TOOP

providing
data
once-only.eu

The Once-Only Principle Project

Generic Federated OOP Architecture (1st version)

Jaak Tepandi, J.P.C.(Jack) Verhoosel, Dimitrios Zeginis, Gunnar Wettergren, Jerry Dimitriou, Carmen Rotuna, Cagatay Carabat, Özlem Albayrak, Erol Yilmaz, Thomas Lampoltshammer, Ermo Täks, Andriana Prentza, Paul Brandt, Petros Kavassalis, Lefteris Leontaridis, Jan Willem Streefkerk

www.toop.eu

Submitted to the EC on 30/06/2017

Horizon 2020
The EU Framework Programme for Research and Innovation

PROJECT ACRONYM: TOOP

PROJECT FULL TITLE: The “Once-Only” Principle Project

H2020 Call: H2020-SC6-CO-CREATION-2016-2

H2020 Topic: CO-CREATION-05-2016 - Co-creation between public administrations: once-only principle

GRANT AGREEMENT n°: 737460

D2.1 Generic Federated OOP Architecture (1st version)

Deliverable Id :	D2.1	
Deliverable Name :	Generic federated OOP architecture (1st version)	
Version :	V1.0	
Status :	Final	
Dissemination Level :	Public	
Due date of deliverable :	M6 (June 2017)	
Actual submission date :	30/06/2017	
Work Package :	WP2	
Organisation name of lead partner for this deliverable:	Tallinn University of Technology	
Author(s):	Jaak Tepandi J.P.C. (Jack) Verhoosel Dimitrios Zeginis Gunnar Wettergren Jerry Dimitriou Carmen Rotuna Cagatay Karabat Özlem Albayrak Erol Yilmaz	Thomas Lampoltshammer Ermo Täks Andriana Prentza Paul Brandt Petros Kavassalis Lefteris Leontaridis Jan Willem Streefkerk
Partners contributing:	All beneficiaries	

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Abstract:

This deliverable presents the first version of a generic federated OOP architecture, supporting interconnection and interoperability of national registries at the EU level. The architecture is in line with existing EU frameworks (EIRA, EIF), takes into account the e-SENS European Interoperability Reference Architecture and is based on the CEF DSIs and the Building Blocks consolidated by the e-SENS project. The first version focuses on interoperability at business and information level, to be extended iteratively in the future versions. The deliverable includes, among others, the requirements, the initial building blocks, and the interface specifications of the generic federated architecture.

The overall logic of the deliverable emerges from the principle of reusing existing frameworks and building blocks provided by CEF, e-SENS, and other initiatives. As the first step, an initial inventory of existing e-Government Building Blocks is proposed. Then the principles of selection of building blocks for OOP applications and several types of high-level view of the architecture are provided. Finally, an analysis of selected building blocks with respect to their relevance, applicability, sustainability, need for further development, and external interfaces is presented.

The next steps are to develop the architecture in more detail and to elaborate other tasks of TOOP T2.1 – development of a framework for specific OOP architectures and providing deployment profiles for building blocks.

This deliverable contains original unpublished work or work to which the authors hold all rights except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

All web-links referred to in this deliverable are valid on the submission date of the deliverable.

Table of contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

List of Figures

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

List of Tables

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

List of Abbreviations

Acronym	Explanation
ABB	Architecture Building Block
BB	Building Block
BRIS	Business Registers Interconnection System
CEF	Connecting Europe Facility
DSI	Digital Service Infrastructure
eIDAS	electronic Identification and Signature
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
EO	Economic Operator
EES	ETSI Rationalised Framework for Enhanced Security Services
LSP	Large Scale Pilot
MA	Maritime Administration
OOP	Once-Only Principle
PA	Pilot Area
PKI	Public Key Infrastructure
PSC	Port State Control
SAT	Solution Architecture Template
SML	Service Metadata Locator
SBB	Solution Building Block
TOOP	The Once-Only Principle Project
WP	Work Package

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Executive Summary

The eGovernment Action Plan 2016-2020 presents the Once Only Principle (OOP) - the public administrations should ensure that citizens and businesses supply the same information only once to a public administration[1]. The Once-Only Principle (TOOP) project is about exploring, demonstrating, and enabling the once-only principle in the European Union. This is done by implementing three 'once-only' pilot projects (TOOP pilots), by developing a generic federated OOP architecture, and by exploring other aspects of OOP and its supporting infrastructure such as OOP drivers and barriers.

TOOP focus area within OOP is on information related to businesses activities and on cross-border sharing of this information2. The generic federated OOP architecture developed within TOOP (hereafter OOP architecture) relates primarily to applications in the TOOP focus area, although its wider usage is not excluded. It builds on analysis of the TOOP requirements, on the experience of previous Large Scale Pilot (LSP) projects, and on the know-how gained with implementation of the TOOP pilots.

The objective of this document is to present the first version of the OOP architecture. This architecture is aimed at supporting more efficient development of applications that support interconnection and interoperability of national registries at the EU level. It has been developed using an exploratory and agile approach and cooperating with the TOOP pilots and other TOOP Work Packages (WPs) and tasks.

The main political and legislative principles underlying the TOOP generic federated OOP architecture are stated in Annex 2 to the European Interoperability Framework Implementation Strategy (Brussels, 23.3.2017 COM (2017) 134 final)[3].

One of the main technical principles for development of the OOP architecture is the reuse of existing frameworks and building blocks provided by CEF, e-SENS, and other initiatives. The TOOP generic federated OOP architecture relies on such frameworks as the European Interoperability Reference Architecture (EIRA)[4], the CEF Building Blocks[5], and the e-SENS deliverable "D6.6 e-SENS European Interoperability Reference Architecture"[6], among others.

Following the above principles, the overall logic of the deliverable is as follows.

- The deliverable scope, methodology, relations to TOOP internal and external environments, quality and risk management, and other issues are presented in Chapter 1;
- The guiding principles are stated in Chapter 2;
- Main requirements for the deliverable and OOP architecture are stated in Chapter 3;
- To understand what potential resources are available for development of OOP applications, an initial inventory of existing e-Government Building Blocks, without specific references to pilot area needs, is proposed in Chapter 4;
- Several types of high-level view of the architecture and principles of selection of building blocks for OOP applications are provided in Chapters 5.1 and 5.2 respectively;

[1] https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation

[2] TOOP D2.6. Position paper on definition of OOP and situation in Europe. 2017

[3] http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF

[4] https://joinup.ec.europa.eu/catalogue/distribution/eira_v1_1_0_overviewpdf

[5] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home

[6] https://www.esens.eu/deliverables?page=3

- Analysis of selected building blocks with respect to their relevance, applicability, sustainability, need for further development, and external interfaces are provided in Chapters 5.3 to 5.10.

The deliverable includes, among others, the requirements, the initial building blocks, and the interface specifications of the generic federated architecture.

The main conclusions of this document are that it is possible to build the generic federated OOP architecture in line with existing EU frameworks such as European Interoperability Reference Architecture (EIRA) and European Interoperability Framework (EIF), based on the Connecting Europe Facility (CEF) Digital Service Infrastructures (DSIs), on the building blocks consolidated by the e-SENS project, and in justified cases, on the new building blocks.

The next steps are to develop the architecture in more detail and to elaborate other tasks of TOOP T2.1 – development of a framework for specific OOP architectures and providing deployment profiles for building blocks. The exploratory and agile approach, together with cooperation with the TOOP pilots and other TOOP tasks, will be continued, resulting in forthcoming deliverables D2.2 (M12, December 2017), D2.3 (M21, September 2018), and D2.4 (M30, June 2019).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

1. Introduction

1.1.Scope and Objective of Deliverable

The eGovernment Action Plan 2016-2020 presents the Once Only Principle (OOP), stating that the public administrations should ensure that citizens and businesses supply the same information only once to a public administration[7]. The Once-Only Principle Project (TOOP) is about exploring, demonstrating, and enabling the once-only principle in the European Union. This is done by implementing three 'once-only' pilot projects (TOOP pilots), by developing a generic federated OOP architecture, and by exploring other aspects of OOP and its supporting infrastructure such as OOP drivers and barriers.

TOOP focus area within OOP is on information related to businesses activities and on cross-border sharing of this information[8]. The generic federated OOP architecture developed within TOOP relates primarily to applications in the TOOP focus area, although its wider usage is not excluded.

The objective of the current TOOP Deliverable D2.1 is to present the first version of the OOP architecture. The architecture is aimed at supporting more efficient development of applications that support interconnection and interoperability of national registries at the EU level. The deliverable includes, among others, the requirements, the initial building blocks, and the interface specifications of the generic federated architecture.

The OOP architecture development plays two different roles in the TOOP project. First, it involves cooperation with the TOOP pilots and continuous mutual exchange of results with the development activities. Second, it is also a separate activity with a dedicated result, the OOP architecture. This dual character implies several aspects of methodology, work practices, and content of the deliverable, that are discussed in the subsequent text.

1.2.WP2 General Objectives and Vision

The general objectives of TOOP WP2 (Technical Architecture, Legal and Governance Aspects) are to develop a generic, federated OOP architecture, to create a framework for development of specific architectures and applications for TOOP, to develop a profile specification of the common building blocks, to identify general legal barriers and drivers regarding privacy, confidentiality and consent needed for the implementation of OOP, to assess the possible impacts of the implementation of OOP in the pilots in WP3, as well as to define a sustainability plan for the maintenance of the architectures, building blocks and drivers/barriers after the end of the project.

The results of WP2 represent the main technological innovation of TOOP - the generic federated OOP architecture that supports the interconnection and interoperability of national registries at the EU level - together with other investigations needed to generalize, extend, and sustain the TOOP results.

1.3.Methodology of Work

1.3.1. Aspects of the Work Methodology

The methodology of work follows from The Once-Only Principle Project aims and activities. The TOOP implements three TOOP pilots, develops a generic federated OOP architecture, and explores other

[7] https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation

[8] TOOP D2.6. Position paper on definition of OOP and situation in Europe. 2017

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

aspects of OOP and its supporting infrastructure such as OOP drivers and barriers. Thus, it includes both research oriented and development oriented activities. These types of activities tend to follow different methodologies, so to define a methodology for this work it is useful to understand which components of the work are research oriented, and which components - development oriented.

The methodology for the research component of the deliverable, including the architecture design, is presented in Chapter 1.3.2.

The OOP architecture is developed in cooperation with the TOOP pilots and other TOOP Work Packages. The main pilot development activities are done in TOOP WP3, but the OOP architecture contributes to the TOOP pilot development and builds on experience of previous LSP projects and the know-how gained with implementation of the TOOP pilots. This cooperation with the TOOP pilots and continuous mutual exchange of results with the development activities gives the current work primarily a development character.

There exist different methodologies for development. To provide a methodology for this work, let us note that this deliverable depends on input form TOOP pilots in WP3, including the pilot requirements. From the other side, it has been planned as input for the pilot definition in WP3, thus it had to be delivered as early as possible to be useful for the pilot definition and implementation. Because of this chicken and egg situation, it has been developed using an exploratory and agile approach in cooperation with the TOOP pilots and other TOOP Work Packages (WPs) and tasks.

Project management for architecture development follows the agile approach presented in Section 1.3.3.

To summarize, the OOP architecture development has a dual character. From one side, it is associated with the development of TOOP pilots as presented above. From the other side, it is a separate activity with a dedicated result – the generic federated OOP architecture. This dual character implies that there are several aspects of methodology that affect the work done in this deliverable. These aspects are as follows.

- The methodology for the research component of the deliverable, including the architecture design, is presented in Chapter 1.3.2.;
- Project management for architecture development follows the agile approach presented in Section 1.3.3.;
- Description and development of the generic federated OOP architecture follows the methods and definitions laid down in Section 2.2. For better readability, it is presented as part of the key concepts chapter.;
- Relationship between the architecture and the software development processes is presented in Section 2.3. For better readability, it is presented as part of the key concepts chapter.

1.3.2. Architecture Development Methodology

Research towards development of the OOP architecture follows the design science research methodology[9], comprising the problem statement and motivation behind it, analysing the objectives and constraints, designing the architecture, demonstration, evaluation, and communication of the results. These steps are followed in cooperation with other TOOP Work Packages throughout the whole project lifecycle.

[9] Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, Samir Chatterjee. A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, Volume 24 Issue 3, Winter 2007-8, pp. 45-78.

In the constraints and design phases of this methodology, component-based software engineering is used. TOOP mostly identifies and reuses existing building blocks, but does not develop new ones. For this case, the component-based software engineering includes the following main steps[10].

- Develop system and architecture outline requirements (Chapter 3 of the current deliverable);
- Identify candidate components of the system (Chapter 4);
- If needed, modify requirements according to the components identified;
- Develop architecture views (Chapters 5.1, 5.2);
- Identify components that will be used in the system (Chapter 5.3 to 5.10);
- Compose the components to create the application (performed in Pilot Areas).

In this deliverable, a **use case** presents a specification of one type of interaction with a system. A **scenario** describes one typical way in which a system is used or in which a user carries out some activity. One use case may involve several scenarios (usually a main success scenario and alternative scenarios). A **user story** is an informal description of one or more system features from the user perspective.

1.3.3. Agile Approach for the Architecture Development Project Management

As stated above, the TOOP has chosen an agile work methodology as an overall approach, however, this must be detailed and implemented in the project. This section proposes a possible implementation. As a reference, this section is the result of discussions with the WP3 management and it is agreed that the work process proposed is suitable and can be used in both work packages. This is essential, since we expect a high level of cooperation between WP2 and WP3.

Examples of this cooperation include the questionnaire on specific conditions and constraints at piloting countries and organisations, developed in cooperation between different TOOP Work Packages, as well as the liaison management process between WP2 and WP3.

There exist several roles and artefacts that must be defined in an agile project. The list below is specific to Scrum, a widespread agile software development framework[11].

1. **Product owner** – From the agile development viewpoint, the product owner should have vision, be available, and have certain skills. As the TOOP T2.1 comprises three subtasks, the suggestion is that for D2.1 the leads of these subtasks fulfil the owner role in the agile development sense. The product owner role will be specified further in the future versions of the architecture document;
2. **Project backlog** – This artefact contains all the identified requirements expressed in natural language. In order to align with the previous work done in WP3 we will use user stories or use cases as the chosen method for describing requirements;
3. **Sprint backlog** – This artefact contains the requirements that we plan to implement during the next sprint. This can be reports, analysis needing to be done or architecture components needing to be defined;
4. **Sprint demo** – After each sprint is completed, WP2 will demonstrate the result of the sprint to the WP2 and WP3 members. This is the final acceptance from WP3 on a deliverable and once accepted it will be taken as completed. Any task needing further work is put back into the product backlog for later sprinting;
5. **Sprint retrospective** – This is an event where we evaluate how we work and adjust the process during the project execution, important that this is done between sprints;

[10] Ian Sommerville. Software Engineering. Ninth Edition. Addison-Wesley, 2011

[11] https://en.wikipedia.org/wiki/Scrum_(software_development)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

6. **TimeBoxing** – In order for any Agile methodology to work a set sprint time must be established (this can be changed at the sprint retrospective) but it is designed to be able to freeze requirements for a specific period of time. The suggestion is that TOOP WP2 uses a sprint length of 2-12 weeks. This will allow for in-depth analysis which will be needed but also a sufficient number of sprints to complete the project. However, the sprint time must be aligned with the realities of an LSP and the fact that multiple sprints will lead up to a project deliverable. So, the connection and length of sprints must be analysed further from a LSP viewpoint.

Suggested work process aligned with the Agile methodology

- The first step in this process is to start populating the project backlog (shared between WP2 and WP3) with information regarding requirements. The suggestion is that this is done using workshops (the first was held in The Hague in April 2017) and teleconference discussions in smaller groups. The number of workshops is decided by WP2 and WP3 management based on need and budget availability. But it may be advisable to have at least 2-3 physical workshops, if possible. Once the initial product backlog has been established, the requirements should come through the work and cooperation between WP2 and WP3. This must be monitored by WP2 and WP3 leaders. This can be done in accordance with the model proposed by WP3 in document "TOOP Agile Methodology";
- Sprint preparation comes next, where we would apply the working method of user stories or use cases detailed through the work process proposed by WP3 in "TOOP Agile Methodology". This relies on user roles and modelling which is a reliable approach and generates good results, even though it can be time consuming and require physical presence to work at its best. A selection of user stories or use cases is taken from the project backlog and chosen for implementation. This selection should be done by the product owner. The final aspect of the sprint planning is task assignment which can be done using a teleconferencing system. It is also advisable to use some sort of software support for the handling of the backlogs and prints. One option is to use Trello, which is suited for the work and free to use. Ii is important to note that Agile methodologies are traditionally applied to software development and user stories or use cases depict functional requirements. However, this is not a general rule and user stories or use cases can also be used to depict requirements related to OOP architecture presented in Chapter 3;
- The next phase is the actual sprint and this must be organized so that WP2 and WP3 cooperate in teams, when needed (team size should be 7+/-2 people). Another way to handle the cooperation between WP2 and WP3 is to use work streams and see it as longer tasks that need multiple iterations (amounting to a maximum of 12 weeks). This can be done in an ad-hoc fashion as part of the task allocation. It is then up to the teams to solve the task(s) given in the 2-12-week sprint period allocated. At the end of the sprint, the deliverables should be uploaded to the document repository for review. Currently three deliverables (D2.2, D2.3, D2.4) are foreseen to follow the D2.1;
- In the demo session, the various deliverables are given 5 min to present (given that participants have prepared and read through them before the meeting) followed by a discussion session and a decision if it is accepted or rejected as completed. If accepted it will be added to the repository if rejected it is put back into the project backlog.

At the moment, there are two suggestions on work process but this is in our opinion not an issue, since they complement each other and this outline has been kept on a high abstraction level in order to be compatible with the diligent work of WP3 on this topic. It is of utmost importance that WP2 and WP3

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

utilize the same method of work since cooperation between the two is natural and expected to be frequent. This of course needs to be agreed in the WP2 and WP3.

1.4.Relations to Internal TOOP Environment

The current deliverable presents the OOP architecture and demonstrates its standpoints on the example of three selected TOOP pilots. It also evaluates and extends the pilot outcomes, exchanges best practice results with other WP2 tasks, and provides architecture-related support to WP3 within the scope of task T2.1. Specific instantiations of the architecture will be implemented in development of the TOOP pilot projects in WP3. The architecture is partially based on the interaction between WP2 and WP3, on the questionnaire and information provided with respect to other tasks in WP2, and other sources. Maintaining and further development of the architecture will be planned by the Sustainability and Governance task of WP2.

1.5.Relations to External TOOP Environment

The results of this deliverable represent the first version of the main technological innovation of TOOP - the generic federated OOP architecture that supports the interconnection and interoperability of national registries at the EU level. It is in line with existing EU frameworks (EIRA, EIF), takes into account the e-SENS European Interoperability Reference Architecture and is based on the CEF DSIs, the Building Blocks consolidated by the e-SENS project and possibly new BBs.

1.6.Legal Issues

Several legal issues had to be clarified when writing the deliverable. These issues were related to European legislation, as well as to national legislation in Member States and Associated Countries that are participating in the WP3 pilots. The solutions found allowed to conclude that it is possible to build the generic federated OOP architecture in line with existing EU frameworks such as the European Interoperability Framework, the European Interoperability Reference Architecture, the CEF Building Blocks, and the e-SENS Building Blocks, among others.

1.7.Structure of the Document

The deliverable includes five chapters and an appendix. The first chapter, introduction, states the deliverable scope, methodology, relations to TOOP internal and external environments, quality and risk management, and other issues.

The second chapter presents the guiding principles for the OOP architecture.

The third chapter proposes the requirements for the generic federated OOP architecture.

The OOP architecture needs to rely on the existing resources, including various types of building blocks. To understand what potential resources are available for development of OOP applications, an initial inventory of existing e-Government Building Blocks, without specific references to pilot area needs, is proposed in Chapter 4.

The fifth chapter provides several generic types of high-level OOP architecture, introduces the principles of selection of building blocks for OOP applications, and analyses the selected building blocks with respect to their relevance, applicability, sustainability, need for further development, and external interfaces.

An overview of the needs of pilot areas is given in the Appendix.

2. Key Concepts

This chapter presents the key concepts related to the TOOP generic federated OOP architecture.

2.1.Guiding Political, Legislative, and Technical Principles

This section presents the guiding political, legislative, and technical principles of the architecture.

The eGovernment Action Plan 2016-2020 presents the Once Only Principle (OOP) - the public administrations should ensure that citizens and businesses supply the same information only once to a public administration[12]. The main political and legislative principles underlying the TOOP generic federated OOP architecture are stated in Annex 2 to the European Interoperability Framework Implementation Strategy (Brussels, 23.3.2017 COM (2017) 134 final)[13].

1. Subsidiarity and proportionality;
2. Openness;
3. Transparency;
4. Reusability;
5. Technological neutrality and data portability;
6. User-centricity;
7. Inclusion and accessibility;
8. Security and privacy;
9. Multilingualism;
10. Administrative simplification;
11. Preservation of information;
12. Assessment of Effectiveness and Efficiency.

TOOP focus area within OOP is on information related to businesses activities and on cross-border sharing of this information. One of the main technical principles for development of OOP architecture is reuse of existing frameworks and building blocks provided by CEF, e-SENS, and other initiatives. The TOOP generic federated OOP architecture relies on such frameworks as the European Interoperability Reference Architecture (EIRA)[14], the CEF Building Blocks[15], and the e-SENS deliverable “D6.6 e-SENS European Interoperability Reference Architecture”[16], among others. It takes these frameworks into account, adding the aspects specific to OOP, analysing the building blocks with respect to their applicability in OOP applications, developing generic views of architecture implementations, and in future versions of the architecture – adding a framework for specific OOP architectures and providing deployment profiles for the building blocks. These frameworks, deliverables, and building blocks provide a rich collection of architecture standards and viewpoints. Deliverable D2.1 refers to this collection as there is little added value in copying them into the current document.

[12] https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation

[13] http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF

[14] https://joinup.ec.europa.eu/catalogue/distribution/eira_v1_1_0_overviewpdf

[15] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home

[16] https://www.esens.eu/deliverables?page=3

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

2.2.Architecture Principles

For the description of our generic, federated OOP Architecture we use the definitions laid down in the ISO/IEC/IEEE 42010 'Systems and software engineering — Architecture description' standard[17]. This standard defines four cases of conformance:

1. architecture description (AD);
2. architecture viewpoint;
3. architecture framework;
4. architecture description language (ADL).

2.2.1. Architecture Description

An architecture description is an artefact describing the architecture for some system of interest. In ISO/IEC/IEEE 42010, system refers to man-made and natural systems, including software products and services and software-intensive systems. Architecture descriptions have a variety of uses. Per ISO/IEC/IEEE 42010, an architecture description conforming to the standard is expected to include:

- identification and overview information of the architecture being expressed;
- identification of the system stakeholders and their concerns;
- definitions for each architecture viewpoint used in the architecture description and a mapping of all concerns to those viewpoints;
- an architecture view and its architecture models for each architecture viewpoint used;
- correspondence rules and correspondences and a record of known inconsistencies among the architecture description's required contents;
- architecture rationale (explanation, justification, reasoning for decisions made about the architecture being described).

ISO/IEC/IEEE 42010 organizes an architecture description into multiple architecture views. An architecture view addresses one or more concerns held by stakeholders of the system being described. An architecture view describes the architecture of the system of interest in accordance with the rules and conventions defined in its architecture viewpoint. Each architecture view must have an architecture viewpoint.

2.2.2. Architecture Viewpoint

A viewpoint formalizes the idea that there are different ways of looking at the same system. In ISO/IEC/IEEE 42010, viewpoints play an integral part of architecture descriptions, architecture frameworks and ADLs, and may also be separately specified. In ISO/IEC/IEEE 42010 an architecture viewpoint is expected to:

- frame one or more concerns held by the stakeholders about the system of interest;
- establish the conventions for one kind of architecture view.

Viewpoint conventions include modelling languages, notations, model kinds, design rules, and/or modelling methods, analysis techniques and other operations on views. Viewpoints establish the rules of conformance for views (such as well-formedness, completeness, interpretability). In framing the stakeholder concerns, a viewpoint defines how architecture views of that type address these concerns.

[17] https://www.iso.org/standard/50508.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

IISO/IEC/IEEE 42010 requires an architecture viewpoint to include:

- identified stakeholder concerns that are framed by the viewpoint (to be addressed by views of that type);
- an identified set of stakeholders holding these concerns;
- the model kinds used (means of representing the relationships/information e.g. N-squared);
- languages, notations, conventions, modelling techniques, operations used on these model kinds.

An architecture viewpoint should include:

- techniques used to create, interpret and analyse;
- correspondence rules and means of checking consistency;
- heuristics, metrics, patterns, examples.

2.2.3. Architecture Framework

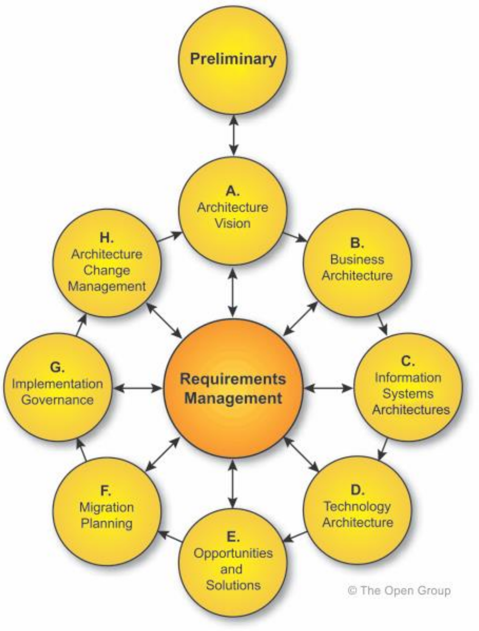
An architecture framework establishes a common practice for using, creating, interpreting, and analysing architecture descriptions within a domain of application or stakeholder community. ISO/IEC/IEEE 42010 formalizes a framework as a set of predefined, interconnected viewpoints.

An architecture framework conforming to the standard includes:

1. identification of the relevant stakeholders in the domain;
2. the concerns arising in that domain;
3. architecture viewpoints framing those concerns and
4. correspondence rules integrating those viewpoints.

Frameworks conforming to the standard often include processes, methods, tools and other practices beyond those specified above. The two most well-known examples of architecture frameworks are The Open Group's Architecture Framework (TOGAF)[18] and Zachman's[19] information systems architecture framework.

For the development process of the generic, federated OOP Architecture, we will use the steps of the Architecture Development Method (ADM) of TOGAF9.1[20]. This methodology follows a cyclic approach towards the development of an architecture, its implementation and maintenance (see the figure at the right-hand side). In TOOP, we focus on phases B to D for the development of the generic, federated OOP architecture, phase E for proposal of possible implementation solutions and phase H for the maintenance of the architecture throughout the project. The phases of the ADM cycle are further divided into steps. For example, the steps within the architecture development phases (B, C, D) are defined by TOGAF as follows:


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management
© The Open Group

[18] https://en.wikipedia.org/wiki/TOGAF
[19] https://en.wikipedia.org/wiki/Zachman_Framework
[20] http://pubs.opengroup.org/architecture/togaf9-doc/arch/

- Select reference models, viewpoints, and tools;
- Develop Baseline Architecture Description;
- Develop Target Architecture Description;
- Perform gap analysis;
- Define candidate roadmap components;
- Conduct formal stakeholder review;
- Finalize the Architecture;
- Create Architecture Definition Document.

Throughout the ADM cycle, there needs to be frequent validation of results against the original expectations, both those for the whole ADM cycle, and those for the phase of the process.

2.2.4. Architecture Description Language

ISO/IEC 42010 requires an architecture description language (ADL) conforming to the standard to specify:

- the concerns framed by the ADL;
- the typical stakeholders who hold these concerns;
- the model kinds implemented by the ADL that frame these concerns;
- any correspondence rules linking those model kinds.

An architecture description language may specify one or more architecture viewpoints, but need not have any. The most well-known examples of architecture description languages are: ArchiMate, BPMN, SysML and UML. The concerns framed by an ADL are not necessarily aligned with those addressed by an architecture framework. The suitability of the ADL for use with an architecture framework will depend on how well it is able to frame the concerns that the framework and its viewpoints. For this reason and because of our choice for the TOGAF architecture framework, we will make use of the Archimate3.0[21] specification as architecture description language.

2.2.5. Architecture Approaches in TOOP Deliverables

The first version of the architecture will comprise information included in the current deliverable. For this deliverable D2.1, we have not yet followed the approach sketched above in this section. We have started with an overview of existing building blocks as they are described by CEF, e-SENS or others. Where possible we have used already Archimate diagrams to model architectural descriptions. For subsequent versions of the architecture (deliverables D2.2, D2.3, D2.4) we will use the architecture development approach presented above.

2.3. Relationship between the Architecture and the S/W development process

TOOP will follow good architectural practices when developing generic OOP architecture. This approach involves a series of decisions based on a wide range of factors, and each of these decisions can have considerable impact on the quality, performance, maintainability, and overall success of the OOP architecture. Thus, changes and additions to OOP architecture will be smooth, fast and cheap.

[21] http://pubs.opengroup.org/architecture/archimate3-doc/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

There is a continuum of architectures, architectural building blocks, and architectural models, that are relevant to the task of constructing an TOOP-specific architecture. The Architecture Continuum, and the relative positioning of different types of architectures within it, is depicted on Figure 1.

