRU)
6. European Car and Driving Licence Information System (EUCARIS)
7. Tachograph Network (TACHOnet)
8. European Patients Smart open Services projects (epSOS)
9. Eurofiling: financial reporting based on XBRL used by the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) and proposed by XBRL Europe
10. Virtual Company Dossier (VCD) used by PEPPOL
11. Omnifarious Container for e-Documents (OCD) used by SPOCS
12. International Commission on Civil Status (ICCS)

I.1. CEN/BII profiles used by e-Prior and PEPPOL

Context

The CEN Business Interoperability Interfaces on public procurement in Europe (CEN/BII) initiative, established as a workshop under CEN, was initially launched in May 2007. Its aim was to help achieve the Digital Single Market by fostering implementation of e-procurement and e-invoicing in Europe, and especially in the European public sector.

The vision of the workshop was to enable all organizations – independent of whether they are public or private and whatever their size and nationality – to conduct electronic business in an effective and efficient manner, significantly lowering costs for transaction processing.

The CEN WS/BII Workshop objective was to spread and facilitate the use of e-procurement standards by suppliers and buyers, and especially public administrations, by:

- Identifying business requirements (including legal requirements) regarding e-procurement standards;
- Providing a general framework for the organizational and semantic levels of interoperability for the electronic procurement documents;
- Supporting the implementation of commonly applied international e-procurement standards;
- Providing organizational support to ensure the governance and maintenance for those requirements.

The business processes covered by CEN BII are depicted in the figure below.

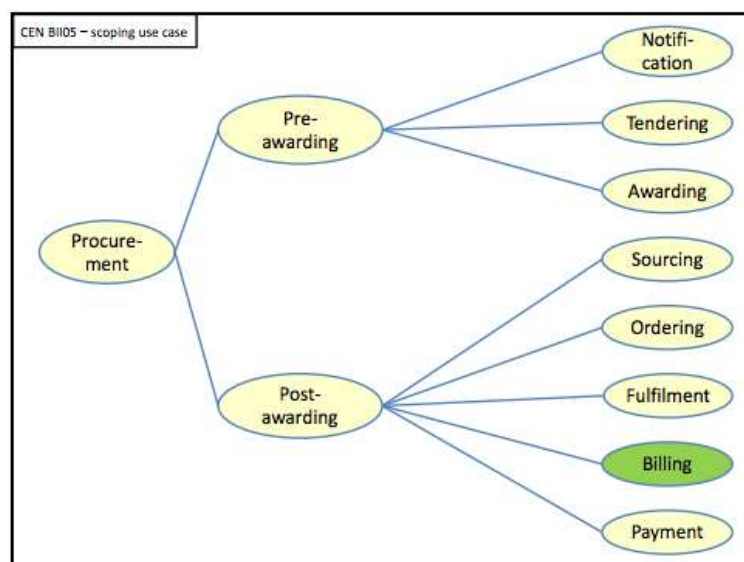


Figure 2 - CEN BII scoping use case

e-Document engineering method

CEN BII does not produce XML Schemas. This means that the Workshop relies on actual XML Schemas for electronic documents published by international standard development organizations such as UN/CEFACT or UBL.

- **Methodology:** CEN BII methodology starts gathering goals and requirements to describe business processes and information models.

The requirements drive definition of business process choreography and information requirement models describing the transactions that are used within the profiles. In the context of the BII, profiles are detailed descriptions of:

- The choreography of the business processes, i.e. a detailed description of the way the business partners collaborate
 - The electronic business transactions exchanged as part of the business process and the sequence in which these transactions are exchanged
 - The business rules governing the execution of that business processes, as well as any constraints on information elements used in the business transaction
 - The information content of the electronic business transactions exchanged by pointing to a given information requirement model for each of the business transactions. These information requirement models contain the concepts and semantics of the CEN BII specification.
- **Library of data elements:** Data elements are collected in information requirement models. Every data element within the information requirement model has an identifier, a business term, its cardinality, a semantic description and a link to the requirement that fulfils.

There is not a single library of information requirements. Each transaction has its own information requirement model that has to be bound to the actual syntax using the syntax binding methodology described in the Guideline on Syntax Binding Methodology¹⁹.

- **Naming and design rules:** CEN BII does not produce XSD Schemas therefore there is no need for naming and design rules to produce schemas.
- **e-Document engineering tools:** The syntax binding process uses the GEFEG.FX tool. This tool allows mapping the information requirement models to actual syntaxes and generates the guidelines of use of the syntax following CEN BII information requirements.

Besides the syntax binding process, CEN BII also defines business rules²⁰ in the profiles and provides validation artefacts implementing them in UBL and

¹⁹ CWA 16558 – Annex K Guideline on Syntax Binding Methodology

²⁰ CWA 16558 – Annex E Guideline on the Business Rules Description Mechanism

UN/CEFACT syntaxes²¹. CEN BII validation artefacts are non-normative Schematron files²² that can be used to ensure the document instances are conformant to the CEN BII specification, beyond the structural syntax that can be validated with the syntax XSD Schemas.

- **Representation techniques:** The information requirement models are represented using RTF documents and an html version²³.

Governance mechanisms

- **Change management**
 - **Organisation roles:** There are two reports in CEN BII regarding governance:
 - Report on Governance Model describes the versioning and Life Cycle Management strategy for CEN BII deliverables.
 - Report on Long Term Governance analyses the different alternatives for ensuring CEN BII deliverables long-term sustainability. Five types of organizations are compared in this report. At the end of CEN BII2, the members of the workshop decided to create a new CEN Workshop Agreement, CEN BII3, to provide governance on the deliverables and to continue the progress on definition of new profiles.
 - **Decision making process:** CEN procedures for setting up and operating a Workshop are kept to the minimum. All the decision-making powers rest within the Workshop stakeholders. The CEN BII is organized with a team of editors that define and write the profiles as agreed within the following task teams:
 - **Architecture:** Defines general methodology and architecture for the profiles.
 - **Notification:** Describes electronic notification business processes.
 - **Pre-Award:** Describes electronic tendering business processes.
 - **Catalogue:** Describes electronic catalogue related business processes.
 - **Post-Award:** Describes electronic ordering, invoicing and fulfilment business processes.

²¹ CWA 16558 – Annex D Guideline on Implementation and the use of Validation Artefacts

²² <http://spec.cenbii.eu/BII2/Tools/bii2-download.html>

²³ E.g. information requirement model for message level response transaction
http://spec.cenbii.eu/BII2/fxhtml/Trdm071-MessageLevelResponse/g_1.htm?http://spec.cenbii.eu/BII2/fxhtml/Trdm071-MessageLevelResponse/g_5.htm

Task teams work in teleconferences and face-to-face meetings to reach consensus on the profiles and information requirements.

- **Documentation:** Report on Versioning and Change Management describes how to create versions of the CEN BII deliverables and how to manage change requests on the specifications.
- **Enforcement policy**
 - **Sharing:** There is no CEN enforcement of the use of deliverables of the CEN BII. Derived initiatives at Member State level can enforce the use of a standard, such as EHF in Norway.
 - **Reuse:** PEPPOL Large Scale Pilot and e-Prior are reusing the CEN BII Profiles. National implementations on e-Invoicing such as EHF in Norway or Svefaktura in Sweden are reusing the PEPPOL and hence CEN BII profiles.
- **Authoritative source:** Authoritative profiles, information models and validation artefacts can be found at:
 - European Committee for Standardization website
 - http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Pages/Ws_BII.aspx
 - CEN BII project site
 - <http://www.cenbii.eu>
- **Licensing framework:** Exploitation rights in respect of CWAs are assigned to CEN-CENELEC and the CEN/CENELEC Members, and the Workshop Agreements have exclusive CEN/CENELEC copyright
- **Quality controls:** To be implemented in CEN BII3 workshop.

Conformance mechanisms

CEN BII conformance is defined in the Guideline on Conformance and Customizations²⁴. This specification describes conformance at document instance level using three different levels:

- **Strict conformance**, when all the elements in the instance belong to the information requirement model and the instance does not break any business rule.
- **Extended conformance**, when there are additional elements that do not belong to the information requirement model of CEN BII.
- **Partial conformance**, when, even if the instance follows the information requirement model pattern of CEN BII, it breaks one or more business rules.

²⁴ CWA 16558 – Annex C Guideline on Conformance and Customizations

This guideline also defines the methodology to create customizations of the specifications, allowing user communities to extend the specifications creating extended customizations or to further restrict the CEN BII rules creating restrictive customizations. Based on these customizations, the guideline describes the potential relationships between systems using different types of customizations as is depicted in Figure 3 - Conformance relations.

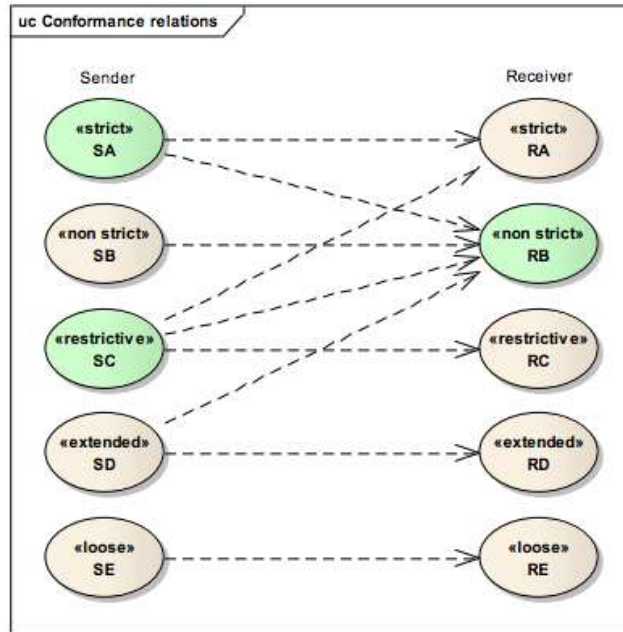


Figure 3 - Conformance relations

- **Application profile** CEN BII2 has defined 22 application profiles. Each application profile describes an electronic relationship between two parties, establishing:
 - The choreography of the business process
 - The information requirement model
 - The business rules and coded values
 - The syntax binding to UBL and UN/CEFACT XSD schemas
- **Validation mechanism:** CEN BII does not produce XSD Schemas to validate document instances. It uses international standards such as UBL or UN/CEFACT as the base for its information requirement models.

The additional constraints and business rules that the document instances must follow are expressed using Schematron validation artefacts.
- **Conformance certification:** CEN BII does not define a conformance certification procedure.

Security mechanisms

- **Authentication:** CEN BII specifies a guideline to describe the Application of Digital Signatures²⁵.

The recommendation in this guideline is the same as the one issued in the Commission Decision on Signature Formats from February 2011²⁶ that recommends following XADES/BES EPES and ETSI ESI Technical Specifications "Baseline Profiles" for XADES to guarantee authentication, integrity and non-repudiation.

- **Integrity mechanism:** Defined in the guideline on Application of Digital Signatures.
- **Confidentiality mechanism:** CEN BII does not define a confidentiality mechanism.
- **Non-repudiation mechanism:** Defined in the guideline on Application of Digital Signatures.

Usage

- **Number of known implementations in production-grade software:** CEN BII specifications have been implemented in several electronic public procurement projects since its first publication on 2010. CEN BII stakeholders have been using the CEN BII profiles to build their national e-procurement and e-invoicing solutions.

The most relevant initiatives using CEN BII deliverables are:

- **Electronic Procurement Invoicing and Ordering (e-PRIOR)**

e-PRIOR is a platform developed under the ISA (Interoperability Solutions for European Public Administrations) programme, by the Directorate-General for Informatics (DIGIT) of the European Commission and it deployed within DIGIT in 2009. Other Directorate-Generals, European Agencies and Institutions are implementing the e-PRIOR system. The e-Prior platform has evolved to the open source Open e-PRIOR that is freely available to all Members States wishing to exchange standardised electronic procurement documents via secured communication channels.

The interfaces of e-PRIOR are based on the Business Profiles defined by CEN's workshop on Business Interoperability Interfaces for Public Procurement in Europe.

²⁵ CWA 16558 – Annex L Guideline on the Application of Electronic Signatures

²⁶ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF>

- PEPPOL

The Pan-European Public Procurement Online (PEPPOL) project has deployed a standards-based IT transport infrastructure that provides services for e-Procurement with standardised electronic document formats based on UBL and CEN BII.

The PEPPOL consortium was comprised of seventeen partners within 11 countries: Austria, Denmark, Finland, France, Germany, Greece, Italy, Norway, Portugal, Sweden, and the United Kingdom, and the project was funded by the Competitiveness and Innovation Framework Programme (CIP) of the European Commission.

- Direktoratet for forvaltning og IKT - DIFI (Norway)

The Agency for Public Management and e-Government (Difi) of Norway has been the responsible for deploying the Norwegian invoicing solution. They have based their EHF solution on the PEPPOL transport infrastructure. By using an access point connected to the PEPPOL transport infrastructure economic operators are able to send and receive EHF (Elektronisk handelsformat) documents in Norway.

The EHF format covers the invoice and credit note documents and they are a customization of the CEN BII information models.

- Single Face to Industry - SFTI (Sweden)

Since June 2010 the CEN/BII profile "Basic Order Only" is recommended as a standard in Sweden for the public sector e-ordering process, under the name "Sveorder".

SFTI decided to use the CEN/BII Basic Order Only, both for ordering process cross border and within Sweden.

Summary table

Table 13 - Analysis of CEN BII

EU – CEN Workshop Agreement on Business Interoperable Interfaces	
DESCRIPTIVE METADATA	
Licence	Exploitation rights in respect of CWAs are assigned to CEN-CENELEC and the CEN/CENELEC Members, and the Workshop Agreements have exclusive CEN/CENELEC copyright
Publisher	European Committee for Standardization
Publisher type	Standardisation Body
Theme(s)	Public Procurement
Access URL	<ul style="list-style-type: none"> • European Committee for Standardization website http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Pages/Ws_BII.aspx

	<ul style="list-style-type: none"> • CEN BII project site http://www.cenbii.eu • CEN BII2 CWA specifications <ul style="list-style-type: none"> ○ CWA 16558 - Architecture ○ CWA 16559 – eNotification ○ CWA 16560 – eTendering ○ CWA 16561 - eCatalogue ○ CWA 16562 – Post-Award
CONTEXT	
Administrative process context	Contracting bodies; electronic procurement systems Economic operators; ERP systems
Geopolitical context	European Union
Legal context	Directive 2004/17/EC and Directive 2004/ 18/EC on public procurement ²⁷ Directive 2006/112/EC on value added tax ²⁸
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	<p>BII creates profiles describing:</p> <ul style="list-style-type: none"> • Scope of a business process with its goals, preconditions and the roles of participating parties; • Choreography of the business process covered, i.e. a detailed description of the way the business partners collaborate to play their respective roles and share responsibilities to achieve mutually agreed goals with the support of their respective information systems; • Electronic business transactions exchanged as part of the business process, with their information requirements, and the sequence in which these transactions are exchanged; • Business rules governing the execution of that business process, as well as any constraints on information elements used in the information requirement models of

²⁷ Directive 2004/17/EC and Directive 2004/ 18/EC
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:134:0001:0113:en:PDF>
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:134:0114:0240:EN:PDF>

²⁸ Council Directive 2006/112/EC on the common system of value added tax
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2006L0112:20130701:EN:HTML>

Analysis of structured e-Document formats used in Trans-European Systems

	the transactions.
Library of data elements	<p>CEN BII does not provide any XML schemas, but relies on the XML Schemas for electronic documents published by UN/CEFACT or UBL.</p> <p>Data elements are collected as a set of information requirements in the information requirement models that are bound to the selected syntax elements.</p>
Naming and Design Rules	Not needed as no XML Schemas are produced
e-Document engineering tools	<p>GEFEG.FX tool is used to create the syntax binding of the information requirement models to the actual syntaxes.</p> <p>Schematron rules are created based on the abstract business rules defining the XPATH expressions to assert the business rule in a specific syntax.</p>
Representation techniques	<ul style="list-style-type: none"> • Word and Rich Text Format documents • Spread sheet models • HTML web pages
GOVERNANCE MECHANISMS	
Goals	Implement cross-border interoperability in public procurement processes and eventually evolve towards business-to-business operations.
Change management	<ul style="list-style-type: none"> • Organisational roles: European Committee for Standardization. Creation of a new CEN BII3 Workshop to provide governance to CEN BII deliverables. • Decision making process: Workshop establishes task teams to work on particular business processes. Decision making process is consensus driven. • Documentation: Report on Versioning and Change Management describes how to create versions of the CEN BII deliverables
Enforcement policy	<ul style="list-style-type: none"> • Sharing: Voluntary • Reuse: Voluntary
Authoritative source	<ul style="list-style-type: none"> • European Committee for Standardization website: http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Pages/Ws_BII.aspx • CEN BII project site: http://www.cenbii.eu
Licensing framework	Class 4 : Free to use, redistribute, and modify via non-copy left licence
Quality controls	To be implemented in CEN BII3 workshop.

CONFORMANCE MECHANISMS	
Application profile	CEN BII has currently defined 22 profiles.
Validation	Based on the use of Schematron validation artefacts.
Conformance certification	Not available
SECURITY MECHANISMS	
Authentication mechanisms	Recommends using electronic signatures to authenticate the source of the message
Integrity mechanisms	Recommends using electronic signatures to guarantee the integrity of the message
Confidentiality mechanisms	Not defined
Non-repudiation mechanisms	Recommends using electronic signatures to guarantee non-repudiation of origin.
USAGE	
Number of e-Document formats	Defined 34 transaction information models bound to UBL 2.1 and UN/CEFACT D11A.
Number of known implementations in production-grade software	Implemented in national and cross border projects: <ul style="list-style-type: none"> • EC ePrior • PEPPOL • DIFI • SFTI • ICEPRO
Number of e-Documents exchanges annually	No information was made available at the time of writing this study.

I.2. e-Document formats used by e-CODEX

Context

[e-CODEX](#)²⁹ (e-Justice Communication via Online Data EXchange) is a Large Scale Pilot in the domain of e-Justice, aiming to implement building blocks supporting the digital proceeding of cross-border legal procedures between European Member States.

So far e-CODEX has focused on creating e-Document formats to support the first two use cases defined in e-CODEX Deliverable 3.10: the **EU Small Claims** and **European Payment Order** procedures [e-CODEX, 2013]. Both procedures are described as follows³⁰:

1. The Small Claims procedure is based on Council Regulation 861/2007³¹ of 11 July 2007 establishing a European small claims procedure. This Regulation seeks to improve and simplify procedures in civil and commercial matters where the value of the claim does not exceed 2000€. The regulation provides 4 standard forms and establishes time limits for the parties and the court in order to speed up litigation.
2. The European Payment Order is based on Council Regulation 1896/2006³² of 12 December 2006 creating a European payment order procedure. This allows creditors to recover their uncontested civil and commercial claims according to a uniform procedure that operates on the basis of standard forms. The procedure does not require appearing before a court. The claimant only has to submit an application, after which the procedure will follow its course. It does not require any further formalities or intervention on the part of the claimant [European Commission, 2013].

e-Document engineering method

- **Methodology:** e-CODEX uses the UN/CEFACT Core Component Technical Specification (CCTS) [e-CODEX, 2012].
- **Library of data elements:** e-CODEX has created a formal library of data elements based on the UN/CEFACT Core Component Library. The library contains extensions that are specific to the domain of legal procedures. The library also reuses elements of the Core Person Vocabulary (at the conceptual level). This repository with a set of shared components serves as

²⁹ <http://www.e-codex.eu/>

³⁰ EU Small Claims and European Payment Order procedures:
<http://ec.europa.eu/justice/civil/commercial/eu-procedures/>

³¹ Council Regulation 861/2007:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007R0861:en:NOT>

³² Council Regulation 1896/2006:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:399:0001:01:en:HTML>

a base to create messages. Currently, the repository consists of a document model, including a physical and logical layer. However, the repository doesn't include a conceptual model yet. On the long term, a domain model will be included in the repository, comprising a conceptual and logical layer, as depicted in Figure 4. This domain model will be described in the future e-CODEX deliverable D.6.9. Specific elements can be added to a general schema. [e-CODEX, 2012].