Figure 1 illustrates how architectures are developed across a continuum ranging from foundational architectures such as TOGAF, through common systems architectures, and domain architectures, to pilot architectures. The arrows in Figure 1 represents the bi-directional relationship that exists between the different architectures in the Architecture Continuum. The leftwards direction focuses on meeting TOOP needs and business requirements, while the rightwards direction focuses on leveraging architectural components and building blocks. The TOOP needs and business requirements are addressed in increasing detail from left to right. The architect will typically look to find re-usable architectural elements toward the left of the continuum. When elements are not found, the requirements for the missing elements are passed to the left of the continuum for incorporation. Those implementing architectures within their own organizations can use the same continuum models specialized for their business.

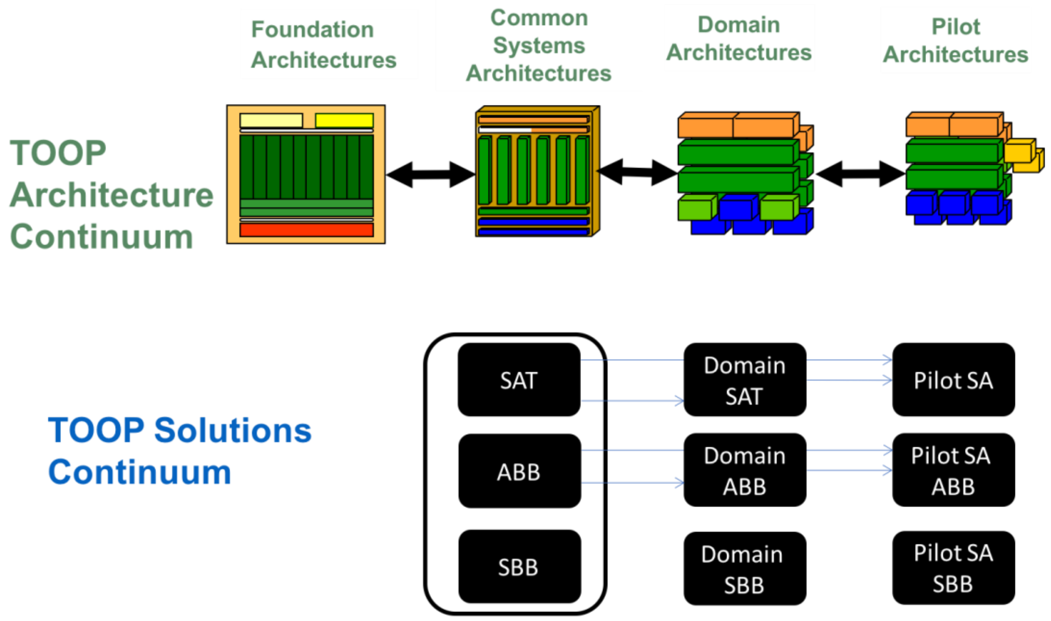
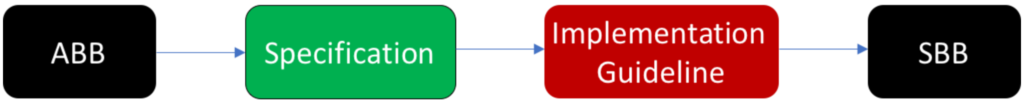


Figure 1: OOP architecture and Solutions Continuum

The TOOP Solutions Continuum represents the implementations of the architectures at the corresponding levels of the Architecture Continuum. At each level, the Solutions Continuum is a population of the architecture with reference building blocks, either ABB or SBB, that represent a solution to the TOOP's business need expressed at that level. A populated Solutions Continuum can be regarded as a systems inventory or re-use library, which can add significant value to the task of managing and implementing improvements to the IT environment.

OOP architecture, which will be designed in WP2, is the highest level of abstraction of the once-only principle. It will be skeleton of developments in WP3 piloting domains. WP2 architects abstract the complexity of TOOP requirements into a manageable model that describes the essence of TOOP system by exposing important details and significant constraints. The preliminary OOP architecture is firstly defined from both generic technical requirements (e.g. from once-only principle) and user requirements (e.g. from WP3 piloting domains). WP2 architects create blue print of the building blocks that will be used in the generic OOP architecture. In other words, they create building block profiles that have provisions for various business and technical requirements.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460



OOP architecture describes the specification of the Architectural Building Block (ABB) and their relationships. These components are then matched against list of particular Software Building Block (SBB). This matching process produces a list of candidate SBBs that could form a part of the WP3 piloting developments. Therefore, OOP architecture contains an SBB repository. With this repository, the generic OOP architecture is re-examined in order to accommodate as many candidates from the SBB repository as possible, and the OOP architecture's requirements are revised if needed. It should be noted that there will be no software development process in WP2.

Development of applications based on the generic OOP architecture may also be characterised as component-based software engineering. This approach involves reuse of relatively independent components in the application under development[22]. In case of OOP architecture, these independent components are various kinds of building blocks reused in OOP related applications. Mapping these components, profiling them, as well as presenting their roles on the overall OOP application views are important tasks of OOP architecture development.

In the next step, WP3 pilot developers will take building blocks of generic OOP architecture and will start to implement some of them according to their use cases. Thus, each piloting domain of WP3 will make profiling on the generic OOP architecture according to its requirements and implement some building blocks (i.e. SBBs) of it in order to demonstrate feasibility of the generic OOP architecture.

[22] https://en.wikipedia.org/wiki/Component-based_software_engineering

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

3. Summary of Requirements for the OOP Architecture

Requirements for the generic federated OOP architecture are related to different artefacts:

- to the OOP architecture itself;
- to the OOP applications in general;
- to specific TOOP pilot applications.

These requirements come from various sources:

- from guiding principles for the OOP architecture and The Once-Only Principle project as formulated in its Technical Annex;
- from dual character of the OOP architecture as an architecture framework and architecture;
- from the TOOP focus area and pilots;
- from standards and best practices.

A summary of these requirements is given below.

3.1.Requirements Resulting from the TOOP Guiding Principles and the Project

Requirements resulting from the guiding political, legislative, and technical principles of the architecture are based on Chapter 2.1 of this document. As an example, according to the subsidiarity and proportionality principle, the Member States should be sufficiently free in development of their OOP application architectures with respect to the recommendations given in the current deliverable. These requirements must be applied to all artefacts related to OOP architecture.

According to the Technical Annex of the Grant Agreement of the TOOP project, 'D2.1 Generic federated OOP architecture (1st version)' (the current document) should include, among others, the requirements, the initial building blocks, and the interface specifications of the generic federated architecture. The Technical Annex does not specify which kind of requirements need to be included, therefore the current chapter presents a summary and selection of requirements. These requirements from the Technical Annex apply mainly to the OOP architecture itself (its first version).

3.2.Requirements Resulting from Architecture Framework Considerations

OOP applications in the TOOP focus area can have very different structures. It is not easy, or even possible, to depict all these structures on one diagram. Therefore, a natural way to formulate an OOP architecture is to present it as an architecture framework - conventions, principles and practices for the description of architectures within the TOOP focus area.

Such an OOP architecture framework would not depict architectures of individual OOP applications, instead it would establish rules for description of individual architectures. The TOOP generic federated OOP architecture relies on such frameworks as the European Interoperability Reference Architecture (EIRA)[23] and the e-SENS deliverable 'D6.6 e-SENS European Interoperability Reference Architecture'[24], among others.

As an architecture framework, the OOP architecture specifies further the reference architectures given above with respect to OOP specific features and analyses the building blocks with respect to their applicability in OOP applications.

[23] https://joinup.ec.europa.eu/catalogue/distribution/eira_v1_1_0_overviewpdf

[24] https://www.esens.eu/deliverables?page=3

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Still there is also considerable interest and need from TOOP Pilot Areas to have high-level views of OOP architecture that would characterise some notable features of specific applications and associate it with appropriate building blocks.

Responding to this need, the OOP architecture development presents generic views of architecture implementations. Selected high-level views on OOP architecture are provided in the Chapter 5.

In future versions of the architecture, deployment profiles for the building blocks and a framework for supporting development of specific OOP architectures will be introduced.

Description and development of the OOP architecture components follows the methodology presented in Section 1.3.

3.3.Requirements Resulting from the TOOP Focus Area and Pilot Areas

An important source of requirements is the TOOP focus area. TOOP focus area within OOP is on information related to businesses activities and on cross-border sharing of this information[25]. The OOP architecture relates primarily to applications in the TOOP focus area, although its wider usage is not excluded. This means that applications dealing with information not related to business activities or designed to operate within one member state are not in the scope of the current deliverable.

To illustrate the TOOP focus area concept, the following non-exhaustive list presents scenarios which are and which are not in the OOP scope.

- The scenario 'A citizen of country C provides some data and this data is shared in the same country by Public Authorities of country C' is not within the scope of the current deliverable, as it does not relate to cross-border sharing of information;
- The scenario 'A citizen of country C provides some data not related to business activities and this data is shared with Public Authorities in many countries' is not within the scope of the current deliverable, as it is dealing with information not related to business activities;
- The scenario 'A citizen of country C provides some data related to business activities and this data is shared with Public Authorities in many countries' is within the scope of the current deliverable, as it is related to businesses activities and to cross-border sharing of this information;
- The scenario 'A business entity of country C provides some data and this data is shared in the same country by Public Authorities of country C' is not within the scope of the current deliverable, as it does not relate to cross-border sharing of information;
- The scenario 'A business entity of country C provides some data and this data is shared with Public Authorities in many countries' is within the scope of the current deliverable, as it is related to businesses activities and to cross-border sharing of information;
- The scenario 'Direct data transfer to EC European Single Procurement Document Service from MS registers' (PA 1) is within the scope of the current deliverable, as it is related to businesses activities and to cross-border sharing of information;
- The scenario 'Cross Border Service Provision (Licences and Permissions)' (PA 1) is within the scope of the current deliverable, as it is related to businesses activities and to cross-border sharing of information;

[25] TOOP D2.6 Position paper on definition of OOP and situation in Europe. 2017

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- The scenario 'Doing Cross Border Business (Basic company data and Legal Person Mandates)' (PA 1) is within the scope of the current deliverable, as it is related to businesses activities and to cross-border sharing of information;
- The scenario 'Business Register provision of information on legal entities – pull (a foreign eGovernment service receives a request on behalf of a legal entity registered in a TOOP country)' (PA 2) is within the scope of the current deliverable, as it is related to businesses activities and to cross-border sharing of information;
- The scenario 'Business Register provision of notifications information on legal entities – push (subscribing to a change notification service offered by the Business Register)' (PA 2) is within the scope of the current deliverable, as it is related to businesses activities and to cross-border sharing of information;
- The scenario 'Online issuing and checking ship and crew certificates' (PA 3) is within the scope of the current deliverable, as it is related to businesses activities and to cross-border sharing of information.

The generic federated OOP architecture developed within TOOP relates primarily to applications in the TOOP focus area, although its wider usage is not excluded. It builds on analysis of the TOOP requirements, on the experience of previous 'Large Scale Pilot' (LSP) projects, and on the know-how gained with implementation of the TOOP pilots.

The requirements resulting from the TOOP focus area must be applied to all artefacts related to OOP architecture.

Requirements evolving from the TOOP pilot areas are described in the Appendix of the current document. These requirements to specific TOOP pilot applications are needed as an input to design requirements for the OOP applications in general. In particular, they are needed to select building blocks for inclusion into the architecture document, for communicating with the pilot developers, for designing the building block related content of the architecture, and for profiling the building blocks. They are also useful for understanding the specific features of TOOP applications and the logic of the architecture. The current version of PA requirements is included in the Annex as a snapshot at the time of publishing, for information purposes, since WP3 has not produced any deliverables yet. This inclusion is an exception for the first iteration and not the rule for the next iterations of the Architecture.

3.4.Requirements Resulting from Standards and Best Practices

The technical best practices include relevant standards related to architecture, requirements, software security, software quality, and other issues.

As to the standards related to the OOP architecture itself, ISO/IEC/IEEE 42010:2011[26] addresses the concepts, development, and descriptions of system architectures. In particular, this standard provides important considerations to distinguish between the architectures and architecture frameworks. OOP applications can have very different structure. Therefore, a preferred way to formulate OOP architecture is to present it as an architecture framework. According to ISO/IEC/IEEE 42010:2011, an architecture framework represents; conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders.

[26] ISO/IEC/IEEE 42010:2011(en) Systems and software engineering — Architecture description

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Such an OOP architecture framework would not depict architectures of individual OOP applications, instead it would establish rules for description of individual architectures. Still there is considerable interest from TOOP Pilot Areas to have high-level views of OOP architecture. Such high-level views should address specific concerns of architecture users. As an example, selected views are included in the current document, providing topologies of different OOP applications, characterizing the scope of the building blocks using these topologies, and presenting some arguments for selection of the architecture.

The above requirements apply mainly to the OOP architecture itself.

For OOP applications, the ISO/IEC 25000 series standards provide guidance with respect to software quality requirements. The ISO/IEC 25010:2011[27] standard defines a quality in use model composed of five characteristics and a product quality model composed of eight characteristics. The ISO/IEC 25012:2008[28] standard defines a general data quality model comprising fifteen characteristics considered by inherent and system dependent points of view. This standard can also be useful for designing specific OOP applications.

Security related considerations are very important for OOP applications. They can be based on the ISO/IEC 27000 series standards - a comprehensive resource in security area, widely used by governmental bodies and businesses both in EU and worldwide. Standard ISO/IEC 27001:2013[29] introduces the notion of Information Security Management System and ISO/IEC 27002:2013[30] provides guidelines for its implementation. Implementing Information Security Management System proposed in these standards can be used as a baseline on which to develop security related topics in OOP applications.

The above requirements apply mainly to the OOP applications in general and to the specific TOOP pilot applications, but they can be used also with respect to the OOP architecture itself.

[27] ISO/IEC 25010:2011*,* Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models

[28] ISO/IEC 25012:2008*,* Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Data quality model

[29] ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements

[30] ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

4. Existing e-Government Building Blocks

This section presents an inventory of existing E-government building blocks without reference to specific requirements of the OOP applications. The goal of this inventory is to understand what potential resources are available for development of OOP applications. This inventory will be used in the subsequent sections to identify and elaborate in more detail the building blocks relevant to TOOP pilots and OOP projects in general. The selection of the building blocks is based on the CEF DSIs, on the building blocks consolidated by the e-SENS project, and in justified cases, on the new building blocks.

As an example of a potential new building block needed, several requirements from the questionnaire on specific conditions and constraints at piloting countries and organisations state that there may be fees for information requests and exchange and therefore some kind of contracts exist on a regional/national level. This may indicate a need for a building block covering contracting capabilities. This kind of questions are left for consideration in the future versions of the architecture.

The building blocks presented below are a result of cooperation between CEF and e-SENS[31]. The CEF building blocks are to a large extent based on e-SENS models. Therefore, the main functionality of the building blocks that are presented both in CEF and e-SENS (eDelivery, eID, eSignature) is similar. Still many aspects of these parallel building blocks concerning their structure, terminology, and components, are different. Therefore, both versions are included in the chapters below.

In this chapter, the CEF building blocks are presented first as it is assumed that resources for their maintenance and support are secured for a longer future duration.

4.1.CEF Building Blocks

CEF Building Blocks provide basic capabilities that can be used in European projects to enable delivery of digital public services across borders[32]. Digital Service Infrastructures (DSIs) describe solutions that support the implementation of EU-wide projects[33]. CEF Building Blocks are basic digital service infrastructures, which are key enablers to be reused in more complex digital services. This document does not address the sector specific DSIs, which however provide valuable information about usage of the CEF building blocks [34].

4.1.1. eDelivery

This section presents the building block in more detail, investigating the following aspects.

- Short overview of the building block;
- Availability of maintaining and supporting organization for this building block;
- Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

The CEF eDelivery is a Digital Service Infrastructure (DSI) Building Block[35] defines a holistic (legal, organizational, semantic and technical) interoperability architecture to implement the technical components needed to exchange electronic data and documents between public administrations and businesses in an interoperable, secure, reliable and trusted way.

[31] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=23003235
[32] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home
[33] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Definitions
[34] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Sector+Specific+DSI
[35] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Using this building block, every participant becomes a node in the network using standard transport protocols and security policies. The eDelivery Building Block is based on a distributed model, allowing direct communication between participants without the need to set up bilateral channels. An implementation of eDelivery works as a collection of distributed nodes that are conformant to the same technical rules and therefore capable of interacting with each other.

The eDelivery BB derives mainly from the e-SENS eDelivery SAT. It consists of specific architectural components that are derived from several e-SENS eDelivery and Trust Establishment ABBs, which contain their respective technical specifications, conformance and interoperability testing processes, conformant software and provided services. These architectural components are:

- Message Exchange;
- Capability Lookup;
- Dynamic Service Location;
- Backend Integration;
- Trust Establishment.

CEF is promoting the re-use of these eDelivery components, recommending three different options:

- Building and testing your own components according to the specifications of the eDelivery DSI;
- Buying one or more products that implement these specifications;
- Reusing the eDelivery DSI sample software.

For all these options, CEF offers a service package that helps you comply with European standards and technical specifications. It includes software, services, documentation and tools to facilitate testing, deployment and operation of the building block.

4.1.1.1. Message Exchange

In CEF eDelivery, Message Exchange is the main use case that is implemented by an Access Point Software component which supports the standards and profiles that message exchange defines and endorses for generic use. The main goal is to promote interoperability, security, scalability, legal assurance and accountability for exchanging of documents and/or data.

The endorsed standards are the e-SENS profile OASIS AS4 and the OpenPEPPOL profile of AS2 IETF[36]. A CEF eDelivery AP is an implementation of the AS4 Profile developed by e-SENS or of the AS2 Profile developed by OpenPEPPOL. AS4 is an open technical specification for the secure and payload-agnostic exchange of data using Web Services. According to OASIS, the AS4 protocol is the modern successor of the AS2 protocol. During an interim period, while expecting a convergence process towards the e-SENS AS4 Profile, CEF eDelivery supports the OpenPEPPOL AS2 Profile currently in use in the e-Procurement domain.

Domibus is the Open Source project of the AS4 Access Point maintained by the European Commission. Third-party software vendors offer alternative implementations of the e-SENS AS4 Profile (commercial or open-source). Each software vendor also provides different added-value services from integration to the support of day-to-day operations. For safeguarding interoperability, CEF eDelivery encourages implementers to consult the list of software products that have passed the conformance tests by the European Commission of the e-SENS AS4 profile[37].

[36] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+specifications

[37] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-SENS+AS4+conformant+solutions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.1.1.2. Capability Lookup

In CEF eDelivery, Capability Lookup is a supportive use case that is implemented by a Service Metadata Publisher (SMP) which supports the standard profiles that the use case defines and endorses. It consists of an open specification for publishing service metadata. To successfully send a business document, using Message Exchange in a dynamic discovery environment, an entity must be able to discover critical metadata about the recipient (Access Point) of the business document, such as types of documents the Access Point is capable of receiving and methods of transport supported. The recipient makes this metadata available to other entities in the network through a Service Metadata Publisher service (SMP). The e-SENS SMP profile describes the request/response exchanges between a Service Metadata Publisher and a client wishing to discover Access Point metadata.

The profile is based on the OASIS Service Metadata Publishing (SMP) Version 1.0 standard[38], which is also the e-SENS Profile implementing the Capability Lookup ABB.

An SMP compliant list of software and services is available at the CEF eDelivery[39].

4.1.1.3. Dynamic Service Location

In CEF eDelivery, Dynamic Service is a supportive use case that further extends the Capability Lookup. It is implemented by a Service Metadata Locator (SML) which supports the standard profiles that the use case defines and endorses. It specifies a standardised way to locate a receivers Service Metadata Publisher. The use of the Dynamic Service Location further promotes the scalability of a network, with respect to its number of end user participants and access points, by providing a decentralized and distributed architecture for the provision of the end user participant to service metadata publisher mapping.

An SML Service is provided by CEF[40], and is currently used in production for the OpenPEPPOL eProcurement network, for eHealth and is being extended for use between eIDAS ERDS systems.

The Dynamic Service Location defines two different technical standards[41]:

- The e-SENS ebCore Party ID profile, based on the OASIS ebCore Party Id Type Technical specification;
- The e-SENS BDXL profile, based on the Business Document Metadata Service Location Version 1.0. from OASIS.

4.1.1.4. Backend Integration

Backend Integration, is a ‘place holder’ use case, which states that there exists a layer between the eDelivery main architectural and software components and the end participant that needs to be defined. The Backend Integration layer highly depends on the actual software architecture of the AP and the end user message handling systems and thus cannot be standardized.

However, several functionalities and processes should be implemented in a Connector Software component that acts as a mediator between the Access Point and the backend system of the end user participant.

The typical functionalities that complement the eDelivery use case and should/may be part of the back-end integration are:

[38] http://wiki.ds.unipi.gr/display/ESENS/PR+-+SMP+-+1.6.0

[39] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/OASIS+SMP+conformant+solutions

[40] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+service

[41] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+specifications

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

- Document / Message Validation;
- Issuing of non-repudiation tokens like REM Evidences;
- Creation of a message, based on the payload, metadata and the message specifications;
- Extraction of the message payload and metadata, and further internal routing based on the extracted metadata.

4.1.1.5. Trust Establishment

In CEF eDelivery, Trust Establishment focuses only on the use of certificates for establishing trust between two or more access points. Two different trust establishment mechanisms (trust models) are mentioned for usage in CEF eDelivery: Public Key Infrastructure (PKI) and Mutual Exchange of Certificates.

Trust establishment in eDelivery is mandatory for the provision of reliable, guaranteed message exchange. For this reason, CEF is providing a PKI Service for publishing certificates both for Access points and SMPs, as an enablement service for easy/early deployment of an eDelivery network of nodes[42].

4.1.2. eID Building Block

This section presents the building block in more detail, investigating the following aspects.

- Short overview of the building block;
- Availability of maintaining and supporting organisation for this building block;
- Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

The CEF eID Building Block[43] allows cross-border authentication in a secure, reliable and trusted way, by making national electronic identification systems interoperable. It enables the mutual recognition of national eIDs between participating Member States, in line with the eIDAS (electronic Identification and Signature) legal framework (see eIDAS Regulation (EU) 910/2014[44]) and with the privacy requirements of all the participating countries.

This allows citizens of one Member State to access online services provided by organisations from other participating EU Member States, using their own national eID.

The technical management of the eID building block DSI is done by the Directorate-General for Informatics (DIGIT) of the European Commission. Directorate-General for Communications Networks, Content and Technology (DG CNECT) of the European Commission is responsible for implementation of the EU policy directly related to eID[45].

The CEF offers several services organizations comply with European legislation on electronic identification, as well as with technical specifications for cross border use including technical specification of eID eIDAS profile, eIDAS-Node software which is a sample implementation of the eID eIDAS profile[46], eID conformance testing service in order to verify compliance of the specific implementation against the eIDAS technical specifications, and support services (e.g., training, service desk).

[42] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service

[43] https://joinup.ec.europa.eu/asset/eia/asset_release/eid-sat-v101-beta

[44] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[45] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+Background

[46] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.1.3. eSignature Building Block

This section presents the building block in more detail, investigating the following aspects.

- Short overview of the building block;
- Availability of maintaining and supporting organisation for this building block;
- Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

The CEF eSignature Building Block[47] facilitates the mutual recognition and cross-border interoperability of eSignatures between the Member States, allowing the public administrations and businesses to trust and use eSignatures that are valid and structured in EU interoperable formats. It helps public administrations and businesses to create and validate electronic signatures across borders.

The technical management of the eSignature DSI is done by the Directorate General for Informatics (DIGIT) of the European Commission. Directorate-General for Communications Networks, Content and Technology (DG CNECT) of the European Commission is responsible for implementation of the EU policy directly related to eSignature.

The CEF has a service package that helps public and private organizations comply with European standards and technical specifications. It includes software, services, documentation and tools to test, deploy and operate the building block.

4.1.4. eInvoicing Building Block

This section presents the building block in more detail, investigating the following aspects.

- Short overview of the building block;
- Availability of maintaining and supporting organisation for this building block;
- Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

The CEF eInvoicing Building Block[48] helps public administrations to comply with EU eInvoicing legislation and assists solution providers in adapting their services accordingly. This building block supports Administration to Business communication and Administration to Administration communication. It is not intended for Business to Business, Citizen to Administration, or Citizen to Business communication.

It is natural to use the CEF eInvoicing in the context of the CEF eDelivery building block. In this case, the eInvoicing building block concerns electronic invoices as such, while eDelivery is about transporting messages, in this case the electronic invoices. The technical management of the eInvoicing DSI is carried out by the Directorate-General for Informatics (DIGIT) of the European Commission.

CEF service package includes services, documentation and tools help to test, deploy and operate the eInvoicing building block. Standard-based eInvoicing has previously been implemented in PEPPOL LSP, which is in full-scale production in the OpenPEPPOL community.

4.1.5. eTranslation

This section provides an overview of the eTranslation, i.e., the Connecting Europe Facility (CEF) Automated Translation (AT) building block. Its purpose is to provide means of information exchange throughout Europe for national and European administrations, overcoming the existing language

[47] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature
[48] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eInvoicing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

barriers within the Union. CEF AT can be used as building block to be integrated into other services as well as there exists a stand-alone instance for documents and text translations. While the CEF AT provides high flexibility in terms of the data to be translated via the possibility to include different knowledge bases, e.g., in the medial or legal domain, it guarantees confidentiality and overall data protection of the contents translated and transmitted.

This section presents the building block in more detail, investigating the following aspects.

- Short overview of the building block;
- Availability of maintaining and supporting organisation for this building block;
- Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

The CEF Automated Translation[49] (CEF AT) is intended to make all DSIs multilingual. It is mainly intended for integration into other digital services, but can also be used as a stand-alone service. Compared to general-purpose web translators, CEF AT provides two important capabilities: confidentiality and security of all translated data and adaptation to specific terminology and usage text types (e.g., tender documents, legal texts, medical terminology).

The CEF Automated Translation building block utilizes the existing Commission Machine Translation service (MT@EC). The MT@EC service enables translation of formatted documents and plain text between any pair of EU official languages. It is developed by the Directorate-General for Translation (DGT). DGT is responsible for the technical management of the Automated Translation building block DSI and its machine translation service (eTranslation).

4.1.5.1. MT@EC

The CEF AT extends the existing MT@EC developed and technically-provided by the DGT within the Interoperability Solutions for European Public Administrations (ISA)[50] program. MT@EC is based on the open source software MOSES, which is a machine translation system, based on a statistical machine translation approach. The translation engines of MT@EC are based and trained on the European advanced multilingual information system (Euramis)[51] translation memories, providing translation capabilities for 24 languages. Requests towards MT@EC can either be send – after authentication through the European Commission Authentication Service (ECAS) portal[52] – or via Web services, i.e., machine-to-machine communication.

[49] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eTranslation
[50] https://ec.europa.eu/isa2/home_en
[51] https://ec.europa.eu/jrc/en/language-technologies/dgt-translation-memory
[52] https://ec.europa.eu/research/participants/portal/desktop/en/home.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.1.5.2. Statistical Machine Translation System – MOSES

The Moses project[53,54] is a data-driven and therefore statistical machine translation software. In this widely-used approach, systems are trained with large mono-lingual corpora to understand the syntax of the intended target system, while parallel data are used to train systems how to translate segments of the source language. These data represent a composition of two languages, where each sentence in one language has its counterpart in the other language associated respectively. The Moses software consists out of two main components, namely the training pipeline and the decoder. The first subsumes a set of to process the aforementioned monolingual and parallel data sets into a machine translation model. The decoder then makes use of the before trained translation model and uses it to translate the provided source language text into the desired target language.

4.1.6. e-HI (Human Interface)

Short overview of the building block

The e-HI (Human Interface) Solution Architecture Template[55] defines legal, organisational, semantic, and technical (application and infrastructure) interoperability architecture for development of EC-centric web-based solutions. The Human Interface SAT applies a requirement of responsive web design and uses a principle of web accessibility. This SAT describes aspects of the Human Interface, but does not concern User Experience.

Availability of maintaining and supporting organisation for this building block

The e-HI (Human Interface) Solution Architecture Template (SAT) v1.0.0 Beta has been published as part of the EIRA framework by the ISA Programme. It is provided under ISA Product Licence v1.3, where the “Owner” is the European Union represented by the European Commission. Any feedback and input in relation to e-HI is invited by email to DIGIT-EIRA@ec.europa.eu.

Availability of specifications and software that can be utilized for specifying and building applications that use this building block

The Human Interface SAT applies a requirement of responsive web design and uses a principle of web accessibility. Its semantic, application and infrastructure views refer to several recommended specifications, standards, methodologies, and web development techniques. Although the e-HI SAT itself does not include detailed specifications and software, guidelines and tutorials for responsive web design, web accessibility standards, as well as other techniques and good practices are available. Therefore, specifications and software that can be utilized for specifying and building applications that use this building block are available outside of e-HI SAT.

The e-HI SAT v1.0.0 Beta is provided as a package comprising the e-HI description, product licence, ArchiMate files, and Archi™ HTML Report plugin model. To utilize this SAT, standard tools can be applied. External interfaces for the applications utilizing the e-HI SAT are determined by the respective interfaces of the recommended specifications, standards, methodologies, and web development techniques. Descriptions and software for these interfaces are available in guidelines and tutorials for the recommended techniques and good practices.

[53] http://www.statmt.org/moses/?n=Moses.Overview

[54] Philipp Koehn, Hieu Hoang, Alexandra Birch, Chris Callison-Burch, Marcello Federico, Nicola Bertoldi, Brooke Cowan, Wade Shen, Christine Moran, Richard Zens, Chris Dyer, Ondrej Bojar, Alexandra Constantin, Evan Herbst (2007) Moses: Open Source Toolkit for Statistical Machine Translation, *Annual Meeting of the Association for Computational Linguistics (ACL), demonstration session*, Prague, Czech Republic.

[55] https://joinup.ec.europa.eu/asset/eia/asset_release/ehi-sat-v101-beta

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Need for e-HI SAT

The e-HI SAT defines a holistic (legal, organisational, semantic and technical) interoperability architecture for development of EC-centric web-based solutions**.** As most OOP applications use web-based components, applicability of e-HI SAT in OOP related projects depends on specific project requirements and may be investigated when starting a new project.

The current release e-HI SAT is a Beta version and is subject to future improvements. It might be considered for OOP applications as an initial set of recommended specifications, standards, methodologies, and web development techniques.

4.2.Building Blocks Consolidated by the e-SENS Project

As presented in Chapter 4.3.2 of the e-SENS deliverable 'D6.6 e-SENS European Interoperability Reference Architecture'[56], an e-SENS building block can of the following type: Solution Architecture Template (SAT), Architecture Building Block (ABB), Solution Building Block (SBB). A SAT comprises a set of ABBs, an ABB directs the development of SBBs.

This document focuses only on SATs listed in Chapter 4.7.1 of the e-SENS D6.6. The descriptions are based on the information provided in the e-SENS Architecture Repository[57]. When other sources are used, they are separately referenced for each building block.

SATs not listed in Chapter 4.7.1 of the e-SENS D6.6, but present e-SENS Architecture Repository are left out of the current document. This decision is based on the assumption that if these SATs have not been not included in one of the final e-SENS deliverables, then they may be not mature enough for use in real-life applications.

4.2.1. eDelivery SAT

This section presents the set of building blocks that consist the SAT in more detail, investigating the following aspects.

- Short overview of the SAT;
- Availability of maintaining and supporting organisation for the set of SAT ABBs;
- Availability of specifications and software that can be utilized for specifying and building applications for each ABB of the SAT.

The e-SENS e-Delivery[58] and trust models are to a large extent underlying the eDelivery building block of CEF[59] presented in the previous chapter.

In e-SENS, e-Delivery is based on the concept of a four-corner model, where end entities exchange messages via gateway intermediaries. The infrastructure only standardises communication between these intermediaries. Communication between gateways and end entities may use e-SENS e-Delivery, but may also use a different solution.

The e-SENS e-Delivery SAT refers to the following ABBs in the e-SENS Architecture Repository: Message Exchange; Capability Lookup; Service Location; Backend Integration. Each ABB consists of one or more profiles, which are maintained either from a standardization organization or the European Commission.

[56] https://www.esens.eu/deliverables?page=3
[57] http://wiki.ds.unipi.gr/display/ESENS/eSENS+Generic+Architecture+Repository
[58] http://wiki.ds.unipi.gr/display/ESENS/SAT+-+eDelivery
[59] https://www.esens.eu/content/e-delivery

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.2.1.1. Message Exchange ABB

The e-SENS Message Exchange Architectural Building Block provides secure and reliable exchange of single or groups of payloads in any structured or unstructured format. It is designed to support the e-Delivery SAT and supports both One Way and Two Way (Request-Response) exchanges. The ABB can be used in four-corner topologies or in point-to-point exchanges. In four-corner topologies, only the interconnect hop (corner 2 to 3) is in scope as the edge hops may use other message protocols.

The ABB can be specified as a profile of open standards message protocols. The e-SENS ABB Specification is based on a profile of the ebMS3 and AS4 OASIS standards, which allows the ABB to be implemented using open source or closed source commercial software products compliant with these standards.

The e-SENS profile is an OASIS AS4 profile[60], heavily based on the ENTSOG (the European Network of Transmission System Operators (TSO) for Gas) AS4 profile for TSOs and on e-CODEX specifications.

AP Software that conforms with the e-SENS AS4 profile is being listed in the CEF eDelivery wiki, with the commission being the actual conductor of the conformance testing of the vendors[61].

4.2.1.2. Capability Lookup ABB

Capability Lookup is a technical service to accommodate a dynamic and flexible interoperability community. A capability lookup can provide metadata about the communication partner’s interoperability capabilities on all levels defined in the European Interoperability Framework (Legal, Organizational, Process, Semantic and Technical interoperability levels). The metadata can be used to dynamically set interoperability parameters and ambitions between the sender and receiver.

A Capability Lookup service is owned by the communication receiver and it expresses the receiver's interoperability capabilities e.g.:

- which business processes the receiver can participate in;
- which eDocuments can be received;
- the security setup;
- the communication protocol setup;
- the location of receiver's gateway.

In the context of setting up an interoperability connection with a Business partner, the sender needs to dynamically resolve the settings e.g., Legal, Organizational, Semantic and Technical capabilities and constraints. The recipient has already stated ‘Defined’ or ‘Entered’ instead of ‘stated’ these in the Capability LookUp service and by requesting the meta data, the sender can adopt and choose the most optimal settings and capabilities.

An example would be several ambitions levels for Business Processes e.g.:

- Exchange of an order;
- Exchange of an order, followed by an order response;
- Exchange of an order, followed by an order response and an invoice.

In this case, the sender can choose the ambition level that corresponds to its Business Process capability.

[60] http://wiki.ds.unipi.gr/display/ESENS/PR+-+AS4+-+1.11

[61] http://wiki.ds.unipi.gr/display/ESENS/SBB+-+Access+Point

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

In the e-SENS project, the SMP (Service Metadata Publisher) specification originally developed by PEPPOL and generalized and standardized by OASIS is used[62]. The SMP specification usually complements the Service Location ABB. It defines an XML-based service metadata data model and a REST binding to retrieve service metadata:

- The Metadata Publisher hosts Metadata for each participant ID at a predefined URL;
- The sender uses this URL in a HTTP GET operation which returns the metadata relating to that recipient's capabilities.

The sender can retrieve the information necessary for setting up an interoperability process. The Service Metadata Publisher stores the interoperability metadata, which enables routing of documents received from a sender to the correct recipient. SMP service metadata is a combination of information on the end entity recipient (its identifier, supported business documents and processes in which it accepts those documents) and the gateway (metadata which includes technical configuration information on the receiving endpoint, such as the transport protocol and its address).

Every community participant is registered in only one SMP registry.

4.2.1.3. Service Location ABB

To use to a metadata service, the sender needs to know the location of that service. The e-SENS Service Location ABB defines a standard location for metadata service providers. The located metadata service can be used to obtain service metadata to properly configure the transport connection to the endpoint for that entity (or service provider) and to send documents or data to an end entity (or its service provider).

The ABB can be specified as a profile of open standards message protocols. The related e-SENS Specification provides a specification based on the based on the BDX Location OASIS specification[63].

Location service lookup is the first step into the dynamic discovery mechanism. It provides address and access information on capability services (Please refer to Capability Lookup ABB). If a message is going to travel in the e-SENS system from an endpoint to another, the capability information of the receiving end-point is first needed in order to decide whether that endpoint is eligible and able to receive that message. To obtain the capability information, location service lookup is the prerequisite. In other words, if the sender entity needs to get information on the capabilities of an endpoint, it first has to learn the location of the capability service.

In e-SENS, the profile that implements service location is the OASIS BDXL (SML) Specification. An implementation guideline of the profile can be found on the e-SENS EIRA[64].

The OASIS BDXL is now officially supported by the commission’s SML Service.

[62] http://wiki.ds.unipi.gr/display/ESENS/PR+-+SMP+-+1.8.0

[63] http://wiki.ds.unipi.gr/display/ESENS/PR+-+BDXL+1.3.0

[64] http://wiki.ds.unipi.gr/display/ESENS/PR+-+BDXL+1.3.0

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

4.2.1.4. Backend Integration ABB

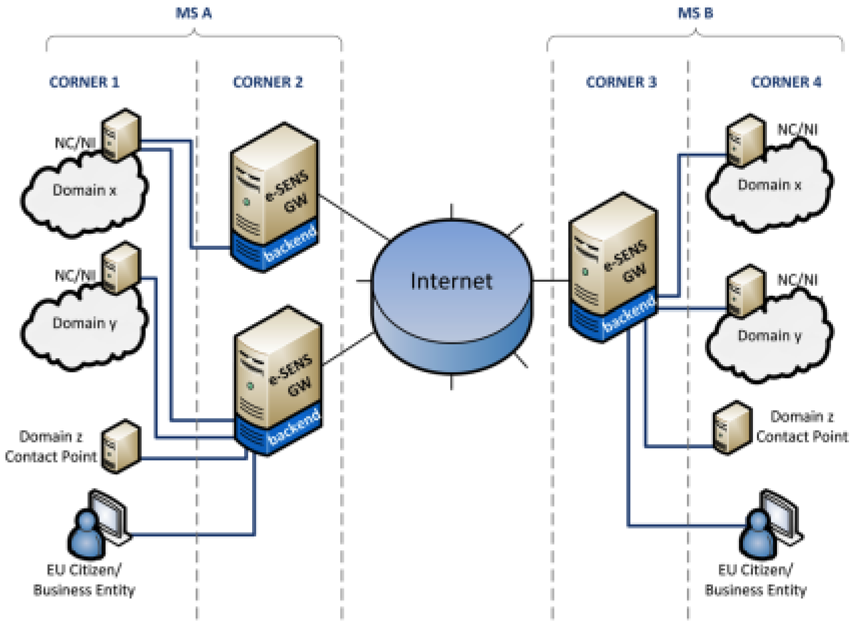


Figure 2: Backend Integration Topology

From the backend perspective, the actors are the end entities (EEs) which connect to the gateway of the 4-Corner Model used in e-SENS. The Backend Integration ABB facilitates the connection between the national infrastructure and the e-SENS infrastructure.

The Backend Integration layer highly depends on the actual software architecture of the AP and the end user message handling systems and thus cannot be standardized.

However, several functionalities and processes should be implemented in a Connector Software component that acts as a mediator between the Access Point and the backend system of the end user participant

The typical functionalities that complement the eDelivery use case and should/may be part of the back-end integration are:

- Document / Message Validation;
- Issuing of non-repudiation tokens like REM Evidences;
- Creation of a message, based on the payload, metadata and the message specifications;
- Extraction of the message payload and metadata, and further internal routing based on the extracted metadata.

4.2.2. eID SAT

This section presents the building block in more detail, investigating the following aspects.

- Short overview of the building block.
- Availability of maintaining and supporting organisation for this building block.
- Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

eID is one of the SATs in e-SENS reference architecture in order to develop the digital infrastructure for improving the quality of public services in the EU. The e-SENS eID SAT[65] was initially based on only STORK and STORK 2.0 eID architecture. Then, it is extended with the eIDAS implementing acts and eIDAS technical specification in particular the Commission Implementing Regulation (EU) 2015/1501 on the eID interoperability framework, the Commission Implementing Regulation (EU) 2015/1502 on Levels of Assurance (LoA), and the eIDAS Technical Specification version 1.1.

The e-SENS eID SAT refers to the following ABBs in the e-SENS Architecture Repository.

- Authentication Exchange Protocol[66];
- Quality Authentication Assurance[67];
- Authentication Exchange Forward[68].

4.2.2.1. Authentication Exchange Protocol ABB

This ABB addresses the protocol used to forward query and get replies from the Identity Provider and the Attribute Provider during a cross-border attribute exchange procedure and after an authentication procedure.

4.2.2.2. Quality Authentication Assurance ABB

Cross-border e-ID solutions are developed to allow citizens' access to some online service across-borders. A cross-border authentication infrastructure allows each country to keep the national authentication infrastructure already in place. However, each country specific authentication mechanism must be compared with those of other countries. This means that each country specific authentication framework must be mapped on a security level on the basis of a common QAA (Quality Authentication Assurance) framework.

The levels assigned to various eID solutions must be based on the most relevant security-related characteristics. The QAA framework must take into account both organizational and technical aspects, namely the identification procedure, the process of issuing identity tokens, the quality of the certification authority, the type and robustness of the identity tokens provided, and the quality of the mechanisms used for user authentication.

This ABB addresses the evaluation of the authentication quality level to determine the security strength of the adopted authentication procedure. It provides the framework to assign a quality level to different authentication solutions in comparable way.

4.2.2.3. Authentication Exchange Forward ABB

This ABB is concerned with the forwarding of authentication requests and response from/to the service provider to/from the Identity Provider. It is curial to perform secure transmission of the authentication information. Thus, PEPS (Pan-European Proxy Server) infrastructure, which provides confidential and robust channels to exchange authentication information, designed and developed in STORK and STORK2.0 projects. The e-SENS project handed over this ABB from STORK2.0 project.

[65] http://wiki.ds.unipi.gr/display/ESENS/SAT+-+eID+-+1.0
[66] http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Authentication+Exchange+Protocol+-+0.5.0
[67] http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Quality+Authentication+Assurance+0.8.0
[68] http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Authentication+Exchange+Forward+-+1.0.0

4.2.3. eSignature SAT

This section presents the building block in more detail, investigating the following aspects.

- Short overview of the building block;
- Availability of maintaining and supporting organisation for this building block;
- Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

The the-SENS e-Signature SAT[69] covers signature-creation (by the signatory) and signature-validation (by a relying party) as its core architecture framework. It relies on the EU e-Signature legislation (mainly the Signature Directive and the e-IDAS Regulation) as the legal backbone, the EU e-Signature Standards Framework as the interoperability backbone, respectively.

It has four ABBs in the e-SENS Reference Architecture:

- eSignature Creation ABB[70];
- eSignature Validation ABB[71];
- eSignature Mobile ABB[72];
- Federated Signing ABB[73].

The current maturity of the e-Signature building block ABBs is In Use Many Single-Domain for eSignature Creation and eSignature Validation ABBs, and In Development for Mobile e-Signature ABB.

4.2.3.1. eSignature Creation ABB

e-Signature Creation ABB is a service that uses an application to generate signatures that adhere to the specification. e-Signature Creation relates to 'electronic identification and authentication' Digital Service Infrastructure Building Blocks (DSI-BB) defined in the Draft guidelines for trans-European telecommunications networks (COM (2013) 329 final).

4.2.3.2. eSignature Validation ABB

Signature Validation Service is a service that uses an application to verify signatures according to the specification.

4.2.3.3. eSignature Mobile ABB

The e-SENS eSignature Mobile ABB focuses on mobile signature standards defined by ETSI Rationalised Framework for Enhanced Security Services (ESS). Mobile cutting-edge technologies have been assessed that can be used to improve existing mobile eID/e-signature solutions, e.g., with regard to user authentication and authorization. Furthermore, actions taken have targeted the provision of a ramp-up solution that supports European countries in deploying own mobile eID/e-signature solutions. A web application has been developed for this purpose that acts as interoperability layer between national infrastructure components and different mobile eID/e-signature solutions.

[69] http://wiki.ds.unipi.gr/display/20150515ESENS/SAT+-+eSignature+-+1.1.1
[70] http://wiki.ds.unipi.gr/display/ESENS/ABB+-+eSignature+Creation+-+1.1.2
[71] http://wiki.ds.unipi.gr/display/ESENS/ABB+-+eSignature+Validation+-+1.1.3
[72] http://wiki.ds.unipi.gr/display/ESENS/ABB+-+eSignature+Mobile+-+1.1.1
[73] http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Federated+Signing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.2.3.4. Federated Signing ABB

Federated signing is a model for electronic signing using a remote signing service where the user authenticates to the remote signing service using a federated identity service.

In traditional remote signing models, the signing service and the signer has a very close relationship caused by the fact that the singing service usually stores the signer's signing key and signature certificate. The user makes use of his/her stored signing key by means of authenticating to the singing service and expressing the will to sign a document.

In federated signing, due to the use of federated identity authentication, the user no longer needs to have a close relationship directly with the signing service. This is the key to the many advantages with federated signing and the primary reason why federated signing is so easy to deploy as cross-border signing solution.

In federated signing, the signing service can generate signatures for any person who can authenticate using a federated identity. This is made possible by having the user's identity provider (IdP) acting as a trust broker between the user and the signing service.

4.2.4. Non-Repudiation and Traceability

Non-Repudiation and Traceability covers the abilities to trace the origin and history of the artefacts (traceability), as well as to provide evidence concerning a claimed event or action (non-repudiation). The non-repudiation and traceability SAT of e-SENS project covers both topics[74]. It entails the following.

- Standard-based and trustable timestamp services (i.e. a qualified Time Stamp) are available on request for transactions and time-related provability needs;
- Evidence emitters are available based on XACML policies and obligations[75]. Evidence is returned to the original transaction initiator (as a signal message) or as a response to a request for evidence information regarding a particular transaction. Evidence can be consumed from evidence storages (notary services, audit record repositories) by authorized clients.

4.2.5. Trust Establishment

This section presents the building block in more detail, investigating the following aspects.

4.2.5.1. Short overview of the building block.

The Trust Establishment SAT [76] enables building trust in the online environment as stipulated by eIDAS. In line with the objectives of eIDAS, e-SENS provides Building Blocks to interconnect IT-solutions used by public administration, their providers and customers in different domains and/or EUMS in an interoperable, secure and trustworthy manner.

'SAT Trust Establishment identifies technical means to establish trust in and between IT-Systems involved in cross-border / cross-solution electronic transactions. These 'Trust Services' (TS) are electronic services which enhance trust and confidence in electronic transactions, provided by 'Trust Service Providers' (TSP). Consumers and Providers of the interconnected distributed solutions must be

[74] http://wiki.ds.unipi.gr/display/ESENS/SAT+-+Non-Repudiation+and+Traceability+1.3
[75] http://wiki.ds.unipi.gr/display/ESENS/Whitepaper+-+Non+Repudiation
[76] http://wiki.ds.unipi.gr/display/20150515ESENS/SAT+-+Trust+Establishment+-+1.2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

able to rely on and validate the authenticity and trustworthiness of each service / service-provider carrying out electronic transactions; this implies mutual trust between services/nodes involved.'[77]

'TSPs and their related service definitions have to be registered and supervised by means of a governance model and policy assessment process; Governance models and policies may differ according to domain-specific requirements. Trust Circle Management systems must provide registration, maintenance and lookup services for TSPs covered by this Trust Circle.' [78]

This SAT refers to the following ABBs in the e-SENS Architecture Repository[79]:

- Trust Network – Mutual Recognized Certificates[80];
- Trust Network – PKI[81];
- Trust Network – Trust Service Status List[82].

4.2.5.1.1. ABB Trust Network - Mutual Recognized Certificates

Mutual exchange of certificates is a widely used simple mechanism of the Direct Trust Model. Due to its restricted scalability, it may be a first choice for interacting communities with a manageable number of participants having knowledge from each other.[83]

Certificates are used for digital signatures on service-request and –response messages for purposes of authentication and integrity, for client authentication (e.g., SSL / TLS) and may optionally also be used for encryption of messages. The certificates are exchanged between all members of a Trust Domain (TD) and kept in a trusted Key Store by all TD nodes which mutually must authenticate each other.[84]

ETSI ESI Standards for Trust Service Providers Supporting Electronic Signatures[85]**:**

EN 319 401 General Policy Requirements for Trust Service Providers;

EN 319 411 Policy & Security Requirements for TSPs Issuing Certificates;

In particular:

Part 1: Policy requirements for TSPs issuing Web Site Certificates;

Part 2: Policy requirements for TSPs issuing Public Key Certificates;

EN 319 412 Certificate Profiles

In particular:

Part 1: Overview and common data structures;

Part 4: Certificate profile for Web Site Certificates issued to organisations;

TS 119 312 Cryptographic Suites;

EN 319 102 Procedures for Signature Creation and Validation;

EN 319 403 Trust Service Provider Conformity Assessment – requirements for conformity assessment bodies assessing Trust Service Providers;

[77] http://wiki.ds.unipi.gr/display/20150515ESENS/SAT+-+Trust+Establishment+-+1.2
[78] http://wiki.ds.unipi.gr/display/20150515ESENS/SAT+-+Trust+Establishment+-+1.2
[79] http://wiki.ds.unipi.gr/display/20150515ESENS/SAT+-+Trust+Establishment+-+1.2
[80] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=26183848
[81] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=26183843
[82] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=26183837
[83] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=18809140
[84] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=18809140
[85] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=18809140

Other related international standards, as far as not already referenced / profiled by the ETSI Standards:

RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2;

RFC 6066 Transport Layer Security (TLS) Extensions: Extension Definitions;

RFC 4510 Lightweight Directory Access Protocol (LDAP).

4.2.5.1.2. ABB - Trust Network – PKI

This Trust Establishment Model is based on using a single PKI issuing Certificates for all members of a Trust Domain (TD). The PKI may be a hierarchical one, having different sub CAs for different types of Trust Services Providers (TSPs) allocated to the Trust Domain. For an example, see e-SENS D6.1 Enterprise Interoperability Architecture n°1, section 6.3.5.7 Open PEPPOL Trust Network.[86]

Certificates are used for digital signatures on service–request and –response messages for purposes of authentication and integrity, for client authentication (e.g., SSL / TLS) and may optionally also be used for encryption of messages. Different from the Mutual Exchange of End Entity (Subject) Certificates, in this model only Issuer certificates are exchanged between all members of a Trust Domain (TD) and kept in a trusted Key Store by all TD nodes which mutually must authenticate each other.[87]

ETSI ESI Standards for Trust Service Providers Supporting Electronic Signatures[88]:

EN 319 401 General Policy Requirements for Trust Service Providers;

EN 319 411 Policy & Security Requirements for TSPs Issuing Certificates;

In particular:

Part 1: Policy requirements for TSPs issuing Web Site Certificates;

Part 2: Policy requirements for TSPs issuing Public Key Certificates;

EN 319 412 Certificate Profiles

In particular:

Part 1: Overview and common data structures;

Part 4: Certificate profile for Web Site Certificates issued to organisations;

TS 119 312 Cryptographic Suites;

EN 319 102 Procedures for Signature Creation and Validation;

EN 319 403 Trust Service Provider Conformity Assessment – requirements for conformity assessment bodies assessing Trust Service Providers.

Other related international standards, as far as not already referenced / profiled by the ETSI Standards:

RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2;

RFC 6066 Transport Layer Security (TLS) Extensions: Extension Definitions;

RFC 4510 Lightweight Directory Access Protocol (LDAP).

[86] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=23003200

[87] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=23003200

[88] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=23003200

4.2.5.1.3. ABB - Trust Network – Trust Service Status List

Trusted Lists (TL) were established by the Commission Decision 2009/767/EC as amended by the Commission Decision 2010/425/EU. TLs aim at supporting the validation of Qualified Electronic Signatures (QES) and Advanced Electronic Signatures (AdES) supported by a Qualified Certificate (AdESQC) in the meaning of Directive 1999/93/EC as EUMS are obligated to expose actual and historical status information on supervised/accredited CSPs established in their country offering qualified certificates. TLs enable EU-wide validation of service supervision/accreditation status and hence quality of Trust Service Providers (TSPs) issuing (qualified) certificates.[89]

ETSI ESI Standards for Trust Service Providers Supporting Electronic Signatures[90]:

EN 319 401General Policy Requirements for Trust Service Providers;

EN 319 411Policy & Security Requirements for TSPs Issuing Certificates;

In particular:

Part 1: Policy requirements for TSPs issuing Web Site Certificates;

Part 2: Policy requirements for TSPs issuing Public Key Certificates;

EN 319 412Certificate Profiles

In particular:

Part 1: Overview and common data structures;

Part 4: Certificate profile for Web Site Certificates issued to organisations;

TS 119 312Cryptographic Suites;

EN 319 102Procedures for Signature Creation and Validation;

EN 319 403Trust Service Provider Conformity Assessment – requirements for conformity assessment bodies assessing Trust Service Providers.

ETSI ESI Standards for Trust Service Status Lists Providers:

TR 119 600Business Driven Guidance for Trust Service Status Lists Providers;

EN 319 601General Policy & Security Requirements for Trust Service Status Lists Providers;

EN 319 611Policy & Security Requirements for Trusted List Providers;

TS 119 602Trust Service Status Lists Format;

TS 119 612Trusted Lists;

EN 319 603General requirements and guidance for Conformity Assessment of TSSLPs;

EN 319 613Conformity Assessment of Trusted List Providers.

Other related international standards, as far as not already referenced / profiled by the ETSI Standards:

RFC 5246 the Transport Layer Security (TLS) Protocol Version 1.2;

RFC 6066 Transport Layer Security (TLS) Extensions: Extension Definitions;

RFC 4510 Lightweight Directory Access Protocol (LDAP);

OASIS-Standards;

Web Services Security SOAP Message Security Version 1.1.1, 18 May 2012;

WS-Security Policy 1.2, 1 July 2007;

[89] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=26183837

[90] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=26183837

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Web Services Security X.509 Certificate Token Profile 1.1.1, 18 May 2012.

4.2.5.2. Availability of maintaining and supporting organisation for this building block.

CEF has adopted term Trust Establishment, but somewhat differently regarding e-SENS approach. It has been placed within CEF architectural framework as a service within BB eDelivery[91]. CEF eDelivery trust models are all based on digital certificates. The way these digital certificates are used in 'run time' to secure the communication between Access Points is shown below.

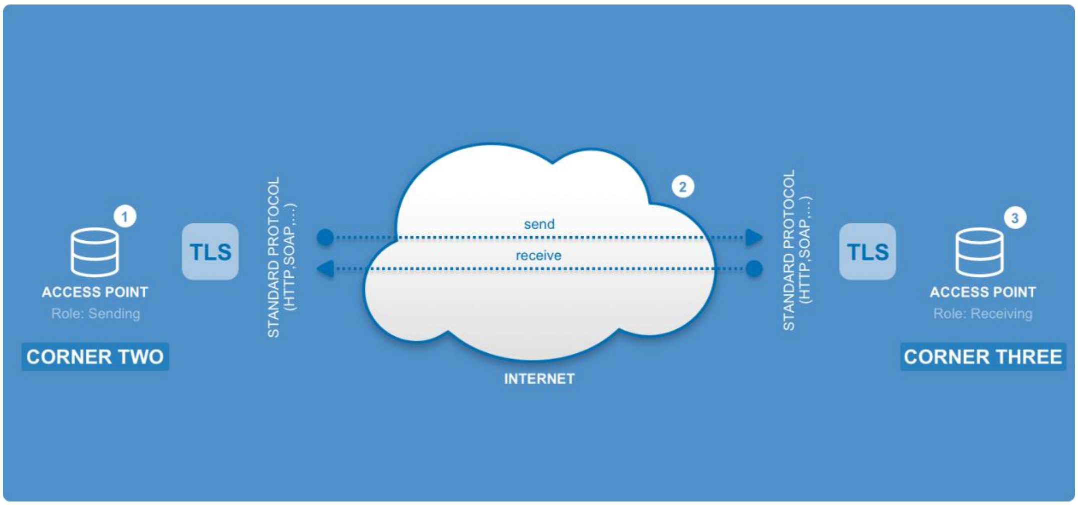


Figure 3: Digital certificates usage to secure the communication between Access Points[92]

- The sending Access Point uses its digital certificate to sign the data and documents, it may also encrypt it using the public key of the receiver;
- The receiving Access Point confirms the digital signature of the sender and decrypts the data using its digital certificate;
- The receiving Access Point sends a signed receipt message to the sending Access Point.

Two trust models are available to create, manage, distribute, store and revoke the digital certificates of the Access Points: either PKI model or a mutual exchange model of digital certificates. The communication between SMP and SML components is secured through two-way TLS.

CEF eDelivery Building Block covers next services:

- PKI service[93];
- Interoperability testing[94];
- Conformance testing[95];
- Deployment service[96];
- Self-assessment tool[97].

[91] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Trust+Establishment
[92] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Trust+Establishment
[93] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service
[94] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Connectivity+testing
[95] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Conformance+testing
[96] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Training+and+Deployment
[97] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home

4.2.5.3. Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

e-SENS defined Trust and Security mechanisms rely on the well-established PKI infrastructure and usage of X509v3 certificates[98] and cryptographic mechanisms to authenticate and secure electronic transactions in distributed environments. X509v3 certificates are used as digital identities of trusted services and their providers.[99]

Parts of Trust Service Status List ABB's functionality are given by infrastructure components implementing SSL/TLS and/or SOAP Message Security (according to the OASIS WS-Security 1.1.1 specification).[100]

Trust List Maintainer, a 'TLManager' is made available by the EC in Joinup. Joinup is a collaborative platform created by the European Commission and funded by the European Union via the" Interoperability solutions for public administrations, businesses and citizens"[101] (ISA2) Programme. It offers several services that aims to help e-Government professionals share their experience with each other. We also hope to support them to find, choose, re-use, develop and implement interoperability solutions.[102]

ETSI provides a 'TSL Conformance Checker'[103].

For Trust List Lookup, implementations have been done by LSPs PEPPOL and SPOCS.

4.2.6. eDocument

This section presents the building block in more detail, investigating the following aspects.

- Short overview of the building block;
- Availability of maintaining and supporting organisation for this building block;
- Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

4.2.6.1. Short overview of the building block

This section provides an overview of the eDocument SAT[104], consolidated by the e-SENS project, highlighting its component architectural blocks and the specifications and standards that can be utilized for specifying and building applications.

The eDocument SAT provides solution architects with a template to be used in creating interoperable and reusable building blocks that support the handling of e-Documents by the public administration. It provides a common and unambiguous terminology and approach to cope with the interoperability needs of electronic document services and an easy integration into existing IT infrastructure due to its service-oriented architecture and loose-coupling with other components.