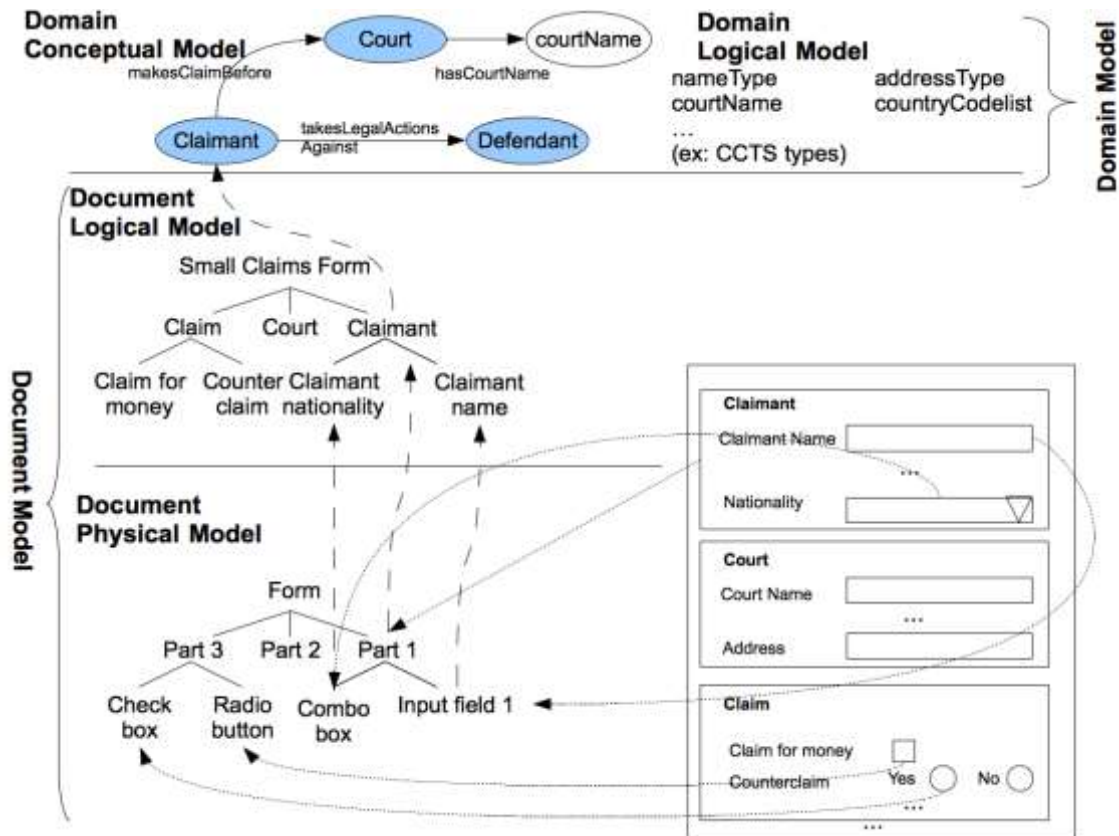


Figure 4 - Domain and Document Model [e-SENS, 2013]

- **Naming and design rules:** In e-CODEX, the XML Schemas are compliant with the Naming and Design Rules of CCTS Version 2.1 for the short term [e-CODEX, 2012].
- **e-Document engineering tools:** For creating the XML Schemas in e-CODEX, the Metadata Workbench is used, which allows creating and managing the Core Components and Business Information Entities. Business Information Entities are context-specific components used to construct the XML Schemas. The Metadata Workbench, illustrated in Figure 5, has been developed by the Dutch Ministry of Security and Justice. The intention is to make the Metadata Workbench available as open-source software in the future. The current version of the tool is not available yet as open-source software. The Dutch Ministry of Security and Justice is looking for a partner to help making the Metadata Workbench available as open-source software.

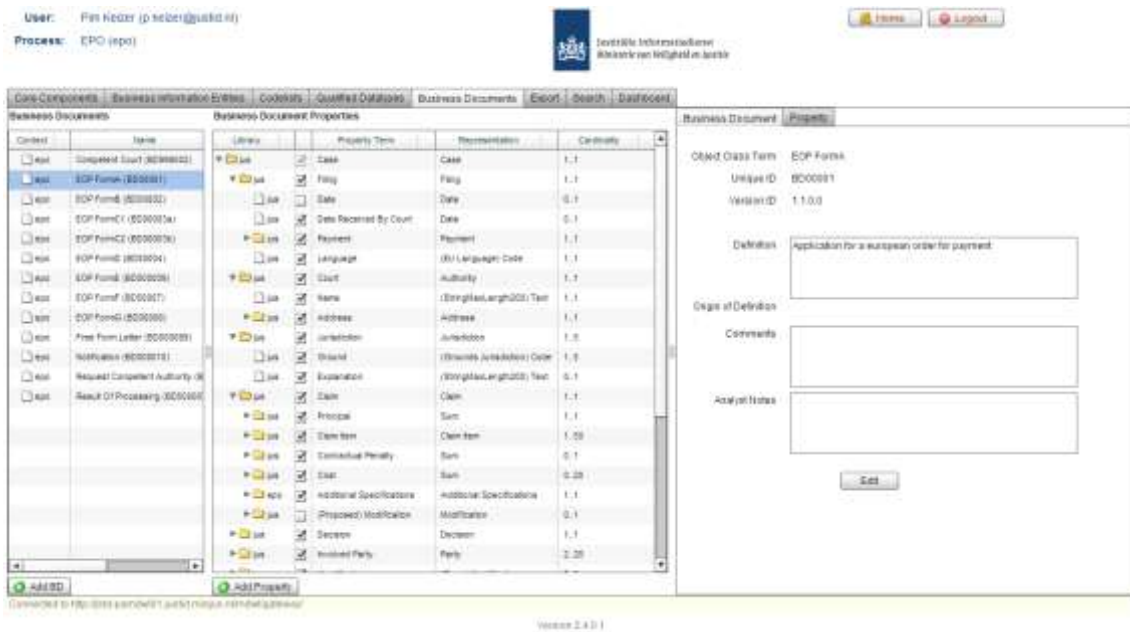


Figure 5 - Screenshot of the Metadata Workbench

- **Representation techniques:** The e-Document formats are represented as XML Schemas. There are plans to also generate Schematron from the Metadata Workbench.

Governance mechanisms

Governance mechanisms frame the regulation of changes to the e-Document formats.

- **Change management:**
 - **Organisation roles:** e-CODEX Deliverable 7.1 on Governance and Guidelines discusses the organisational setup installed to ensure that all solution building blocks developed in the context of e-CODEX integrate well into a working solution [e-CODEX, 2011]. Nonetheless, the e-CODEX consortium – being a temporary organisation – does not have a mandate to maintain the e-Document formats beyond the lifespan and outside the context of the e-CODEX large-scale pilot. It is not yet clear which organisation will assume this role. This will be taken up in the sustainability part of the e-CODEX project, as will be described in the future e-CODEX deliverables D1.12 and D6.9.
 - **Decision making process:** The e-CODEX consortium does not seem to operate a formally described and open change management process. e-CODEX deliverable D6.3 does define the roles, responsibilities and tasks that must be performed within e-CODEX are outlined in order to create the e-Document formats according to the several requirements [e-CODEX, 2012].

Any changes that must be applied to the data formats of e-CODEX are requested through the JIRA ticketing system. These are discussed in collaboration with the participating partners.

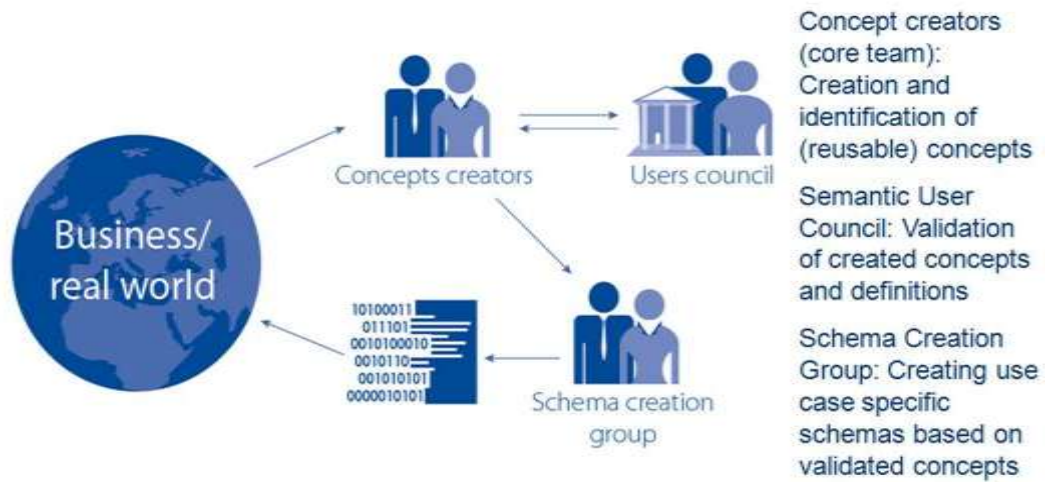


Figure 6 - From business to XML Schemas [e-CODEX, 2012]

As shown in Figure 6, the decision-making procedure is affected by a team of concept creators, a user council and a schema creation group. The core team of concept creators aims at creating, editing and extending a concept based on certain specifications. This concept is then presented to the user council for acceptance of usage. Once approved, the concept is processed by the Schema Creation Group and created into a schema [e-CODEX, 2012].

- **Documentation:** No relevant documentation is available regarding the formal description of the change management process.
- **Enforcement policy:** In e-CODEX, the participation in the pilot, and thus the adoption of the e-Document formats, is on a voluntary basis.
- **Authoritative source:** The e-Document formats (e-CODEX European Payment Order and Small Claim XML Schemas) are openly available on the Joinup portal under the European Union Public Licence.
- **Licensing framework:** The EUPL is a class 3 licence, giving the rights to use, redistribute, and modify via copy left.
- **Quality controls:** There is no formal quality management process in place. By using the open JIRA ticketing system, peers are able to review the metadata on their quality.

Conformance mechanisms

The conformance mechanism allows evaluating the e-Document formats against an application profile, a validation mechanism and a conformance certification.

- **Application profile:** e-CODEX does not specify an application profile for its e-Document formats.
- **Validation mechanism:** In e-CODEX, validation rules are expressed in Schematron [e-CODEX, 2012], which is used to ensure that e-Documents respect the validation rules that cannot be specified with XML Schemas. Currently, the creation of Schematron files is a manual process. Integration with the Metadata Workbench is planned for the future in order to export Schematron files.
- **Conformance certification:** A conformance certification is not available. However, no significant problems have been noted in connecting partners to e-CODEX.

Security mechanisms

Deliverable 4.2 in e-CODEX Work Package 4 on e-Signature and e-Identity discusses how a secure electronic communication is established [e-CODEX, 2012]. It mentions among others the following components:

- **Authentication:** The concept of the "Trust OK"-Token is introduced providing validation information in the document carriers [e-CODEX, 2012]. The "Trust OK"-Token basically is a confirmation document signed by the Connector. Within the "Circle of Trust" (see Figure 7), it is used to assure the authenticity of the delivered documents. The important task to preserve the link between the "Trust OK"-Token and its associated documents and signatures is fulfilled by choosing the ASiC-S container, a data container holding different data objects and associated signatures within a ZIP file. The usage of DG MARKT DSS³³ tool – a Java based open source software module that can be used to create, extend and validate XAdES, PAdES and CAdES e-Signatures – is recommended to verify a signature's validity in a cross-border setting.
- **Integrity mechanism:** To ensure that the content of a document is not modified, the e-CODEX Connector checks the applied signatures on the business documents by a signature validation and the DSS tool or by relying on the nationally accepted solution [e-CODEX, 2012].
- **Confidentiality mechanism:** Point-to-point encryption via SSL is used to protect data at transmission.
- **Non-repudiation mechanism:** Non-repudiation of origin and of receipt is ensured through the validation report of the signatures on business documents generated in the "Trust OK"-token.

³³ Digital Signature Service, <https://joinup.ec.europa.eu/software/sd-dss/description>

To avoid that every Service Provider has to implement the above-mentioned security concepts, e-CODEX Deliverable 4.3 describes the creation of a Java library³⁴ that provides these functionalities [e-CODEX, 2013].

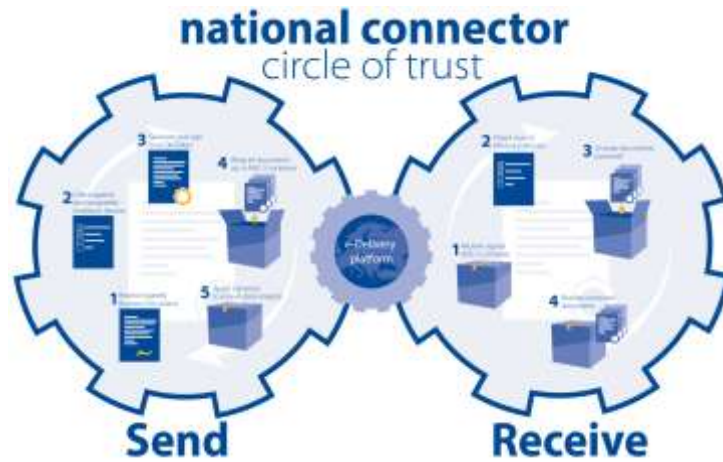


Figure 7 - Basic workflow of the e-CODEX central trust service

Usage

- **Number of e-Document formats:** e-CODEX Deliverable D6.4 describes that for each form in the European Payment Order and Small Claims procedures, a separate e-Document format (Business Document Schema) is created. This brings the number of e-Document formats to:
 - **European Payment Order procedure:** 11 e-Document formats, namely:
 - EOPFormA_BD00001
 - EOPFormB_BD00002
 - EOPFormC1_BD00003a
 - EOPFormC2_BD00003b
 - EOPFormD_BD00004
 - EOPFormE_BD00009
 - EOPFormF_BD50007
 - EOPFormG_BD00008
 - FreeFormLetter_BD000099
 - Notification_BD000010
 - ResultOfProcessing_BD500007

³⁴ Download the e-CODEX Trust Library : <https://www.iol.nrw.de/bscw/bscw.cqj/d3873040/ecodex-container-1.00-project.zip>

- **Small Claims procedure:** 7 e-Document formats, namely:
 - o SC FormA_BD001001
 - o SC FormB_BD001002
 - o SC FormC PartI_BD001007
 - o SC FormC PartII_BD001003
 - o SC FormD_BD001004
 - o Free Form Letter_BD001099
 - o Withdrawal_BD001006
- **Number of known implementations in production-grade software:** Here, we count the number of different implementations performed by e-CODEX service providers that connect via a Gateway and common software libraries to the e-Delivery platform [e-CODEX, 2012]. This is depicted in Figure 8.

Concerning the implementation of the e-CODEX Connector and the gateways in order to connect to the e-CODEX platform and to exchange data formats, one base software is used by all participating parties. However, each country needs to adapt the software to its needs, as the software connects with each national back-end system. This means that each country which has installed the software is considered as a separate implementation. Currently, six countries (Austria, Germany, Italy, Estonia, Greece and Turkey) have installed the software and two more countries (the Netherlands and France) are expected to implement the software by April 2014.



Figure 8 - e-CODEX high-level architecture [e-CODEX, 2012]

- **e-CODEX Service Provider:** An e-CODEX user has the ability to *create, submit and receive files* via the e-Justice portal or the national system of the user, which can be considered as an e-CODEX Service Provider. An e-CODEX Service Provider complies with the standards of e-CODEX and is connected to an e-CODEX gateway via a connector. The Service Provider can be a governmental national application, the e-Justice portal or a private solution.
- **e-Justice portal (gateway):** The EU e-Justice³⁵ portal provides standard forms that citizens and courts can use for cross-border judicial cooperation in civil matters and commercial matters. The data from these standard forms are exported in a proprietary XML format. In a next phase of the e-CODEX large-scale pilot, the data from the forms of the e-Justice portal will be converted in the e-Document format of e-CODEX in order to be sent to the courts through the infrastructure of e-CODEX. This new version of the forms will first be tested on the European Payment Order forms. However, the e-Justice portal is currently not ready to be directly connected as an additional entry point to the e-CODEX platform. In the future, the e-Justice portal will be able to connect to the e-CODEX Connectors of the Member States.
- **e-CODEX Connector:** The e-CODEX Connector is responsible to connect the national solution to the gateway of the system. The connection between the e-CODEX Connector and the national gateway needs to be implemented on the national entry point. Outgoing files, including messages and evidences, of the national back-end system of the sending country are transferred to the e-CODEX Connector. The e-CODEX Connector contains a content mapper, which adapts the national message format of the file to the e-CODEX standard. Furthermore, the Connector includes a security module, which adds a "Trust OK"-token to the document to verify the electronic signature of the file. Once the file has been transferred to the receiving party, the e-CODEX Connector of the receiving country transforms the e-CODEX standard of the file back to the national message format of the receiving country. The "Trust OK"-token is verified and the Connector ensures that no changes have been applied to the document.

Any protocol or semantic translations are also performed through the e-CODEX Connector.

- **National e-CODEX gateways:** The national e-CODEX gateways are systems which are responsible for transmitting data between the sending and receiving parties. The gateways are subject to certain security conditions. Each e-CODEX gateway serves as interface between the e-Justice Portal or national system and the e-Delivery platform. Described in the e-CODEX deliverable D7.3, the objectives of the e-CODEX gateways are to *"establish a connection to other gateways and connectors, format the content of a message to be sent to the eBMS3.0 standard and extract the*

³⁵ e-Justice portal, https://e-justice.europa.eu/content_dynamic_forms-155-en.do

contents of a received eBMS3.0 message, providing a transport signature and providing a timestamp for outgoing messages and checking of the transport signature, providing of a timestamp and sending of an acknowledgment of receipt for incoming messages” [e-CODEX, 2012].

The e-CODEX gateways are not aware of the e-Document formats used.

- **e-CODEX e-Delivery platform:** The e-Delivery platform stands for the secure data transmission between e-CODEX gateways. Currently, the architecture of the e-Delivery platform is decentralized. The e-Delivery platform is not aware of the e-Document formats used [e-CODEX, 2012].
- **Number of e-Document exchanges annually:** So far, e-CODEX did not yet disclose the number of legal procedures that have been processed through its e-Delivery service.

Summary table

Table 14 – Analysis of e-CODEX

e-Justice Communication via Online Data EXchange (e-Codex)	
DESCRIPTIVE METADATA	
Licence	European Union Public Licence (EUPL) ³⁶
Publisher	e-CODEX
Publisher type	Supra-national and national authority
Theme(s)	Law
Access URL	<ul style="list-style-type: none"> • e-CODEX European Payment Order XML Schemas: https://joinup.ec.europa.eu/catalogue/asset_release/e-codex-european-payment-order-xml-schemas • e-CODEX Small Claim XML Schemas: https://joinup.ec.europa.eu/catalogue/asset_release/e-codex-small-claim-xml-schemas
CONTEXT	
Administrative process context	Legal authorities; justice systems
Geopolitical context	European Union

³⁶ European Union Public License: <http://joinup.ec.europa.eu/software/page/eupl>

Legal context	<ul style="list-style-type: none"> European Payment Order: Council Regulation 1896/2006³⁷ e-CODEX Small Claim XML Schemas: Council Regulation 861/2007³⁸
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	UN/CEFACT CCTS [e-CODEX, 2012]
Library of data elements	Repository of shared concepts based on CCL
Naming and Design Rules	UN/CEFACT XML Naming and Design Rules Technical Specification Version 2.1
e-Document engineering tools	Metadata Workbench
Representation techniques	XML Schema
GOVERNANCE MECHANISMS	
Goals	Cross-border legal procedures between EU Member States
Change management	<ul style="list-style-type: none"> Organisational roles: not applicable Decision making process: Concept creators; Semantic User Council; Schema Creation Group [e-CODEX, 2012]. Documentation: not applicable
Enforcement policy	<ul style="list-style-type: none"> Sharing: voluntary Reuse: voluntary
Authoritative source	Federated repository on Joinup Portal under EUPL
Licensing framework	Class 3: Free to use, redistribute, and modify via copy left licence.
Quality controls	No formal quality management process

³⁷ Council Regulation 1896/2006:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:399:0001:01:en:HTML>

³⁸ Council Regulation 861/2007:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007R0861:en:NOT>

CONFORMANCE MECHANISMS	
Application profile	Not provided
Validation	XSD Schema and Schematron
Conformance certification	Not available
SECURITY MECHANISMS	
Authentication mechanisms	"Trust OK"-Token; DSS-based validation of signatures and ASIC-S containers
Integrity mechanisms	Signature validation and DSS tool
Confidentiality mechanisms	Point-to-point encryption via SSL (This is of course no confidentiality mechanism part of the e-Document container, but of the infrastructure)
Non-repudiation mechanisms	Validation report of signatures in "Trust OK"-Token
USAGE	
Number of e-Document formats	18 (11 e-Document formats under European Payment Order and 7 e-Document formats under Small Claims)
Number of known implementations in production-grade software	8 : one base-software is implemented separately per participating country (Austria, Germany, Italy, Estonia, Greece, Turkey – the Netherlands, France in the future)
Number of e-Documents exchanged annually	Not disclosed

I.3. Electronic Exchange of Social Security Information (EESSI)

Context

The EU regulations on social security coordination require that social security bodies across the EU exchange information electronically by 1 May 2014. The Electronic Exchange of Social Security Information is an IT system between national social security institutions that supports this requirement. Through the EESSI, all information exchanges between European social security bodies will take place using structured electronic documents [EESSI, 2013].

As from 1 May 2014, the exchange of social security data will be structured in structured electronic documents (SED) and exchanged via the EESSI platform³⁹.

The implementation of SEDs and the EESSI platform brings benefits both for the public as for public administrators. The project allows a faster management, calculation and payment of claims of citizens. Moreover, it standardizes the flow of information between social security bodies, it optimises the verification and collection of data and it facilitates multilingual communication because of structured documents [EESSI, 2013].

The structured electronic documents (SED) are the following⁴⁰:

- **Applicable legislation (A series)**

The A-series SED consists of 8 forms, each to be used for exchanging a specific type of social security data related to applicable legislation. Such cases include the exchange of information regarding the determination of applicable legislation (A003), regarding requests for more information (A005; A006), etc.

- **Pensions (P series)**

The P-series SED consists of 140 forms, each to be used for exchanging a specific type of social security data related to pensions. Most of these forms concern pension claims (P2000: old age, P2100: survivors, P2200: invalidity).

- **Sickness (S series)**

The S-series SED consists of 103 forms, each to be used for exchanging a specific type of social security data related to sickness. Such cases include the exchange of information regarding the payment of individual claims (S101), regarding the cancelation of entitlements for former frontier workers (S077), regarding requests for an administrative check or a medical examination (S063), etc.