An e-Document instance may carry messages that are intended to be consumed in a programmatic way by the recipient. This implies the message-oriented document is structured and each element of

[98] https://www.itu.int/rec/T-REC-X.509

[99] http://wiki.ds.unipi.gr/display/20141201ESENS/SAT+-+Trust+Services

[100] http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html

[101] https://ec.europa.eu/isa2/

[102] https://joinup.ec.europa.eu/software/tlmanager/release/all

[103]http://portal.etsi.org/Services/CentreforTestingInteroperability/Activities/ElectronicSignature/TSLConformanceproject.aspx

[104] http://wiki.ds.unipi.gr/display/ESENS/SAT+-+eDocument+-+0.6.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

the e-document structure or schema has been agreed and incorporated into the contract between the e-Document producer and consumer.

The e-Document proposed solutions result in the following e-Document services: transformation and structuring, presentation and processing, profiling, packaging and document routing.

The eDocument SAT comprises specific architectural building blocks which support the corresponding application services:

1. **Document Provisioning** ABB: it describes how to produce and consume an e-Document. The reason for merging the producer and consumer's functionality is because part of it is common to both (e.g., the validation, transforming a document to another format, etc);
2. **Document Container** ABB: it includes specifications for the container format and it is useful in case there are specific requirements for attaching additional documents to the message such as signatures, additional metadata, schematron rules, annotations, etc. If no additional information is needed the recommendation is not to use the container as it is adding up to the complexity;
3. **Document Business Envelope** ABB: includes specifications for the routing envelope which should be used when high level metadata describing the business context of the document is needed or in collaboration to eDelivery solutions.

4.2.6.1.1. Document Provisioning

Document Provisioning[105] is a reference architecture model, in line with EIRA architecture principles defined by Interoperability Solutions for European Public Administrations (ISA) Programme[106], and is responsible for the provision of any electronic document. Its main objective is to ensure the technical, the syntactic interoperability in the e-Documents domain.

The e-Document Production model comprises one or more of the following activities related to an e-Document:

- convert or transform;
- structure;
- attach business rules;
- validate;
- annotate.

These activities correspond to the functions defined and supported by Document Provisioning as follows:

Conversion and Transformation

The conversion functionality provides guidelines for e-Documents that might require to be converted from one file type to another, thus ensuring the technical interoperability between the parties involved in a message exchange. In addition to the conversion function, a transformation function is also supported which refers to the construction of a second XML tree from a source XML tree in order to achieve the syntactic interoperability.

[105] http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Document+Provisioning+-+0.7.0

[106] http://ec.europa.eu/isa/

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Structuring

The structuring functionality is covered by the e-Document engineering methodology defined in 'Guidelines for public administrations on e-Document engineering methods'[107] by ISA. The process of creating a customized e-Document exchange format is called Application Profiling.

Annotation

The Annotation functionality refers to textual comment or a note that is about, or refers to, an e-Document or an identifiable data element. The recommended specification is 'Open Annotation (OA) Data Model'[108] defined by the W3C Open Annotation Community Group[109]. This functionality covers annotation requirements that may arise in a specific domain without the need to modify their e-Document formats.

All the annotations must be placed in a single annotation document, a special structured JSON document that will conform to a predefined schema which will be packed together with its associated electronic document in an eDocument container format.

Business Rules

The validation process of an e-Document assures its conformance to an agreed e-Document format and other business rules defined. For achieving this task, e-SENS Document Provisioning ABB recommends the usage of 'Schematron'[110], a rule-based XML schema language which is an ISO/IEC standard along with 'XML Path Language (XPath) 2.0'[111] expressions, a W3C Recommendation, in order to serialize and attach to an e-Document many of the business rules defined. Schematron detects the presence or absence of patterns in an e-Document and reports the result.

Extraction or Presentation

The final steps of the process model outlined in Document Provisioning is the extraction of structured information which refers to an e-Document and the presentation of these data to the end user.

4.2.6.1.2. Document Container

eDocument provides for Document Packaging ABB[112] an eContainer format. The eContainer specifications include functions to cover the container structure, detailed example on the usage of the container with signatures and timestamps and document level encryption.

Document Packaging ABB provides the following services:

- Packaging: forms the structure of the container and ensures container integrity validation;
- Attaching Signatures: adding signatures and reference the signed documents;
- Attaching Timestamps: adding trusted timestamp;
- Document encryption: encrypting documents inside container;
- Logging: log document operations in context to support audit trailing.

e-SENS Container defines a profile for eDocuments that provides the necessary features for public administration use cases, and not only, as it is applicable to a wide range of communities when there

[107] https://joinup.ec.europa.eu/sites/default/files/4d/23/56/ISA%20Programme%20-%202014%20-%20Guidelines%20for%20public%20administrations%20on%20e-Document%20engineering%20methods_v1.00.pdf

[108] http://www.openannotation.org/spec/core/

[109] https://www.w3.org/community/openannotation/

[110] http://standards.iso.org/ittf/PubliclyAvailableStandards/c040833_ISO_IEC_19757-3_2006(E).zip

[111] http://www.w3.org/TR/xpath20/

[112] http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Document+Container+-+0.6.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

is a clear need for interoperability of Advanced Signatures (XadES[113], CadES[114]), trusted timestamp usage, document encryption and journaling to be interchanged across borders.

The specification proposed for the Container are ASiC Specifications 'ETSI TS 102 918 V1.1.1 (2011-04) Electronic Signatures and Infrastructures (ESI)'; 'Associated Signature Containers (ASiC)'[115] and 'ASIC Profile ETSI TS 103 174 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI)'; 'ASiC Baseline Profile'[116].

4.2.6.1.3. Document Routing

Document Business Envelope ABB[117] ensures adding the information required to electronically deliver the e-Documents from one participant involved in a transaction to another, thus supporting automated business processes.

The information added could be the receiver and the sender address, the type of the payload and the business scope. The envelope carries sufficient information about its included payload allowing the recipient to decide the appropriate processing of the payload.

For e-SENS routing functionality the recommended standard is 'UN/CEFACT Business Document Header SBDH'[118] that facilitates: routing of business documents from one point to another through eDelivery services, associating a data message with its originator which is important from a business and legal perspective and encoding information on business process, business transaction, agreement, and business quality-of-service.

4.2.6.2. Availability of maintaining and supporting organisation for this building block.

The e-Documents SAT, developed by the e-SENS project, is envisaged to be taken over by CEF after an analysis that will be carried out in the summer of 2017.

4.2.6.3. Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

Document Container is based on ASiC specification which is maintained by ETSI, an organisation producing a range of specifications, standards, reports and guides, each with its own particular purpose. ASiC has been implemented in several projects and is still running in various open source implementations.

Document Routing relies on SBDH specification maintained by GS1[119] organisation, an organisation which provides and maintains several industry standards regarding the identification, capturing and exchange of business-critical information.

Document Provisioning includes W3C XSL, XSLT[120], Schematron, Open Annotation (OA) Data Model specifications.

[113] http://uri.etsi.org/01903/v1.3.2/ts_101903v010302p.pdf

[114] http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/01.07.04_60/ts_101733v010704p.pdf

[115] http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.01.01_60/ts_102918v010101p.pdf

[116] http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.01.01_60/ts_103174v020101p.pdf

[117] http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Document+Business+Envelope+-+0.6.0

[118] http://www.gs1.org/standard-business-document-header-sbdh

[119] http://www.gs1.org/

[120] http://www.w3.org/TR/xslt

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

XSL is a family of recommendations, maintained by W3C organisation, for defining XML document transformation and presentation. It consists of three parts: XSL Transformations (XSLT) a language for transforming XML, XML Path Language[121] (XPath) an expression language used by XSLT (and many other languages) to access or refer to parts of an XML document and XSL Formatting Objects[122] (XSL-FO) an XML vocabulary for specifying formatting semantics.

Schematron has been standardized by the ISO as 'Information technology, Document Schema Definition Languages (DSDL), Part 3: Rule-based validation, Schematron' (ISO/IEC 19757-3:2016). This standard is available free on the ISO Publicly Available Specifications[123] list. Schematron is a rule-based validation language for making assertions about the presence or absence of patterns in XML trees.

Open Annotation (OA) Data Model is a W3C specification defining an interoperable framework for creating associations between related resources, annotations, using a methodology that conforms to the Architecture of the World Wide Web. Open Annotations can easily be shared between platforms, with sufficient richness of expression to satisfy complex requirements while remaining simple enough to also allow for the most common use cases, such as attaching a piece of text to a single web resource.

The e-Document engineering methodology, covering the structuring functionality, is defined in 'Guidelines for public administrations on e-Document engineering methods' methodology and is maintained by ISA programme[124].

4.2.7. Semantics: existing building blocks

This section presents the building block in more detail, investigating the following aspects.

- Short overview of the building block.
- Availability of maintaining and supporting organisation for this building block.
- Availability of specifications and software that can be utilized for specifying and building applications that use this building block.

The e-SENS Semantics SAT[125] aims at creating a layer of semantic resources, concepts and codes, as well as creating the services to enable semantic mappings between terms and resources or between terms.

This SAT refers to the following ABBs in the e-SENS Architecture Repository: Semantic Mapping Service; Terminology Service; Domain Knowledge Management System. In addition to the ABBs of e-SENS the ISA2 program also defines components that are usable as semantic building blocks. These are also dealt with below.

4.2.7.1. e-SENS Semantic Mapping Service

See: http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Semantic+Mapping+Service-new.

The provision of public services requires several documents to be submitted. However, all documents are not named in the same way in all countries and certain documents do not exist in all countries. Moreover, some documents are not official and have to comply with several criteria defined in the procedure itself. Thus, the equivalence between documents is essential to enable cross-border services and transactions in Europe. The Semantic Mapping Service aims to offer interoperability from

[121] http://www.w3.org/TR/xpath
[122] http://www.w3.org/TR/xsl
[123] http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
[124] https://ec.europa.eu/isa2/
[125] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=26182414

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

a legal and official document perspective. In this way, the user should be able to retrieve personalised information about the process and required documents according to the country of origin, the type of business/activity and the location of offered services.

Semantic technologies provide many concepts and tools to make machine-understandable descriptions of data, programs, and infrastructure, thus enabling the interoperability with the provision of document equivalence mapping. Core Vocabularies are the starting point for defining mappings to guarantee cross-domain and cross-border interoperability that can be attained by interoperability agreements between Public Administrations and Service providers.

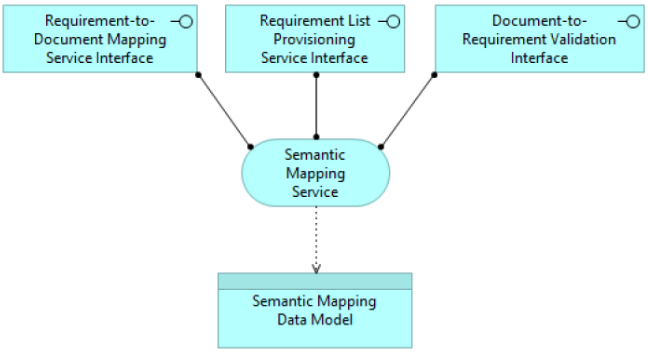

Requirement-to-Document Mapping Service Interface
Requirement List Provisioning Service Interface
Document-to-Requirement Validation Interface
Semantic Mapping Service
Semantic Mapping Data Model

Figure 4: Archimate Application View, showing the Service's application interfaces

In a nutshell, the Semantic Mapping Service offers the following functionalities: i) provision of a requirement list mapped in the requesters national legislation and the EU directives, ii) provision of a requirement-to-Document mapping based on the requestor's national legislation and iii) provision of a validation service stating that the actual documents provided are fit for the mapped requirements.

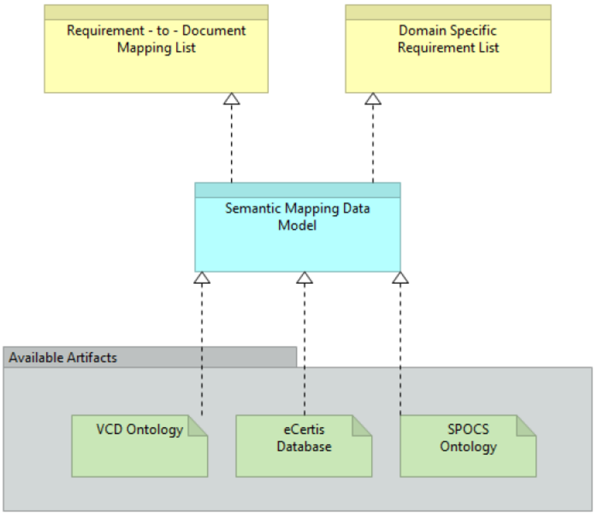

Requirement - to - Document Mapping List
Domain Specific Requirement List
Semantic Mapping Data Model
Available Artifacts
VCD Ontology
eCertis Database
SPOCS Ontology

Figure 5: Archimate Information View

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.2.7.1.1. e-CERTIS

For the eProcurement domain, there is e-Certis 2.0[126] that has been implemented by DG GROW. e-Certis is aligned with the e-SENS Semantic Mapping Service and particularly in its multi-domain applicability which is part of the design and in which e-SENS contributed to. The e-Certis service implements the three application interfaces of the ABB, by providing a mapping of the EU Directive for eProcurement (2014/24/EU) with the Member State legislation, and the Member State legislation with the evidence/attestations that prove the legislation requirements. The e-Certis service is currently live and considered in production and it is being used to provide semantic mapping in the ESPD (European Single Procurement Document) services and the VCD (Virtual Company Dossier) services and artefacts.

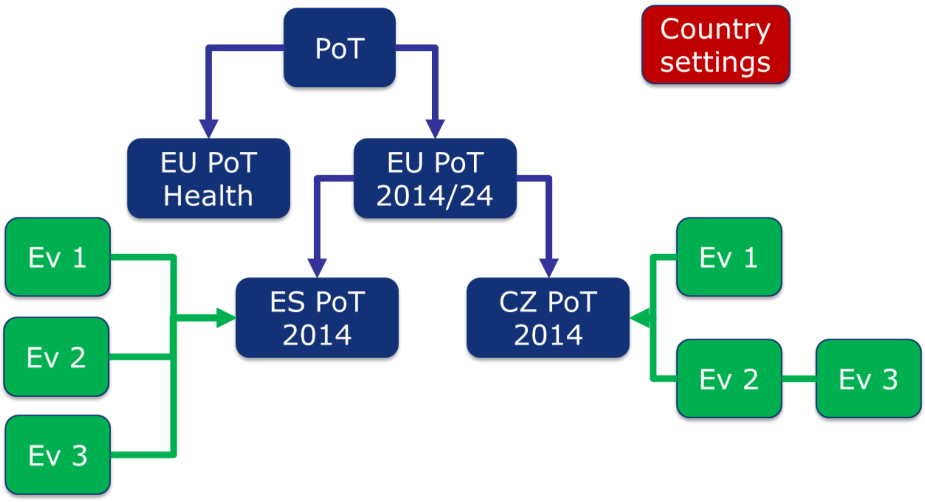


Figure 6: Example Instance - Payment of Taxes Criterion, as implemented in e-Certis 2.0

e-Certis has been used to provide a proof-of-concept in the e-SENS Business Registration pilot for mapping documents / evidences required when an Economic Operator wants to establish a new business via a cross-border electronic service.

4.2.7.2. e-SENS Base Registry Service

The e-SENS project has worked on the Terminology Service. This service has been renamed to the Base Registry Service by the end of the project. A base registry (BR) is a trusted authentic source of information under the control of an appointed public administration or organization appointed by government. In the e-SENS environment it can be a source of information that is trusted as authentic by a community of users. This is the ISA definition and it is a generalization of the terminology server BB. Here the trusted information can be of any type while the terminology server is a trusted source for [127] This Building Block complements the Trust Models with trusted Information Sources. ISA defines

[126] https://ec.europa.eu/growth/tools-databases/ecertis/

[127] ISA Definitions: http://ec.europa.eu/isa/actions/documents/isa_1.2_d1.2_base_registry_definition.pdf
A base registry (BR) is a trusted authentic source of information under the control of an appointed public administration or organization appointed by government, whereby:
• Trusted means that the governing administration/organization is managing the registry/source conformant to best practices in all EIF-domains (not the least semantics/security) and conformant to legal/regulatory requirements
• Authentic means that it is recognized as THE source, which represents the correct status of information.
It is kept constantly up-to-date and of the highest possible quality

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

an abstract model for base registries, but the Base Registry Service implements these registries in the form of services (already called terminology services in e-SENS) that leverage servers (terminology server). The main example is the e-CERTIS portal in ESPD –VCD pilot, but also SMP and SML are trusted sources.

4.2.7.3. e-SENS Domain Knowledge Management System

The page on the e-SENS WIKI for this e-SENS building block is not accessible as a log in is necessary. Therefore, the exact status of this building block is not possible to describe.

4.2.7.4. ISA2 Core Person Core Vocabulary

See: https://joinup.ec.europa.eu/asset/core_person/description

The Core Person Vocabulary is a simplified, reusable and extensible data model that captures the fundamental characteristics of a person, e.g., the name, the gender, the date of birth, the location.

4.2.7.5. ISA2 Registered Organisation Core Vocabulary

See: https://joinup.ec.europa.eu/asset/core_business/description

The Core Business Vocabulary is a simplified, reusable and extensible data model that captures the fundamental characteristics of a legal entity, e.g., the legal name, the activity, address, etc. An RDF syntax of the Core Business Vocabulary has now been formally published on the W3C standards track as a First Public Working Draft. It has been revised and renamed into Registered Organization Vocabulary[128] (RegOrg) and it is now an extension of the broader Organization Ontology[129](Org).

The objective of these changes is to achieve better alignment with the broader Organization Ontology, which describes core ontology for organizational structures. However, the fundamentals of the Core Business Vocabulary[130] remain unchanged, in particular the use of the ADMS[131] Identifier class to capture the actual registration information.

Together, Org and RegOrg offer a powerful means to describe any organization, its organizational units, its registered entities, its locations and its staff. The ISA program is also currently further building on these vocabularies in the Core Public Service Vocabulary Working Group[132].

Initially, this vocabulary was created by a group chaired by DG MARKT of the European Commission and sponsored by the ISA Program. This core vocabulary was designed to enable interoperability

- Under control, means that only parties that have a necessity & finality & authorization can access the information in proportionality with their needs.
- Appointed means: that the governing administration/organization has a legal basis / authority to collect and maintain the respective information.

A cross-border interoperable base registry (CIBR) is a base registry, opened through a single point of access to two or more electronic public services in other countries, using a multilingual interface and a standardized interface format and protocol. The CIBR is managed and operated by a legally based governance model providing cross-border interfacing services to electronic public services.

[128] http://www.w3.org/TR/vocab-regorg/

[129] http://www.w3.org/TR/vocab-org/

[130] https://joinup.ec.europa.eu/asset/core_business/description

[131] https://joinup.ec.europa.eu/asset/adms/description

[132] http://joinup.ec.europa.eu/asset/core_public_service/description

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

among business registers and any other ICT based solutions exchanging and processing information related to registered businesses.

4.2.7.6. ISA2 Core Location Vocabulary

See: https://joinup.ec.europa.eu/asset/core_location/description

The Core Location Vocabulary is a simplified, reusable and extensible data model that captures the fundamental characteristics of a location, represented as an address, a geographic name, or a geometry. The Core Location Vocabulary is one of the three Core Vocabularies that have been developed in the context of Action 2.1[133] of the (ISA²) programme[134]. The specification is developed by a multi- disciplinary Working Group[135], with a total of 69 people from 22 countries, 18 EU and 4 non-EU countries (USA, South-Africa, Norway and Croatia), and several EU Institutions.

4.2.7.7. ISA2 Core Public Service Vocabulary

See: https://joinup.ec.europa.eu/asset/core_public_service/description

Public services have been documented to follow different flavours of national, regional and local public service models even if within the same country. At the same time, several e-Government portals within the EU are currently delivering public services in an unstructured and non-machine-readable way. This results in delivering low quality public services and, hence, increases the administrative burden as well as the cost of the public service provision.

The Core Public Service is a simplified, reusable and extensible RDF vocabulary designed under the auspices of the ISA programme of the European Commission (Interoperability Solution for European Public Administrations) to describe and homogenise public service data that originates from local, regional, and national public administrations in a technology independent way. The vocabulary emerges as the common denominator of existing national, regional and local public service models, providing a lingua franca that enables the seamless exchange of services and information across different e-Government systems. It is a Core Vocabulary which means that it represents a simplified data model that (i) captures the minimal, global characteristics/attributes of an entity in a context-neutral fashion, (ii) is highly reusable, and (iii) is extensible. Examples of the fundamental characteristics of the Core Public Service Vocabulary include the title, description, inputs, outputs, providers, locations, etc. of a public service. The Core Public Service vocabulary promises to facilitate:

- searching for public services that address the same need across different e-Government portals
- discovering information about a particular public service even from cross-border portals that use different structures and service models
- aggregating or combining public service data from e-Government portals of different levels of public administration
- creating re-usable machine-readable public service descriptions that follow the Linked Open Government Data paradigm

[133] http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-1action_en.htm

[134] http://ec.europa.eu/isa/isa2/index_en.htm

[135] https://joinup.ec.europa.eu/asset/core_business/document/core-vocabularies-working-group-members

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.2.7.8. ISA2 Core Criterion and Core Evidence Vocabulary

See: https://joinup.ec.europa.eu/asset/criterion_evidence_cv/description

The Core Criterion and Core Evidence Vocabulary (CCCEV) is designed to support the exchange of information between organizations defining criteria and organizations responding to these criteria by means of evidences. By using the CCCEV, public organisations have the potential to implement new capabilities in their information systems to:

- Allow users picking up criteria from common repositories, standardising the criteria used in different sectors and domains.
- Enable the automatic response to criteria, lowering the language barrier for cross-border processes and exchanges.
- Automatic assessment through the analysis of criteria and provided evidence.
- Promote the standardisation of criteria and evidence among attestation and certificate providers, and even across different Member States.
- Increase the transparency of the assessment and therefore the selection processes, reducing complains and a subjective assessment.

4.2.7.9. ISA2 Core Public Organisation Vocabulary

See: https://joinup.ec.europa.eu/asset/cpov/description

The Core Public Organisation Vocabulary aspires to become a common data model for describing public organisations in the European Union.

4.3.Building Blocks from Other Sources

4.3.1. X-Road

X-Road is a system for enabling secure and interoperable communication between organizations.

The following list contains main design goals and design decisions of the X-Road system[136].

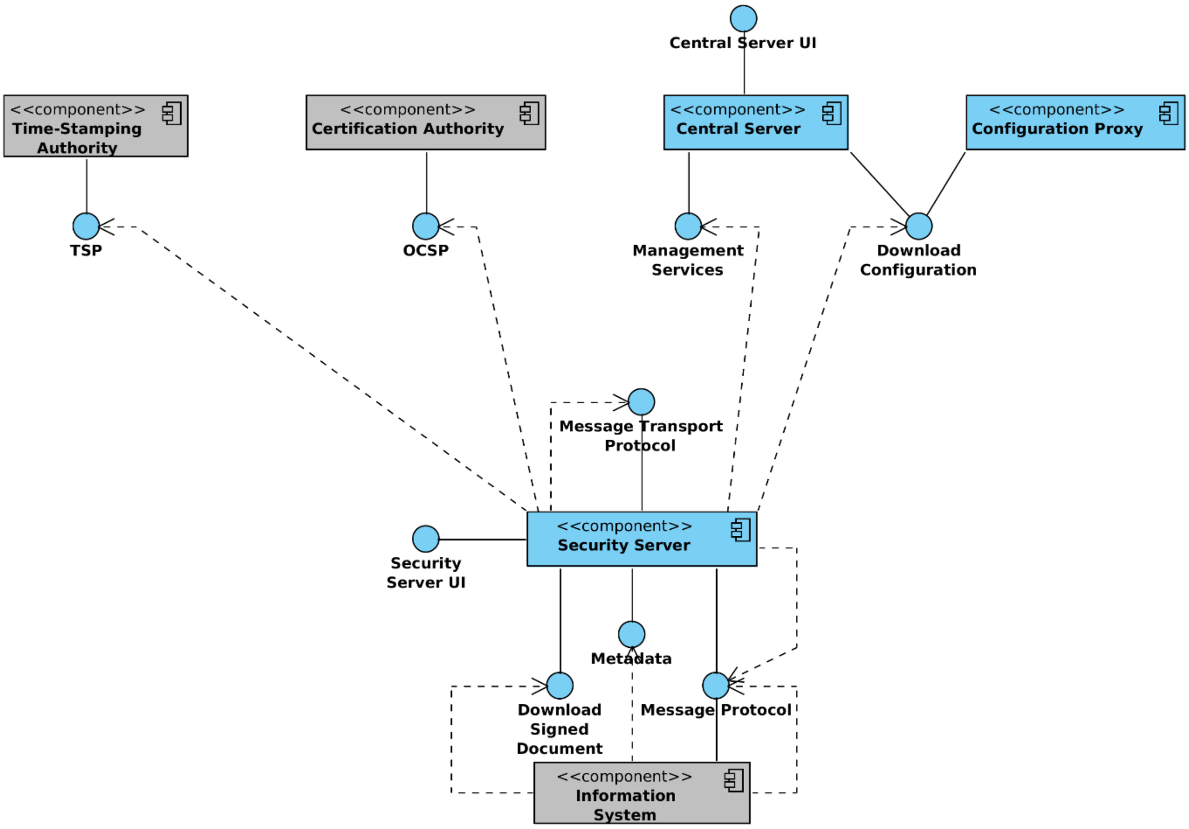
- X-Road is **decentralized** – the data exchange happens directly between organizations. There are no intermediaries. If the two organizations have established secure connection, the continuous data exchange depends only on availability of the organizations and the network between them.
- **Ownership of data** – X-Road does not change ownership of data. The data owner (service provider) controls who can access particular services.
- **Availability** is a central concern – the protocols are designed so that there is no single bottleneck in the system. Additionally, no component should become a single point of failure.
- All the messages processed by the X-Road are usable as **digital evidence**. The technical solution must comply with requirements for digital seals according to eIDAS. This implies support for secure signature creation devices (SSCDs).
- All the communication is implemented as **service calls** using the SOAP protocol. The services are described using the WSDL language.
- **Cross-border services** – it is possible for an organization to invoke services provided by an organization belonging to a different instance of X-Road.

[136] https://www.ria.ee/riigiarhitektuur/wiki/lib/exe/fetch.php?media=an:x-tee_kohtumised:arc-g_x-road_arhitecture_1.2_y-879-3.docx

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- **Encapsulating the security protocol** – the security measures and the security protocol are encapsulated in standard components. The organizations are not required to implement security-related functionality for data exchange.
- **Standardization** – X-Road aims to standardize the communication protocol between organizations. This enables the organizations to connect to any number of service providers without implementing additional protocols. X-Road core does not perform protocol and data conversion. If necessary, these conversions can be performed by the organization's information system.
- **No predetermined roles** – once an organization has joined the X-Road infrastructure, it can act as both service client and service provider without having to perform any additional registration.
- **Two-level authentication** – X-Road core handles authentication and access control on the organization level. End-user authentication is performed by information system of the service client.

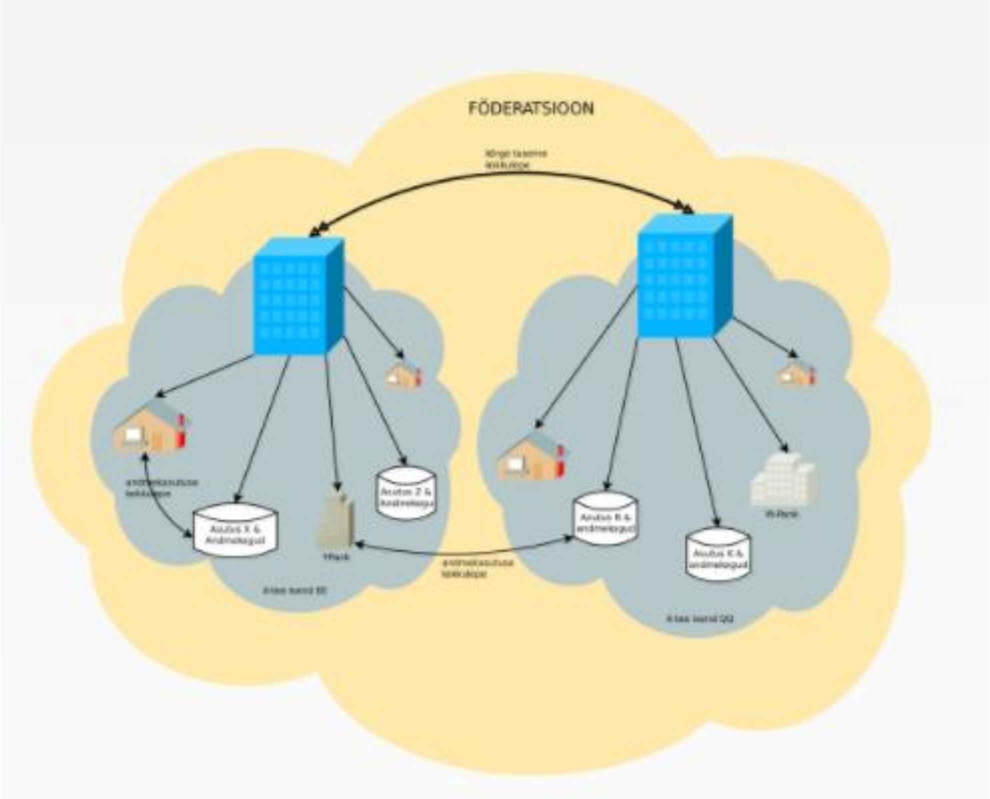
The following figure shows the main components and interfaces of the X-Road system.