³⁹ The EESSI platform: <http://ec.europa.eu/social/main.jsp?catId=868&langId=en>

⁴⁰ The full list of forms per SED can be obtained from <http://ec.europa.eu/social/main.jsp?catId=868&langId=en>

- **Family benefits (F series)**

The F-series SED consists of 27 forms for information exchange regarding family benefits. Such forms include requests for reimbursement (F012), applications for additional benefits (F021), etc.

- **Accidents at work and occupational diseases (DA series)**

The DA-series SED consists of 63 forms for information exchange regarding accidents at work and occupational diseases. Examples of such forms include the request of reimbursement of advance payments (DA056), the request for authorisation to receive scheduled treatment in a member state other than the member state of residence (DA006), etc.

• **Unemployment (U series)**

The U-series SED consists of 28 forms for sharing information related to unemployment matters. The information exchanged using these forms concerns family info (U006), registration info on cross border workers (U018), etc.

• **Horizontal issues (H series)**

“A key characteristic of these issues is that the clear responsibility, authority and jurisdiction to resolve them often do not reside with a single work unit, agency or department” [LeBlanc & Smith, 2002]. The European commission identified four horizontal – or cross cutting – issues: democracy and human rights, environmental sustainability, gender equality and HIV/AIDS⁴¹. The H-series SED consists of 66 forms for the exchange of information regarding these issues.

• **Recovery (R series)**

The R-series SED consists of 36 forms for information exchange regarding recovery matters. Examples of such forms include the request for recovery/precautionary measures (R017), for reimbursement of costs (R028), etc.

e-Document engineering method

At the time of writing this report, the EESSI system was still under development. No further information could be obtained at this stage.

Governance mechanisms

At the time of writing this report, the EESSI system was still under development. No further information could be obtained at this stage.

Conformance mechanisms

At the time of writing this report, the EESSI system was still under development. No further information could be obtained at this stage.

⁴¹ Cross cutting issues : http://ec.europa.eu/europeaid/what/development-policies/cross-cutting-issues/index_en.htm

Security mechanisms

At the time of writing this report, the EESSI system was still under development. No further information could be obtained at this stage.

Usage

At the time of writing this report, the EESSI system was still under development. No further information could be obtained at this stage.

I.4. European Criminal Records Information System (ECRIS)

Context

ECRIS is an ICT system that was implemented to enable an efficient exchange of information on criminal convictions between EU member states. The system is based on a decentralised IT architecture: conviction data is stored solely in national repositories and exchanged upon request from another member state. As it is obligatory for a Member State to share the conviction data of their citizens upon request, it is obligatory for a convicting Member State to notify information and updates on the conviction of EU nationals to the Member State of nationality.

The ECRIS system was expected to be implemented in all Member States by April 2012. To date, 25 Member States are exchanging criminal record information through ECRIS.

The exchange of information is done electronically through a standardised European format which was set up specifically for the exchange of criminal records, as described in the Council Decision of 6 April 2009 on the establishment of ECRIS [Council of the European Union, 2009]:

"Therefore, a standardised format allowing information to be exchanged in a uniform, electronic and easily computer-translatable way as well as any other means of organising and facilitating electronic exchanges of information on convictions between central authorities of Member States should be set up".

e-Document engineering method

- **Methodology:** No standardised e-Document engineering method has been used.
- **Library of data elements:** The ECRIS domain model constitutes a reusable library of data elements. The domain model has both a UML (conceptual model) and XSD (logical model) representation⁴². ECRIS itself does not reuse existing data elements.

At value level, ECRIS promotes the use of reference tables, which categorizes offences and penalties based on codes, facilitates automatic translation and enhances the understanding of information transmitted.

The ECRIS Technical Specifications - Business Analysis further elaborates on the use of reference tables.

Some of the information elements described in the domain model have been codified and only allow using one of a list of predefined values.

⁴² ECRIS Detailed Technical Specifications:
<http://register.consilium.europa.eu/doc/srv?!=EN&t=PDF&gc=true&sc=false&f=ST%2011275%202011%20REV%201>

The **common reference tables** define lists of values that are common for all Member States. The definitions and detailed content of these common reference tables can be found in the spread sheet "Common Reference Tables".

In addition to the common reference tables, the domain model foresees that for some fields **national reference tables** may be used. These tables are not common but are specific to the emitting Member State. Each Member State may decide to share its national reference table with one or more other Member States so as to facilitate the information exchanges.

The ECRIS format is documented in the ECRIS Technical Specifications – Technical Architecture⁴³ and the ECRIS Detailed Technical Specifications⁴⁴.

- **Naming and design rules:** There are no XML Schema design rules; however, the naming conventions are based on ISO 11179. Furthermore, an "Object:Property" scheme is used, where Object is the class term, and Property is an element belonging to the referenced class term. The names are written with a CamelCase format. For example, the "Person" class has a property named "PersonSurName".
- **e-Document engineering tools:** XML Spy from Altova was used to create the XML ECRIS Artefacts.
- **Representation techniques:** the format is defined using XML Schema, derived from a conceptual model in UML.

Governance mechanisms

Governance mechanisms frame the regulation of changes to the e-Document formats.

- **Change management**
 - **Organisation roles:**
 - Board of experts: discussing and initiating changes
 - Council: managing change proposals
 - Parliament: formal approval if needed
 - **Decision making process:** Changes are initiated through a board of experts from the 28 Member States and are sent for approval to the Council. Depending on the nature of the changes, the Council may send the proposal to the Parliament.

⁴³ ECRIS Technical Specifications – Technical Architecture:
<http://register.consilium.europa.eu/doc/srv?!=EN&t=PDF&gc=true&sc=false&f=ST%2015456%202010%20INIT>

⁴⁴ ECRIS Detailed Technical Specifications:
<http://register.consilium.europa.eu/doc/srv?!=EN&t=PDF&gc=true&sc=false&f=ST%2011275%202011%20REV%201>

The ECRIS format has been adopted in a semi-open specification process. There is a dedicated forum which is accessible only for Experts to post ideas and participate in discussions; administrations first need to be invited to join the specification process (semi-open).

"The Council, acting by a qualified majority and after consulting the European Parliament, shall adopt any modifications of Annexes A and B as may be necessary" [Council of the European Union, 2009], where Annexes A and B refer to the reference tables of offences, penalties and measures.

If a backward incompatible change must be applied to the Technical Specification, an XML versioning system is used. All implementations must support both the old and new versions of the XML schemas during the migration period. Until now, such backward incompatible changes have not been introduced yet.

- **Documentation:** The change management process is described in the Council Decision 2009/316/JHA of 6 April 2009.
- **Enforcement policy:** In the enforcement policy, sharing and reusing the data formats of ECRIS is legally required in order to electronically exchange the information between the central authorities of the EU countries.
- **Authoritative source:** The General Secretariat of the Council manages the metadata.
- **Licensing framework:** Shared and reused metadata falls under a traditional and proprietary licence. No modifications are allowed at national level.
- **Quality controls:** A verification mechanism is present to validate the quality of a specification, e.g. peer-to-peer reviews.

Conformance mechanisms

The conformance mechanisms are described in the ECRIS Technical Specifications – Verification of conformity [General Secretariat of the Council, 2010].

- **Application profile:** An application profile is not applicable within this context as the ECRIS e-Document format is not an application profile. The ECRIS e-Document formats have been developed from scratch.
- **Validation mechanism:** The Detailed Technical Specifications provide validation rules via test cases divided into two categories:
 - Automatic validation: the conditions can be verified in an automated manner by the software.
 - Manual validation: the conditions can only be verified by human operators.

The validation of e-Documents happens at both the emitting and receiving side.

- **Conformance certification:** The ECRIS Technical Specifications – Verification of conformity [General Secretariat of the Council, 2010] describes all the tests that must be performed to ensure conformity of the implementation with the technical specifications. A large majority of these tests are automated.

Security mechanisms

Information of the security mechanisms of ECRIS can be found in the ECRIS Technical Specifications – Security Analysis [General Secretariat of the Council, 2010].

In ECRIS, e-Documents are only transferred between known and trusted servers, communicating with HTTPS over the sTESTA network. The e-Document formats themselves do not contain additional security mechanisms.

- **Authentication:** no authentication mechanism available. As responses to requests are always sent to real IP address of the requesting Member State, there is no need for further authentication mechanisms.
- **Integrity mechanism:** provided by the sTESTA network.
- **Confidentiality mechanism:** provided by the use of HTTPS over sTESTA.
- **Non-repudiation mechanism:** no specific non-repudiation mechanism available. The servers participating in the ECRIS network are trusted. As such, acknowledgments are considered sufficient.

Usage

- **Number of available e-Document formats:** In the Business Analysis, four e-Documents formats are described:
 - **Notifications:** Criminal records and offences;
 - **Requests:** Specific request for a specific person (this includes nominal information and identity information)
 - **Response on requests:** A response containing the nominal information, identity information and the associated criminal records. It is a “notification” in a specific information flow;
 - **Acknowledgements:** administrative and error messages.

In the ECRIS Framework Decision, the two annexes A and B describe all the codes of the criminal offences and sanctions included in the common reference tables and the national reference tables. 188 offences categories are counted in the reference table, along with 70 penalties and measures categories [EUR-Lex, 2009].

- **Number of known implementations in production-grade software:** In 2012, an implementation labelled as the ECRIS RI (Reference Implementation) was developed by DG JUST. ECRIS RI is a software that enables the exchange of data concerning criminal records between Member States: “*The ECRIS RI offers an integration interface which by means of web*

services. It allows external access to the RI functionalities. This enables the connection of the RI with Member States legacy systems such as the criminal record registers for example.” [European Commission, 2013]

The Reference Implementation software is designed to be used by all Member States. Currently, of the 25 participating Member States, 21 use the Reference Implementation, while the 4 others (Luxemburg, Spain, Lithuania and Finland) use their own implementation software complying with the standards. In the long-term, when all 28 Member States will be interconnected, 24 of them should be using the Reference Implementation, while the 4 others use their own implementation as mentioned before. This leads to a total of five implementations.

- **Number of e-Document exchanges annually:** In 2013, 862,643 e-Documents were exchanged, with an average of 71,887 e-Documents exchanges per month. As the project matures, this number is expected to grow.

Summary table

Table 15 - Analysis of European Criminal Records Information System (ECRIS)

European Criminal Records Information System (ECRIS)	
DESCRIPTIVE METADATA	
Licence	No licence available
Publisher	General Secretariat of the Council
Publisher type	Supranational Authority
Theme(s)	Criminal Records, Convictions
Access URL	http://ec.europa.eu/justice/criminal/european-e-justice/ecris/index_en.htm https://e-justice.europa.eu/content_criminal_records-95-en.do?init=true
CONTEXT	
Administrative process context	Data exchange of criminal records between EU member states
Geopolitical context	All EU Member States
Legal context	<p>Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States.</p> <p>Council Framework Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records</p>

	Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	None
Library of data elements	At schema level, ECRIS does not reuse existing data elements. At value level, ECRIS promotes the use of reference tables categorizing offences and penalties.
Naming and Design Rules	There are no explicit XML Schema design rules, however the naming conventions are based on ISO 11179.
e-Document engineering tools	XML Spy
Representation techniques	UML and XML Schema
GOVERNANCE MECHANISMS	
Goals	Share criminal records data of EU citizens upon request, and notify information concerning the criminal records of EU-nationals to the Member State of the offender's nationality.
Change management	<ul style="list-style-type: none"> • Organisational roles: Commission Expert Group, the Council of the EU and the European Parliament • Decision making process: The group of experts discusses and initiates any changes. The Council of the EU manages and approves these change proposals and eventually sends it to the European Parliament. • Documentation: Council Decision 2009/316/JHA of 6 April 2009
Enforcement policy	<ul style="list-style-type: none"> • Sharing: Legal requirement • Reuse: Legal requirement
Authoritative source	The General Secretariat of the Council ⁴⁵
Licensing framework	No licence available
Quality controls	No information found

⁴⁵ The General Secretariat of the Council: <http://www.consilium.europa.eu/documents>

CONFORMANCE MECHANISMS	
Application profile	Not available
Validation	Automatic and manual validation
Conformance certification	Tests described in the ECRIS Technical Specifications – Verification of conformity
SECURITY MECHANISMS	
Authentication mechanisms	Not disclosed
Integrity mechanisms	Not disclosed
Confidentiality mechanisms	Encrypted data transmission via the sTESTA network and HTTPS
Non-repudiation mechanisms	Non-repudiation of origin and receipt: messages at each level
USAGE	
Number of e-Document formats	4 (Notifications, Requests, Response on requests, Bulk acknowledge) 188 offences categories in the reference table + 70 penalties and measures categories in the reference table (258 categories)
Number of known implementations in production-grade software	5 (one Reference Implementation software and four own implementations)
Number of e-Documents exchanges annually	2013: 862,643 messages exchanged (average of 71,887 messages per month)

I.5. European Register of Road Transport Undertaking (ERRU)

Context

In order to better monitor the compliance of road transport with the rules in force, the European Commission has set up ERRU⁴⁶, a system that allows a better exchange of information between Member States [**European Commission - Mobility and Transport**].

ERRU will particularly allow the exchange of information about:

- transport managers who are declared unfit to manage the activities of a road transport undertaking;
- most serious infringements committed by hauliers in any Member State, which may lead to the loss of good repute;
- other infringements committed by hauliers in any Member State.

The ERRU system provides a means to interconnect the national registries through the exchange of structured (XML) messages to a central hub.

e-Document engineering method

The rules concerning the "interconnection of national electronic registers on road transport undertakings", as published in the Official Journal of the European Union [European Commission , 2010]⁴⁷, describe that the interconnection takes the form of an XML messaging framework. Member states can chose to exchange XML messages via a central hub or peer-to-peer (see Figure 10).

In order to allow that, ERRU provides an XML Schema Definition (XSD), resulting in standard XML exchange messages for all users of the system with common fields and understanding across countries. No other tool is available for creating documents: each Member State has to develop its own gateway and process platform to their local information and databases.

An XSD schema foresees a standard header for all types of messages (also common with the RESPER system⁴⁸) and the elements can be re-used whenever possible.

The e-Document formats haven't been created using a standardised e-Document engineering method. The ERRU XML Messaging Reference Guide provides guidelines for generating accurate and standard documents.

⁴⁶ http://ec.europa.eu/transport/modes/road/access/erru_en.htm

⁴⁷ Commission Regulation (EU) No 1213/2010 of 16 December 2010 establishing common rules concerning the interconnection of national electronic registers on road transport undertakings <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32010R1213:EN:NOT>

⁴⁸ Réseau permis de conduire/Driver Licence Network: <http://ec.europa.eu/idabc/en/document/3989.html>

- **Library of data elements:** Each type of message has its own information requirement model bound to the actual syntax using the syntax binding methodology described in the XML Messaging Reference Guide and compliant with the XSD Schema.
- **Naming and design rules:** No explicit naming and design rules have been followed for the creation of the ERRU XML Schemas.
- **e-Document engineering tools:** ERRU only provides the XSD Schemas, but no tools to build e-Documents. ERRU provides software requirements to help Member States designing a solution for exchanging XML messages.
- **Representation techniques:** The information requirement models in the XML guidelines are represented by XSD Schemas.

Governance mechanisms

- **Change management**
 - **Organisation roles:** A Steering Committee inside the European Commission is responsible for the good use of the ERRU system. The Committee can take decisions impacting ERRU.

An ERRU Working Group (ERRU WG), made up of experts of the Member States is in charge of making recommendations to the Steering Committee and meets when necessary.

A project team deals with daily questions.
 - **Decision making process:** If a change is proposed by the Steering Committee, an agreement of the ERRU WG is needed in order to enforce this change.
 - **Documentation:** No formal documentation is available to describe the process.
- **Enforcement policy**
 - **Sharing:** Legal requirement for Member States since December 2012 (Commission Regulation (EU) No 1213/2010 of 16 December 2010 establishing common rules concerning the interconnection of national electronic registers on road transport undertakings Text with EEA relevance⁴⁹)
 - **Reuse:** Legal requirement for Member States since December 2012 (Commission Regulation (EU) No 1213/2010 of 16 December 2010 establishing common rules concerning the interconnection of national electronic registers on road transport undertakings Text with EEA relevance⁵⁰)

⁴⁹ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32010R1213:EN:NOT>

⁵⁰ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32010R1213:EN:NOT>

- **Authoritative source:** no authoritative source is defined.
- **Licensing framework:** no explicit licence is defined.
- **Quality controls:** no quality control is defined.

Conformance mechanisms

Conformance to ERRU specifications is defined in the XML Messaging Reference Guide.

- **Application profile:** not available
- **Validation mechanism:** The validation of an XML message is done using XSD Schema. If an error is detected, a status code is returned within the replying XML message. Furthermore, the use of ID Correlation enforces the validation by generating for each exchange an ID that has to be the same throughout the conversation.
- **Conformance certification:** none

Security mechanisms

Regarding security mechanisms, specifications can be found in the ERRU Network and Security Reference Guide.

ERRU uses sTESTA network via HTTPS, with Digital Certificates. It allows for authentication, integrity and confidentiality mechanisms, as the data transmitted (XML messages) between the Competent Authority applications and the central ERRU system is encrypted through the use of HTTPS and digital certificates (one digital certificate will be issued per CA application). A PKI Infrastructure provides and maintains digital certificates.

- **Authentication:** Ensured by digital certificates and use of HTTPS
- **Integrity mechanism:** Ensured by digital certificates and the use of HTTPS; this does not ensure integrity of the document but rather reliability of the transmission.
- **Confidentiality mechanism:** All the certificates are issued according to X.509v3 standards, and the signature algorithm is Sha256 with RsaEncryption (2048-bits key length).
- **Non-repudiation mechanism:** not available.

Usage

- **Number of e-Document formats:** Eight types of XML messages can be exchanged; their format is described as part of the ERRU XML guidelines:
 1. Infringement Notification Message
 - a. MS2ERRU_Infringement_Req
 - b. ERRU2MS_Infringement_Req
 2. Infringement Response Message
 - a. MS2ERRU_Infringement_Res

- b. ERRU2MS_Infringement_Res
- 3. Search Request Message
 - a. ERRU2MS_CheckGoodRepute_Req
 - b. MS2ERRU_CheckGoodRepute_Req
- 4. Search Response Message
 - a. MS2ERRU_CheckGoodRepute_Res
 - b. ERRU2MS_CheckGoodRepute_Res
- 5. Statistics Data Message
 - a. SYS2ERRU_Statistics_Data
- 6. Types Message
 - a. ERRU_Infringement_Types
 - b. ERRU_Global_Types
 - c. ERRU_Statistics_Types
 - d. ERRU_CheckGoodRepute_Types
- 7. Acknowledgement Message (used to acknowledge the receipt of a message)
 - a. MS2ERRU_Infringement_Ack
 - b. ERRU2MS_Infringement_Ack
 - c. ERRU2SYS_Statistics_Ack
- 8. Invalid Message
 - a. ERRU2MS_Invalid_Message
- **Number of known implementations in production-grade software:**

ERRU is implemented in two categories of systems: at ERRU XML Central Messaging system hosted by European Commission, and at local Competent Authority (CA application developed by each Member State to use the ERRU services), as stated in the high-level structure for a centralized architecture option depicted in Figure 9, and in the high-level structure for a peer-to-peer architecture option depicted in Figure 10. About one third of the Member States has implemented ERRU.