Central Server UI
<<component>> Time-Stamping Authority
<<component>> Certification Authority
<<component>> Central Server
<<component>> Configuration Proxy
TSP
OCSP
Management Services
Download Configuration
Message Transport Protocol
Security Server UI
<<component>> Security Server
Metadata
Download Signed Document
Message Protocol
<<component>> Information System

X-Road can be deployed in a trust federation where separate ecosystems, each having their own central components are able to communicate with each other. This architecture is illustrated in the figure below[137].

[137] https://www.ria.ee/en/x-road-trust-federation.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460



4.3.1.1. Need for this building block

X-Road is suitable for secure and interoperable data exchange between organisations. It has a proven track record and more than one countries have deployed it. It is suitable for situations where countries wish to govern their own ecosystems but organisations within those organisations are still able to communicate directly with each other. It is suitable to use at a global scale, e.g. as is envisaged in Pilot Area 3. If other building blocks do not allow for this then X-Road should be considered or other BB-s should be modified accordingly.

4.3.1.2. Adequacy of Specifications and Software

X-Road, its components and protocols are open source and documented[138].

4.3.1.3. Adequacy of Maintaining and Supporting Organisation

X-Road is jointly developed by Estonia and Finland. Since both countries' governments' functioning depend on X-Road, it is maintained and developed continuously. The components are not complicated to deploy: all required documentation exists and free online training courses for service developers and system administrators[139] are available[140].

[138] https://github.com/ria-ee/X-Road
[139] https://moodle.ria.ee/course/view.php?id=7&section=2
[140] https://moodle.ria.ee/course/view.php?id=15

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.3.1.4. Need for Further Development

X-Road is fully functioning. In 2016 there were 246 databases, 975 institutions, 1789 services on X-Road processing 574,6 million inquiries[141] in Estonia (data per year 2016).

4.3.1.5. External Interfaces for X-Road

All components are open source and available to deploy with installation and user guides.

[141] https://www.ria.ee/en/statistics-about-x-road.html

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

5. Views, Building Blocks, and Interface Specifications for OOP Architecture

This chapter presents views, building blocks, and interface specifications for OOP architecture. Conceptual and business views are provided in Chapter 5.1. Chapter 5.2 investigates in more detail the building blocks needed for the pilots as well as for OOP applications in general, providing principles of selection of building blocks for OOP applications and several types of high-level view of the architecture with selected building blocks.

Analysis of selected building blocks with respect to their relevance, applicability, sustainability, need for further development, and external interfaces are provided in Chapters 5.3 to 5.10. The list of building blocks in this chapter may be complemented in future versions of the architecture.

5.1.Conceptual and Business Views

Based on the TOOP focus area and the requirements for the OOP architecture, the following figure depicts a conceptual view of a simplified cross-border OOP case. It includes the data consumer and data provider, who can communicate via the TOOP federation infrastructure by different means: by using an OOP layer, with the aid of data aggregators, or by direct communication.

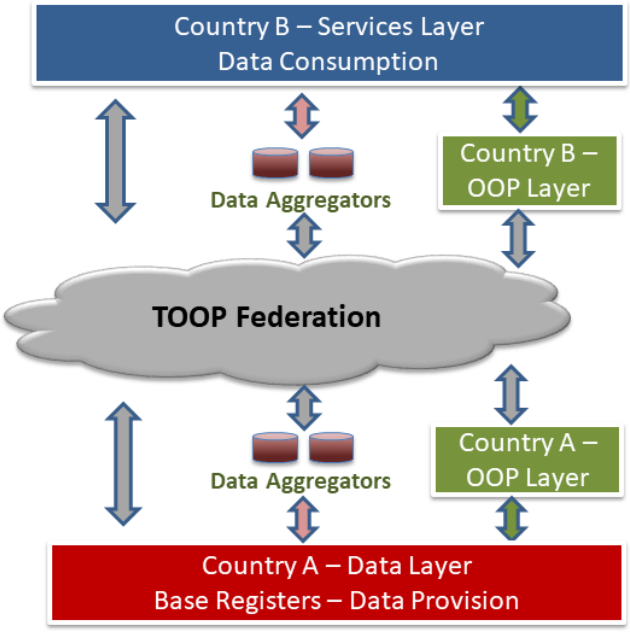


Figure 7: The Cross-Border OOP Case (Simplified)

Complementing this view with domain-specific data consumers and providers gives the following view. It comprises an additional possibility of communication through domain federation in case of a well-defined and standardised domain.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

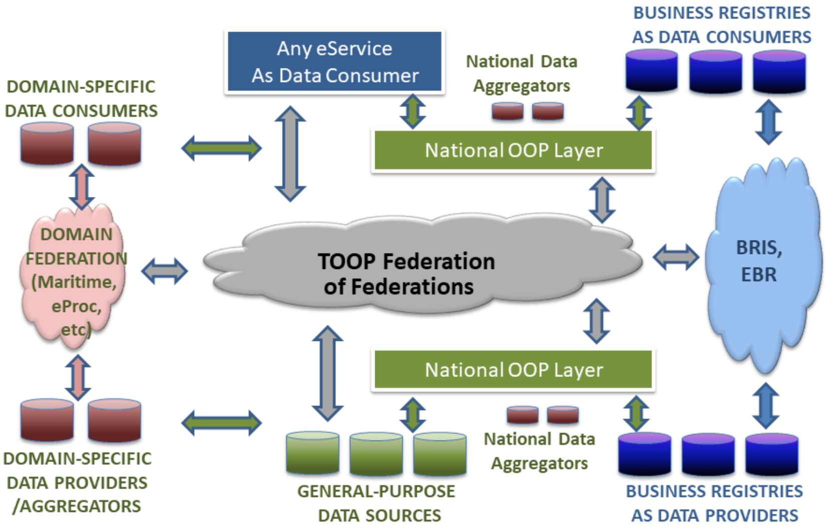

BUSINESS REGISTRIES AS DATA CONSUMERS
Any eService As Data Consumer
National Data Aggregators
DOMAIN-SPECIFIC DATA CONSUMERS
National OOP Layer
DOMAIN FEDERATION (Maritime, eProc, etc)
TOOP Federation of Federations
BRIS, EBR
National OOP Layer
National Data Aggregators
DOMAIN-SPECIFIC DATA PROVIDERS /AGGREGATORS
GENERAL-PURPOSE DATA SOURCES
BUSINESS REGISTRIES AS DATA PROVIDERS

Figure 8: How TOOP Pilots Fit into the Big Picture

The baseline pull scenario (the data consumer requests business data from data provider in another country) is depicted on the following figure. Another important case is the push scenario, where the data consumer subscribes to a notification service offered by the data provider. This scenario, along with selected other scenarios from those introduced in the requirements chapter, will be further studied, analysed, amended, enhanced and elaborated in the forthcoming deliverables.

These scenarios depict applications that satisfy the requirements in Chapter 3, but by themselves they are not requirements, as the applications in TOOP focus area may be implemented in many different ways.

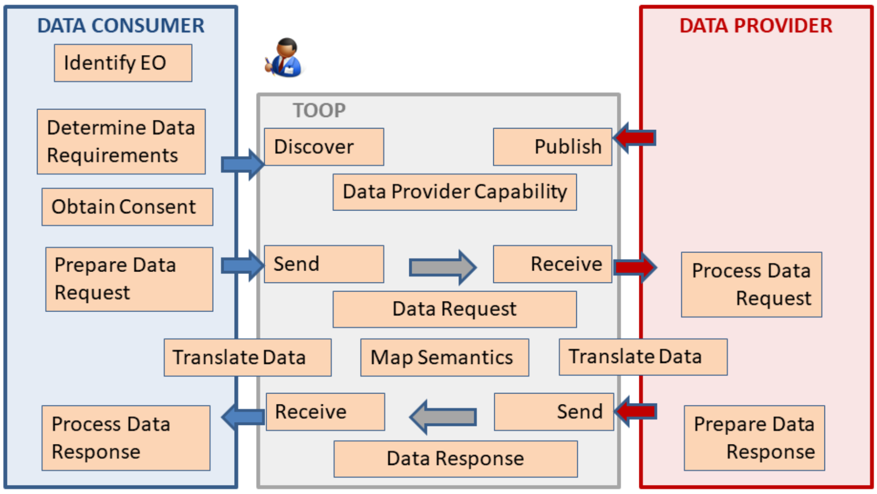


Figure 9: Baseline Scenario: Simple Pull

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

5.2.Views Involving Building Blocks and Interface Specifications

5.2.1. Selection of Building Blocks for OOP Architecture

Requirements evolving from the TOOP pilot areas are described in the Appendix of this deliverable. These requirements to specific TOOP pilot applications are also used among the inputs for designing requirements for the TOOP focus area applications in general. In particular, generic scenarios present steps that are executed similarly in many OOP applications. They allow to identify capabilities needed for these steps, and associate building blocks that provide the needed capabilities.

The following table describes generic steps in information exchange that the OOP architecture and building blocks (BBs) need to make possible. These steps indicate both the need for an appropriate building block, as well as the need for external interfaces of the building blocks.

Nr	Step	BB
1.	Identify the Economic Operator	eID/eSeal[142] ← mandates
2.	eService decides what data is needed	Decide whether to use Transport or Attribute request Semantics
3.	Discover where the data is located • Determine endpoint • Determine MS realm • Determine a Domain Realm (e.g., Maritime Cloud?)	Capability & location look-up Semantics (to define the meaning of capabilities)
4.	Determine terms and conditions (value, price, legal validity) related to the data at Data Provider side (*not always necessary)*	Capability lookup
5.	Request the data	eDocument + eDelivery + trust + semantics (of the payload)
6.	Validate and parse the request by the Data Provider	Non-repudiation and traceability + trust + transformation + semantics + eDocuments
7.	Construct the response	eDocuments + semantics
8.	Send response	eDelivery + trust
9.	"Turnaround" (data to be received by the Data Consumer)	Semantics needed for automatically filling out form fields

Table 1: A Generic Use Case for TOOP

Matching of pilot areas and building blocks can be done via the generic scenarios like the one provided above, or through mapping of pilot requirements and building blocks.

[142] https://ec.europa.eu/futurium/en/content/confirm-it-e-seal

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Mapping of pilot requirements and building blocks comprises analysing pilot requirements, identifying the capabilities needed to fulfil these requirements, finding the building blocks that provide the identified capabilities, and implying the need for the building blocks found in this way.

Based on the pilot area requirements presented in Chapter 3 and Appendix, a preliminary mapping of TOOP pilot areas and building blocks is given in the table below.

	PA1	PA2	PA3
eDelivery	Y	Y	Maybe
eID	Y	Y	Maybe
eSignature	Maybe	Maybe no	N
eInvoicing	N	N	N
eTranslation	Maybe	Maybe no	Maybe (nice to have)
E-HI (Human Interface)	N	N	Maybe
Non-repudiation and traceability	Maybe	Maybe	Maybe
Trust establishment	Y	Y	Maybe
eDocument	Maybe	Maybe	Maybe
Semantics	Y	Y	Maybe

Table 2: Preliminary Mapping of Building Blocks and Pilot Areas

The main criteria for inclusion of building blocks in this chapter are as follows.

- Need for this building block follows from the TOOP requirements as presented in Chapter 3;
- To be useful for TOOP pilots, a building block should comprise specifications and software that can be used for specifying and building applications. Therefore, availability of such specifications and software is an important criterion for selecting building blocks needed for OOP applications;
- To be useful in long-term applications, a building block must be maintained and supported. Availability of maintaining and supporting organisation is another important criterion for including a building block in the current chapter.

The above two tables indicate that the building blocks identified so far can be categorized into three basic groups.

1. Building blocks that provide capabilities needed by all or most TOOP Pilot Areas (eDelivery, eID, Trust establishment, Semantics);
2. Building blocks that provide capabilities needed or probably needed by some TOOP Pilot Areas (eSignature, eTranslation, Non-repudiation and traceability, eDocument);
3. Building blocks that provide capabilities not needed by the TOOP Pilot Areas (eInvoicing).

Building blocks from the first two groups need to be represented in the OOP architecture.

The list of building blocks in this chapter can be complemented in future versions of the architecture.

5.2.2. High-Level Views of OOP Architecture with Building Blocks

Several types of OOP architecture are characterized below, providing topologies of different OOP applications, characterizing the scope of the building blocks using these topologies, and presenting some arguments for selection of the architecture.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- eDelivery 4 Corner Model (for eDelivery 4, 3, and 2 Corner Models, please see the eDelivery Tutorial[143]);
- eDelivery 3 Corner Model;
- eDelivery 2 Corner Model;
- Regional OOP Layer / Enterprise Service Bus Model;
- Other models, such as various kinds of peer-to-peer networks (these models are not discussed in the current report, but may be presented in future versions of OOP architecture documents).

The scope of a Building Block on these high-level architecture diagrams is indicated by its coverage. For example, the eID Building Block, if used, may provide its capabilities throughout the entire architecture; the eTranslation Building Block is more likely to provide capabilities on the data consumer or provider level; and so on.

The following high-level architecture diagram depicts the scope of main building blocks for a general OOP architecture - eDelivery 4 Corner Model. It is highly scalable and eliminates risks of single point of failure and service provider lock-in. Note: in a real-life application, some building blocks given in the diagram may be missing.

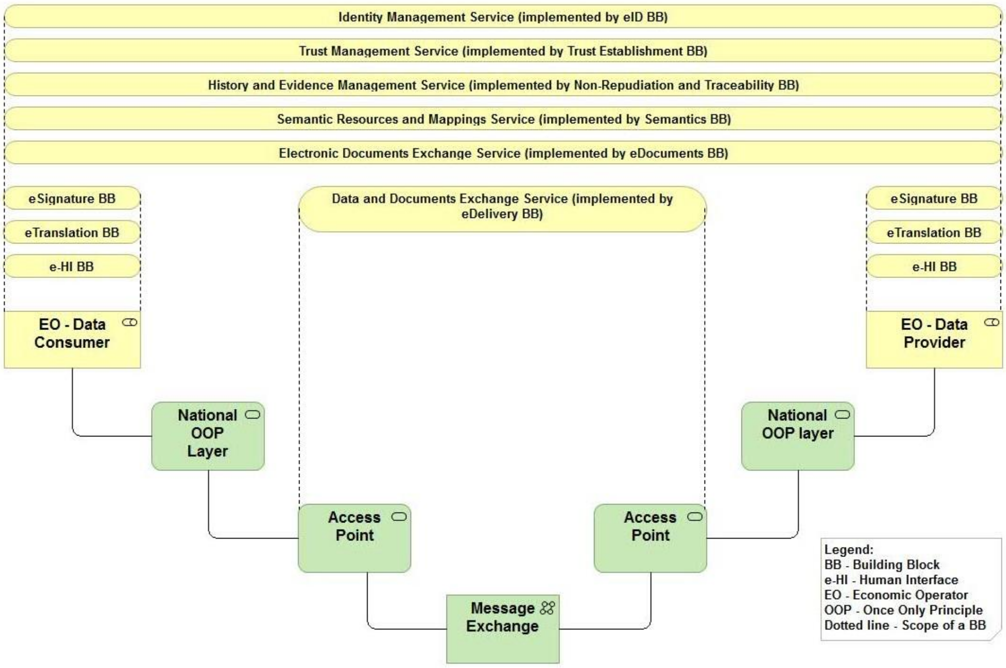

Identity Management Service (implemented by eID BB)
Trust Management Service (implemented by Trust Establishment BB)
History and Evidence Management Service (implemented by Non-Repudiation and Traceability BB)
Semantic Resources and Mappings Service (implemented by Semantics BB)
Electronic Documents Exchange Service (implemented by eDocuments BB)
eSignature BB
eTranslation BB
e-HI BB
Data and Documents Exchange Service (implemented by eDelivery BB)
eSignature BB
eTranslation BB
e-HI BB
EO - Data Consumer
EO - Data Provider
National OOP Layer
National OOP layer
Access Point
Access Point
Message Exchange
Legend:
BB - Building Block
e-HI - Human Interface
EO - Economic Operator
OOP - Once Only Principle
Dotted line - Scope of a BB

Figure 10: High-level view of OOP architecture (eDelivery 4 Corner Model)

The eDelivery 2 Corner Model is depicted below. Note 1: the eDelivery 3 Corner Model has similarities to the Regional OOP Layer / Enterprise Service Bus Model and is omitted here. Note 2: in a real-life application, some building blocks given in the diagram may be missing.

[143] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+How+it+works

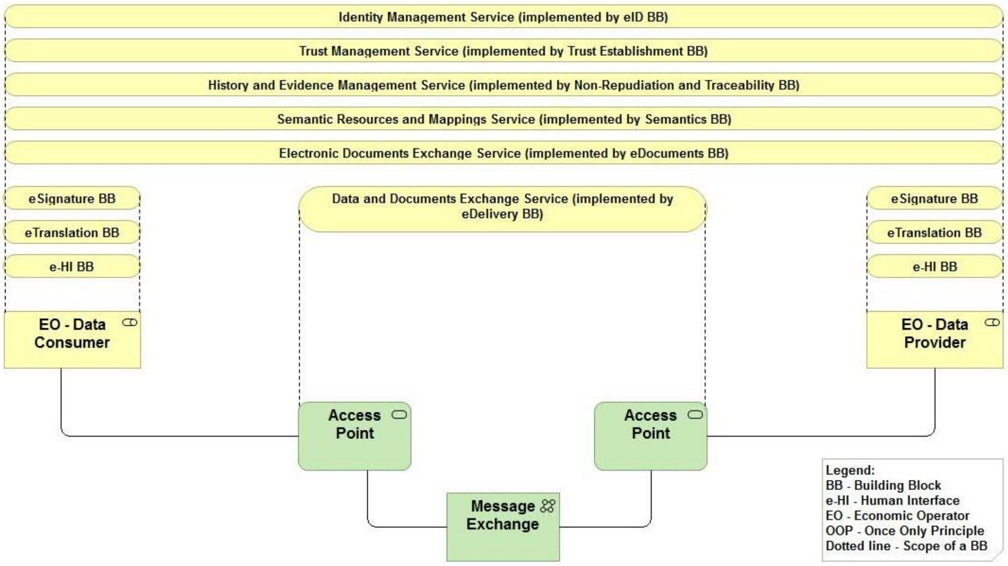

Identity Management Service (implemented by eID BB)
Trust Management Service (implemented by Trust Establishment BB)
History and Evidence Management Service (implemented by Non-Repudiation and Traceability BB)
Semantic Resources and Mappings Service (implemented by Semantics BB)
Electronic Documents Exchange Service (implemented by eDocuments BB)
eSignature BB
eTranslation BB
e-HI BB
Data and Documents Exchange Service (implemented by eDelivery BB)
eSignature BB
eTranslation BB
e-HI BB
EO - Data Consumer
EO - Data Provider
Access Point
Access Point
Message Exchange
Legend:
BB - Building Block
e-HI - Human Interface
EO - Economic Operator
OOP - Once Only Principle
Dotted line - Scope of a BB

Figure 11: High-level view of OOP architecture (eDelivery 2 Corner Model)

In applications with established and agreed data exchange and semantics standards, where all stakeholders operate under similar legislation and are willing to use a specific regional OOP infrastructure, a Regional OOP Layer / Enterprise Service Bus Model can be utilised. Such architectures (depicted below) may be useful for example in specific application sectors. Note: in a real-life application, some building blocks given in the diagram may be missing.

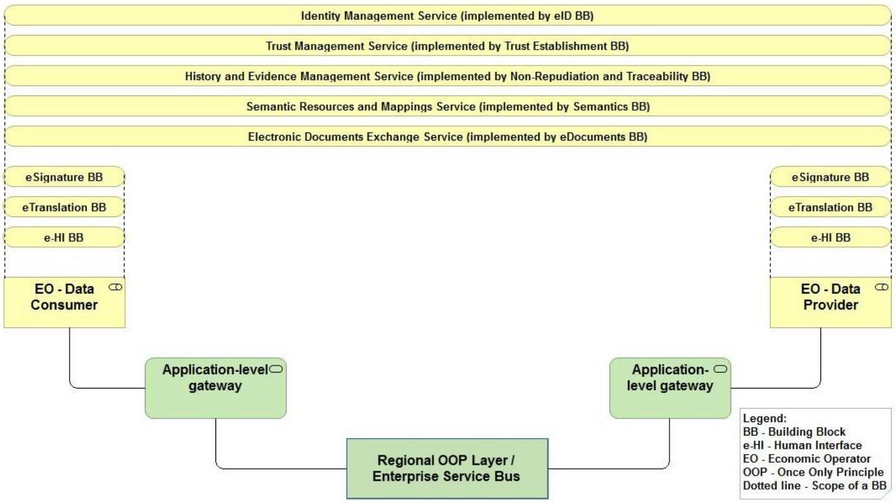

Identity Management Service (implemented by eID BB)
Trust Management Service (implemented by Trust Establishment BB)
History and Evidence Management Service (implemented by Non-Repudiation and Traceability BB)
Semantic Resources and Mappings Service (implemented by Semantics BB)
Electronic Documents Exchange Service (implemented by eDocuments BB)
eSignature BB
eTranslation BB
e-HI BB
eSignature BB
eTranslation BB
e-HI BB
EO - Data Consumer
EO - Data Provider
Application-level gateway
Application-level gateway
Regional OOP Layer / Enterprise Service Bus
Legend:
BB - Building Block
e-HI - Human Interface
EO - Economic Operator
OOP - Once Only Principle
Dotted line - Scope of a BB

Figure 12: High-level view of OOP architecture (Regional OOP Layer / Enterprise Service Bus Model)

The following figure presents a more detailed diagram for the eDelivery 4 Corner Model enriched with important components of the eDelivery and eID Building Blocks. It also depicts the backend interface and different options of connecting through the regional OOP Layer or without it. The e-HI Building Block has been removed as being potentially out of scope for the OOP architecture. Whether the e-HI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

BB and some other Building Blocks will be part of the generic federated OOP architecture is a question to be solved in the next versions of the architecture.

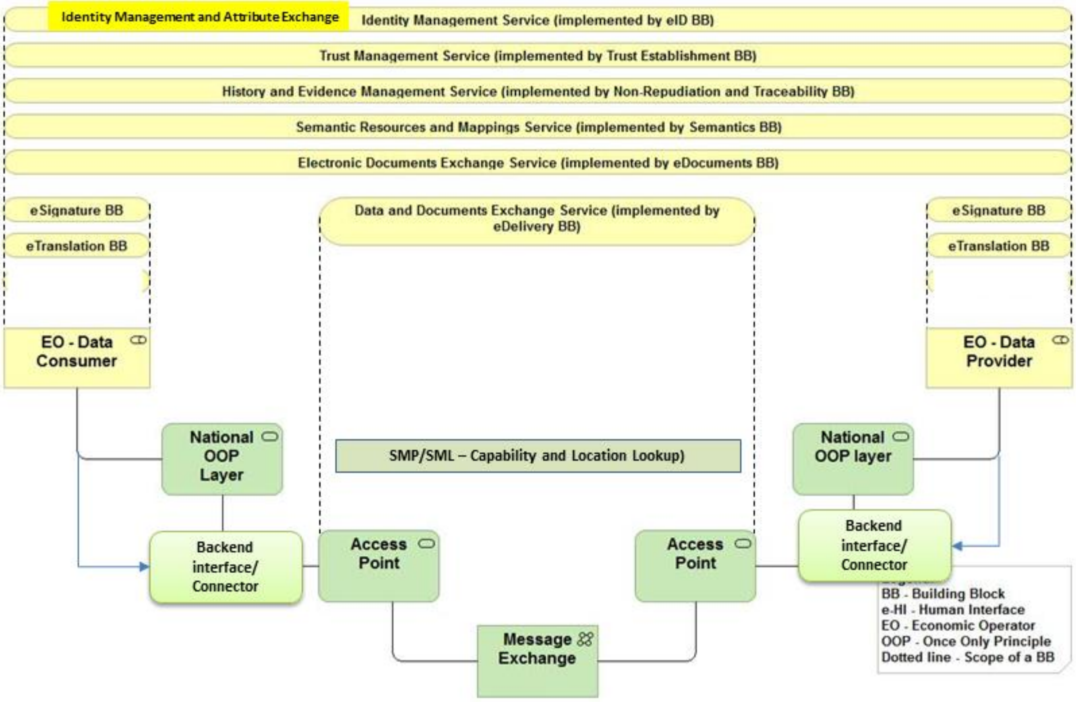

Identity Management and Attribute Exchange
Identity Management Service (implemented by eID BB)
Trust Management Service (implemented by Trust Establishment BB)
History and Evidence Management Service (implemented by Non-Repudiation and Traceability BB)
Semantic Resources and Mappings Service (implemented by Semantics BB)
Electronic Documents Exchange Service (implemented by eDocuments BB)
eSignature BB
eTranslation BB
Data and Documents Exchange Service (implemented by eDelivery BB)
eSignature BB
eTranslation BB
EO - Data Consumer
EO - Data Provider
National OOP Layer
SMP/SML – Capability and Location Lookup)
National OOP layer
Backend interface/ Connector
Access Point
Access Point
Backend interface/ Connector
Message Exchange
BB - Building Block
e-HI - Human Interface
EO - Economic Operator
OOP - Once Only Principle
Dotted line - Scope of a BB

Figure 13: High-level view of OOP architecture (eDelivery 4 Corner Model, detailed)

5.2.3. Interface specifications for the OOP architecture

There can be several viewpoints on interface specifications for the generic federated architecture.

- External interfaces of the building blocks (e.g., provided services).
- External interfaces of an application developed in compliance with the architecture (e.g., user interfaces).
- Interfaces of the users of the architecture documentation (e.g., system architects).

Because of the tight deadlines of the current deliverable, it focuses on the most critical viewpoint from the above list – on external interfaces of the building blocks. These external interfaces for the building blocks needed for the pilots as well as for OOP applications in general are given in the chapters below. Other viewpoints will be presented in the future versions of the architecture as necessary.

The external interfaces can be presented on different level of detail. Deliverable D2.1 provides a general view of the interfaces. In the forthcoming versions of the architecture, profiling of the common building blocks on specification level will be provided as well, so that these specifications can be used by designers and implementers in WP3. The OOP architecture documents will focus on the common aspects of profiling the building blocks. The architecture development does not comprise implementation, testing, or maintaining the building blocks.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

5.3.eDelivery

This section presents the eDelivery building block in more detail, investigating the following aspects.

- Need for this building block by the TOOP pilots, as well as for OOP applications in general.
- Adequacy of specifications and software that can be utilized for specifying and building applications that use this building block.
- Adequacy of maintaining and supporting organisation for this building block.
- Need for further development of this building block to be used in OOP applications.
- External interfaces for this building block needed for the pilots as well as for OOP applications in general.

5.3.1. Need of eDelivery in TOOP Pilots and Applications

The OOP is based on the exchange of information between authorized services, so that the human actor will only need to provide this once (or not even once). It is also, evident from the initial analysis of the Pilot Areas Requirements that most of the Use Case scenarios require the exchange of information in a secure, reliable way, using a message exchange process. The fundamental service interface for the message exchange, according to the High-Level architecture, is eDelivery, using most of its specifications as they are defined in CEF and e-SENS, namely the Message Exchange ABB, the Service Location ABB, the Capability Lookup ABB and the Backend Integration ABB. Thus, use of eDelivery is considered crucial in OOP PAs and its ABBs need to be thoroughly checked and possibly further profiled to fit the needs of the PAs.

5.3.2. Specifications Adequacy and Usable Software

The eDelivery SAT and its ABBs define a set of specifications and standards properly profiled to provide secure, reliable messaging, with dynamic discovery of services and capabilities.

5.3.2.1. Message Exchange ABB – EBMS3 / AS4

The e-SENS/CEF AS4 Profile is a profile of the ebMS3 and AS4 OASIS Standards. It has provisions for use in four-corner topologies, but can also be used in point-to-point exchanges. This specifications profile can be implemented using open source or closed source commercial software products compliant with these standards. It is designed to support both One Way and Two Ways (Request-Response) exchanges[144].

Regarding the available software, CEF eDelivery wiki maintains a list of both open source and commercial software that implement the e-SENS AS4 Profile and have passed successfully the CEF AS4 conformance testing[145]. The list contains 8 conformant solutions, 3 being open source and the rest being commercial software.

5.3.2.2. Capability Lookup ABB – OASIS BDX SMP

The e-SENS SMP profile is an open specification for publishing service metadata within a 4-corner network. To successfully send a business document in a 4-corner network, an entity must be able to discover critical metadata about the recipient (Access Point) of the business document, such as types of documents the Access Point is capable of receiving and methods of transport supported. The

[144] http://wiki.ds.unipi.gr/display/ESENS/PR+-+AS4+-+1.11
[145] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-SENS+AS4+conformant+solutions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

recipient makes this metadata available to other entities in the network through a Service Metadata Publisher service.

The e-SENS SMP profile describes the request/response exchanges between a Service Metadata Publisher and a client wishing to discover Access Point metadata. The profile is based on the OASIS Service Metadata Publishing (SMP) Version 1.0 standard.

Currently, the list of the software supporting the OASIS BDX SMP consists of two entries, the phoss SMP Server[146] and the EC's OASIS SMP Sample Implementation, both being open source and free to use.

5.3.2.3. Service Location ABB – OASIS BDXL (SML)

The e-SENS BDXL profile is an open specification for locating Access Points within a network. It offers a dynamic system to discover the URLs of services like SMPs and access points and their corresponding metadata. The profile is based on the Business Document Metadata Service Location Version 1.0. from OASIS[147].

The current SML/BDXL software component is maintained by the European Commission[148]. It implements the PEPPOL Transport Infrastructure SML specifications and the OASIS Business Document Metadata Service Location (BDXL) specifications.

5.3.3. Maintenance Adequacy

All specifications and standards composing the eDelivery SAT have been handed over to the EC and officially eDelivery is a CEF Building Block[149]. The EC, through CEF and DG-DIGIT are now actively maintaining the eDelivery Building Blocks, which are based on OASIS standards.