Analysis of structured e-Document formats used in Trans-European Systems

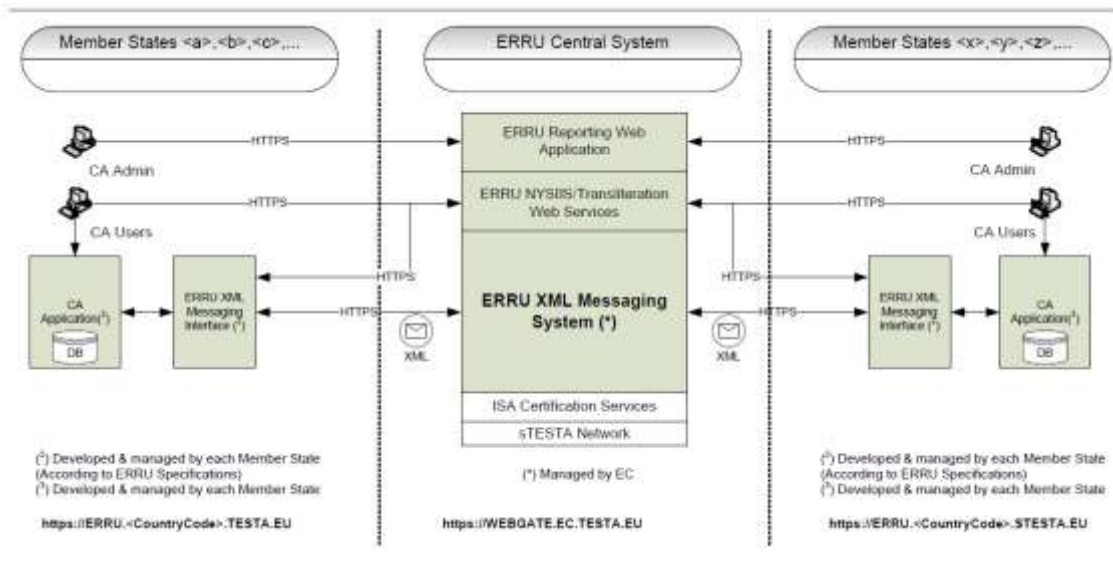


Figure 9 - High level structure for centralized architecture for ERRU (ERRU XML Messaging Reference Guide)

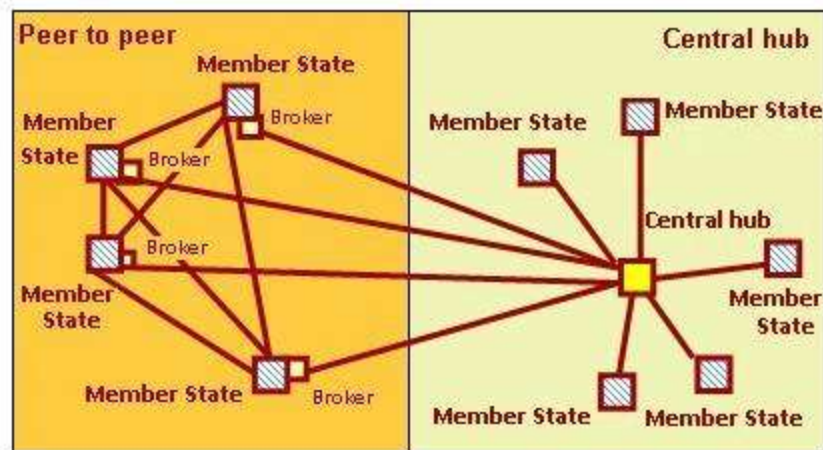


Figure 10 - High level structure for peer-to-peer architecture for ERRU (ERRU XML Messaging Reference Guide)

Summary table

Table 16 - Analysis of European Register of Road Transport Undertaking (ERRU)

European Register of Road Transport Undertaking (ERRU)	
DESCRIPTIVE METADATA	
Licence	No licence
Publisher	European Commission / Directorate-General for Mobility &

Analysis of structured e-Document formats used in Trans-European Systems

	Transport
Publisher type	Supra-national authority
Theme(s)	Road Transport, Infringement
Access URL	http://ec.europa.eu/transport/modes/road/access/erru_en.htm
CONTEXT	
Administrative process context	Road transport
Geopolitical context	Recommendation to all member states, no view on implementation.
Legal context	Commission Regulation (EU) No 1213/2010 of 16 December 2010 establishing common rules concerning the interconnection of national electronic registers on road transport undertakings Text with EEA relevance
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	ERRU XML Messaging Reference Guide provides guidelines for generating standard documents
Library of data elements	No common library used.
Naming and Design Rules	No formal XML Naming and design rules are used.
e-Document engineering tools	Tools are provided by Member States
Representation techniques	XML guidelines, XSD Schema
GOVERNANCE MECHANISMS	
Goals	Exchange information to better monitor the compliance of road transport with the rules in force
Change management	<ul style="list-style-type: none"> • Organisational roles: Steering committee inside European Commission for decisions and ERRU Working Group (ERRU WG) with experts of the Member States meets on a need basis. A project team deals with the daily questions. • Decision making process: If there is a need for changes, the Steering Committee inside European Commission proposes changes, and agreement of the ERRU WG is needed

	<ul style="list-style-type: none"> • Documentation: No formal documentation
Enforcement policy	<ul style="list-style-type: none"> • Sharing: Legal requirement • Reuse: Legal requirement <p>Mandatory use for the Member States since December 2012 (Commission Regulation (EU) No 1213/2010 of 16 December 2010 establishing common rules concerning the interconnection of national electronic registers on road transport undertakings Text with EEA relevance⁵¹)</p>
Authoritative source	None
Licensing framework	No explicit licence
Quality controls	None
CONFORMANCE MECHANISMS	
Application profile	Not available
Validation	Against XML Schema definition (XSD) and use of ID Correlation
Conformance certification	Not available
SECURITY MECHANISMS	
Authentication mechanisms	Digital Certificates and HTTPS
Integrity mechanisms	Digital Certificates and HTTPS
Confidentiality mechanisms	Certificates according to X.509v3 standards; signature algorithm Sha256 with RsaEncryption (2048-bits key length).
Non-repudiation mechanisms	Not available
USAGE	
Number of e-Document formats	<p>8 types of XML messages:</p> <ol style="list-style-type: none"> 1. Infringement Notification Message 2. Infringement Response Message

⁵¹<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32010R1213:EN:NOT>

	<ul style="list-style-type: none"> 3. Search Request Message 4. Search Response Message 5. Statistics Data Message 6. Types Message 7. Acknowledgement Message (used to acknowledge the receipt of a message) 8. Invalid Message
Number of known implementations in production-grade software	<p>2 categories of systems: ERRU XML Messaging system hosted by European Commission and local Competent Authority applications (CA applications developed by each Member State to use the ERRU services)</p> <p>About 1/3 of the Member States has implemented ERRU</p>
Number of e-Documents exchange annually	<p>More than 150.000 requests were forwarded to the MS in 2013</p>

I.6. European Car and Driving Licence Information System (EUCARIS)

Context

EUCARIS is a data exchange network for mobility related information, such as vehicle registration data, driving licences data, and the accompanying personal data.

EUCARIS uses a peer-to-peer concept for the data exchange. It uses a decentralised set-up in which all participating countries are connected to each other via National Contact Points (NCPs) and are able – by means of an interface – to search in each other's register, without influencing the national chosen set up of their registers. Hence, there is no centralised system and no central register.

The NCP organization depends on the nature of the data exchange. It is always a public organization, usually a registration authority or a police organization.

The message exchanges incorporated into EUCARIS have various legislative origins. The EUCARIS treaty (art. 2, 4, 5, 7 and 9) describes the following inquiry and notification types [EUCARIS, 2013]:

- **Registration of Vehicles**
 - o Vehicle Inquiry (VHInfo)
 - o Notification of registration of the imported vehicle
 - o Notification of destruction of a vehicle
 - o Inquiry for vehicle odometer readings (mileage)
- **Issue of Driving Licences**

- Driving Licence Inquiry on licence number or on name and date of birth (DLInfo)
- **Collection of traffic fines**
 - Inquiry of vehicle and owner/holder data, for the collection of traffic fines, on the basis of a bilateral/multilateral treaty or agreement between Member States. The inquiry consists of a single case as well as a multi case variant (sVHOH, mVHOH)

Based on Council Decision 2008/615/JHA⁵² (combatting cross-border crime and terrorism), the Prüm decision, EUCARIS offers:

- Inquiry of vehicle and owner/holder data on VIN and on reference date, or on registration number and on reference date. Integrated into this inquiry:
 - Vehicle Insurance inquiry

Based on Directive 2011/82/EU⁵³ (Cross-Border Exchange), EUCARIS offers:

- Inquiry of vehicle and owner/holder data, for the collection of traffic fines regarding road safety related traffic offences. The inquiry consists of a single case as well as a multi-case variant (sCBE, mCBE).

EUCARIS can also be used for the European Register of Road Transport Undertaking (ERRU). A Member State can choose to use either the Central Hub system or EUCARIS for the message exchange. Both these systems form the message exchange network, where the component EUCARIS broker ensures that all countries can communicate with each other, irrespective of the system it uses. EUCARIS broker translates message formats from the EUCARIS version to the Central Hub version, and vice versa.

Based on Directive 2006/126/EC⁵⁴ on driving licenses, EUCARIS offers:

- Driving license information network (RESPER)

Finally, EUCARIS offers message exchanges for:

- Vehicle information, triggered via a vehicle emergency call (Harmonised eCall European Pilot⁵⁵)
- Digital Certificate of Conformity (CoC = "birth certificate" of a vehicle) via the Initial Vehicle Information (IVI) message exchange.

⁵² Council Decision 2008/615/JHA:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:0011:EN:PDF>

⁵³ Directive 2011/82/EU:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:288:0001:0015:EN:PDF>

⁵⁴ Directive 2006/126/EC:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:403:0018:0060:EN:PDF>

⁵⁵ Harmonised eCall European Pilot: <http://www.heero-pilot.eu/view/en/home.html>

The list of available message exchanges has grown over the years and is expected to grow further in the future.

For all of these message exchanges, EUCARIS provides the framework to exchange messages between NCPs. For most of the message exchanges supported, EUCARIS also offers a web based client with which inquiries can be launched and results can be reviewed. The client is in English by default, but can be configured by the Member State to support any desired language, where individual users can choose their preferred language. The use of the EUCARIS client is optional in all cases; Member States are free to develop their own clients.

In general, EUCARIS supports three general types of message exchanges:

- **Synchronous message exchange.** Services are triggered by sending a request message (from a client application, which is EUCARIS web client or a customized client). The request message is processed within a synchronous session, yielding a response message as result. Examples of synchronous services are VInfo, VOwner-Holder-Owner Prüm, and sCBE. Where appropriate, a broadcast is possible for synchronous message exchanges. For example, one client of one Member State launches a request to all Member States supporting the message exchange, resulting in one consolidated response containing the responses of all participating Member States.
- **Asynchronous requests and responses.** In this case, the request is delivered into a queue (i.e. the download queue of the country that processes the request). Processing is done asynchronously (e.g. a request sits in a queue until it is picked up; the processing might be done overnight). Using a queue once again, the response message is delivered to the country that sent the request. Examples of asynchronous requests and response dialogues are mCBE and mVHOH.

Note: For an asynchronous request and response, EUCARIS does not keep track of requests and response. It just processes messages and delivers them into the queue without being aware of requests and responses.

When delivering the message to the recipient, the message can either be pushed to the recipient or the recipient can pull the message from EUCARIS.

- **Notifications.** A notification is a message that does not necessarily require a response. When a response is available, this is often an acknowledgement of delivery. Notifications are transferred from the sender to the recipient using the upload queue (of the sender) and download queue (of the recipient). Examples of notifications are RESPER NotificationDLStatus and ERRU Notification of Infringement.

In delivering the message to the recipient, there is a choice to either push the message to the recipient or the recipient pulling the message from EUCARIS.

Besides the message exchange mechanism and a web client, EUCARIS offers some additional tooling such as:

- EUCARIS broker, for conversion of messages between EUCARIS format and the format of another message exchange system
- Optional add-ons, e.g.
 - Support to process multi case messages using the single case national interface (for mVHOH and mCBE)
 - Pre-processing and post-processing tooling (for eCall)
 - "Secure tunnel", a facility with which a configurable amount of security can be added to (Internet based) communication in the Member State domain between NCP and a public organisation that submits data to or receives data from EUCARIS.
- Usage statistics collection tooling (to extract usage statistics from the logging of all participating Member States)
- Log viewer tooling
- Availability monitoring
- Test clients, stubs

e-Document engineering method

- **Methodology:** The definitions of the data are derived from the EU directives and guidelines. There is no formal methodology to build the e-Documents.
- **Library of data elements:** No library is defined
- **Naming and Design Rules:** XSD Schema
- **e-Document engineering tools:** No tool has been defined
- **Representation techniques:** The information is specified in the XML message protocol, based on the data derived from EU directives and guidelines [EUCARIS, 2013]. According to the EUCARIS website⁵⁶, this means that each data-element has been described in a very exact way. The definitions of the data are derived from the EU directives and guidelines, if possible. Not only the interpretation of each data-element, but also the content of the data has been standardised, so each country will use the same code to indicate to other countries that a car is 'blue', even if in their own registry a completely different description or code is used. Furthermore, it allows for translation of the code descriptions into various languages.

For standardisation, European legislation is used wherever possible (e.g. 1999/37/EC for a definition of all vehicle technical data that appears on vehicle registration documents, and 2006/126/EC for a definition of all data appearing on an EU harmonised driving license).

Governance mechanisms

- **Change management**

⁵⁶ <https://www.eucaris.net/technology>

- **Organisation roles:** The EUCARIS Participants Board is responsible for EUCARIS memberships and EUCARIS functionality. It appoints a Nominated Party to chair the committee (currently Germany), and a Nominated Party for Operations (NPO), i.e. a Member State responsible for maintenance and development (currently the Netherlands). A Nominated Party is appointed for 5 years.
- **Decision making process:**
- Changes are carried out by the NPO. It issues system updates (new or adapted software), extension updates (a new message exchange) and configuration updates (addition of member states). New releases of the EUCARIS application are always compatible with former releases. However, an extension update might require an upgrade to a certain version of system update first.
 - o For message exchanges based on the EUCARIS treaty, the specifications can only be changed by the EUCARIS Participants Board in consultation with the Member States. The acceptance of new Member States or a new functionality is under auspices of the EUCARIS Participants Board.
 - o For message exchanges based on EU legislation (e.g. Prüm, CBE, ERRU, RESPER), the dataset associated with the legislation is a basis for the specification. Changes can only be made if the dataset (and thus the legislation) changes. The maximum number of Member States using the message exchange is also defined by the legislation, i.e. the Member States that have ratified it.

A new Member State, or a State extending its service with a new message, will only be accepted in the production environment of EUCARIS after a formal test procedure (carried out by the NPO). During this procedure the Secretary State checks both requests from customised client applications and response message.

For Prüm and CBE, the legislation imposes an additional requirement for the acceptance, i.e. to pass an evaluation visit by a delegation of the working group.

- **Enforcement policy**

- **Sharing:** Prüm Treaty / EU Council Decision 2008/615/JHA⁵⁷ of 23 June 2008 states that EUCARIS needs to be implemented by each Member States by July 2011

⁵⁷ EU Council Decision 2008/615/JHA:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:0011:EN:PDF>

- **Reuse:** Prüm Treaty / EU Council Decision 2008/615/JHA of 23 June 2008 stated that EUCARIS needs to be implemented by each Member States by July 2011
- For CBE 2011/82/EU⁵⁸, the legislation states that for the message exchange EUCARIS must be used, and must be implemented by November 2013.
- For ERRU and RESPER Member States must use a message exchange facility, which is either a Central Hub System or EUCARIS. The legislation also gives implementation dates, December, 2012, and January 19, 2013, respectively.
- **Authoritative source:** All specifications are available on the private section of www.eucaris.net. An account can be requested via eucaris2help@rdw.nl.
- **Licensing framework:** No licence is defined
- **Quality controls:** No quality controls are defined.

Conformance mechanisms

- **Application profile:** No application profiles are defined.
- **Validation mechanism:** The validation of an XML message is done using an XSD Schema.
- **Conformance certification:** No conformance certification is defined.

Security mechanisms

The security between the Member States is controlled by the EUCARIS server core. The messages are transferred over an SSL connection (1-sided SSL: only a server certificate).

The messages sent to the back-end are plain text XML-messages since the connection between the application and the back-end shall be in a protected environment.

All messages exchanged between the States are signed with the use of a certificate (XML-Signature). The EUCARIS server will verify the signature of the incoming messages and then forward the unsigned message to the registration server or requesting client application. This ensures **authentication** and **integrity**.

Furthermore, for a message exchange to be successful, both the sender country and the recipient country must have set an authorisation for the exchange.

EUCARIS uses sTESTA II network in order to exchange messages.

⁵⁸ Directive 2011/82/EU:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:288:0001:0015:EN:PDF>

Analysis of structured e-Document formats used in Trans-European Systems

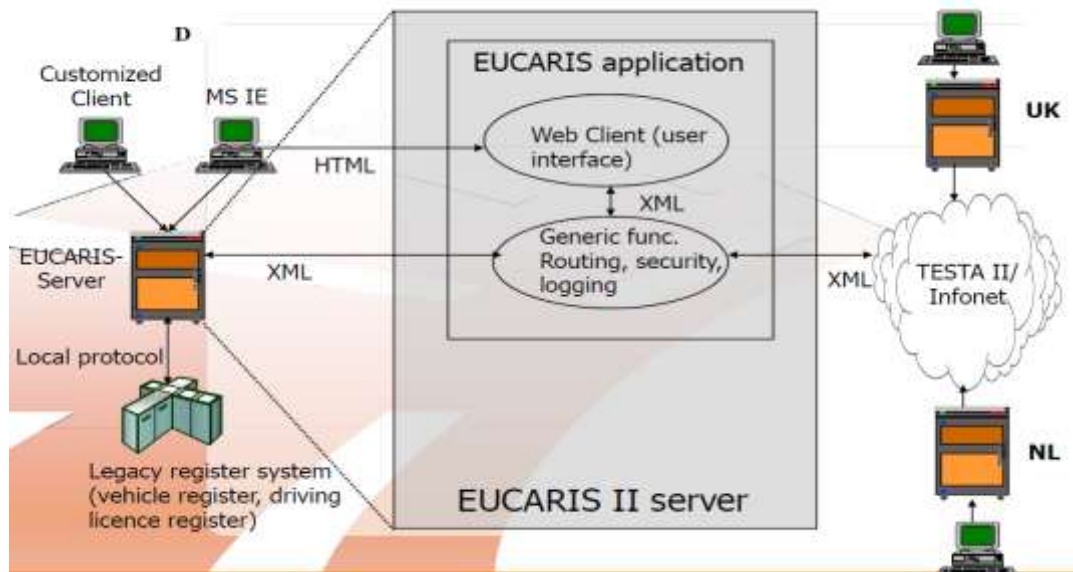


Figure 11 - Architectural model of EUCARIS⁵⁹

⁵⁹ Mr Hens Peeters Weem, Workshop Session 1: Modernizing Vehicle Inspection / Workshop C: Mutual Recognition, 2009 CITA Conference, 13 -16 Oct. Gothenburg, Sweden , Global Challenges – Opportunities for Change

Usage

- **Number of e-Document formats:** 29 message types are available (March 2014):
 1. VInfo
 - a. (sync) Request by vehicle registration number
 - b. (sync) Request by vehicle identification number
 - c. (sync) Request by vehicle document Id
 2. Vehicle: (async) Notification of registration
 3. Vehicle: (async) Notification of destruction
 4. Mileage
 - a. (sync) Request by vehicle identification number
 5. DLInfo
 - a. (sync) Request by license number
 - b. (sync) Request by personal data of license holder
 6. Prüm (vehicle, owner, holder, insurance data)
 - a. (sync) Request by vehicle registration number and reference date-time. Request for insurance data is (optionally, for the Member States that support it) integrated into this request.
 - b. (sync) Request by vehicle identification number and reference date-time
 7. CBE (owner holder information for collection of traffic fines)
 - a. (sync) sCBE: single case request, by vehicle registration number + reference date-time + CBE offence code
 - b. (async) mCBE: multiple case request, by vehicle registration number + reference date-time + CBE offence code
 8. Owner-Holder information (for collection of traffic fines, bilateral treaty)
 - a. (sync) sVHOH: single case request, by vehicle registration number + reference date-time + (non-CBE) offence code
 - b. (async) mVHOH: multiple case request, by vehicle registration number + reference date-time + (non-CBE) offence code
 - c. (async) FileTransfer: Message allowing transfer of some bilaterally agreed message format (not specified by or known to EUCARIS), as message attachment
 9. eCall
 - a. (sync) Request by Vehicle Identification Number
 - b. (sync) Request by vehicle registration number

10. ERRU

- a. (sync) Check Good Repute
- b. (async) Notification of infringement
- c. (async) Notification of infringement response

11. RESPER

- a. (sync) Search Driving License by Name
- b. (sync) Get Driving License Details
- c. (async) Notification Driving License Status
- d. (async) Notification Driving License Status Response
- e. (async) Secure Message

12. CoC or IVI (Initial Vehicle Information)

- a. (sync) CoC retrieval by vehicle identification number
- b. (async) CoC forwarding notification
- c. (async) CoC validation request
- d. (async) CoC validation response

- **Number of known implementations in production-grade software:**

In March 2014, the following Member States were using EUCARIS for the following message exchanges:

Austria: Prüm

Belgium: CBE, DLInfo, mVHOH, Prüm, VHInfo

Bulgaria: CBE, eCall, Prüm

Cyprus: DLInfo, VHInfo (accepted for Prüm, not yet evaluated)

Czech Republic: DLInfo, VHInfo (outbound only)

Estonia: DLInfo, VHInfo

Finland: ERRU, Prüm

France: CBE, mVHOH, Prüm

Germany: CBE, DLInfo, ERRU, mVHOH, Prüm

Gibraltar: DLInfo, VHInfo (outbound only)

Great Britain: DLInfo, VHInfo

Hungary: DLInfo, VHInfo (accepted for CBE, Prüm, not yet evaluated)

Iceland: DLInfo, VHInfo

Ireland: (accepted for Prüm, not yet evaluated)

Isle Of Man: DLInfo, VHInfo (outbound only)

Italy: DLInfo, eCall, VHInfo (accepted for Prüm, not yet evaluated)

Jersey: DLInfo, VHInfo (outbound only)

Latvia: DLInfo, VHInfo (accepted for Prüm, not yet evaluated)

Lithuania: CBE, DLInfo, Prüm, VHInfo

Luxembourg: DLInfo, Prüm, VHInfo

Malta: (accepted for Prüm, not yet evaluated)

The Netherlands: CBE, DLInfo, eCall, ERRU, mVHOH, Prüm, RESPER, VHInfo

Poland: CBE, Prüm

Romania: DLInfo, IVI, Prüm, RESPER, VHInfo

Slovakia: DLInfo, Prüm, VHInfo

Slovenia: Prüm

Spain: Prüm

Sweden: DLInfo, Prüm, VHInfo

Switzerland: mVHOH

About 8 countries are testing with the EUCARIS NPO for implementation of Prüm, CBE, ERRU or RESPER, DLInfo or VHInfo.

For ERRU, RESPER, about 5 countries have been accepted by EUCARIS, but have not yet been accepted by EU (Central Hub).

The IVI pilot will be launched in 2014.

- **Number of e-Documents exchanges annually:** In the first half of 2013, the total number of VHInfo inquiries was 14,500,000. The total number of DLInfo inquiries was 895,000. The total number of Prüm inquiries was 1,600,000. For other message exchanges, the numbers are not known.

Summary table

Table 17 - Analysis of European Car and Driving Licence Information System (EUCARIS)

e-Documents used by the European Car and Driving Licence Information System (EUCARIS)

DESCRIPTIVE METADATA	
Licence	No licence
Publisher	EUCARIS Nominated Party for Operations, under auspices of EUCARIS Participants Board.
Publisher type	Supra-national authority
Theme(s)	Road Transport, Vehicle crime, Vehicle registration, Driving licence registration, Traffic offence enforcement
Access URL	http://www.eucaris.net

CONTEXT	
Administrative process context	Exchange of vehicle registration and driving Licence information.
Geopolitical context	Austria , Belgium , Bulgaria , Cyprus , Czech Republic , Denmark , Estonia , Federal Republic of Germany , Finland , France , Gibraltar , Greece , Guernsey , Hungary , Iceland , Isle of Man , Italy , Jersey , Latvia , Lithuania , Luxembourg , Malta , Norway , Poland , Portugal , Republic of Ireland , Romania , Slovakia , Slovenia , Spain , Sweden , Switzerland , The Netherlands , UK Northern Ireland , United Kingdom
Legal context	<p>EUCARIS treaty⁶⁰ (art. 2, 4, 5, 7 and 9).</p> <ul style="list-style-type: none"> • The exchange of vehicle registration data is foreseen by the Prüm Decision, Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. • The exchange of vehicle registration data in the context of the CBE directive 2011/82/EU of 25 October 2011 facilitating the cross-border exchange of information on road safety related traffic offences. • The exchange of driving license data via the EU driving licence network (RESPER), as foreseen in 2006/126/EC on driving licences. • Commission Regulation (EU) No 1213/2010 of 16 December 2010 establishing common rules concerning the interconnection of national electronic registers on road transport undertakings Text with EEA relevance
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	The definitions of the data are derived from the EU directives and guidelines. A formal methodology is not used.
Library of data elements	No standard library is used.
Naming and Design Rules	XSD Schema
e-Document engineering tools	No tool has been defined
Representation techniques	Specified in the XML message protocol, based on the data derived from EU directives and guidelines

⁶⁰ EUCARIS treaty: <http://www.official-documents.gov.uk/document/cm70/7064/7064.pdf>

GOVERNANCE MECHANISMS	
Goals	General exchange mechanism for all transport related data between national contact points in all of Europe
Change management	<ul style="list-style-type: none"> • Organisational roles: EUCARIS Participants Board and Member States. Development and maintenance by a Nominated Party of Operations. • Decision making process: EUCARIS Participants Board in consultation with the Member States • Documentation: Prüm decision, CBE directive, directive on driving licenses, ERRU commission regulation
Enforcement policy	<ul style="list-style-type: none"> • Sharing: Legal requirement: Prüm Treaty / EU Counsel Decision 2008/615/JHA of 23 June 2008 (theoretically mandatory by July 2011) • Reuse: Legal requirement: Prüm Treaty / EU Counsel Decision 2008/615/JHA of 23 June 2008 (theoretically mandatory by July 2011) • CBE: Article 4, for the investigation of road safety related traffic offences, the Member States' national contact points shall allow access to vehicle registration data, using existing software applications such as the one especially designed for the purposes of Article 12 of Decision 2008/615/JHA • ERRU: Mandatory use for the Member States since December 2012 (Commission Regulation (EU) No 1213/2010 of 16 December 2010 establishing common rules concerning the interconnection of national electronic registers on road transport undertakings Text with EEA relevance⁶¹) • RESPER: Directive 2006/126/EU article 5, for driving license checks, Member States shall use the EU driving licence network once it is operational
Authoritative source	None
Licensing framework	No licence
Quality controls	None

⁶¹<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32010R1213:EN:NOT>

CONFORMANCE MECHANISMS	
Application profile	Not available
Validation	Using XML Schema definition (XSD)
Conformance certification	Not available
SECURITY MECHANISMS	
Authority mechanisms	Digital certificates, signed messages for external web services, no signature for public web services
Integrity mechanisms	Signed messages for external web services, no signature for public web services. Use of sTesta II network.
Confidentiality mechanisms	No confidentiality mechanism that is part of the e-Document. Confidentiality is achieved in the transport layer, via SSL encryption. Use of sTesta II network.
Non-repudiation mechanisms	Not known
USAGE	
Number of e-Document formats	29
Number of known implementations in production-grade software	35 participants
Number of e-Documents exchanges annually	In the first half of 2013: 17,000,000 enquiries.

I.7. Tachograph Network (TACHOnet)

Context

In order to enforce the regulation on driving times and resting periods, the Council Regulation (EEC) 3821/85⁶² dictates that new vehicles above 3.5 tonnes or carrying more than 9 people including the driver, should have a tachograph installed⁶³. A tachograph is a device installed in a vehicle that automatically records its speed, distance and the driver's activity. The driver card allows the unique identification of a driver in the vehicle and keeps track of all the information recorded by the tachograph. For an effective implementation of the tachograph regulations, a driver should only hold one driver card that he must use in every vehicle he drives. In order to ensure the uniqueness of the driver card and to avoid fraud of a unique driver possessing several cards, a telematic network to exchange information about tachograph cards within EU Member States was put in place: TACHOnet⁶⁴. The goals of TACHOnet are:

- to ensure fair competition between road transport operators;
- to enhance road safety by avoiding driver's fatigue; and
- to create even social conditions for mobile transport workers.

e-Document engineering method

TACHOnet provides an XML Schema Definition (XSD). These e-Document formats have not been created using a standardised e-Document engineering method. The TACHOnet XML Messaging Reference Guide provides guidelines for generating standard documents.

- **Library of data elements:** Each e-Document format has its own information requirement model that has to be bound to the actual syntax using the syntax binding methodology described in the XML Messaging Reference Guide⁶⁵ and compliant with the XSD Schema.
- **Naming and design rules:** No explicit naming and design rules have been followed for the creation of the TACHOnet XML Schemas.
- **e-Document engineering tools:** TACHOnet only provides XSD Schemas, but no tools to build e-Documents.
- **Representation techniques:** The information requirement models in the XML guidelines are represented using XSD Schemas.

⁶² Council Regulation (EEC) 3821/85:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0451:FIN:EN:PDF>

⁶³ Tachograph: http://ec.europa.eu/transport/modes/road/social_provisions/tachograph/index_en.htm

⁶⁴ TACHOnet: http://ec.europa.eu/transport/modes/road/social_provisions/tachograph/tachonet_en.htm

⁶⁵ XML Messaging Reference Guide:
http://ec.europa.eu/transport/modes/road/social_provisions/doc/tcn_xmlmessagingrefguide_v1.5.pdf

Governance mechanisms

- **Change management**
 - **Organisation roles:** The long-term goal of the project is to keep and maintain the information on drivers and tachograph cards. According to feedback of TACHOnet Working Group (made up of Member States experts) or users, the European Commission could modify TACHOnet. A project team deals with daily questions.
 - **Decision making process:** The European Commission could change the TACHOnet XSD Schemas, with approval from the TACHOnet Working Group. With the last change in 2011, the old version of the XSD was deprecated. When a new version comes out, every MS has to upgrade at the same time, as two versions cannot coexist. This will change in the future, where several versions would be able to coexist in the system.
 - **Documentation:** No formal documentation is available to describe the process.
- **Enforcement policy:** A European Regulation was settled on the installation and use of the tachograph for the enforcement of driving time and rest periods of professional drivers in the field of road transport. A Commission Regulation introduced the new digital recording equipment and personal smart cards for drivers. On 13 January 2010, the Commission adopted a Recommendation praising Member States to use the TACHOnet messaging system to exchange information on truck and coach drivers when checking tachograph cards. A modification of the tachograph regulation, adopted on 15 January 2014, will modify Article 26, and will make the use of TACHOnet *compulsory* two years after its publication, most likely from January 2016.
- **Authoritative source:** No authoritative source is defined.
- **Licensing framework:** No explicit licence is defined.
- **Quality controls:** No quality control is defined.

Conformance mechanisms

Conformance to TACHOnet specifications is defined in the XML Messaging Reference Guide:

- **Application profile:** No application profiles are defined.
- **Validation mechanism:** The validation of an XML message is done using an XSD Schema. If an error is detected, status code is returned within the replying XML message. Furthermore, the use of ID Correlation enforces the validation by generating for each exchange an ID that has to be the same throughout the conversation.
- **Conformance certification:** No conformance certification is defined.

Security mechanisms

Regarding security mechanisms, specifications can be found in the TACHOnet Network and Security Reference Guide. TACHOnet uses sTESTA network via HTTPS, with Digital Certificates. This allows for **authentication, integrity and confidentiality mechanisms**, as the data transmitted (XML messages) between the CIA (Card Issuing Authority) applications and the central TACHOnet system will be encrypted through the use of HTTPS and digital certificates (one digital certificate will be issued per CIA application). A PKI Infrastructure would provide and maintain digital certificates.

The generic PKI architecture is based on the market standards:

- Certificates follow the X.509 V3 standard⁶⁶
- Compatible with the PKIX standard

The issued digital certificates are RSA certificates with a 2048-bit key length valid for one year.

- **Non-repudiation mechanism:** No non-repudiation mechanism is defined.

⁶⁶ X.509 V3 : <http://www.ietf.org/rfc/rfc3280.txt>

Usage

- Number of e-Document formats:** The exchanged information uses 4 types of XML messages: *CheckIssuedCards*, *CheckCardStatus*, *ModifyCardStatus* and *IssuedCardsDL* [Directorate General: Energy & Transport, 2011].
- Number of known implementations in production-grade software:** TACHOnet is implemented in two systems: at TACHOnet central system and in the CIA applications (at least one per Member State), with interface from these CIA applications to EA (enforcement authorities), as stated in the TACHOnet global architecture depicted in Figure 12.
- Number of e-Document exchanges annually:** Over 1 million of requests have been made during the period of January 2013 to August 2013 across the CIA applications and TACHOnet central system. The TACHOnet system is in production since 2006 and 37 countries are currently connected: 25 Member States and 12 non-EU countries, which are Contracting Parties to AETR (Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Croatia, Iceland, Lichtenstein, Monaco, Norway, and Switzerland).

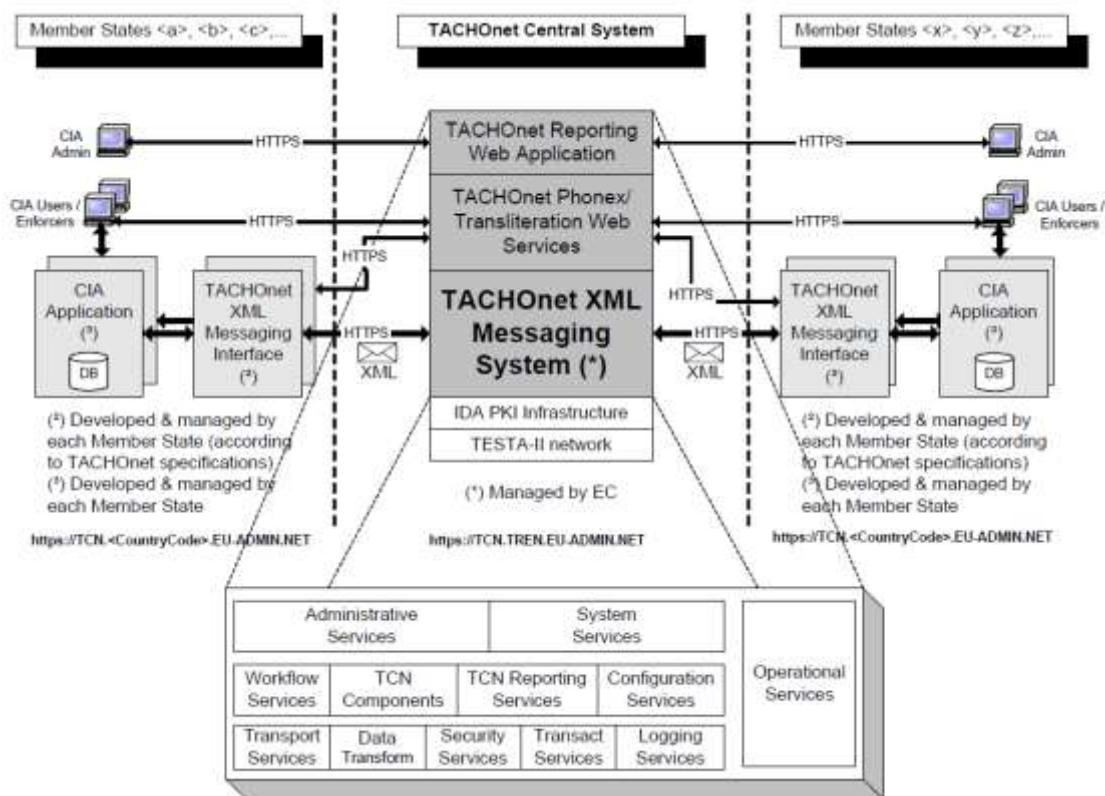


Figure 12 - TACHOnet global architecture (TACHOnet XML Messaging Reference Guide)

Summary table

Table 18 - Analysis of Tachograph Network (TACHOnet)

Tachograph Network (TACHOnet)	
DESCRIPTIVE METADATA	
Licence	No licence
Publisher	European Commission / Directorate General: Energy & Transport
Publisher type	Supra-national authority
Theme	Driving Time, Resting Period, Road Transport, Tachograph
Download URL	http://ec.europa.eu/transport/modes/road/social_provisions/tachograph/tachonet_en.htm
CONTEXT	
Administrative process context	Road transport
Geopolitical context	Recommendation to all Member States.
Legal context	<p>Council Regulation (EEC) no 3821/85 (installation and use of the tachograph for the enforcement of driving time and rest periods of professional drivers in the field of road transport)</p> <p>Commission Regulation (EU) No 1266/2009</p> <p>Commission Recommendation of 13 January 2010 on the secure exchange of electronic data between Member States to check the uniqueness of driver cards that they issue</p> <p>Modification of the tachograph regulation, adopted on 15 January 2014</p>
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	TACHOnet XML Messaging Reference Guide provides guidelines for generating standard documents
Library of data elements	There is no library of data elements.
Naming and Design Rules	No formal XML Naming and design rules are used.
e-Document engineering tools	There are no global e-Document engineering tools for e-Document engineering.

Analysis of structured e-Document formats used in Trans-European Systems

Representation techniques	XML guidelines, XSD Schema
GOVERNANCE MECHANISMS	
Goals	<ul style="list-style-type: none"> • Exchange information about tachograph cards within EU Member States
Change management	<ul style="list-style-type: none"> • Organisational roles: European Commission, with approval of TACHOnet Working Group (Member States' experts). A project team deals with the daily questions. • Decision making process: Deprecation of the old version of XSD (when a new version comes out, every MS has to change at the same time) in 2011, different versions would likely coexist in the future implementation of TACHOnet • Documentation: No formal documentation
Enforcement policy	<ul style="list-style-type: none"> • Sharing: Voluntary • Reuse: Voluntary • Voluntary use; will be mandatory (likely from January 2016) since the modification of the tachograph regulation, adopted on 15 January 2014
Authoritative source	None
Licensing framework	No explicit licence
Quality controls	None
CONFORMANCE MECHANISMS	
Application profile	Not available
Validation	Against XML Schema definition (XSD) and use of ID Correlation
Conformance certification	Not available
SECURITY MECHANISMS	
Authentication mechanisms	sTESTA network via HTTPS; PKI Infrastructure provides and maintains digital certificates
Integrity mechanisms	sTESTA network via HTTPS; PKI Infrastructure provides and maintains digital certificates;

Analysis of structured e-Document formats used in Trans-European Systems

Confidentiality mechanisms	sTESTA network via HTTPS; PKI Infrastructure provides and maintains digital certificates;
Non-repudiation mechanisms	Not available
USAGE	
Number of e-Document formats	Only one XSD definition, with 4 message types: CheckIssuedCards, CheckCardStatus, ModifyCardStatus and IssuedCardsDL
Number of known implementations in production-grade software	2 kind of systems: TACHOnet central system and the CIA (Card Issuing Authority) applications, with interface for each Member State for EA (enforcement authorities) 25 Member States and 12 non-EU countries have implemented TACHOnet
Number of e-Documents exchanges annually	1 million requests from 1 st of January to August 2013

I.8. European Patients Smart open Services projects (epSOS)

Context

epSOS is a large-scale pilot on e-Health with a total budget of € 36.5 million that is co-funded by the European Commission Competitiveness and Innovation Programme (CIP) within the ICT Policy Support Programme. According to the epSOS homepage, the goals are to improve the quality and safety of healthcare for citizens when travelling to another European country. Moreover, it concentrates on developing a practical e-Health framework and ICT infrastructure that enables secure access to patient health information among different European healthcare systems. The framework entails benefits for both patients and health professionals in seeking and offering health services⁶⁷.

By connecting the e-Health infrastructures between the Participating Nations, the epSOS architecture allows to exchange information across borders. epSOS includes 45 institutions from 25 EU states. During the pilot phase of the project, which is currently ongoing, 8 countries are providing **e-Dispensation services**, five are providing **e-Prescription services** and eleven are participating in the **Patient Summary services**.

e-Document engineering method

The epSOS Evolving Document on Architecture and Design – Interoperability Specification (EED Design – Interoperability Specification) [epSOS , 2014] gives overview of epSOS architecture and design, including a description of epSOS Semantic Framework Specification.

The basis of the e-Document formats are the HL7 Clinical Document Architecture (CDA) 2.0 standard. The standard, based on XML, have three levels of interoperability⁶⁸:

- CDA Level 1: The CDA includes the CDA Header and an unstructured body that may be a PDF, a DOC, or a scanned image.
- CDA Level 2: The CDA includes the CDA Header plus an XML structured body with narrative blocks.
- CDA Level 3: As CDA Level 2 plus coded entries for representing individual data fields (e.g. laboratory data, blood pressure, medications, etc.).

epSOS e-Documents may be represented by both CDA Level 1 and Level 3 instances. CDA Level 1 is used to embed the original document generated by the country of origin, under PDF format. CDA Level 3 is used for representing the same

⁶⁷ About epSOS: <http://www.epsos.eu/home/about-epsos.html>

⁶⁸ Technical solutions of patient consent: <http://www.epsos.eu/technical-background/systems-standards/technical-solutions-of-patient-consent.html>

information, but in a structured way in XML. The structured information is transcoded and translated when exchanged between countries.

- **Library of data elements:** On schema level, epSOS e-Documents formats are based on the HL7 CDA 2.0 standard, with epSOS CDA extensions for medications. For each document type epSOS has defined a specific profile (CDA document template), derived from known CDA templates (see e.g. IHE Patient Care Coordination (PCC) domain⁶⁹ [epSOS , 2014]). HL7 implements the Reference Information Model (RIM)⁷⁰ as a library of clinical data elements and domains.

On the value level, epSOS provides its own code lists for value sets, outlined in the Master Value Set Catalogue (MVC). The MVC originates from established code systems like SNOMED CT, ICD-9, ICD-10, LOINC, ATC, and HL7.⁷¹ The epSOS MVC is the foundation of the epSOS Master Translation/Transcoding Catalogue (epSOS MTC) that allows the transcoding and translation of coded elements present in epSOS Documents. This is called the epSOS Semantic Framework, as depicted in Figure 13.

- **Naming and Design Rules:** At schema level, XML naming and design rules of HL7 have been followed in the CDA profiles (CDA templates).
- **The e-Document engineering tools:** Multiple tools are available for the design and implementation of HL7 data formats. This concerns the V3 Implementation Tools and the V3 Modelling & Methodology Tools⁷².
- **Representation techniques:** The HL7 CDA data formats are based on XSD.

⁶⁹ IHE Patient Care Coordination http://wiki.ihe.net/index.php?title=Patient_Care_Coordination

⁷⁰ HL7 Reference Information Model: <http://www.hl7.org/implement/standards/rim.cfm>

⁷¹ Semantic Issues: <http://www.epsos.eu/technical-background/semantic-issues.html>

⁷² V3 Implementation and Modelling & Methodology tools:
<http://www.hl7.org/participate/toolsandresources.cfm?ref=nav>

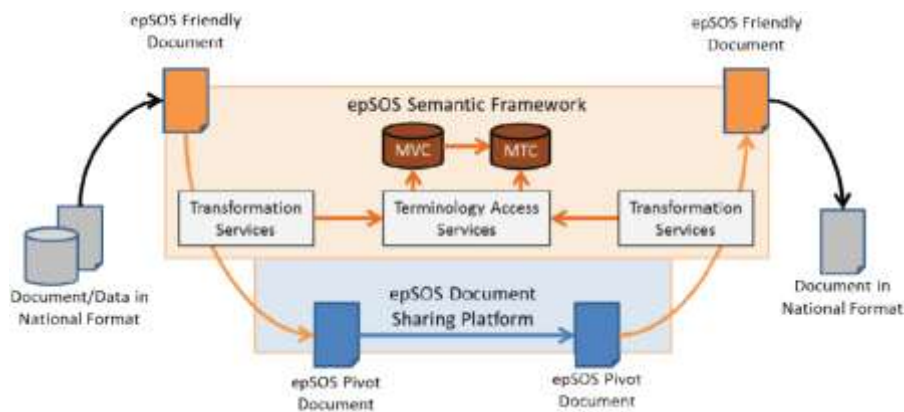


Figure 13 – epSOS Semantic Services [epSOS , 2014]

Governance mechanisms

- **Change management:** The data formats based on the HL7 CDA standard are governed by the HL7 Technical Steering Committee. The management process regarding the decision-making practices is documented in the HL7 Governance and Operations Manual⁷³.