5.3.4. External Interfaces

The external interfaces of eDelivery are considered the actual service interfaces that are provided through eDelivery software, like AS4 Message Service Handlers, SMP Servers and SML/BDXL Services. The external interfaces are also considered only the ones that are usable for

5.3.4.1. CEF/e-SENS AS4 External Interface

For AS4, the high-level external interface is the interface that is exposed by the conformant software of the Message Exchange ABB. This interface must be able to receive messages which are created according to the e-SENS AS4 Profile, meaning that they should be digitally signed and encrypted. The Service exposing the message reception interface must be able to decrypt and validate the authenticity of the message, by validating the carried signature of the message. Every system implementing the AS4 Specification, must expose message reception external interface.

5.3.4.2. OASIS BDX SMP External Interface

For the OASIS BDX SMP, the high level external interfaces are the ones that are defined in the OASIS BDX SMP REST API specification[150]. The manipulation of the SMP records are implementation specific

[146] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/OASIS+SMP+conformant+solutions
[147] http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html
[148] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+service
[149] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Background
[150] http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/cos01/bdx-smp-v1.0-cos01.html#_Toc458092062

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

and no service interface has been standardized and thus can be considered as a proper external interface.

5.3.4.3. OASIS BDXL External Interface

The OASIS BDXL has an official service deployed in the EC. For reading Service Location data, using BDXL Records, the service exposes an interface for querying the DNS for specific U-NAPTR records[151]. For creating/updating the U-NAPTR records under a specific domain, managed by the EC (*.edelivery.tech.ec.europa.eu), a definition of a web service interface, which can be considered as external for TOOP, is available in the BDMSL Documentation from the EC[152].

5.4.eID

This section presents the eID building block in more detail, investigating the following aspects.

- Need for eID BB by the TOOP pilots, as well as for OOP applications in general.
- Adequacy of specifications and software that can be utilized for specifying and building applications that use eID BB.
- Adequacy of maintaining and supporting organisation for eID BB.
- Need for further development of eID BB to be used in OOP applications.
- External interfaces for eID BB needed for the pilots as well as for OOP applications in general.

5.4.1. Need for eID BB in TOOP Pilots and Applications

eID BB is composed of a set of protocols, formats and data definitions to implement the cross-border infrastructure of an authentication architecture that minimizes data disclosure and permits interoperability based on national standards. It provides a cross-border framework to make inter-operable country-specific authentication infrastructure through digital identity. In particular, to allow a legitimate user to securely access services in a foreign European country through one or more identity attributes.

The ‘once-only’ principle in the context of digital public sector is that citizens and/or organizations should supply certain standard information only once to a public administration. Public administration offices then take actions to share this data by respecting data protection rules. eID is the key digital enabler for digital public services and interoperability frameworks for providing online authentication in the adoption of the once only principle.

The main goal of the ‘once-only’ principle is to reduce the administrate burden when citizens and/or organizations are required to provide the same information again and again to public administrations. Thus, public administrations will have the cross-border interoperable architecture to re-use information already supplied by citizens and/or organizations in a transparent and secure way. The Once-Only Principle Project will develop cross-border and interoperable ‘once-only’ architecture and implement it in its specific pilot cases. The first step is to authenticate himself/herself to the TOOP system in order to perform such information to public administrations. Therefore, eID BB will be needed

[151] http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/cos01/BDX-Location-v1.0-cos01.html#_Toc477177888

[152] https://ec.europa.eu/cefdigital/wiki/download/attachments/32769146/Interface%20Control%20Document%20for%20the%20BDMSL%20-%20v1.0.pdf?version=1&modificationDate=1474305657168&api=v2

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

5.4.2. Adequacy of specifications and software

In accordance with the eIDAS Regulation (EU 910/2014)[153], the mutual recognition of eIDs by public administrations in the EU will enter into force in September 2018. Electronic identification means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person who represents a legal person.

The eIDAS-Node software is a sample implementation of the eID eIDAS profile and it is maintained by CEF eID team. It contains the necessary modules to help Member States become eIDAS compliant, as it enables them to communicate with eIDAS-enabled counterparts in a centralised or distributed fashion. The sample implementation is composed of the following tools:

- ***eIDAS-Node***: an implementation of the eID eIDAS profile able to communicate with other nodes of the eIDAS-Network. The eIDAS-Node can either request (via an eIDAS-Node Connector) or provide (via an eIDAS-Node Proxy Service) cross-border authentication;
- ***Testing tools (demo SP and demo IdP)***: additional tools for setting up a demo environment for testing purposes.

5.4.3. Adequacy of maintaining and supporting organisation

The technical specifications for the eIDAS interoperability framework have been developed by the European Commission with the help of member states collaborating in a technical sub-committee of the eIDAS Expert Group.

5.4.4. Need for further development of eID BB

CEF eID team offers three ways for using eIDAS compliant eID BB and they are summarized in below.

1. Build your own eID BB: You build and test your own components according to the specifications of the eID DSI. This can be done using an in-house development team or by an external contractor;
2. Buy your eID BB: You buy a product(s) that implements the specifications of the eID DSI. This can be a Commercial or Open Source software product. Additional services can be involved;
3. Re-use sample implementation as eID BB: You reuse the sample software of the eID DSI or one of its stand-alone services. The latest eIDAS-node version 1.2 was released in March 2017[154].

5.4.5. External Interfaces for eID BB

A Member States must recognise eID means issued under ‘notified’ eID schemes from other Member States for cross-border access to its public services requiring e-identification based on the reciprocity principle (art.6). Notified eID schemes shall specify the assurance level of the eID means (art.8.1). There will be three Level of Assurance (LoA).

1. Assurance level low: recognition is voluntary (art.6.2);
2. Assurance level substantial: recognition is mandatory (art.6.1(b));
3. Assurance level high: recognition is mandatory (art.6.1(b)).

[153] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, see: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[154] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+v1.2

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

The CEF eID team provides the sample implementation for an eIDAS-Node as an example of the interpretation of the eIDAS technical specifications. eIDAS technical specification has four main pillars:

1. Interoperability architecture;
2. Message format;
3. Attribute profile;
4. Crypto Requirements.

eIDAS-Network is defined as the components necessary to achieve interoperability of notified eID schemes according to the eIDAS Regulation. Stakeholder of the eIDAS-Network are relying party, citizen, and operators of components of the eIDAS-Network.

Interoperability between different eID-schemes is achieved via defining the technical interfaces between eIDAS-Connectors (i.e., eIDAS-Nodes requesting a cross-border authentication) and eIDAS-Services (i.e., eIDAS-Nodes providing cross-border authentication).

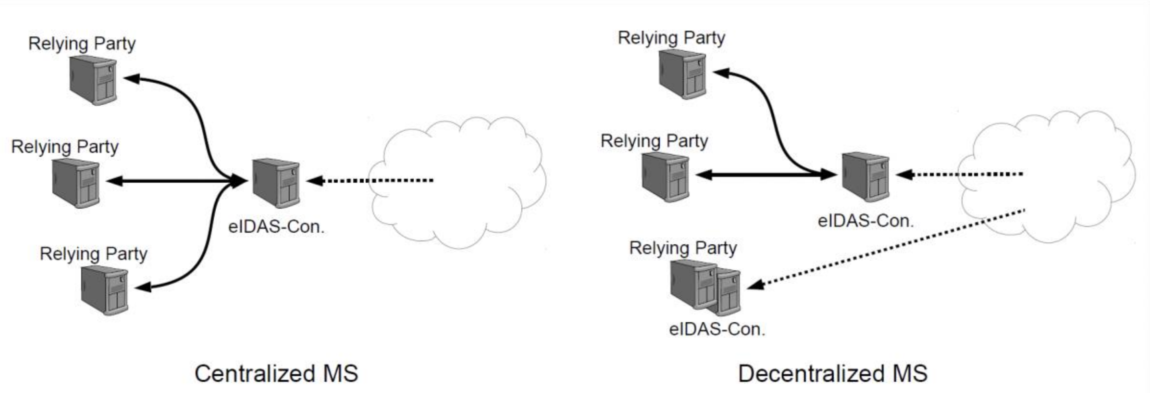
Sending MS can choose between two integration scenarios for their eID-scheme.

1. Proxy-based: The Sending MS operates an eIDAS-Proxy-Service, relaying authentication requests and authentication assertions between an eIDAS-Connector operated by the Receiving MS and the eID scheme of the Sending MS;
2. Middleware-based: In this scenario, the Sending MS does not operate a Proxy for the purpose of authentication of persons to relying parties of another MS. The Sending MS provides a Middleware to another MS, which is operated by the operator(s) of the eID-Connector(s) of the Receiving MS.

A MS notifying their eID scheme as a Middleware-based scheme must provide the necessary Middleware to Receiving MSs

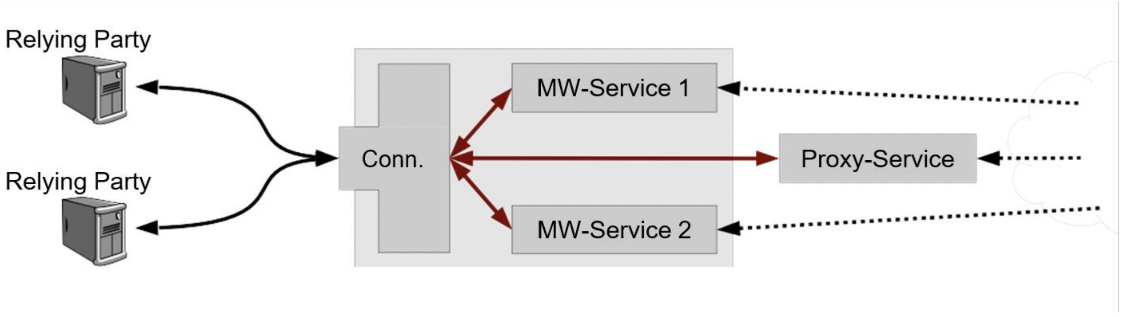
Each Receiving MS shall operate one or more eIDAS-Connectors. It is up to the Receiving MS to decide the national deployment of Connectors. Connectors need not to be operated by the MS itself, but can also be operated by public and/or private relying parties established in that MS.

In the following, MSs operating exactly one Connector are called Centralized MSs, while MSs operating several Connectors are called Decentralized MSs.

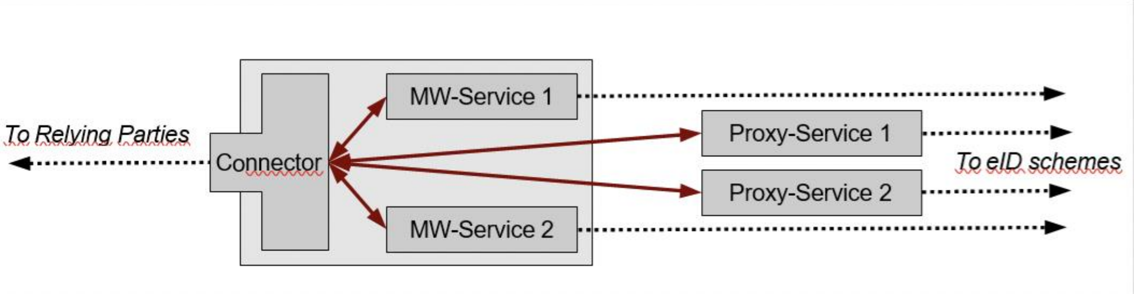


An eIDAS-Connector is operated together with eIDAS-Middleware-Services for communication with middleware-based eID schemes. The interfaces between the eIDAS-Connector and relying parties, and between the eIDAS-Services and the eID-scheme are part of the national system of the Receiving MS and the Sending MS respectively.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460



An operator of an eIDAS-Connector operates one instance of the eIDAS-Connector, and one eIDAS-Middleware-Service for each type of notified middleware based eID schemes.



The eIDAS-Connector provides the following interfaces:

1. Interface between eIDAS-Connector and Relying Party;
2. Interface between eIDAS-Connector and eIDAS-Service;
3. Interface between eIDAS-Service and eID Scheme.

eIDAS message format is a SAML 2.0 profile that took into consideration Kantara Initiative eGovernment Implementation Profile of SAML V2.0 and STORK 2.0 D4.4 First version of Technical Specifications for the cross border Interface[155].

Attribute profile covers the minimum data set based on ISA Core Vocabulary. The minimum data set for natural persons and legal person is defined in Implementing Act 2015/1501[156]. The minimum data set for natural persons have mandatory and optional parts.

- Mandatory:
  - current first / family name;
  - date of birth;
  - unique identifier.
- Optional:
  - First / family name at birth;
  - place of birth;
  - current address.

The minimum data set for legal person have mandatory and optional parts:

- Mandatory;

[155] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+eIDAS+profile?preview=/23003348/35223089/eIDAS%20Message%20Format_v1.1-2.pdf

[156] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1501&from=en

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

  - current legal name;
  - unique identifier.
- Optional:
  - current address;
  - VAT number;
  - tax reference number;
  - EORI (Economic Operators' Registration and Identification) number, or some further identifiers defined in EU legislation.

Within the eIDAS Interoperability Framework, communication between eIDAS nodes (i.e., eIDAS-Services and eIDAS-Connectors) is perfomed via the citizen's browser. Here, the content of the communication between eIDAS nodes is performed using cryptographically protected SAML messages. To secure the transport layer of this communication between these components and the citizen's browser, Transport Layer Security (TLS) is used.

The general requirements for TLS is defined in below.

- If supported by the citizen's browser, the eIDAS node must use TLS 1.2;
- Otherwise, TLS 1.1 MAY be used if usage of TLS 1.2 is not possible.

Prior TLS versions must not be accepted. Apart from these general requirements; eIDAS nodes must only use cipher suites that provide perfect forward secrecy. Until 2017, eIDAS nodes must use extended validation certificates or qualified website certificates for TLS. As of 2018, newly issued TLS certificates for eIDAS nodes must be qualified. There exist also other recommendations, e.g., TLS compression should not be used, the heartbeat extension should not be used.
The general requirements for SAML is defined in below.

- SAML request and SAML response messages must be signed by the sending party;
- The signature of a SAML assertion is OPTIONAL;
- The (signed) SAML assertion within the SAML response message must be encrypted.

Ephemeral keys or random numbers (for nonces or generation of ephemeral keys) shall be used only once. It is required that random numbers to be used within SAML are generated with cryptographically secure random number generators that provide sufficient entropy (according to the security level of 120 bits). Apart from these requirements, it is required to use elliptic curve minimum 256 bit and RSA minimum 3072 bit for signatures, key agreement, or key transport and also AES for content encryption.

It is expected that such an eIDAS-node will be a part of the eIDAS-Network which is the network of interconnected national eID schemes in the Member States. The interconnection of these national eID schemes is established through the implementation of the eIDAS-Node at Member State level that is integrated with the national eID scheme and thereby makes this national eID available to be used for cross- border authentication of users that have such a national eID. In addition, any national attribute providers that can provide information linked to the identity of the user will also need to be connected/integrated with the eIDAS-Node.

Such an eIDAS-Node can either request a cross-border authentication or provide a cross border authentication.

- Cross-border authentication request: When a service provider connected to a national eID scheme encounters a user from another Member State, this request is routed through the eIDAS-Node of the receiving Member State to request the cross-border authentication from eIDAS-Node in the country of the user in the sending Member State through the eIDAS-Connector.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- Provide a cross border authentication: the eIDAS-Node in the sending Member State of the user requesting to use the service in another country will provide the cross-border authentication through the eIDAS-Service. This eIDAS-Service can be operated in two ways:
    - eIDAS-Proxy-Service: an eIDAS-Service operated by the Sending Member State and providing personal identification data;
    - eIDAS-Middleware-Service: an eIDAS-Service running Middleware (also referred to as a Middleware Service plugin integrated into an eIDAS-Node in a non- Middleware country) provided by the Sending Member State, operated by the Receiving Member State and providing personal identification data.

Given the need for different parties to be connected to the eIDAS-Network the eIDAS-Node provides four different interfaces:

- **Interface for National eID and Attributes Provider**: this Member State specific interface is used to connect the eIDAS-Node in the user's Member State to their National eID (Identity Provider) and Attribute Provider:
    - An Identity Provider can be defined as: the stakeholder that provides the means of electronic identity to a person whose identity has been established. The provider of the electronic identity can be a public administration or a private sector provider (on behalf of or officially recognised by the government). The identity provider can also play the role of Service Operator or Implementer or may leave this to other actors.
    - An Attribute Provider can be defined as: the stakeholder that provides additional information related to the identity by providing a service that can be defined as "a service trusted by one or more entities that provides digital identity-related attributes' (i.e. specific data describing that identity that may be either a natural or a legal person)".
- **Interface for Service Providers in the Member State where the eIDAS-Node is deployed**: A Member State's eIDAS-Node has an interface to communicate with multiple Service Providers in that Member State. Through this interface, the Service Provider sends authentication requests to the eIDAS-Node and receives the authentication responses;
- **Interface for other eIDAS-Nodes in Member States using the proxy-based infrastructure**: an eIDAS-Node has an interface for communication with eIDAS-Nodes in other Member States. This results in the cross-border interoperability of the eID solution. This interface is established through the eIDAS-Service and e-IDAS Connector (as described above) these respectively request and provide identity information to the other eIDAS-Node;
- **Interface for users requesting access to the Service Provider**: this interface is used for the communication between the eIDAS-Node and the user's proxy via their browser. It is used when requesting the user to select their country of origin.

5.5.eSignature

This section presents the eSignature building block in more detail, investigating the following aspects.

- Need for eSignature BB by the TOOP pilots, as well as for OOP applications in general;
- Adequacy of specifications and software that can be utilized for specifying and building applications that use eSignature BB;
- Adequacy of maintaining and supporting organisation for eSignature BB;
- Need for further development of eSignature BB to be used in OOP applications;
- External interfaces for eSignature BB needed for the pilots as well as for OOP applications in general.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

TOOP pilots need eSignature building block due to the requirements related to mutual recognition and cross-border interoperability of eSignatures between the Member States. There assumed to be sufficient amount of specifications and software that can be utilized for specifying and building applications that use eSignature building block. eSignature building block is one of the most mature and widely utilized building blocks.

5.5.1. Need for eSignature BB

The once-only principle states that citizens and businesses should have the right to supply certain standard information only once, because public administration offices take action to internally share this data, so that no additional burden falls on citizens and businesses.

eSignature can only be used by a natural person to 'sign', i.e. mainly to express consent on the data the eSignature is put. Legal persons are able to use certificates for eSeals (whose aim is not to sign but to ensure the integrity and origin of data), therefore certificates for eSignatures are be issued to legal persons anymore and existing qualified eSignatures certificates issued to legal persons are not used to create a legally valid (qualified) eSignature.

Within the 'once-only' concept, eSignature is broadly used to ensure that information can be relied upon and is accurate and complete. In addition, it is also used in order to prevent intervening persons or systems to deny or challenge their access to authentic data sources.

5.5.2. Adequacy of specifications and software

Effective July 1st, 2016 the EU Regulation 2014/910, also known as eIDAS, is in force. This Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market replaces the EU Directive 1999/93. Being a Regulation and not just a Directive, it is directly applicable in all 28 EU member states without need of being transposed into local laws. It will replace the overwhelming part of all national signature laws associated to the 1999 Directive.

Whereas the eSignature Directive only covered electronic signatures, the Regulation's legal framework now captures a broader array of trust services, which are: electronic signatures, electronic seals, electronic time stamps, electronic registered delivery service and website authentication. This is a closed list of trust services but Member States remain free to recognize at a national level other types of trust services. The trust services in the Regulation can be qualified or not. To be qualified they need to adhere to stricter requirements, but being qualified can result in a different legal effect (e.g., qualified electronic signatures are considered equivalent to handwritten signatures). By establishing the legal effect of trust services, the Regulation also provides some clarification regarding the admissibility of electronic evidence before court. Not only for the mentioned trust services, but also for electronic documents. The Regulation states that electronic documents shall not be denied legal effect and admissibility as evidence in legal proceedings only because they are in electronic form. In some countries, factually this does not make a difference, since courts often already accepted electronic evidence. However, it still increases legal certainty, as it is now clear that they can be used in all Member States (though the final effect will still depend on the reliability of the digital evidence). The Regulation also establishes the requirements to provide the listed trust services and the supervision of the trust service providers. A national Trusted List is published and maintained in line with the Commission Implementing Decision (EU) 2015/1505. A provider/service will be qualified when it appears in the Trusted Lists. To prove this status the EU trust mark logo can be used so potential users are sure the online transactions will be carried out in a safe, convenient and secure way.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Public sector bodies are able to recognise the formats of advanced eSignatures and eSeals (according to the Commission Implementing Decision (EU) 2015/1506) whenever they require an advanced eSignature or eSeal.

Voluntary use of EU Trust mark is available. The trust mark clearly differentiates qualified trust services from other trust services; the aim is to foster confidence in and of essential online services, for users to fully benefit and consciously rely on electronic services. The trust mark is defined in Commission implementing Regulation (EU) 2015/806.

5.5.3. Adequacy of maintaining and supporting organisation

The European Commission maintains sample software compliant to the eSignature specifications. In other words, the CEF provides eSignature BB which is named Digital Signature Services (DSS). It is an open-source library supporting the creation and validation of electronic signatures in line with European legislation and standards. In addition to a range of new features, version 5.0 is fully compliant with Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, better known as the eIDAS Regulation.

In order to help service providers and public administration test interoperability and conformity of the eSignature solutions, ETSI provides an eSignature conformance checker. This free online tool performs numerous checks in order to verify the conformity of the ETSI Advanced Electronic Signatures. The tool performs conformance tests on:

1. XAdES (XML Advanced Electronic Signature ETSI 101 903, TS 103 171 and EN 319 132-1&2)
2. CAdES (CMS Advanced Electronic Signature ETSI TS 101 733)
3. ASiC (Associated Signature Container ETSI TS 102 918)
4. PAdES (PDF Advanced Electronic Signature ETSI TS 102 778)

5.5.4. Need for further development of eSignature BB

The eSignature building block supports the use of cross-border interoperable electronic signatures in Europe.

5.5.5. External interfaces for eSignature BB

As defined in Commission Implementing Decision 2015/1506/EU, Member States requiring an advanced electronic signature or an advanced electronic signature based on a qualified certificate as provided for in Article 27(1) and (2) of eIDAS Regulation ((EU) No 910/2014), shall recognise XML, CMS or PDF advanced electronic signatures at conformance levels B, T or LT or using an associated signature container.

These XML, CMS, PDF and container formats and levels are defined in the corresponding standards:

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2
Associated Seal Container Baseline Profile	ETSI TS 103174 v.2.2.1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

5.6.eTranslation

This section presents the eTranslation building block in more detail, investigating the following aspects.

5.6.1. Adequacy of specifications and software

The eTranslation service provided by the European Commission is available for single users of or entire public authorities, either through direct access via the existing Web interface or for developers via an API for integration into another system. Yet, there is no public software nor API specification available, and projects, which would like to incorporate the service, have to explicitly request access. As of this time (May 2017), the responsible helpdesk service for the eTranslation service has not reacted to our requests regarding documentation of the respective interface documentation. Other projects, which already included the eTranslation service into their architecture are, e.g., the European Data Portal[157,] the e-Justice Portal[158], or the Online Dispute Resolution Forum[159].

5.6.2. Adequacy of maintaining and supporting organisation

The eTranslation service is hosted and maintained by the European Commission and is actively used and continuously developed further. In addition, the open source framework Moses, that the eTranslation services it builds on, is actively pursued as well, with the last major version (Moses2) being released in September 2016. While no public documentation of the eTranslation service is available, the components of Moses as well as their deployment are well-documented[160].

5.6.3. Need for further development of this building block

The eTranslation service builds on so-called parallel data, which are required for the system to learn the use of a language in each context. While the EC uses the service mainly to translate their documents into the official MS languages, these parallel data are focused on legal texts. Therefore, if the eTranslation service is going to be used within the pilots, training data have to be provided, in order to achieve high quality and reliable translation results. In addition, if a tight coupling for the intended translation service to the OOP architecture would be necessary, adoption of the official eTranslation service could be challenging, as it cannot easily be modified. In this case, the adoption of the underlying open source framework Moses should be considered.

5.7.Traceability and Non-Repudiation

This section presents the Traceability and Non-Repudiation building block in more detail, investigating the following aspects.

- Need for this building block by the TOOP pilots, as well as for OOP applications in general;
- Adequacy of specifications and software that can be utilized for specifying and building applications that use this building block;
- Adequacy of maintaining and supporting organisation for this building block;
- Need for further development of this building block to be used in OOP applications;
- External interfaces for this building block needed for the pilots as well as for OOP applications in general.

[157] https://www.europeandataportal.eu
[158] https://e-justice.europa.eu/home.do
[159] https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home.show&lng=EN
[160] http://www.statmt.org/moses/manual/manual.pdf

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Non-repudiation is a much-desired property in the e-government systems and applications. Generally speaking, a non-repudiation service provides assurance to all parties of a transaction: a) assurance of the origin or delivery of data in order to protect the sender against false denial by the recipient that the data has been received, b) protection of the recipient against false denial by the sender that the data has been sent. Several mechanisms such as digital signature of message hash, recipient acknowledgments with signature and non-repudiation tokens are frequently used to provide non-repudiation.

Traceability is defined as the 'ability to trace the history, application, or location of that which is under consideration' (ISO 9000:2005). Traceability is essentially associated with: a) the capacity of an information system to keep track of the ongoing and past transactions through the collection and analysis of traceability data, b) its ability to chronologically interrelate traceability data in a way that is verifiable. Such requirements frequently need the support of a reliable logging and transaction monitoring framework and an accurate synchronized clock among the participant of the business transaction under analysis.

5.7.1. Need for this building block

TOOP Pilot 3 has expressed a strong interest in using traceability and non-repudiation techniques in the delivery process of electronic documents such as ship and crew certificates. Similar needs have been expressed by the two other pilots, but to a lesser degree. The global OOP architecture needs to include effective, flexible and standards-based mechanisms for non-repudiation and traceability. Integrity, non-repudiation and tracking of the information exchanged between the core TOOP components needs to be implemented as a separate layer of the OOP architecture.

5.7.2. Adequacy of specifications and software

The core functionality of OOP architecture for traceability and non-repudiation should be based on e-SENS Non-Repudiation and Traceability SAT[161]. TOOP will adopt the core elements of the specifications of this building block. A certain simplification however of the specifications that will be embedded in TOOP software might be necessary in order to strengthen OOP architecture with functional and rigorous tools for traceability and non-repudiation.

5.7.3. Adequacy of maintaining and supporting organization

The Non-Repudiation and Traceability SAT developed by the e-SENS project should be adopted by CEF.

5.7.4. Need for further development

There may be a need to simplify the e-SENS Non-Repudiation and Traceability SAT. As a result, core TOOP mechanisms for non-repudiation and traceability should mainly include:

- The extended use of digital signatures and timestamps;
- The development of a monitoring tool that can provide at any moment the complete history of a transaction (i.e. a document exchange) that is enabled by the TOOP applications.

5.7.5. External interfaces for this building block

Two specific interfaces need to be developed in order to implement the functionality described in the previous paragraph:

[161] http://wiki.ds.unipi.gr/display/ESENS/SAT+-+Non-Repudiation+and+Traceability+1.3

- Smart interfaces for electronically signing and/or timestamping TOOP documents that are exchanged between the different parties;
- A generic interface for searching, retrieving and monitoring transactions based on the Unique Transaction ID (or other key transaction elements).

5.8.Trust Establishment

Trust Establishment is necessary, present in both architectural frameworks: e-SENS and CEF. Building trust in the online environment is stipulated by eIDAS. In line with the objectives of eIDAS, e-SENS provides Building Blocks to interconnect IT-solutions used by public administration, their providers and customers in different domains and/or EUMS in an interoperable, secure and trustworthy manner. e-SENS SAT refers to the following ABBs in the e-SENS Architecture Repository[162]:

- Trust Network – Mutual Recognized Certificates[163];
- Trust Network – PKI[164];
- Trust Network – Trust Service Status List[165].

CEF has not adopted the e-SENS SAT Trust Establishment in originally presented mode. e-SENS independent Building Block is within CEF Framework allocated within CEF BB e-Delivery[166]:

- Message Exchange[167];
- Trust Establishment[168];
- Dynamic Service Location[169];
- Capability lookup[170];
- Backend Integration[171].

There is partial overlap within these two approaches, mainly between e-SENS ABB Trust Network- PKI and CEF eDelivery PKI Service. Considering the reliability of services, CEF is chosen for further analysis.

5.8.1. Need for Trust Establilshment

Trust establishment is important part of data change, which does contain roughly two critical stages: request of data and validation of the data request. This highlights PKI role within data exchange process. Within CEF framework, PKI is a set of roles, policies, procedures and systems needed to create, manage, distribute, and revoke digital certificates. The PKI service of CEF eDelivery enables issuance and management of digital certificates used to ensure confidentiality, integrity and non-repudiation of the information exchanged between the CEF eDelivery components i.e. between Access Points (AP) and Service Metadata Publishers (SMP)[172].

[162] http://wiki.ds.unipi.gr/display/ESENS/SAT+-+Trust+Establishment+-+1.2
[163] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=18809140
[164] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=18809138
[165] http://wiki.ds.unipi.gr/pages/viewpage.action?pageId=18809136
[166] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+How+it+works
[167] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Message+Exchange
[168] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Trust+Establishment
[169] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Dynamic+Service+Location
[170] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Capability+lookup
[171] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Backend+Integration
[172]https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service

5.8.2. Adequacy of specifications and software

Main standard for CEF eDeivery Trust Establishment Is ETSI - Electronic Signatures and Infrastructures[173].