The value sets of epSOS and the epSOS CDA profiles (CDA templates) are governed by the epSOS Change Management Committee, which comprises a number of actors and roles to manage all the changes in the different domains. The Committee includes a project coordinator, a project management team leader and specific experts. All Participating Nations must be involved in the change management process. The change management process affects three levels: the changes in requirements, specifications and implementations. The process is monitored and documented.

- **Enforcement policy:** Member states participate in the epSOS pilot on a voluntary basis. When participating, they do have to conform strictly to the specifications laid out by the epSOS committees. The [eHealth Network](#) (eHN) from the art 14 in the Patients rights' Directive has the power to issue guidelines and recommend to the Member States about the content and has done so based on the epSOS work.
- **Authoritative source:** HL7 provides an authoritative source for the CDA. epSOS' structural metadata, such as the epSOS CDA profiles (CDA templates), the epSOS Master Value Catalogue (epSOS MVC) and epSOS Master Translation/Transcoding Catalogue (epSOS MTC), is stored in the epSOS document repository, which is not publicly accessible.

⁷³ HL7 Governance and Operations Manual:
http://www.hl7.org/documentcenter/public_temp_A4762387-1C23-BA17-0C2D07749E2D643F/membership/HL7_Governance_and_Operations_Manual.pdf

- **Licensing framework:** The HL7 CDA and the epSOS CDA profiles are licenced under an open, permissive licence. Because the epSOS Master Value Catalogue reuses codes from other international standards, the epSOS Master Value Catalogue (MVC) is not available under an open licence.
- **Quality controls:** New versions must be qualified before going to production. A quality control is set up through three levels of conformance gates.
- **Metadata schema:** At schema level, the metadata is described according to the epSOS CDA templates and fully complies with international standards and profiles. epSOS is able to translate its reference data through the use of the Master Translating/Transcoding Catalogue (MTC)⁷⁴.

Conformance mechanisms

- **Application profile:** The epSOS e-Document formats can be seen as application profiles of the HL7 CDA release 2 format, with additional restrictions – such as vocabulary bindings with the value sets of the Master Value Catalogue (MVC) – and extensions for representing medications.
- **Validation mechanisms:** epSOS e-Documents are validated against the rules defined by the epSOS CDA Implementation Guides.
- **Conformance certification:** epSOS defines a three stages conformance process to be used to on-board new partners.

Security mechanisms

The following features are in place [epSOS , 2014]:

- **Authentication mechanisms:** the epSOS NCT-to-NCP (National Contact Point) Message Transportation Service allows transmission of authenticated healthcare provider attributes and access control context.
- **Integrity mechanisms:** the epSOS NCT-to-NCP (National Contact Point) Message Transportation Service provides embedding of a digital evidence token.
- **Confidentiality mechanisms:** the epSOS Trusted Node Infrastructure provides message and channel encryption.
- **Non-repudiation mechanisms:** the epSOS NCT-to-NCP (National Contact Point) Message Transportation Service provides transactional non-repudiation and originator claims transferal (non-payload).

⁷⁴ MTC:

[http://www.epsos.eu/faq-glossary/glossary.html?tx_a21glossary\[back\]=3852&tx_a21glossary\[uid\]=1262&cHash=7b682f71f93f5d12dee61db166b369fd&no_cache=1&sword_list\[0\]=mtc](http://www.epsos.eu/faq-glossary/glossary.html?tx_a21glossary[back]=3852&tx_a21glossary[uid]=1262&cHash=7b682f71f93f5d12dee61db166b369fd&no_cache=1&sword_list[0]=mtc)

Usage

The epSOS project is currently testing cross-border e-Health services related to two areas; the use of a Patient Summary to access important medical data and the use of electronic prescriptions for facilitating the access to prescribed medication abroad.

- **Number of e-Document formats:** The five underlying e-Document formats are the following:
 - **The Patient Summary** includes general information about the patient, an overview of the most relevant patient data such as allergies and a history of surgical procedures, a list of medication that the patient is taking and data about the Patient Summary itself. This set of data should allow a health professional to provide care in an unexpected or planned medical intervention.
 - **The ePrescription format** supports prescribing medicine to a patient. The ePrescriptions system allows an efficient transmission of prescriptions to pharmacies in participating countries⁷⁵.
 - **The eDispensation format** uses common modules with the ePrescription format. By electronically retrieving a patient's prescription, the corresponding medicine is dispensed. Such information is then reported through software, which adjusts the concerned data. Data updates must be communicated to the Participating Nations.
 - **The Healthcare Encounter Report** aims at informing other countries about the healthcare situation of a patient in the initial country. HCER uses the same content modules (section and entry levels) of the Patient Summary.
 - **The Medication Related Overview** lists medication and other related information that has been created by Participating Nations. Described in the MVC, *"Implementations vary widely from country to country, and also the content of this overview might vary from user to user: prescribers and pharmacists do not have the same overview in all countries"* [epSOS, 2013].
- **Number of known implementations in production-grade software:** There exist two reference National Contact Point (NCP) implementations. *NCP-in-a-Box* is a proprietary product from an industry consortium mainly constituted by Fraunhofer, Elga, and Tiani. [OpenNCP](#) is a newer open-source product with some parts licenced under the GPLv3 licence and others under the Apache 2 licence also found on [Joinup](#).eu. OpenNCP provides a feature to render epSOS CDA documents (patient summary and e-Prescription documents) to HTML. It can be seen as a reference implementation capable of testing the interoperability of an e-Document format.

⁷⁵ epSOS services: <http://www.epsos.eu/epsos-services.html>

- **Number of e-Document exchanges annually:** the number of annual transactions was not made available at the time of writing this study.

Summary table

Table 19 - Analysis of European Patients – Smart open Services (epSOS)

e-Documents by European Patients – Smart open Services (epSOS)	
DESCRIPTIVE METADATA	
Licence	CDA: Open licence by HL7 ⁷⁶ MVC: Not available under a licence
Publisher	CDA: Health Level Seven (HL7) MVC: epSOS consortium (for the Value Set Definition ⁷⁷)
Publisher type	CDA: HL7: Standardisation Body MVC: epSOS consortium: Supra-national Authority
Theme(s)	Social questions – Health
Access URL	CDA: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7 epSOS Patient Summary, ePrescription, eDispensation and Common Modules - CDA R2 Implementation Guide: epSOS Document Repository epSOS HealthCare Encounter Report- CDA R2 Implementation Guide: epSOS Document Repository epSOS Medication Related Overview Encounter Report- CDA R2 Implementation Guide: epSOS Document Repository MVC: not publicly accessible
CONTEXT	
Administrative process context	Cross-border exchange of personal health data (Patient Summary data sets)
Geopolitical context	Europe (Participating Nations)

⁷⁶ HL7's Standards Licensed At No Cost: <http://www.hl7.org/implement/standards/nocost.cfm?ref=nav>

⁷⁷ The Publication of the underlying Code System is under the responsibility of each SDOs (e.g. IHTSDO for SNOMED CT)

Legal context	Article 14 (2) (b) (i) of the Directive 2011/24/EU on patients' rights in cross-border healthcare have established a voluntary eHealth network to define guidelines on data that are to be exchanged across border.
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	HL7 Version 3 Methodology (schema level)
Library of data elements	<ul style="list-style-type: none"> • CDA: HL7 Reference Information Model (RIM) and CDA Hierarchical Descriptor ⁷⁸ (logical level) • HL7 CDA R2 XML schema with epSOS extensions. It includes HL7 CDA R2 XML Schema, that implements the Version 3 Data Types - Implementation Technology Specification for XML (schema level) • epSOS Patient Summary, ePrescription, eDispensation and Common Modules - CDA R2 Implementation Guide • epSOS HealthCare Encounter Report- CDA R2 Implementation Guide • epSOS Medication Related Overview Encounter Report- CDA R2 Implementation Guide • epSOS MVC (Master Value Set Catalogue) comprises terms based on standardized code systems (value sets)
Naming and Design Rules	HL7 Naming Convention (schema level)
e-Document engineering tools	CDA: HL7 V3 Implementation tools and V3 Modelling & Methodology tools
Representation techniques	PDF and XML (CDA Level 1.0); XML (CDA Level 3.0)
GOVERNANCE MECHANISMS	
Goals	Develop e-Health framework and ICT infrastructure for secure access to patient health information among European healthcare systems
Change management	<ul style="list-style-type: none"> • Organisational roles: HL7 Technical Steering Committee (schema) • Decision making process: Decision making practices described in HL7 Governance and Operations Manual (schema) • Documentation: HL7 Governance and Operations Manual (schema)

⁷⁸ HL7 Reference Information Model: <http://www.hl7.org/implement/standards/rim.cfm>

Analysis of structured e-Document formats used in Trans-European Systems

Enforcement policy	<ul style="list-style-type: none"> • Sharing: Voluntary • Reuse: Oversight board
Authoritative source	epSOS Document Repository
Licensing framework	Class 1: Traditional, proprietary licence
Quality controls	3 levels of conformance gates
CONFORMANCE MECHANISMS	
Application profile	epSOS specified CDA documents based on HL7 CDA Release 2.0 standard
Validation	epSOS Documents Implementation Guides Gazelle External Validation Services ⁷⁹
Conformance certification	IHE conformance statement plus further currently project specific testing
SECURITY MECHANISMS	
Authentication mechanisms	The epSOS NCT-to-NCP (National Contact Point) Message Transportation Service allows transmission of authenticated healthcare provider attributes and access control context.
Integrity mechanisms	The epSOS NCT-to-NCP (National Contact Point) Message Transportation Service provides embedding of a digital evidence token.
Confidentiality mechanisms	The epSOS Trusted Node Infrastructure provides message and channel encryption.
Non-repudiation mechanisms	The epSOS NCT-to-NCP (National Contact Point) Message Transportation Service provides transactional non-repudiation and originator claims transferal (non-payload).
USAGE	
Number of e-Document formats	5: The Patient Summary, the ePrescription format, the eDispensation format, the Healthcare Encounter Report and the Medication Related Overview
Number of known	2: NCP-in-a-Box and OpenNCP

⁷⁹ <http://gazelle.ihe.net/EVSCClient/home.seam>

Analysis of structured e-Document formats used in Trans-European Systems

implementations in production- grade software	
Number of e- Documents exchanged annually	No information was made available at the time of writing this study.

I.9. Eurofiling: financial reporting based on XBRL

Context

The European Banking Authority (formerly Committee of European Banking Supervisors), the European Insurance and Occupational Pensions Authority (EIOPA) and XBRL Europe maintain four specifications for financial reporting:

- **COREP:** The European Banking Authority (EBA) Common Reporting Framework (COREP) is the common **solvency ratio reporting framework for credit institutions and investment firms** under EU capital requirements regime [Eurofiling Initiative, 2010]. The COREP Framework is based initially on Recasted European Directives 2000/12/CE and 93/6/EEC released in July 2004 [COREP, 2006] and currently in accordance with Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 [EBA, 2013].
- **FINREP:** The European Banking Authority (EBA) Financial Reporting Framework (FINREP) is designed for **credit institutions** that use IAS/IFRS for their published **financial statements** and that have to provide similar information in the periodic prudential reports they are required to submit to their supervisory authorities [Eurofiling Initiative, 2009]. FINREP is designed in compliance with the international financial reporting standards (IAS/IFRS) or the Capital Requirements Directive 2006/48/EC [FINREP, 2005] and currently in accordance with Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 [EBA, 2013]
- **Solvency II:** Solvency II is a project by EIOPA concerning the establishment of the European insurance and reinsurance undertakings [EIOPA, 2014]. In 2009, the Council of the European Union and the European Parliament have approved the Solvency II Directive, which is scheduled for application as of 1 January 2016 [EIOPA, 2013].
- **XBRL Europe Business Registers:** The national Business Registers collect the annual accounts and related information of each company in the country. Common concepts and tags described in the XBRL Europe Business Register (xEBR) Taxonomy contribute to the harmonisation of financial statements and company identification in order to be interoperable [XBRL Europe, 2013]. Contrary to the Eurofiling initiatives, where the specifications are imposed by law at the European level, XBRL Europe has a bottom-up approach, where specifications are created as needed by the countries. The xEBR Working Group works at ensuring the interoperability between the countries.

In 2005, the Committee of European Banking Supervisors (CEBS) and XBRL in Europe hosted a conference in the Chartered Accountants' Hall in London to discuss the promises and challenges involved in the propagation of XBRL in the financial sector [CEBS, 2005]. This conference was the starting point of XBRL as format for Financial Supervision.

In 2013, the European Banking Authority published a draft concerning the implementation of uniform reporting requirements covering the FINREP and COREP guidelines, the Implementing Technical Standards:

"On 26 July 2013 the EBA published final draft Implementing Technical Standards (ITS) on supervisory reporting, in accordance with Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (colloquially known as Capital Requirements Regulation or CRR). (...)

As the final draft ITS on supervisory reporting will become part of the single rulebook with the particular aim of specifying uniform prudential reporting requirements, the implementation of the reporting requirements imposed on credit institutions and investment firms shall be based on uniform technical specifications of a granular level of detail" [EBA, 2013].

"These ITS will cover reporting of own-funds and capital requirements (currently under the COREP Guidelines), reporting of financial information (currently under the FINREP Guidelines) and reporting on large exposures (currently under the COREP Large Exposures Guidelines)" [EBA, 2013].

e-Document engineering method

The use of XBRL is recommended for financial reporting. The Eurofiling project is an open joint initiative of the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) in collaboration with XBRL Europe, as well as stakeholders as banks, solutions providers, academy and individuals [Eurofiling, about us]. The collaborative network collaborates in the development of the technical specifications of the reporting frameworks (COREP, FINREP and Solvency II). Being a community of experts, Eurofiling helps generating an applicable methodology for the taxonomies along with public testing and improvements to be made to the data formats. XBRL Europe also collaborates with national Business Registers in the European xEBR Taxonomy.

As noted on the legal notice, Eurofiling is licenced under the European Union Public Licence [Eurofiling Initiative, 2011].

XBRL is an XML general-purpose language for business reporting. Regulatory supervisors, such as the EBA, EIOPA, and Business Registers usually create an **XBRL taxonomy** for their regulatory reporting requirements that defines the specific data elements that are used for individual items of data (such as "net profit"), their attributes and their interrelationships.

- **Methodology:** The Data Point Model Methodology is formalized under the CEN Workshop on XBRL, and used to define the COREP, FINREP and

Solvency II XBRL taxonomies [CEN/WS XBRL, 2013]. A *DataPointModel* defines structures of data describing the characteristics of the information exchanged in the context of supervisory reporting processes. A Data Point Model consists of a dictionary of business concepts and their properties, which are represented in tables and corresponding textual explanation. To reflect the defined structures in a machine-readable form, it can be accompanied by an XBRL taxonomy.

- **Library of data elements:** Data Point Models are published for COREP 2.0.0, FINREP 2.0.0 and Solvency II. Identified common elements are published in Eurofiling repository.
- **The naming and design rules:** the XBRL Taxonomies follow the naming and design rules of the XBRL specification.
- **e-Document engineering tools:** The tools used to produce XBRL Taxonomies are either commercial tools as well as Supervisory developed tools [Jones, 2013].
- **Representation techniques:** the formats are defined as XBRL taxonomies, consisting of XML Schemas and XBRL linkbases.

Governance mechanisms

- **Change management**
 - **Organisation roles:**
 - XBRL Europe, Eurofiling: collaborative network of experts for discussing changes
 - EBA and EIOPA: authorities that promulgate new formats
 - **Decision making process:** Methodologies, Practices, Standards and Changes are discussed by the collaborative network of experts within XBRL Europe and Eurofiling. They are then contributed to the EBA and EIOPA authorities who develop, communicate and publish the new formats.

New editions of data formats are published for review under a unique "released" URL. Once the review period has concluded, the official URLs are updated to point to the new edition. New editions are announced on the mailing list and discussed using conference calls. Previous releases remain accessible, users can thus choose between using the URL of a specific frozen release, or an official URL that is updated, but tested for backward compatibility.

- **Documentation:** Not available.

- **Enforcement policy:** The sharing and reuse of the XBRL format is currently voluntary between reporting authorities and national authorities within the same country ("first level"). Such authorities have the option to apply the traditional approach or make use of XBRL. It is up to each country to decide whether the use of XBRL is made mandatory. On the "second level", i.e., communication between national authorities and European authorities, the use of XBRL is in the process of being made mandatory.
- **Authoritative source:** The ITS and DPM are pending publication in the Official Journal of the European Union, and adoption as EU Regulations that will be directly applicable throughout the EU. XBRL Taxonomies are to be published by the respective regulator as EBA and EIOPA. Common EBA/EIOPA definitions are published by Eurofiling. The non-profit XBRL International publishes the language source [XBRL Specification].
- **Licensing framework:** The EUPL is a class 3 licence, give the rights to use, redistribute, and modify via copy left.
- **Quality controls:** Test cases are made public by EBA and EIOPA. XBRL Taxonomies are tested by National Supervisors and Software Vendors before publication. Drafts are also made public for comments. The main challenge is the lack of comprehensive test cases, as all the EBA and EIOPA information is confidential, and simulating actual business cases is too complex [Eurofiling Minutes, 2014].

Conformance mechanisms

- **Application profile:** The Taxonomy is one particular IT representation of the Data Point Model, representing the requirements of the templates, instructions and wider text of the ITS as captured in the DPM. The definition of those requirements remains purely in the ITS, with the detailed identification and classification of them expressed in the DPM.
- **Validation mechanism:** To facilitate uniform implementation and avoid implementation problems, validation rules (quantitative relations between rows and columns of each template, and among templates) are included in the ITS. These have been translated into XBRL formula assertions. Validations tools are common for any XBRL Taxonomy, as COREP, FINREP, Solvency II or xEBR. A more or less updated list of industry solutions is public⁸⁰ along with several Open Source experiences⁸¹ is public [WikiXBRL]
- **Conformance certification:** There are no mechanisms to certify that a system conforms to the EBA reporting requirements.

⁸⁰ http://wikixbrl.info/index.php?title=XBRL_Industry_Solutions

⁸¹ http://wikixbrl.info/index.php?title=Open_Source_and_XBRL

Security mechanisms

The CEN Workshop on XBRL project (developed as part of the Eurofiling collaborative network) defines an e-Document container format that allows secure transferring of structured and unstructured data.⁸² Containers can be encrypted using W3C XML Encryption, which ensures the **confidentiality**. The data is encrypted with a symmetric algorithm (AES-256) with a generated secret key. The secret key is itself encrypted with an asymmetric algorithm (RSA-OAEP). An electronic signature with XAdES-BES/EPES format can also be attached to the container. The signature algorithm used is RSA with a SHA512 hash. The scheme provides **authentication, integrity and non-repudiation of origin**.