5.8.3. Adequacy of maintaining and supporting organisation

CEF has taken over e-SENS SAT Trust Establishment, but not it's responding about structure or proposed context. CEF allocates Trust Establishment as subcomponent of eDelivery[174]. e-SENS Trust Establishment related standards are described in Ch. 4.2.5 of this document.

5.8.4. Need for further development of this building block

e-SENS SAT Trust Establishment is developed in line with the objectives of eIDAS[175]. More conceptual analysis is needed to decide over adequacy or usability within OOP environment and whether it should be used according to CEF eDelviery framework.

5.8.5. External interfaces for this building block

According to CEF approach, Access Points need to establish trust between each other. This is possible using digital certificates. PKI service is a "set of roles, policies, procedures and systems needed to create, manage, distribute, store and revoke digital certificates. The CEF eDelivery PKI service enables issuance and management of the digital certificates used in the CEF eDelivery components, e.g., between **CEF eDelivery Access Points** (AP)[176] and **Service Metadata Publishers** (SMP)[177], to ensure confidentiality, integrity and non-repudiation of the data moving across systems. This service is provided to policy domains interested in creating a trust circle for information exchange using the technical specifications and components of CEF eDelivery. The use of the CEF eDelivery PKI is optional, policy domains may choose to use any other PKI service or mutual trust mechanism."[178]

Information about the **Service Metadata Locator** (SML) is available here (currently not any software components are available).[179] The full description of the Service Desk processes and the distribution of related roles and responsibilities are available in the Service Offering Description available online on the CEF Digital Single Web Portal[180].

5.9.eDocument

This section presents the eDocument building block in more detail, investigating the following aspects.

- Need for this building block by the TOOP pilots, as well as for OOP applications in general;
- Adequacy of specifications and software that can be utilized for specifying and building applications that use this building block;
- Adequacy of maintaining and supporting organisation for this building block;
- Need for further development of this building block to be used in OOP applications;

[173] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+specifications
[174] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Trust+Establishment
[175] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[176] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+software
[177] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+software
[178] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service
[179] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+software
[180] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Service+desk

- External interfaces for this building block needed for the pilots as well as for OOP applications in general.

5.9.1. Need for this building block

Developing interoperable reusable cross-border solutions for public administration, involves exchanging information between participants citizens, businesses and public administrations. The information exchanged comprises data and documents that must comply to a mutually agreed standard in order to ensure interoperability between participants.

The once-only principle applied to electronic documents means that users, citizens and businesses, must have the right to provide electronic documents only once to a public authority. In order to reduce the administrative burden, public administrations should share electronic documents at internal level and reuse them in accordance to data protection regulations.

eDocument building block supports public administrations to exchange electronic documents and data with other public administrations and businesses, in an interoperable, reliable and trusted scenario.

eDocument addresses the following services: document structuring and transformation, presentation and processing, profiling, packaging and document routing. Through the use of eDocument, every participant can send and receive in a standardised manner electronic documents through standard transport protocols and security policies.

eDocument building block contributes to achieving once-only principle goals by providing high-level electronic document design, facilitating the exchange of data together with meta-information and allowing automated machine processing, thus it may be useful for solutions developed in TOOP pilots and other OOP compliant applications

5.9.2. Adequacy of specifications and software

eDocument building block relies on several specifications and standards that are overviewed bellow:

5.9.2.1. ASiC Specification

ASiC is an ETSI specification which describes a container structure binding together several data objects: documents, XML data, spreadsheet, multimedia content with Advanced Electronic Signatures or time-stamp tokens into one single digital container. This uses package formats based on ZIP and supports CadES, XadES, detached signature(s) and RFC 3161[181] time-stamp tokens formats.

For an increased interoperability among organisations that use a document container, it is necessary to create an agreed profile. Profiling means identifying a common set of options that are appropriate to the target environment.

Any ASiC container has an internal directory structure including:

- a root folder, for all the container content, possibly including sub-folders reflecting the content directory structure;
- a META-INF sub-folder, in the root folder, for metadata about the content, including signatures associated with the container content.

[181] https://www.ietf.org/rfc/rfc3161.txt

It can be used in two basic formats:

- ASiC-S (Simple) containing only one signed data object and its detached signature(s) or a time-stamp token. CAdES or XAdES detached Signature(s) or Time-stamp token are applied to a single data object;
- ASiC-E (Extended) containing a set of signed data object and possible metadata and its detached signature(s) or time-stamp token(s). CAdES or XAdES Signatures or Time-stamp Tokens applied to a set of files.

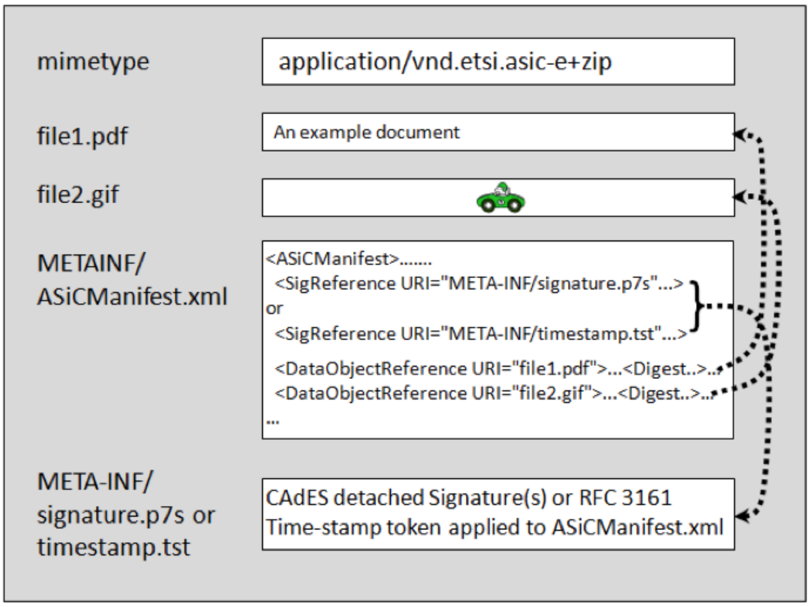

mimetype
application/vnd.etsi.asic-e+zip
file1.pdf
An example document
file2.gif
METAINF/
ASiCManifest.xml
<ASiCManifest>.......
<SigReference URI="META-INF/signature.p7s"...>
or
<SigReference URI="META-INF/timestamp.tst"...>
<DataObjectReference URI="file1.pdf">...<Digest..>..
<DataObjectReference URI="file2.gif">...<Digest..>..
...
META-INF/
signature.p7s or
timestamp.tst
CAdES detached Signature(s) or RFC 3161
Time-stamp token applied to ASiCManifest.xml

Figure 14: ASiC-E with CAdES signature [182]

ASIC enables in a domain independent context, authentic exchange of eDocuments and additional metadata.

ASiC software implementation

A generic implementation of ASiC-E archives in accordance with ETSI 102 918 v1.3.1. is available and open source on GitHub[183].

5.9.2.2. SBDH

For e-Documents routing process in OOP applications an available solution is UN/CEFACT Business Document Header SBDH[184] standard that allows end entities to encode information on business process, Business transaction, agreement, and business quality-of-service. The SBDH is widely adopted in e-business communities like GS1.

SBDH holds the information required to electronically route the e-Documents between participants involved in a transaction, thus supporting the automation of business processes.

Examples of information carried within the envelope are the receiver and the sender address, the type of the payload and the business scope.

[182] http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.01.01_60/ts_102918v010101p.pdf

[183] https://github.com/difi/asic

[184] http://wiki.ds.unipi.gr/display/ESENS/PR+-+SBDH

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

SBDH is useful at the business application and middleware levels to ensure routing and identifying of business documents. The information placed in the SBDH at the business payload level, travels with the business information to many different workflows from sender to receiver. In addition to the business payload information, it is useful to the business application and middleware to know the creator and receiver of the document. SBDH is agnostic of the message transport protocol used.

The SBDH facilitates three main business needs:

- The routing of business documents from one point to another. This refers not only to the transfer of information from an external originator to receiver, but also from one intermediate application to another;
- The simplified processing of documents. Processing refers to taking action on data, for example transforming it from one format into another. Information in the SBDH can reduce the effort required to determine the correct processing actions;
- Associating a data message with its originator is important from a business and legal perspective. It is especially important when using intermediaries for data transfer, as information from the transport protocol, may be lost after the initial transmission.

Information in the SBDH can be categorized into the following 4 categories:

- Document Routing contains the 'Sender' and 'Receiver' data structures;
- Document Identification includes information which will be used by the middleware to identify and route the message to the appropriate business application without having to open or parse the business document payload;
- Document Processing Context used to provide parameters for processing the business document in the context of a business choreography exchange;
- Payload, the area where the actual business information content of the message is included.

Document Routing information is found in the 'Sender' and 'Receiver' data structures of SBDH and it is used to identify the message sender and message receiver using unique identifiers for and optionally with additional contact information details.

SBDH Software implementation

A generic implementation of Standard Business Document Header is the PEPPOL implementation available and open source on GitHub[185].

5.9.2.3. W3C XSL and XSLT

W3C XSL[186] is a set of recommendations for defining XML document transformation and presentation including XSL Transformations (XSLT)[187] a language for transforming XML, XML Path Language (XPath)[188] an expression language used by XSLT (and many other languages) to access or refer to parts of an XML document and XSL Formatting Objects (XSL-FO), an XML vocabulary for specifying formatting semantics.

XSLT (Extensible Stylesheet Language Transformations) is a language for transforming XML documents into other XML documents, or other formats such as HTML for web pages, plain text or XSL Formatting Objects, which may subsequently be converted to other formats, such as PDF, PostScript and PNG. XSLT is widely supported in modern web browsers.

[185] https://github.com/difi/peppol-sbdh

[186] https://www.w3.org/Style/XSL/

[187] http://www.w3.org/TR/xslt

[188] http://www.w3.org/TR/xpath

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

When using XSLT the original document is not changed rather a new document is created based on the content of an existing one. Typically, input documents are XML files, but anything from which the processor can build an XQuery and XPath Data Model can be used, such as relational database tables or geographical information systems.

5.9.2.4. Open Annotation (OA) Data Model

The primary aim of the Open Annotation Data Model(OADM)[189] defined by the W3C Open Annotation Community Group is to provide a standard description mechanism for sharing Annotations between systems. It may be used either for sharing information with others, or the migration of private Annotations between devices. The shared Annotations must be able to be integrated into existing collections and reused without loss of significant information. The model should cover as many annotation use cases as possible, while keeping the simple annotations easy and expanding from that baseline to make complex uses possible.

OADM can meet annotation requirements that may arise in a business domain without the need to modify the e-Document formats.

5.9.2.5. Schematron

Schematron[190], an ISO standard, is a rule-based validation language for making assertions about the presence or absence of patterns in XML trees. It is a structural schema language expressed in XML using a small number of elements and XPath.

It can require that the content of an element be controlled by one of its siblings. Or it can request or require that the root element, regardless of what element that is, must have specific attributes. Schematron can also specify required relationships between multiple XML files. Schematron rules can be created using a standard XML editor or XForms[191] application.

It is intended to satisfy the annotation requirements that may arise in a business domain without the need to modify the e-Document format.

5.9.3. Adequacy of maintaining and supporting organisation

The e-Documents SAT, developed by the e-SENS project, is envisaged to be taken over by CEF after an analysis that will be carried out in the summer of 2017.

5.9.4. Need for further development of this building block

During e-SENS project, an assessment on the maturity of the building blocks was conducted and the results were included in deliverable 'D3.2 Assessment on the maturity of building blocks'[192]. Also, sustainability plans were included in 'D3.7 Sustainability plans for e-SENS building blocks'[193], which revealed eDocuments BBs current maturity status and sustainability plans.

The ASiC building block is a mature eDocument BB as it has been piloted and is now running in various open source implementations. ASiC, based on international standardisation activities in ETSI, is implemented and used in production used by e-CODEX and e-SENS projects.

[189] http://www.openannotation.org/spec/core/

[190] http://standards.iso.org/ittf/PubliclyAvailableStandards/c040833_ISO_IEC_19757-3_2006(E).zip

[191] https://en.wikipedia.org/wiki/XForms

[192] https://www.esens.eu/sites/default/files/e-sens_d3.2.pdf

[193] https://www.esens.eu/sites/default/files/e-sens_d3.7.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

The Document Provisioning ABB may need further elaboration of domain specific standards, their relationships, as well as languages and tools for document provisioning in different domains in order to evaluate its maturity or to propose further actions for their development.

SBDH is in an acceptable stage of maturity and its adoption may help public administrations in OOP applications scenarios by providing a consistent interface between applications and improving possibilities for automated processing of documents.

In the deliverable 'D3.2 Assessment on the maturity of building blocks: second cycle'[194], several recommendations were given for SBDH improvement: 'The most important recommendations concern development of a finalised version of the UN/CEFACT STANDARD BUSINESS DOCUMENT HEADER Technical Specification Version 1.3, issued on 2004-6-04 (draft); licensing on a (F)RAND and royalty-free basis; and providing data about usage of SBDH in different industries, business sectors or functions'.

5.9.5. External interfaces for this building block

eDocument building block supports the handling electronic documents by the public administration while providing a common and unambiguous terminology and approach to cope with the interoperability needs. eDocument building block facilitates the automated exchange of data together with meta-information, thus it may be useful for solutions developed in TOOP pilots and other OOP applications.

An e-Document carries information as payload and supports functions to be used in creating, processing and presenting the information to the end-user, functions exposed as e-Document services.

The e-Document solutions are constrained to realising the e-Document services: document provisioning (transformation and structuring, presentation and processing, profiling), document packaging and document routing.

Thus, the following building blocks that are needed for the pilots were identified:

- Document Provisioning: describes how to produce (transform documents and structure) and consume (present and process) an e-Document;
- Document Container: describes the packaging;
- Document Routing: describes the routing envelope used for the delivery of electronic documents.

5.9.5.1. Document Provisioning

Document Provisioning recommends specifications and standards that will aid and support the defined process models and their corresponding functionalities. It will ensure the technical, the syntactic and the semantic interoperability in the e-Documents domain.

For Document Provisioning the following services were identified:

- Document Structuring and Transformation Service:
    a) Structure and describe a document using semantic tools (schemes, vocabularies);
    b) Annotate the document;
    c) Attach validation and business rules (schematron rules);
    d) Transform an e-Document from one structured format to another for further processing according to an agreement between involved parties;

[194] https://www.esens.eu/sites/default/files/e-sens_d3.2_part2.pdf

- Document Presentation and Processing Service:
    a) Validate against the schematron rules;
    b) Process the business rules;
    c) Extract structured information so it can be available to the recipient;
    d) Present the document to end-user in a standard format;
- Document Profiling Service:
    a) Provides guidelines and 'best practice' in profiling the e-Document functionality to specific domains or use cases.

5.9.5.2. Document Container

Document Container proposes for public administration use cases, an interoperable specification for the container format that involves advanced signatures, trusted timestamp usage, document encryption and journaling to be interchanged across borders.

For Document Container the following services were identified:

- Document Packaging Service forms the structure of the container and container integrity validation. The result is a Container with different mimetypes such as zip;
- Signatures Attaching Service indicates adding signatures and reference to the signed documents. The outcome is a container signature element;
- Adding Timestamp Service enables adding trusted timestamp;
- Document Encryption Service enables encrypting documents inside container. The result of the process is an encrypted data object.

5.9.5.3. Document Routing

Document Routing services support the electronic routing the e-Documents between participants involved in the transaction and supports automated documents delivery, through eDelivery transport solution.

The routing envelope contains a set of standard elements necessary to determine the routing and processing of documents, optionally providing service and correlation information, at the business domain level, between trading partners. It can hold information concerning the receiver and the sender address, the type of the payload and the business scope.

Document Routing service involves the following component services:

- Include Routing Information Service which adds the information needed for routing the document;
- Embed the e-Document Service which embeds the e-Document into the routing envelope.

5.10. Semantics

This section presents the Semantics SAT in more detail. The main challenge for the semantics building blocks is to enable semantic interoperability between IT systems of different member state governments within the EU. We define semantic interoperability as the ability of software to accept data from external sources such that the software does not draw invalid conclusions about the state of affairs about the shared reality.

5.10.1. Need for this building block

Unfortunately, when semantics are concerned, the most applied design solution is to develop a centrally coordinated definition on terms, resulting in a monolithic semantic architecture. It is exactly

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

this semantic monolith that will show an impediment to the once-only principle. We will establish the foundations for an alternative approach towards a loosely-coupled semantic architecture.

5.10.1.1. An architecture for semantic interoperability

The core to the solution is to strive for a loosely coupled semantic architecture. Loose coupling is a result of the application of three architectural principles:

1. Separation of concerns:
   In its classical context of use, separation of concerns refers to clustering homogeneous functionality, i.e., assuring that (i) functions nor data are duplicated, in order to exclude contradictions and support maintainability, and (ii) that closely related (atomic) functions are grouped together into one single component in order to minimise connections between components. In the semantic context, separation of concerns refers to clustering semantics to their managing origin, in order to allow for heterogeneous semantics and subsequent higher consistency, correctness, accuracy, and completeness. Furthermore, a distinction is necessary between the ontological commitment as well as the expressiveness that the model allows, i.e., the categories that the model commits to, and, the semantics that the model (ontology) expresses itself [195]*. Note that for the creation of the semantic building blocks, functionality is required as well, albeit oriented towards semantics and semantic interoperability, and therefore, the classical context of separation of concerns apply as well.*
2. Transparency, a.k.a. Information hiding:
   In its classical context, transparency means a clear separation between <u>what</u> functionality a component establishes from <u>how</u> the component establishes its functionality. This separation is necessary to provide for stability in the use of the component at the one hand, and allowing for innovation, evolution and performance improvements at the other hand. In the semantic context, the same distinction is made between <u>what</u> is meant with the data and <u>how</u> we represent semantics and interpret data. Semantic transparency refers to the difference between the syntax that is used to convey data from the semantics that we assign to the syntax. As a result, this principle provides for stability in semantics while each and every component can apply its own native syntax to communicate with each other, allowing for evolution in semantics, and innovation and improvements in conceptualising reality and assignment of semantics to syntax.

In below, the semantic interoperability view is depicted that shows several consequences of the application of the above principles. The figure depicts how two different applications can provide for the capability of semantic interoperability between them. We will address the characteristics one by one:

a) The horizontal dotted line represents the separation between reality and its counterpart in the virtual IT environment. In the observed reality, also known as the domain of the signified, each application is interested in a certain part of reality, depicted as their 'Universe of Discourse' (UoD). For two applications to become interoperable, an overlap in their UoD's is required,

[195] This is a more technical aspect on semantics, the need for which is not apparent. As an example, consider the UML specification with its four levels of modeling: M0 represents the real world, M1 its virtual counterpart, i.e, the data, M2 the model that instantiates into M1, and M3 the meta-model that provides for the elements that can be used to model, i.e., a class, an object and their instance relation. In this case, the ontological commitment of UML is provided by M3, while the semantics of the model is provided by M2. Since you cannot model anything other than the categories that are allowed by M4, the semantics that we assign to the elements of M4 limits our possibility to express the semantics of the model at M3.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

otherwise there is nothing to communicate about. This part is denoted as the *shared universe of discourse*.

b) Each piece of software will maintain its own conceptualisation of its own UoD. This happens in the domain of the signifier, where the conceptualisation, represented as *ontology*, can only refer to reality. This referral is bi-directional: on *interpreting* an ontology, the concepts from the ontology are given meaning in that they refer to the entities in reality that they denote; on referring to an entity in reality to which it was not intended to refer, remains an interpretation albeit an invalid one. Vice versa, on *signifying* an entity in the UoD, a particular (construct of) concept(s) are assigned a meaning, that is, agreed to refer to that particular entity. Note that the referral between the signifier and the signified is conceptual only and does not pertain to any actual connection whatsoever.

c) A *data set* represents, eventually, an *instantiation* from the ontology. The semantic structures and rules that apply for the concepts from the ontology will apply equivalently for the data. In this way, no data exist that has not been conceptualised into the ontology first. The rules that are formalised by the ontology will be enforced on the data as well as on the software that is operating on the data.

d) The *alignment* provides for the formal relationships that hold between the concepts from both ontologies. It cannot be built without knowledge about both ontologies as well as the shared UoD they refer to. The latter will be the grounding for assuring correctness of the alignment. Besides a unique identification, an alignment consists of several *correspondences*, each of which specifies two concept expressions and a correspondence relation that specifies how both concept expressions refer to each other. A concept expression refers to one ontology only, and can either be a named, atomic concept, or a combination of named, atomic concepts that together form a (potentially unnamed) compound concept. Many relations can be defined to apply; however, the most common ones are *equivalence* (≡), *more specific than* (≤), *more generic than* (≥), *is of type* (E), *is type of* (∃), and, *is disjoint with* (⊥).

e) The *semantic mediation* process can be described simply as an automated, real-time translation between the two native terms of the ontology. Since data represent an instance of an ontological concept, the translation addresses mostly the translation of the ontological concept. To that end, it needs knowledge how to translate the source concept into the target concept, and it gets this from (a particular correspondence from) the alignment. Whenever the correspondence relation specifies equivalence, indeed the mediation represents a translation from a source concept into a target concept, according to the correspondence specification. For other correspondence relations, complications arise due to the inequivalence between the correspondence relation, e.g., *is more generic than*, and the equivalence relation that translating one concept into another essentially represents. In these cases, a thorough understanding of the source and target concepts in their ontological context at the one hand, and the logical consequences of the correspondence relation at the other hand, are required to prevent phantom semantics to occur.
In addition to the translation of the concepts, the correspondence might specify a transformation of the data as well, e.g., unit conversion, data resolution differences, and more.

The semantic interoperability view specifies only one process, i.e., the semantic mediation. Despite being a complicated process, the most important aspect of the semantic interoperability view is the fact that semantic interoperability can be achieved as a run-time data translation and transformation process that is dependent on a proper configuration by ontologies and an alignment only. Clearly, the characteristic of loosely coupled semantics is achieved by introduction of the semantic mediation process that is fed by ontologies and alignments. Aspects (a) – (c) are introduced by the principle of semantic separation of concerns, whilst aspects (d) and (e) implement a Chinese wall, introduced by the principle of semantic transparency, that prevents collaborating applications from infections with knowledge on how the collaborating peer has assigned meaning to its syntax.

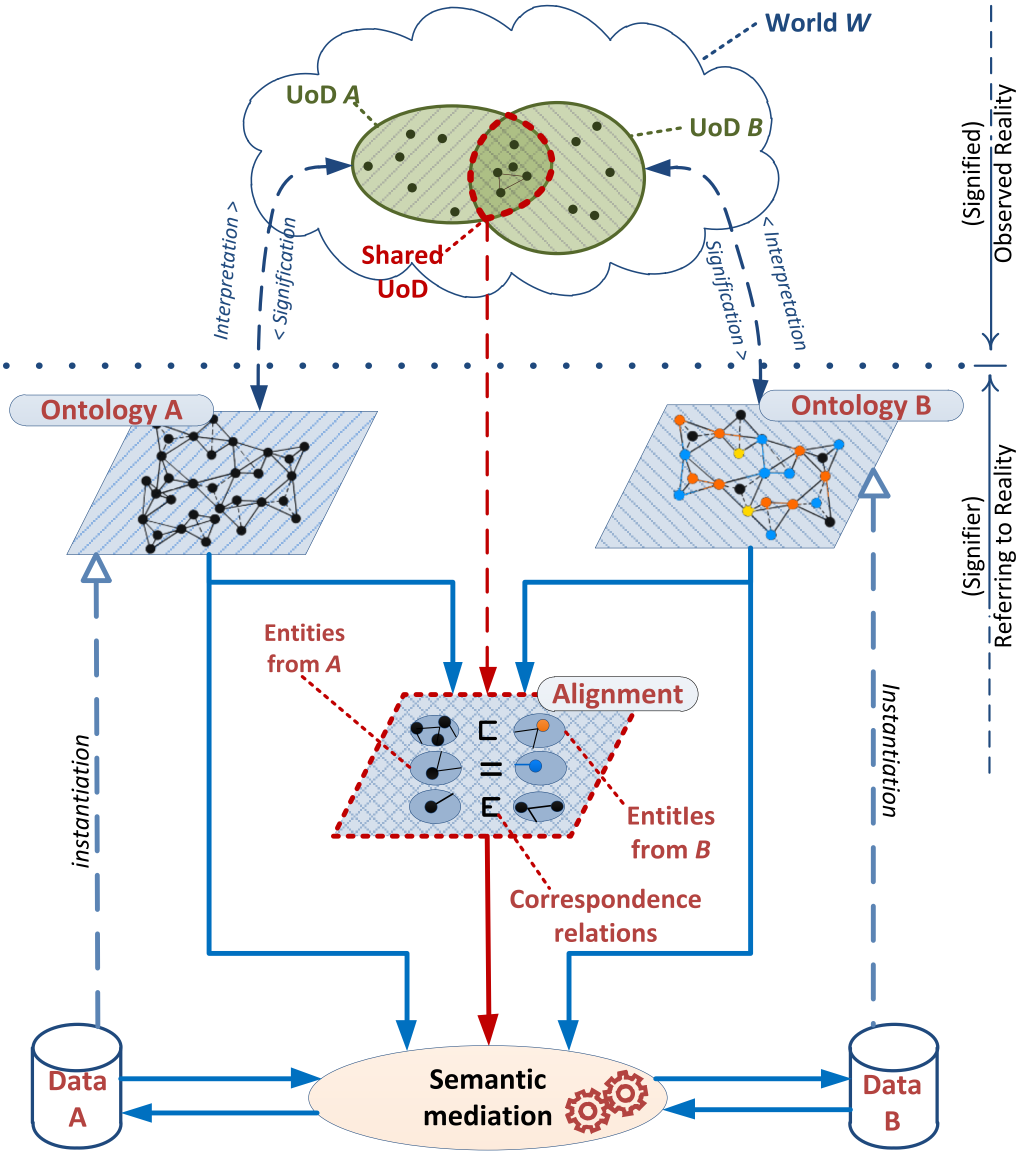


Figure 15: The semantic interoperability view

Based on this view we can derive that there is a need for different building blocks with the following functionality:

1. Semantic mapping, matching and mediation service;
2. Base registry service to store authentic data;
3. Alignment governance, registry and discovery service.

5.10.2. Adequacy of specifications and software

In the Semantics area, there are a few specifications that can be utilized by applications that need semantics support for OOP.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

5.10.2.1. Semantic mapping, matching and mediation BB

This building block provides functionality to find mappings and matches between the concepts and their relationships in different ontologies. This is a functionality that is needed at design-time and results in for instance mappings between ontologies used in different systems in different member states. These mappings are used in the semantic reconciliation building block to perform semantic alignment at run-time when this is asked for by member state systems in the pull and push scenario's in OOP cross-border applications.

Semantic definitions in different member states need to be aligned. Here, existing core vocabularies or top-level ontologies may present a valuable contribution to the semantic reconciliation process. The purpose of the semantic reconciliation is the specification of a complete, correct and sufficient alignment between the ontologies of collaborating peers.

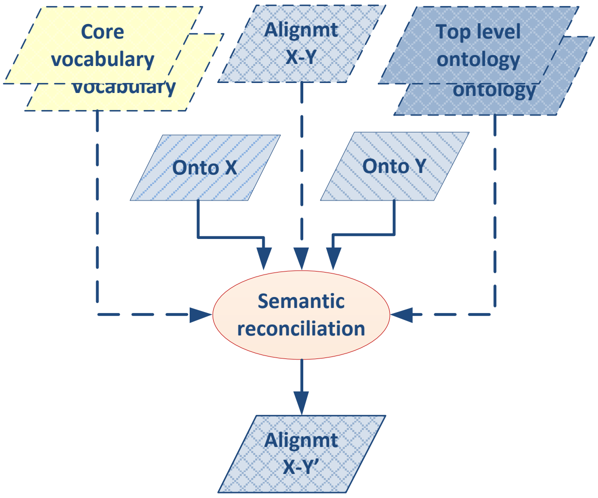


Figure 16: Design time: Semantic reconciliation generates an alignment between two ontologies

Unfortunately, for collaborating systems, the data will leave the warm nest of the application software and are enforced upon strange lands where the language differs, the rules apply strangely and unexpectedly, the constants vary, and the obvious variations and differences remain absent[196]. To prevent this influx of foreign data into native environments, the semantic mediation process assures that a valid translation and transformation of data takes place. The quintessence of this process has already been presented above.

This building block provides functionality for the actual reconciliation between terms in different systems, countries, member states or languages, when requested by a public service. Thus, at that point the specific alignment is discovered and applied to find a mapping with a set of terms requested for by a public service. This functionality is defined by the e-SENS Semantic Mapping Service BB.

5.10.2.2. Alignment governance, registry and discovery BB

An important characteristic that emerges due to the semantic architecture view as defined above, is that the major role of the alignment. Without a correct alignment, semantic mediation will induce phantom semantics or fail altogether. Correctness of the alignment is not only a matter of initial design; the correctness of the alignment is also vulnerable under the pressure of evolution and

[196] The data feel misunderstood, and indeed they are.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

operational maintenance, especially since alignments are highly dependent on both subject ontologies. Whenever a collaborating party decides to alter its ontology, this needs to be reflected in all alignments that make use of that ontology. To guarantee the internal consistency of the set <Alignment A-B; Ontology A; Ontology B>, as well as the synchronised deployment of the set, a governance process is deemed necessary that can accept the responsibility for delivering contingency in semantic interoperability.