Usage

- **Number of e-Document formats:** 4 data formats: COREP, FINREP, Solvency II and XBRL Europe Business Registers
- **Number of known implementations in production-grade software:** about 10 commercial tools are available implementing the XBRL Taxonomies. The Openfiling⁸³ provides additional open-source artefacts.
- **Number of e-Documents formats exchanges annually:** In each country using XBRL, about 10,000 for COREP and FINREP, and about 1 million for Business Registers

⁸² Improving transparency in financial and business reporting — Metadata container:
http://cen.eurofiling.info/wp-content/uploads/data/CWA_XBRL_WI002-E.pdf

⁸³ <http://www.openfiling.info/>

Summary table

Table 20 - Analysis of Financial Reporting based on XBRL

Financial Reporting based on XBRL	
DESCRIPTIVE METADATA	
Licence	European Union Public Licence ⁸⁴ [Eurofiling Initiative, 2011]
Publisher	European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA)
Publisher type	Supra-national authority
Theme(s)	Finance
Access URL	FINREP: http://www.eurofiling.info/finrepTaxonomy/taxonomy.shtml COREP: http://www.eurofiling.info/corepTaxonomy/taxonomy.shtml Solvency II: http://www.eurofiling.info/solvencyII/index.shtml
CONTEXT	
Administrative process context	<ul style="list-style-type: none"> • COREP: Financial institutions reporting their credit risk, market risk, operational risk, own funds and capital adequacy ratios to national supervisors • FINREP: Financial institutions reporting data concerning their balance sheet and income statement to their national supervisory authority • Solvency II: Financial institutions reporting data concerning insurance and reinsurance undertakings
Geopolitical context	European Union
Legal context	<ul style="list-style-type: none"> • COREP: Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast); Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions (recast)

⁸⁴ European Union Public Licence: <http://joinup.ec.europa.eu/software/page/eupl>

	<ul style="list-style-type: none"> • FINREP: International financial reporting standards IAS/IFRS or Capital Requirements Directive 2006/48/EC. • ITS: Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (colloquially known as Capital Requirements Regulation or CRR).
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	Data Point Model Methodology [CEN/WS XBRL, 2013]
Library of data elements	Data Point Model
Naming and Design Rules	Naming and design rules of the XBRL specification
e-Document engineering tools	Unspecific
Representation techniques	XBRL Taxonomy, XML Schema
GOVERNANCE MECHANISMS	
Goals	<ul style="list-style-type: none"> • COREP: Create a harmonised business model for the European solvency reporting requirements. • FINREP: Use standardized data formats and data definitions for prudential reporting in all countries. • Solvency II: Create a harmonised supervisory system in insurance.
Change management	<ul style="list-style-type: none"> • Organisational roles: <ul style="list-style-type: none"> ○ XBRL Europe, Eurofiling: open discussions and contributions ○ EBA and EIOPA: formal development, communication and publication of the changes • Decision making process: Publication of new editions of data formats for review under unique URL. They are published on the mailing list and discussed using conference calls. Once approved, the official URLs are updated. • Documentation: Not available
Enforcement policy	Sharing and reuse: National decision on first level (primary reporting between reporting entities and National authorities); mandatory on second level (between National authorities and European authorities)

Analysis of structured e-Document formats used in Trans-European Systems

Authoritative source	<ul style="list-style-type: none"> • ITS: Official Journal of the European Union (pending) • COREP, FINREP and Solvency II: EBA, EIOPA, Eurofiling and XBRL repository of XBRL taxonomies and modules
Licensing framework	Class 3 : Free to use, redistribute, and modify via copy left licence
Quality controls	Quality Control Process for Taxonomy Development
CONFORMANCE MECHANISMS	
Application profile	XBRL
Validation	Validation rules in ITS; XBRL Validation Tools: Market driven [WikiXBRL]
Conformance certification	Non-existent
SECURITY MECHANISMS	
Authentication mechanisms	Electronic signature to container
Integrity mechanisms	Electronic signature to container
Confidentiality mechanisms	Encrypted containers (W3C XML Encryption)
Non-repudiation mechanisms	Electronic signature to container
USAGE	
Number of e-Document formats	4 : COREP, FINREP, Solvency II and XBRL Europe Business Registers
Number of known implementations in production-grade software	30 commercial tools
Number of e-Documents exchanges annually	10,000 by authority/year (1 million for Business Registers)

I.10. Virtual Company Dossier (VCD) used by PEPPOL

Context

PEPPOL (Pan European Public Procurement On Line) is a Large Scale Pilot that created a standards-based network through which public authorities and economic operators exchange standardised electronic documents for public procurement.

These electronic documents follow PEPPOL Business Interoperability Specifications (BIS) for common eProcurement processes such as e-Catalogue, e-Orders, and e-Invoices. The Virtual Company Dossier (VCD) was also developed for suppliers to submit company information in a standardized 're-usable' format.

The eProcurement specifications (PEPPOL BIS) maintained by OpenPEPPOL build on the work of the CEN Workshop on Business Interoperability Interfaces for Public Procurement in Europe (CEN BII).

PEPPOL facilitates the pre-award and post-award procurement process with standardised components by focusing on the most complex eProcurement elements (marked yellow in the graphic below):

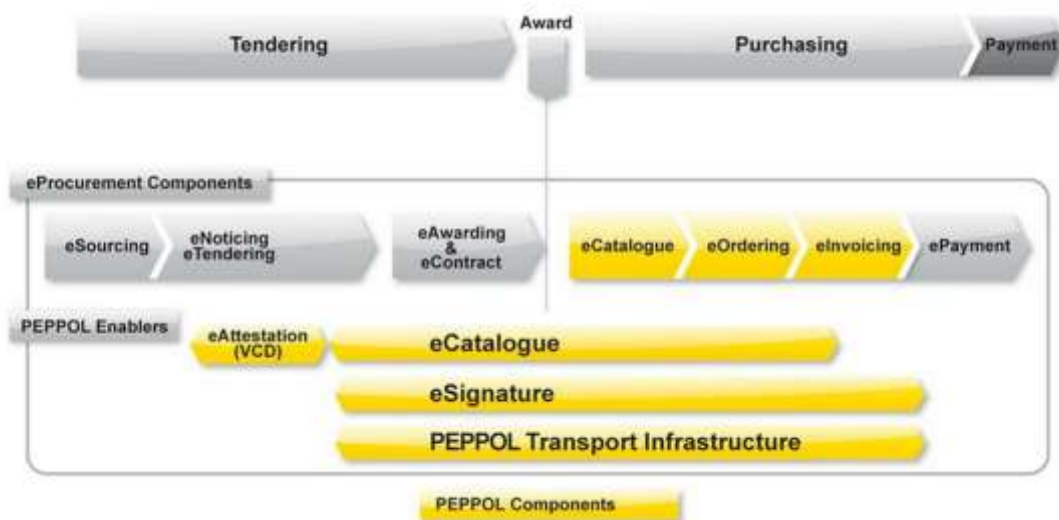


Figure 14 - PEPPOL Components

The Virtual Company Dossier (VCD) was the work package within PEPPOL with the goal to create a set of tools to support national and cross-border qualification of tenderers and mapping of national criteria.

Economic operators willing to participate in public tenders require proof of fulfilment of qualitative selection criteria requested by contracting authorities. The economic operator must collect evidences from different (national) sources and provide them to the contracting authority. The different legal regimes in a cross-border environment make the issuance of a VCD a complex task for economic operators.

VCD provides an interoperable electronic document solution that supports the exchange of evidences across borders. Apart from the electronic documents used to

transport the evidences from economic operators to contracting authorities, the VCD project has developed additional tools to ease the process for both economic operators and contracting authorities.

- **European VCD System (EVS)** providing decision support to derive evidences in order to meet the required criteria defined in the Call for Tenders. The Ontology Management System provides the editing and management functionality for the different ontologies;
- **National VCD System (NVS)** providing a full range of VCD functionalities to the economic operator - from the initial selection of criteria (via the VCD Designer) to the finalisation of a validated VCD Container (through the VCD Builder). A core functionality of the NVS is to enter data and to upload evidences to a VCD;
- **VCD Viewer** - allowing users to view the content of VCD Packages.

e-Document engineering method

- **Methodology:** VCD has used the UBL methodology to build the schemas.
- **Library of data elements:** VCD has reused the UBL library of common Business Information Entities to build the schemas. They have reused the common classes such as Party or Address and have created new classes extending the original UBL classes when they have needed to define new concepts such as Contracting Authority or Economic Operator.
- **Naming and design rules:** VCD XML Schemas are compliant with the Naming and Design Rules of UBL 2.1.
- **e-Document engineering tools:** The eDoCreator⁸⁵ online website has been used to produce the final XSD schemas.
- **Representation techniques:** The e-Document formats are represented under XML Schemas.

Governance mechanisms

- **Change management**

There are no specific VCD governance mechanisms. Those of the OpenPEPPOL project apply.

⁸⁵ <http://79.125.15.30:8080/srdc/eDoCreator/#>

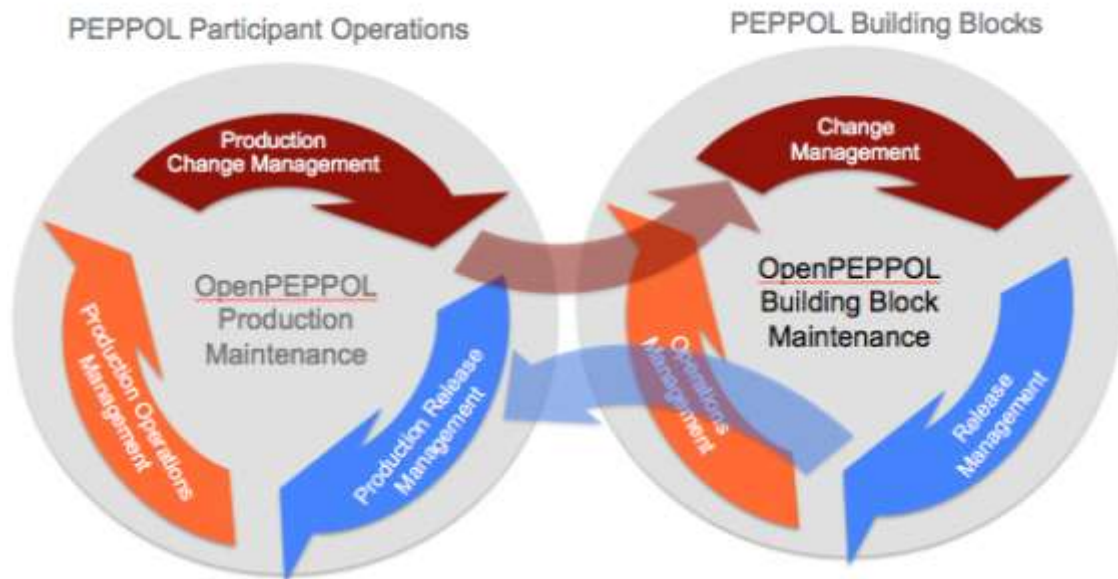


Figure 15 - OpenPEPPOL Change Management

- **Organisation roles:** OpenPEPPOL AISBL is an organization with a General Assembly a Managing Committee and several Coordination Communities. The governance of the VCD belongs to the Pre-Award Coordination Community.
- **Decision making process:** VCD is a project within the OpenPEPPOL Pre-Award Coordination Community. The decision making process is defined within this Coordination Community.
- **Documentation:** No documentation on the governance mechanism is available.
- **Enforcement policy:** The usage of the VCD models and tools is voluntary.
- **Authoritative source:** The OpenPEPPOL website (<http://www.peppol.eu>) contains the authoritative deliverables for the VCD project.
- **Licensing framework:** EU Public Licence
- **Quality controls:** There is no quality control methodology for the production of schemas and artefacts in the VCD project.

Conformance mechanisms

- **Application profile:** VCD has used a profiling tool, called Schemaprof⁸⁶ to define application profiles summarizing the requirements of conform VCD message on the basis of VCD schemas and VCD Schematrons. Based on these application profiles, a Generic Test System can be instantiated or configured in order to create a profile-specific Test System.
- **Validation mechanism:** The VCD community has developed a profile-specific conformance test system⁸⁷ for the VCD in order to allow different user communities to proof the conformance of their VCD implementations.

Business rules have been implemented in VCD using Schematron, as per the CEN BII validation methodology⁸⁸

- **Conformance certification:** There is no official conformance certification process.

Security mechanisms

Authentication and integrity are ensured in the three layers within the VCD:

1. Each evidentiary document can be signed.
 2. The company VCD metadata can be signed⁸⁹.
 3. The VCD package can be signed.
- **Authentication:** Both the VCD and the VCD Package can be signed using advanced digital signature (XAdES).
 - **Integrity mechanism:** Integrity is also preserved using advanced digital signatures.
 - **Confidentiality mechanism:** The VCD Package does not define encryption mechanisms to ensure the confidentiality of the contained information. The evidences included in the VCD can be encrypted.
 - **Non-repudiation mechanism:** There is not any specific non-repudiation mechanism when creating the VCD and the VCD package other than using XAdES and qualified certificates.

⁸⁶ Schemaprof: <http://iwm.uni-koblenz.de/schemaprof/>

⁸⁷ http://www.peppol.eu/peppol_components/peppol-eia/eia#conformance-test/pre-award-eprocurement/services-components

⁸⁸ http://www.peppol.eu/peppol_components/peppol-eia/eia#conformance-test/pre-award-eprocurement/models

⁸⁹ UBL XAdES Profile Version 1.0:
<http://docs.oasis-open.org/ubl/prd2-UBL-2.1/doc/dsig/cd11-UBL-DSig-1.0.html>

Usage

- **Number of known implementations in production-grade software:**
 During the PEPPOL Pilot, four different countries implemented their National VCD Systems using the VCD tools and electronic documents. These National VCD Systems are web-based applications:
 - National VCD System Greece
 - National VCD System Germany
 - National VCD System Austria
 - National VCD System Italy

Strictly according to the original PEPPOL specification, there is only one productive system left in Greece which is operated by the University of Piraeus for the management of university contracts. However conceptually the VCD has been implemented and adopted in Italy by AVCP (Autorità per la Vigilanza sui Contratti Pubblici di Lavori) due to simplification of qualification procedures. A comparable system is built up in France by SGMAP (Secrétariat Général pour la Modernisation de l'Action Publique).

Looking at the future, part of the Building Blocks of VCD will be harmonized with OCD from SPOCS in e-SENS to demonstrate cross domain use of its major components particularly the semantic document mapping service and the eDocument container concept. In eProcurement the VCD will be piloted as part of the e-SENS eTendering use case in e-SENS to incorporate firstly new mandatory regulations in the field of qualification on European level (particularly ESPD and eCERTIS). As AVCP will be one piloting partner other national activities such as the simplification of qualification procedures in Italy or the "marchés publics simplifiés" (MPS) in France will be considered.

Summary table

Table 21 - Analysis of the Virtual Company Dossier

Virtual Company Dossier	
DESCRIPTIVE METADATA	
Licence	EUPL Licence
Publisher	PEPPOL
Publisher type	Supra-national and national authority
Theme(s)	Public Procurement
Access URL	VCD components: http://www.peppol.eu/peppol_components/peppol-eia/eia#ict-architecture/pre-award-eprocurement/services-components

CONTEXT	
Administrative process context	Contracting authorities and economic operators
Geopolitical context	European Union
Legal context	Directives on public procurement ⁹⁰
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	<p>The methodology for creating the e-Documents is twofold:</p> <ul style="list-style-type: none"> - The XML schemas containing the metadata have been produced using the UBL methodology. - The VCD package structure containing XML metadata documents plus additional files has been designed without a formal methodology.
Library of data elements	<p>VCD XML e-Documents have a specific data element library for its domain.</p> <p>Some of the common elements have been reused from the UBL 2.0 library, for instance: Party, Person, Document Reference, Attachment, Address or Contact.</p> <p>Some other elements have been created as extensions of UBL elements such as Economic Operator or Contracting Authority.</p>
Naming and Design Rules	The UBL Naming and Design Rules have been used to create the XML schemas.
e-Document engineering tools	eDoCreator ⁹¹
Representation techniques	<p>UML</p> <p>XSD Schema</p> <p>Schematron files to validate business rules</p>
GOVERNANCE MECHANISMS	
Goals	Implement cross-border exchange of evidences to fulfil participation and awarding criteria in public procurement

⁹⁰ Directive 2004/17/EC:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:134:0001:0113:en:PDF>

Directive 2004/18/EC:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:134:0114:0240:EN:PDF>

⁹¹ eDoCreator: <http://79.125.15.30:8080/srdc/eDoCreator/#>

	processes.
Change management	<ul style="list-style-type: none"> • Organisational roles: OpenPEPPOL • Decision making process follows OpenPEPPOL Pre-award Coordination Community procedures. • Documentation OpenPEPPOL describes the versioning strategy for the VCD deliverables.⁹²
Enforcement policy	<ul style="list-style-type: none"> • Sharing: Voluntary • Reuse: Voluntary
Authoritative source	http://www.peppol.eu/peppol_components/virtual-company-dossier
Licensing framework	Class 4 : Free to use, redistribute, and modify via non-copy left licence
Quality controls	Not defined
CONFORMANCE MECHANISMS	
Application profile	VCD has used a tool for profiling the XSD schemas. The tool is called Schemaprof ⁹³
Validation	Business rules have been implemented using Schematron. VCD has used the CEN BII validation methodology ⁹⁴ as a basis and evolved with VCD own requirements according to the VCD testing framework ⁹⁵
Conformance certification	A conformance test system has been developed ⁹⁶
SECURITY MECHANISMS	
Authentication mechanisms	Advanced digital signatures (XAdES)

⁹² OpenPEPPOL Versioning Strategy : https://joinup.ec.europa.eu/svn/peppol/PEPPOL_EIA/3-Life_Cycle_Management/3-LCM-PreAward_eProcurement/31-LCM-Strategy/LCM%20Strategy_VCD%20Components%20Versioning%20Strategy%20100.pdf

⁹³ Schemaprof: <http://iwm.uni-koblenz.de/schemaprof/>

⁹⁴ CEN BII validation methodology : http://www.peppol.eu/peppol_components/peppol-eia/eia#conformance-test/pre-award-e-procurement/models

⁹⁵ VCD Testing Framework : https://joinup.ec.europa.eu/svn/peppol/PEPPOL_EIA/2-Conformance_Test/2-CT-PreAward_eProcurement/22-CT-Framework/CT%20Framework_VCD%20Testing%20Framework.pdf

⁹⁶ Conformance test system : http://www.peppol.eu/peppol_components/peppol-eia/eia#conformance-test/pre-award-e-procurement/services-components

Analysis of structured e-Document formats used in Trans-European Systems

Integrity mechanisms	Advanced digital signatures
Confidentiality mechanisms	No encryption mechanisms to ensure the confidentiality of the contained information; evidences in the VCD can be encrypted.
Non-repudiation mechanisms	No specific non-repudiation mechanism; use of XAdES and qualified certificates
USAGE	
Number of e-Document formats	2: VCD Package and VCD
Number of known implementations in production-grade software	4: National VCD System Greece; National VCD System Germany; National VCD System Austria and National VCD System Italy
Number of e-Documents exchanges annually	No information was made available at the time of writing this study.

I.11. Omnifarious Container for e-Documents (OCD) used by SPOCS

Context

The EU Services Directive requires all procedures involved in establishing a business and providing services in another EU country to be fully online. The objective of the [Services Directive](#) is to release the growth potential of services markets in Europe by removing legal and administrative barriers to trade in the services sector.

Implementing the Services Directive involves creating Points of Single Contact (PoSC) that can act as intermediaries between service providers and national public administrations. The goal of these PoSC is essentially to fulfil two functions: information dissemination and case management/processing.

The SPOCS (Simple Procedures Online for Cross-border Services) project is streamlining those procedures and offering seamless cross-border technology. The aim of SPOCS was to develop an interoperability layer to foster the services economy in Europe by facilitating the Service Providers to apply via the PoSC for businesses. The process followed within the SPOCS to reach live testing consisted in:

1. Specifying the SPOCS building blocks (Syndication, e-Documents, e-Delivery, e-Safe and e-Services)
2. Developing the SPOCS building blocks
3. Deploying the building blocks in piloting countries
4. Assessing the results and iteratively adapting the specifications and modules as needed
5. Scaling and sustaining the SPOCS building blocks.

The e-Documents building block defined the Omnifarious Container for e-Documents (OCD). It is a container that enhances the interoperability between different e-Documents. It mainly consists of three layers.

- A Payload Layer has the capacity to incorporate all types of electronic documents.
- A Metadata Layer with information on the documents and the container; provides for semantic interoperability.
- A Common Authentication Layer that ensures the validation of the whole container.

An authentication module verifies whether the format of the electronic signatures of the container is valid according to the Commission Decision⁹⁷. Eventual proprietary signatures and e-Signature formats are validated by an external mechanism [SPOCS, 2012].

⁹⁷ Commission Decision:

http://joinup.ec.europa.eu/site/spocs/eDocuments/references/EC-COM_2011_130.pdf

Apart from the container function with the structure of documents in the payload layer and the packaging in ZIP or PDF files, it is worth highlighting the OCD Metadata Layer that gives a unified description of the documents attached in the payload layer, making the use and the handling of information more efficient and enabled for automation. The metadata layer uses an XML document to describe the metadata of the OCD container; therefore there has been a process to create such XML Schema. The XML document covers both metadata about the documents included in the OCD and metadata about the contents to become input into several processing activities and it has been a generalization of the VCD project.

e-Document engineering method

The OCD metadata layer is based on a XML document. The XML follows the structure dictated by an XML Schema. SPOCS project was looking at several initiatives and finally they decided to mainly adopt the VCD schema from PEPPOL, which in turn is adopting the UBL Schemas.

- **Methodology:** OCD has used the UBL methodology to build the schemas.
- **Library of data elements:** OCD has reused the VCD library of common Business Information Entities that was based on the UBL library. They have used the VCD library as is.
- **Naming and design rules:** OCD XML Schemas are compliant with the Naming and Design Rules of UBL 2.1.
- **e-Document engineering tools:** The eDocCreator⁹⁸ online website has been used to produce the final XSD schemas.
- **Representation techniques:** The e-Document formats are represented under XML Schemas.

Governance mechanisms

- **Change management**

SPOCS project ended in 2012; therefore its structure is no longer available. The results of SPOCS, and therefore the OCD models and tools are to be managed by the new Large Scale Pilot project e-SENS.

 - **Organisation roles:** The maintenance process of the SPOCS deliverables and the convergence of the OCD and the VCD models are being driven by e-SENS Semantics and e-Documents competence cluster.
 - **Decision making process:** Follows e-SENS subgroup policies.
 - **Documentation:** No documentation on the governance mechanism is available.
- **Enforcement policy:** Use of OCD is based on voluntary basis.

⁹⁸ eDocCreator: <http://79.125.15.30:8080/srdc/eDoCreator/#>

- **Authoritative source:** SPOCS website: <http://www.eu-spocs.eu/>
- **Licensing framework:** European Union Public Licence (EUPL) version 1.1.
- **Quality controls:** According to the SPOCS Risk Management Plan & Project Quality Plan each deliverable has to follow the quality management process.

Conformance mechanisms

- **Application profile:** There are no application profiles but pilot examples developed during the SPOCS Large Scale Pilot.
- **Validation mechanism:** The OCD metadata document has to be conformant to the OCD XSD schema. There are no additional business rules defined as Schematron validation artefacts.

The SPOCS Project developed a tool to verify the OCD container, checking whether the format is valid (PDF or ZIP format, layers, etc.)

- **Conformance certification:** No conformance certification process available.

Security mechanisms

The Common Authentication Layer is used to sign the whole contents of the OCD package. There is also the possibility to sign the OCD Metadata and each contained document in the Payload layer. The use of advanced digital signatures (*AdES) is mandatory in OCD to fulfil the EU Signature Directive.⁹⁹

- **Authentication:** Using *AdES signatures in the three layers.
- **Integrity mechanism:** Using *AdES signatures.
- **Confidentiality mechanism:** OCD supports XML Encryption for ZIP based containers.
- **Non-repudiation mechanism:** Using *AdES signatures in the three layers.

Usage

SPOCS has made available¹⁰⁰ an implementation in the form of two modules that create and extract ZIP and PDF based OCD containers, and provide a verification of these containers.

No further metrics on the usage of the OCD specification were available at the time of writing this study.

⁹⁹ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures:
http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=quichett&lq=en

¹⁰⁰ <http://joinup.ec.europa.eu/site/spocs/eDocuments/index.html>

Summary table

Table 22 - Analysis of the Omnifarious Container for e-Documents

Omnifarious Container for e-Documents	
DESCRIPTIVE METADATA	
Licence	European Union Public Licence (EUPL) version 1.1
Publisher	SPOCS
Theme(s)	Public Services
Access URL	General site: http://www.eu-spocs.eu/ Schema artefacts: https://joinup.ec.europa.eu/svn/spocs/semantic-validator/
CONTEXT	
Administrative process context	Public entities and citizens
Geopolitical context	European Union
Legal context	Directive 2006/123/EC of 12 December 2006 on services in the internal market applies to the provision of a wide range of services – to private individuals and businesses Directive on digital signatures
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	The creation of the OCD XML Schema has followed the PEPPOL VCD methodology, based on UBL.
Library of data elements	Reused the VCD library of common elements to create the Metadata XML Schema.
Naming and Design Rules	The Metadata XSD Schema has been built based on the UBL Naming and Design Rules.
e-Document engineering tools	eDoCreator on-line tool
Representation techniques	XSD Schema
GOVERNANCE MECHANISMS	

Analysis of structured e-Document formats used in Trans-European Systems

Goals	SPOCS aims to build the next generation of online portals (Point of Single Contact or PSC), which every European country now has in place, through the availability of high impact cross- border electronic procedures.
Change management	<ul style="list-style-type: none"> • Organisational roles: Handed over to e-SENS Large Scale Pilot. • Decision making process: Following the e-SENS subgroup for Semantics and e-Documents procedures. • Documentation: Can be found in the SPOCS site or in Joinup.
Enforcement policy	<ul style="list-style-type: none"> • Sharing: Voluntary • Reuse: Voluntary
Authoritative source	https://joinup.ec.europa.eu/svn/spocs/semantic-validator
Licensing framework	Class 4: Free to use, redistribute, and modify via non-copy left licence
Quality controls	SPOCS Risk Management Plan & Project Quality Plan
CONFORMANCE MECHANISMS	
Application profile	No application profiles defined during the Pilot.
Validation	<p>OCD Metadata within the OCD Container has to be validated against a XSD Schema.</p> <p>The OCD Container structure has to be validated using specific tools developed within the Pilot project.</p>
Conformance certification	No formal conformance certification process established.
SECURITY MECHANISMS	
Authentication mechanisms	Advanced digital signatures (*ADES) in the three levels of the OCD Package
Integrity mechanisms	Advanced digital signatures
Confidentiality mechanisms	OCD Containers support XML Encryption
Non-repudiation mechanisms	Advanced digital signatures
USAGE	

Analysis of structured e-Document formats used in Trans-European Systems

Number of e-Document formats	The OCD Container has a schema for the OCD Metadata.
Number of known implementations in production-grade software	SPOCS has made available an implementation in the form of two modules that create and extract ZIP and PDF based OCD containers, and provide a verification of these containers. http://joinup.ec.europa.eu/site/spocs/eDocuments/index.html
Number of e-Documents exchanges annually	No information was made available at the time of writing this study.

I.12. International Commission on Civil Status (ICCS)

Context

The International Commission on Civil Status, an intergovernmental organisation consisting of 15 member states, intends to facilitate the cross-border exchange of information regarding civil status data between registrars [CIEC, 2013]. Since its foundation in 1948, the ICCS organization has developed 33 conventions, written 9 recommendations to its member states and compiled documentation on legislation and case-law of the member states.

In the context of the active conventions, specific document templates have been formulated in order to facilitate the harmonized document creation by the member states. These templates guide the document completion since they impose:

- a) a specific structure,
- b) specific validation/business logic that should accompany the document completion, and
- c) a specific way of rendering the document according the language of the sender/receiver.

From the very beginning of the template generation process, a lot of aspects that target interoperability were taken under consideration. One of these aspects is multilingualism. In order to overcome the language barrier, which is a critical issue, ICCS has introduced a coded system where each literal that is rendered in the documents is accompanied by a code that can be translated to all languages of ICCS using a translation matrix (attached in every generated form).

Another aspect of interoperability relates to the legal consensus of the document's context. Every convention contains the minimum set of mandatory fields that must be filled in order for this form to be valid.

One of the conventions drawn up by the ICCS, Convention 16, concerns the issue of multilingual extracts from Civil Status Records¹⁰¹. Convention 16 was ratified by 10 countries: Belgium, Spain, France, Italy, Luxemburg, The Netherlands, Portugal, Switzerland, Turkey and Austria¹⁰².

Moreover, Convention 16 enables the exchange of Civil Status Certificates extracts. To enable the electronic exchange of these extracts, XML schemas were developed.

Other Conventions also enable the electronic exchange of documents described with XML Schemas. These concern Convention 3 on the international exchange of information relating to civil status, Convention 20 on the issue of a certificate of legal capacity to marry and Convention 26 on the international exchange of information relating to civil status.

¹⁰¹ ICCS Convention 16: <http://www.ciec1.org/Conventions/Conv16Angl.pdf>

¹⁰² ICCS list of conventions: <http://www.ciec1.org/SignatRatifTablRecapit.pdf>

The XML schemas not only serve as a framework for encompassing civil status information that is exchanged between different offices. They also serve as a framework for mapping XML representations of national systems to and from the ICCS representation, thus transforming the data using XSL transformations.

e-Document engineering method

- **Methodology:** The used methodology is straightforward:
 - From each convention, all fields (and their groups) have been extracted
 - The respective translation codes have been converted in enumerations
 - An XSD representation for each Convention has been created using mandatory restrictions, datatype restrictions (e.g. max Firstname.length=120characters), etc.
 - A Web Form that is able to bind the aforementioned XSD has been generated per Convention
- **Library of data elements:** No library of common data elements has been used. The conventions and documents, on which the XSD Schemas are based, predate the exchange of electronic documents and libraries of data elements.
- **Naming and design rules:** Not available.
- **e-Document engineering tools:** The XML Spy tool was used for creating the XML Schemas.
- **Representation technique:** All extracts of Civil Status Certificates are represented as XML schemas (containing specific placeholders for security purposes).

Governance mechanisms

- **Change management**
 - **Organisation roles:** CIEC-ICCS is an intergovernmental organisation. The organisational roles responsible for metadata governance are the organs of the ICCS, being the General Assembly, the Bureau, the President and the Secretary General.
 - **Decision making process:** Every ICCS member is able to propose enhancements. All decisions are taken by the General Assembly. The General Assembly meets 3 times a year in order to manage the organizational methods, change management processes, ratification requests, etc. If a change must be applied in a document which is participating in a Convention, a new document obsoleting the said Convention is created. That new document has to be ratified by all countries.

- **Documentation:** Documentation concerning the structure and the organisation of ICCS is outlined in the information note of CEC¹⁰³.
- **Enforcement policy:** Member States choose which conventions they sign. As such, sharing and reuse of the e-Document formats are voluntary.
- **Authoritative source:** Concerning the extracts of Convention 16 on the information exchange of civil status, metadata is provided on the repository of the CIEC-platform¹⁰⁴.
- **Licensing framework:** Under the IPR of ICCS organization. There is no official digital licensing for the moment.
- **Quality controls:** Every ICCS member is able to propose enhancements. The documents themselves are controlled through procedures of the General Assembly. However, there is no standard operating procedure for validating the transition of the documents to the e-Document formats. By Convention 33, each active Member State, i.e., a Member State having signed at least one convention and contributing financially to the platform, provides a technical representative. The technical representative validates the conformity of the XML Schemas to the corresponding standard documents.

Conformance mechanisms

- **Application profile:** No assertion mechanism
- **Validation mechanism:** The XSD Schemas can be used for validation.
- **Conformance certification:** No certification mechanism.

Security mechanisms

The exchange of civil-status data is promoted by the ICCS-CIEC Data Exchange Platform¹⁰⁵, which was an outcome of Convention 33. This electronic platform enables the exchange of civil-status data with standardised applications and documents, such as the XML schemas, in a highly secure way.

- **Authentication:** PKCS11 digital certificates
- **Integrity mechanism:** Digital document signing and encryption
- **Confidentiality mechanism:** Asymmetric (hybrid) encryption
- **Non-repudiation mechanism:** Digital document signing and encryption

¹⁰³ ICCS: General Information: <http://www.ciec1.org/CIEC-note-information-ENG-MAJ-sept2013.pdf>

¹⁰⁴ Repository CIEC-platform: <http://www.ciec-platform.org/CIECPublicEnvironment>

¹⁰⁵ ICCS Data Exchange Platform : <http://ciec-platform.org/>

Usage

- **Number of e-Document formats:** In order to enable the electronic exchange of birth, marriage and death registration extracts of Convention 16, three XML schemas were developed:
 - Convention 16: Extract from death registration
 - Convention 16: Extract from marriage registration
 - Convention 16: Extract from birth registration
- Convention 3, Convention 20 and Convention 26 also contain XML Schemas:
- Convention 3: two XML Schemas
 - Convention 20: one XML Schema
 - Convention 26: eight XML Schemas
- **Number of known implementations in production-grade software:** The data is exchanged between national authorities through the CIEC-ICCS Platform, which leads to one known implementation.
 - **Number of e-Document formats exchanges annually:** Not communicated.

Summary table

Table 23 - Analysis of International Commission on Civil Status (ICCS)

ICCS – CIEC Civil Status Forms	
DESCRIPTIVE METADATA	
Licence	Under the IPR of ICCS
Publisher	ICCS-CIEC
Publisher type	Non-profit organisation
Theme(s)	Social questions
Access URL	<ul style="list-style-type: none"> • Extract from birth registration: http://www.ciec-platform.org/CIECPublicEnvironment/Repository/xsd/Convention16BirthAct.xsd • Extract from marriage registration: http://www.ciec-platform.org/CIECPublicEnvironment/Repository/xsd/Convention16MarriageAct.xsd • Extract from death registration: http://www.ciec-platform.org/CIECPublicEnvironment/Repository/xsd/Convention16DeathAct.xsd

Analysis of structured e-Document formats used in Trans-European Systems

CONTEXT	
Administrative process context	The data from the ICCS XML Schemas are used for the exchange of civil status data. This includes i.e. status, family, nationality, etc.
Geopolitical context	Each State complying with ICCS-CIEC Convention 16: Belgium, Spain, France, Italy, Luxemburg, The Netherlands, Portugal, Switzerland, Turkey and Austria
Legal context	ICCS Convention 16
DOCUMENT ENGINEERING METHODOLOGY	
Methodology	Based on Formal Convention documents
Library of data elements	None
Naming and Design Rules	None
e-Document engineering tools	XML Spy
Representation techniques	XML Schemas
GOVERNANCE MECHANISMS	
Goals	Cross-border exchange of information of civil status data between registrars
Change management	<ul style="list-style-type: none"> • Organisational roles: General Assembly of CIEC-ICCS • Decision making process: <ul style="list-style-type: none"> ○ ICCS member: initiate enhancements ○ General Assembly: manage and approve decisions • Documentation: Information note CEC
Enforcement policy	Sharing and reuse: voluntary
Authoritative source	Repository of origin: ICCS-CIEC Civil Status Forms
Licensing framework	Under the IPR of ICCS: Class 1: traditional, proprietary licence
Quality controls	Procedures of General Assembly

CONFORMANCE MECHANISMS	
Application profile	No assertion mechanisms
Validation	XSD Schema
Conformance certification	Not available
SECURITY MECHANISMS	
Authentication mechanisms	Digital certificates
Integrity	Digital document signing and encryption
Confidentiality	Hybrid encryption
Non-repudiation	Digital document signing and encryption
USAGE	
Number of e-Document formats	14
Number of known implementations in production-grade software	1 , CIEC-ICCS Platform ¹⁰⁶
Number of e-Documents exchanges annually	No information was made available at the time of writing this study.

¹⁰⁶ CIEC-ICCS Platform: <http://www.ciec-platform.org/>

Annex II. DESCRIBING FAMILIES OF E-DOCUMENT FORMATS WITH ADMS

This Annex gives an overview of the work that was carried out to describe the identified e-Document formats with the Asset Description Metadata Schema (ADMS) using the Joinup¹⁰⁷ platform. Creating a machine-readable description of e-Document families achieves that these descriptions are created once and can be published on many platforms that can read the ADMS RDF format.

Table 24 – Overview of e-Document formats described with ADMS

e-Document formats described with ADMS	
CEN/BII	https://joinup.ec.europa.eu/catalogue/repository/cen/bii-profiles
e-CODEX	https://joinup.ec.europa.eu/catalogue/repository/e-codex-catalogue-interoperability-solutions
ECRIS	https://joinup.ec.europa.eu/catalogue/asset_release/e-document-formats-used-european-criminal-records-information-system-ecris
ERRU	https://joinup.ec.europa.eu/catalogue/asset_release/erru-european-register-road-transport-undertaking
TACHOnet	https://joinup.ec.europa.eu/catalogue/asset_release/tachonet-xml-messaging-reference-guide-and-xml-schema
epSOS	https://joinup.ec.europa.eu/catalogue/repository/epsos-european-patients-smart-open-services-projects
Eurofiling	https://joinup.ec.europa.eu/catalogue/repository/eurofiling-financial-reporting-based-xbrl
VCD	https://joinup.ec.europa.eu/catalogue/repository/peppol-pan-european-public-procurement-line
OCD	https://joinup.ec.europa.eu/catalogue/repository/spocs-simple-procedures-online-cross-border-services
ICCS	https://joinup.ec.europa.eu/catalogue/repository/iccs-ciec-civil-status-forms

¹⁰⁷ Joinup, catalogue of interoperability solutions: <https://joinup.ec.europa.eu/catalogue/all>

Annex III. LIST OF IDENTIFIED TRANS-EUROPEAN SYSTEMS

The table below provides a list of seventy Trans-European Systems that have provided as an input to this study [Kurt Salmon, 2013].

Table 25 – List of identified Trans-European Systems

Abbreviation	Description (link)
AFIS	Anti-Fraud Information System
BRIS	Business Registers Interconnection System
CCN/CSI	Common Communications Network/Common Systems Interface
CCN2	Common Communications Network Version 2.0
CECIS	Common Emergency Communication and Information System (http://ec.europa.eu/echo/policies/disaster_response/cecis_en.htm)
CISE	Common Information Sharing Environment (http://ec.europa.eu/dgs/maritimeaffairs_fisheries/consultations/cise/index_en.htm)
CPCS	Consumer Protection Cooperation System (http://ec.europa.eu/idabc/en/document/5364/5637.html)
DUES	Dual Use e-System
DW	
EBR	European Business Register (http://www.ebr.org/)
ECLI	European Case Law Identifier (https://e-justice.europa.eu/content_european_case_law_identifier_ecli-175-en.do http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_civil_matters/jl0056_en.htm)
ECN	European Competition Network (http://ec.europa.eu/competition/ecn/)
E-CODEX	eJustice Communication via Online Data Exchange (http://www.e-codex.eu/home.html)
ECRIS	European Criminal Records Information System (http://ec.europa.eu/justice/criminal/european-e-justice/ecris/)

Analysis of structured e-Document formats used in Trans-European Systems

eDAMIS	Electronic Data files Administration and Management Information System (https://webgate.ec.europa.eu/edamis/login/index.cfm?TargetUrl=disp_login http://ec.europa.eu/idabc/en/document/3537/5927.html)
EIXM	European Information Exchange Model (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/eixm/index_en.htm)
e-Justice Portal	e-Justice Portal – ‘Justice at a click’ (https://e-justice.europa.eu/home.do?plang=en&action=home)
eModNet	European Marine Observation and Data Network (http://ec.europa.eu/dgs/maritimeaffairs_fisheries/consultations/modnet/index_en.htm)
e-Prior	Electronic Procurement Invoicing and Ordering (https://joinup.ec.europa.eu/software/openeprior/description)
epSOS	European Patients – Smart Open Services (http://www.epsos.eu/)
ERRU	European Register of Road Transport Undertaking (http://ec.europa.eu/transport/modes/road/access/erru_en.htm)
ESBR	European System of Business Registers
ESDEN	
ESSI	Electronic Exchange of Social Security Information (http://ec.europa.eu/social/main.jsp?langId=en&catId=869)
eTrustex	Trusted Information Exchange Platform (https://joinup.ec.europa.eu/software/openetrustex/description)
EUCARIS	European CAR and driving Licence Information System (https://www.eucaris.net/)
EUDRANET	European Union Drug Regulating Authorities Network (http://ec.europa.eu/idabc/en/document/2291.html)
EUPHIN	European Union Public Health Information Network (http://ec.europa.eu/idabc/en/document/2259/5926.html)
EURES	European Employment Services (https://ec.europa.eu/eures/)
EURODAC	European Dactyloscopy (http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33081_en.htm)

Analysis of structured e-Document formats used in Trans-European Systems

EUROPHYT	European Union Notification System for Plant Health Interception (http://ec.europa.eu/food/plant/plant_health_biosafety/europhyt/index_en.htm)
EUROSUR	European Border Surveillance System (http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l14579_en.htm)
FIDES3	Fisheries Data Exchange System (http://ec.europa.eu/idabc/en/document/2254/5926.html)
FNS	Fraud Notification System (https://fns.olaf.europa.eu/)
Food System	Food System
Géant	Multi-Gigabit European Research and Education Network and Associated Services (GN3) (http://www.geant.net)
GENIS	Generic and Interoperable Notification Services (http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-11action_en.htm)
ICSMS	Information and Communication System for the pan-European Market Surveillance (https://webgate.ec.europa.eu/icsms/App/index.jsp)
ICT	
IMI/ SOLVIT	Internal Market Information System (http://ec.europa.eu/internal_market/imi-net/index_en.htm)
Inspire	Infrastructure for Spatial Information in Europe (http://inspire.jrc.ec.europa.eu/)
IRI	Interconnection of the National Insolvency Registers (https://e-justice.europa.eu/content_interconnected_insolvency_registers_search-246-en.do)
MH	Metadata Handler (http://ec.europa.eu/eurostat/ramon/index.cfm?TargetUrl=DSP_CVD)
MT @EC	Machine Translation Service by the European Commission (http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-8action_en.htm)
NF-NET	Novel Foods and Food Ingredients Network (http://ec.europa.eu/idabc/en/document/2269/5926.html)
PEPPOL	Pan-European public procurement on-line (http://peppol.eu)

Analysis of structured e-Document formats used in Trans-European Systems

RAPEX	Rapid Alert System for Non-Food Consumer Products (http://ec.europa.eu/consumers/safety/rapex/alerts/main/index.cfm)
RESPER	Réseau permis de conduire/Driver Licence Network (http://ec.europa.eu/idabc/en/document/3989.html)
SARI	State Aid Reporting Interactive
SEIS	Shared Environmental Information System (http://ec.europa.eu/environment/seis/)
SERV	
SHASE	Shared Services
SIGL2	Integrated System for Managing Export and Import Licences (http://trade.ec.europa.eu/sigl/)
SIMSTAT	Single Market Statistics (http://epp.eurostat.ec.europa.eu/portal/page/portal/pgp_ess/news/ess_news_detail?id=152857730&pg_id=2737&cc=ESTAT EUROSTAT)
SINAPSE	Sinapse – creation of e-Communities (http://europa.eu/sinapse/)
SIS	Schengen Information System (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm)
SISII	Second Generation Schengen Information System (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm)
SOLVIT	Problem Solving in the Internal Market (http://ec.europa.eu/solvit/)
SPEED 2	Single Portal for Entry or Exit of Data
SPOCS	Simple Procedure Online for Cross-Border Services (http://www.eu-spocs.eu/)
SSN	Safe Sea Network (http://emsa.europa.eu/operations/safeseanet.html)
sTESTA	Secured Trans European Services for Telematics between Administrations (http://ec.europa.eu/idabc/en/document/2097.html)
STORK	Secure Identity Across Borders Linked (https://www.eid-stork.eu)
TACHONET	Tachograph Network (http://ec.europa.eu/transport/modes/road/social_provisions/tachog)

Analysis of structured e-Document formats used in Trans-European Systems

	raph/tachonet_en.htm)
ULYSSES	Ulysses (http://ec.europa.eu/research/transport/projects/items/ulysses_en.htm)
UMF II	Universal Message Format II (https://joinup.ec.europa.eu/community/umf/home)
VIES	VAT Information Exchange System (http://ec.europa.eu/taxation_customs/taxation/vat/traders/vat_number/)
VIS	Visa Information System (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/)
XML Gate	XML Gate
YEA	Your Europe Advice (http://europa.eu/youreurope/advice/index_en.htm)