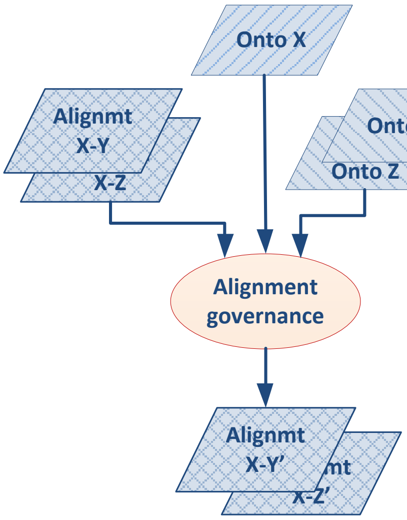


Figure 17: Design time: ontologies and alignments are tightly coupled

This building block provides functionality to search and find existing alignments between ontologies. This enables the possibilities to discover new or existing mappings when an alignment with a data source in another member state is requested by a specific public administration service. To our knowledge, such a building block does not yet exist in the public-sector domain. Thus, a new development trajectory might be in order. This might be the e-SENS Domain Knowledge Management System, but this needs to be verified.

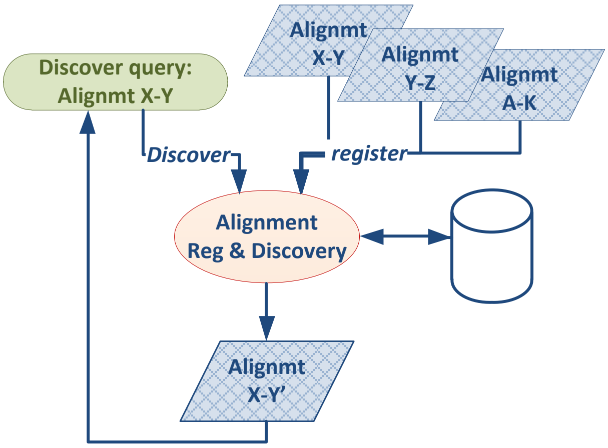


Figure 18: Runtime: an alignment registration and discovery service provides the semantic alignment

5.10.2.3. Base registry service BB

A base registry (BR) is a trusted authentic source of information under the control of an appointed public administration or organization appointed by government. In the e-SENS environment it can be

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

a source of information that is trusted as authentic by a community of users. This is the ISA definition and it is a generalization of the terminology server BB. Here the trusted information can be of any type while the terminology server is a trusted source for[197]. This Building Block complements the Trust Models with trusted Information Sources. ISA defines an abstract model for base registries, but we implement these registries in the form of services (already called terminology services in e-SENS) that leverage servers (terminology server). The main example is the e-CERTIS portal in ESPD –VCD pilot, but also SMP and SML are trusted sources.

5.10.2.4. Linked data technology and specifications

Linked data is based on Semantic Web philosophy and technologies but in contrast to the full-fledged Semantic Web vision, it is mainly about publishing structured data using the Resource Description Framework (RDF) data model and Unified Resource Identifiers (URIs) rather than focusing on the ontological level or inferencing. They facilitate semantic interoperability through the creation of typed links between data from different sources to interoperate at data level. These may be as diverse as data maintained by two organisations and modelled with different ontologies. Technically, Linked Data refers to data published on the Web in such a way that it is machine-readable, its meaning is explicitly defined, it is linked to other external data sets, and can in turn be linked to from external data sets. In this way, they promise the creation of the “Web of data” as data from decentralized and heterogeneous sources can be interlinked through typed links. Web of data aims at replacing data silos with a giant distributed dataset built on top of the Web architecture.

In the context of Linked Data, it is considered a good practice to reuse terms from well-known and standardized vocabularies wherever possible to make it easier for client applications to process Linked Data. Only if these vocabularies do not provide the required terms should data publishers define new, data source-specific terminology[198]. Regarding the OOP context, many core vocabularies have already been defined by the EU ISA programme and it is highly suggested to reuse them. Regarding the

[197] ISA Definitions:
http://ec.europa.eu/isa/actions/documents/isa_1.2_d1.2_base_registry_definition.pdf
A base registry (BR) is a trusted authentic source of information under the control of an appointed public administration or organization appointed by government, whereby:
Trusted means that the governing administration/organization is managing the registry/source conformant to best practices in all EIF-domains (not the least semantics/security) and conformant to legal/regulatory requirements
Authentic means that it is recognized as THE source, which represents the correct status of information.
It is kept constantly up-to-date and of the highest possible quality
Under control, means that only parties that have a necessity & finality & authorization can access the information in proportionality with their needs.
Appointed means: that the governing administration/organization has a legal basis / authority to collect and maintain the respective information.
A cross-border interoperable base registry (CIBR) is a base registry, opened through a single point of access to two or more electronic public services in other countries, using a multilingual interface and a standardized interface format and protocol. The CIBR is managed and operated by a legally based governance model providing cross-border interfacing services to electronic public services.

[198] Bizer, C., Cyganiak, R., Heath, T. (2007). How to publish Linked Data on the Web. http://www4.wiwiss.fu-berlin.de/bizer/pub/LinkedDataTutorial/

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

alignment of ontologies, relations between concepts of ontologies can be expressed using either the SKOS[199] or XKOS[200] vocabularies:

- SKOS enables 1-1 mappings using properties like skos:closeMatch, skos:narrowMatch, skos:broadMatch etc.
- XKOS enables n:m mappings. xkos:ConceptAssociation can describe the relationship of any number of source concepts to any number of target concepts rather than expressing the association through a set of pair-wise associations.

5.10.3. Adequacy of maintaining and supporting organisation

The Semantics SAT and its building blocks, developed by the e-SENS project, is not envisaged yet to be taken over by CEF. Nevertheless, the core vocabularies that are used in the semantics SAT are being maintained by the ISA program.

5.10.4. Need for further development of these building blocks

The e-SENS Semantic Mapping Service and the ISA Core Vocabularies are mature enough to be used by OOP applications. Further development might be needed in the support for alignment governance, registry and discovery as well as the base registry building blocks. Besides these building blocks there might be a need for further development of core vocabularies that are more specific for the OOP domain or that combines existing ontologies and vocabularies into an OOP ontology or vocabulary.

5.10.5. External interfaces for these building blocks

The Semantics building blocks support the mapping of different semantics of terms in different member states. It enables the design-time development of mappings and alignments between ontologies and the terms that they comprise, the governance, registry and discovery of these alignments and the run-time mediation or reconciliation upon request by a public service.

Thus, the following building blocks that are needed for the pilots were identified:

- Semantic Mapping Service: describes how to make a mapping between existing ontologies or vocabularies used in different member states. Existing core vocabularies are an important basic tool for this service;
- Alignment governance, registry and discovery: describes how alignments and mappings can be governed, registered and discovered by public services;
- Base registry: describes how basic, authentic data can be stored and made available.

5.10.5.1. Semantic Mapping Service

See: http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Semantic+Mapping+Service+-+0.6.0 for specifications of external interfaces for this building block.

[199] https://www.w3.org/2009/08/skos-reference/skos.html

[200] http://rdf-vocabulary.ddialliance.org/xkos.html

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

The Semantic Mapping Service offers the following functionalities:

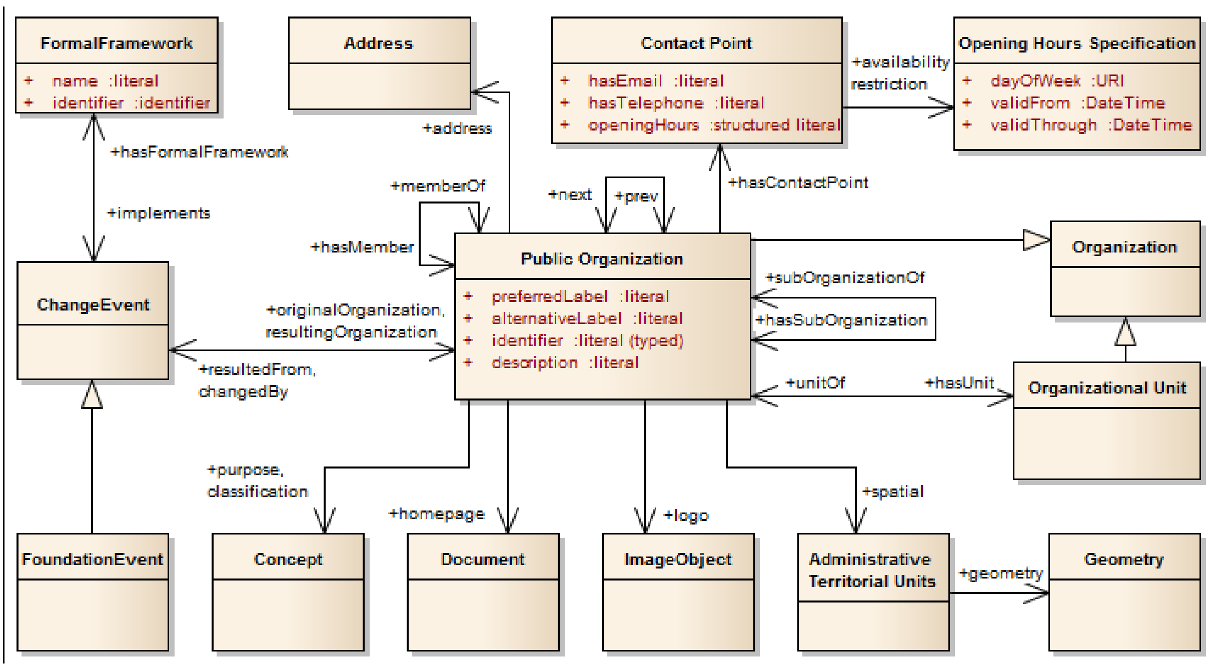
- Provision of a requirement list mapped in the requesters national legislation and the EU directives;
- Provision of a requirement-to-Document mapping based on the requestor's national legislation;
- Provision of a validation service stating that the actual documents provided are fit for the mapped requirements.

The service can make use of existing core vocabularies as developed by ISA program. Although there is no ‘external interface’ to a core vocabulary or an ontology, we give a brief pictorial overview of the various vocabularies to indicate which data elements are concerned.

5.10.5.2. ISA2 Core Person Core Vocabulary

See: https://joinup.ec.europa.eu/asset/core_person/description

Below is a snapshot of the ontology for this vocabulary.

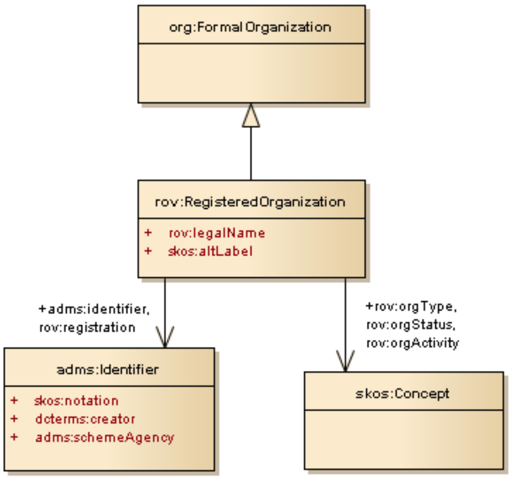


5.10.5.3. ISA2 Registered Organisation Core Vocabulary

See: https://joinup.ec.europa.eu/asset/core_business/description

Below is a snapshot of the ontology for this vocabulary.

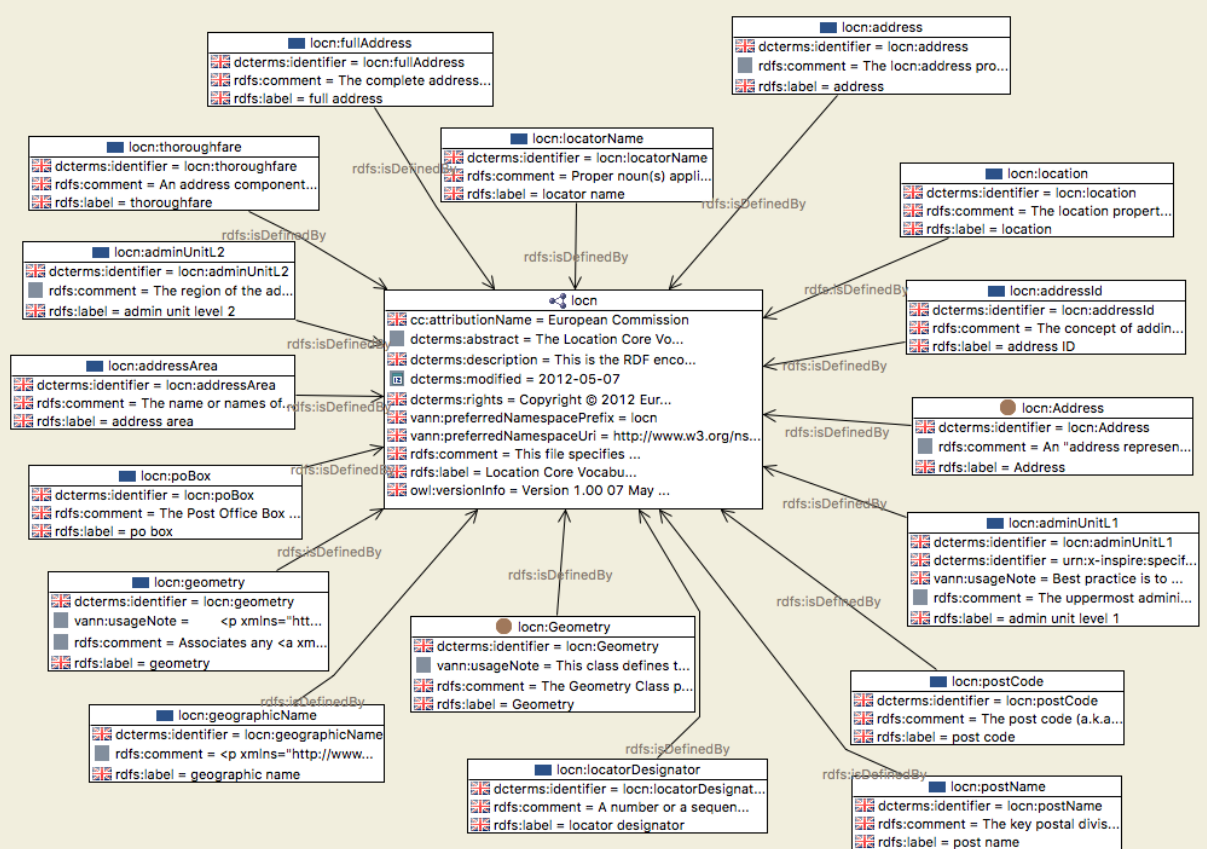
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460



5.10.5.4. ISA2 Core Location Vocabulary

See: https://joinup.ec.europa.eu/asset/core_location/description

Below is a snapshot of the ontology for this vocabulary.

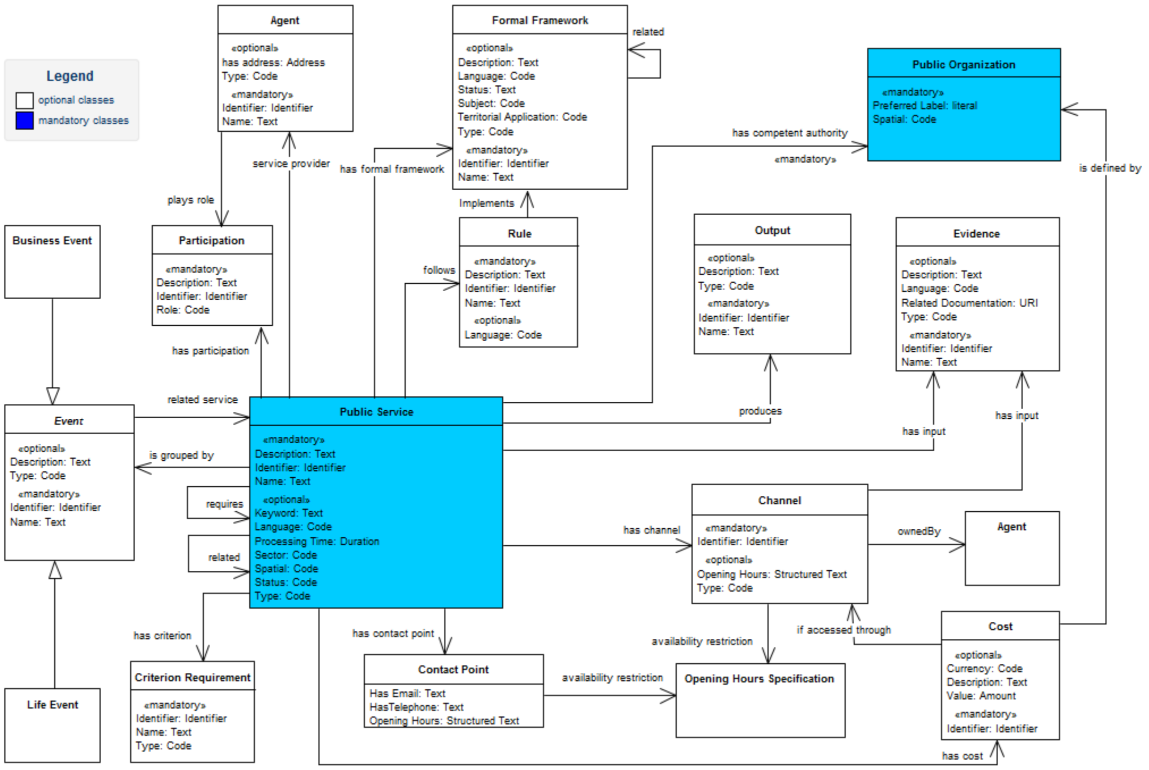

locn:fullAddress
dcterms:identifier = locn:fullAddress
rdfs:comment = The complete address...
rdfs:label = full address
locn:address
dcterms:identifier = locn:address
rdfs:comment = The locn:address pro...
rdfs:label = address
locn:thoroughfare
dcterms:identifier = locn:thoroughfare
rdfs:comment = An address component...
rdfs:label = thoroughfare
locn:locatorName
dcterms:identifier = locn:locatorName
rdfs:comment = Proper noun(s) appli...
rdfs:label = locator name
locn:location
dcterms:identifier = locn:location
rdfs:comment = The location propert...
rdfs:label = location
locn:adminUnitL2
dcterms:identifier = locn:adminUnitL2
rdfs:comment = The region of the ad...
rdfs:label = admin unit level 2
locn
cc:attributionName = European Commission
dcterms:abstract = The Location Core Vo...
dcterms:description = This is the RDF enco...
dcterms:modified = 2012-05-07
dcterms:rights = Copyright © 2012 Eur...
vann:preferredNamespacePrefix = locn
vann:preferredNamespaceUri = http://www.w3.org/ns...
rdfs:comment = This file specifies ...
rdfs:label = Location Core Vocabu...
owl:versionInfo = Version 1.00 07 May ...
locn:addressId
dcterms:identifier = locn:addressId
rdfs:comment = The concept of addin...
rdfs:label = address ID
locn:addressArea
dcterms:identifier = locn:addressArea
rdfs:comment = The name or names of...
rdfs:label = address area
locn:Address
dcterms:identifier = locn:Address
rdfs:comment = An "address represen...
rdfs:label = Address
locn:poBox
dcterms:identifier = locn:poBox
rdfs:comment = The Post Office Box ...
rdfs:label = po box
locn:adminUnitL1
dcterms:identifier = locn:adminUnitL1
dcterms:identifier = urn:x-inspire:specif...
vann:usageNote = Best practice is to ...
rdfs:comment = The uppermost admini...
rdfs:label = admin unit level 1
locn:geometry
dcterms:identifier = locn:geometry
vann:usageNote = <p xmlns="htt...
rdfs:comment = Associates any <a xm...
rdfs:label = geometry
locn:Geometry
dcterms:identifier = locn:Geometry
vann:usageNote = This class defines t...
rdfs:comment = The Geometry Class p...
rdfs:label = Geometry
locn:postCode
dcterms:identifier = locn:postCode
rdfs:comment = The post code (a.k.a...
rdfs:label = post code
locn:geographicName
dcterms:identifier = locn:geographicName
rdfs:comment = <p xmlns="http://www...
rdfs:label = geographic name
locn:locatorDesignator
dcterms:identifier = locn:locatorDesignat...
rdfs:comment = A number or a sequen...
rdfs:label = locator designator
locn:postName
dcterms:identifier = locn:postName
rdfs:comment = The key postal divis...
rdfs:label = post name
rdfs:isDefinedBy

5.10.5.5. ISA2 Core Public Service Vocabulary

See: https://joinup.ec.europa.eu/asset/core_public_service/description

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

The model of the Core Public Service Vocabulary is depicted at the following figure.

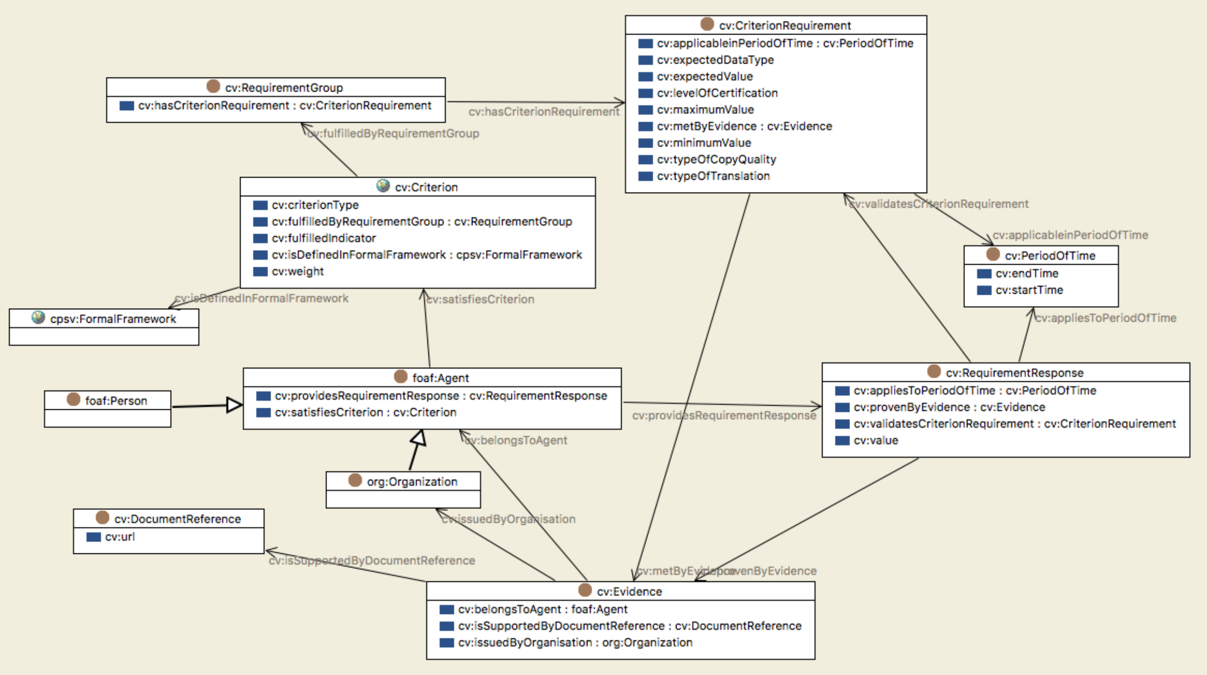


5.10.5.6. ISA2 Core Criterion and Core Evidence Vocabulary

See: https://joinup.ec.europa.eu/asset/criterion_evidence_cv/description

Below is a snapshot of the ontology for this vocabulary.

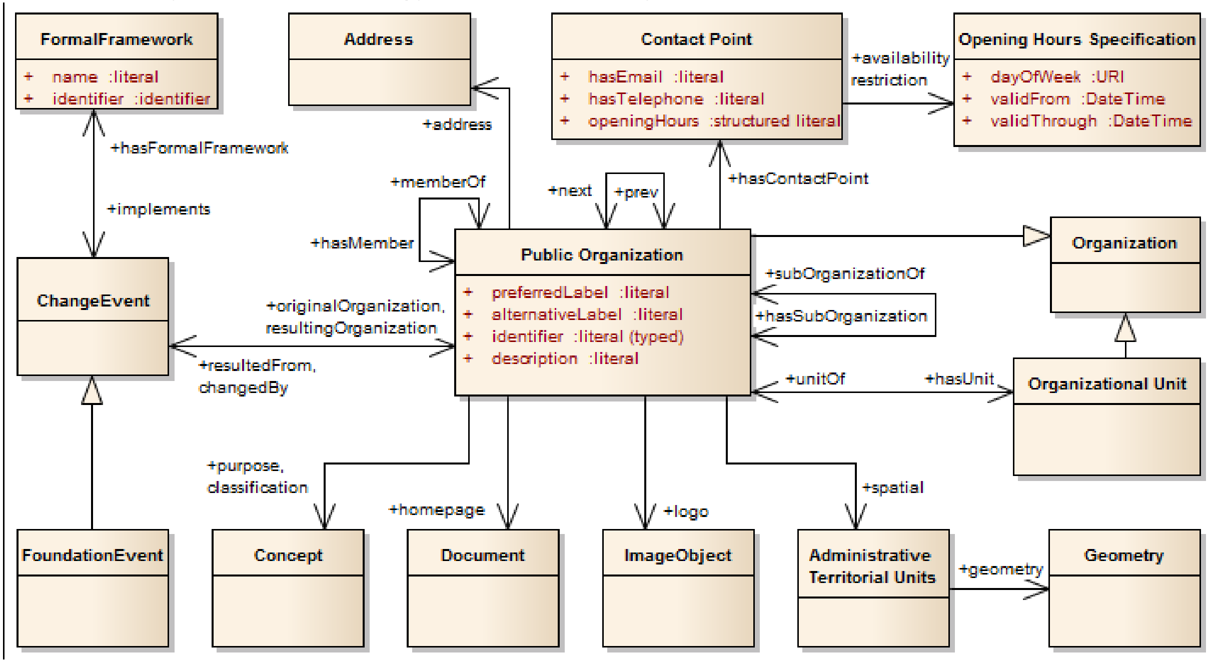
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460


cv:CriterionRequirement
cv:applicableinPeriodOfTime : cv:PeriodOfTime
cv:expectedDataType
cv:expectedValue
cv:levelOfCertification
cv:maximumValue
cv:metByEvidence : cv:Evidence
cv:minimumValue
cv:typeOfCopyQuality
cv:typeOfTranslation
cv:RequirementGroup
cv:hasCriterionRequirement : cv:CriterionRequirement
cv:hasCriterionRequirement
cv:fulfilledByRequirementGroup
cv:Criterion
cv:criterionType
cv:fulfilledByRequirementGroup : cv:RequirementGroup
cv:fulfilledIndicator
cv:isDefinedInFormalFramework : cpsv:FormalFramework
cv:weight
cv:validatesCriterionRequirement
cv:applicableinPeriodOfTime
cv:PeriodOfTime
cv:endTime
cv:startTime
cv:isDefinedInFormalFramework
cv:satisfiesCriterion
cpsv:FormalFramework
cv:appliesToPeriodOfTime
foaf:Person
foaf:Agent
cv:providesRequirementResponse : cv:RequirementResponse
cv:satisfiesCriterion : cv:Criterion
cv:RequirementResponse
cv:appliesToPeriodOfTime : cv:PeriodOfTime
cv:provenByEvidence : cv:Evidence
cv:validatesCriterionRequirement : cv:CriterionRequirement
cv:value
cv:providesRequirementResponse
cv:belongsToAgent
org:Organization
cv:DocumentReference
cv:url
cv:issuedByOrganisation
cv:isSupportedByDocumentReference
cv:metByEvidence
cv:provenByEvidence
cv:Evidence
cv:belongsToAgent : foaf:Agent
cv:isSupportedByDocumentReference : cv:DocumentReference
cv:issuedByOrganisation : org:Organization

5.10.5.7. ISA2 Core Public Organisation Vocabulary

See: https://joinup.ec.europa.eu/asset/cpov/description

Below is a snapshot of the ontology for this vocabulary.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Conclusion

This deliverable presents the first version of a generic federated OOP architecture. It depends on input form TOOP pilots in WP3, in particular on pilot requirements. From the other side, it has been planned as input for the pilot definition in WP3, thus it had to be delivered as early as possible to be useful for the pilot definition and implementation. To deal with this conflicting situation, it has been developed using an exploratory and agile approach and comprises the most important aspects of the generic federated architecture: the requirements, the initial building blocks, and the interface specifications, among others.

The next steps are to develop the architecture in more detail and to elaborate other tasks of TOOP T2.1 – development of a framework for specific OOP architectures and providing deployment profiles for building blocks. The exploratory and agile approach, together with cooperation with the TOOP pilots and other TOOP tasks, will be continued, resulting in forthcoming deliverables D2.2, D2.3, and D2.4.

Annexes: Preliminary List of Requirements for the TOOP Pilots

This Appendix presents preliminary requirements evolving from the TOOP pilot areas. These requirements are needed to select building blocks for inclusion into the architecture document, for communicating with the pilot developers, for designing the building block related content of the architecture, and for profiling the building blocks.

As noted in Ch 1.3, this deliverable has been developed using an exploratory and agile approach. The requirements presented in this chapter are useful for architecture development as an early indication of pilot needs, but they are preliminary and subject to change. The architecture developers have neither information nor mandate needed to modify them. For this reason, elaboration of the requirements (for example, formulating them as user stories or use cases or using standard relevant phrases, such as MUST, SHOULD, and so on[201]) is left to WP3.

As a summary, the PA requirements are produced in WP3 and will be reported in WP3 deliverables. The current version is included in the D2.1 Annex as a snapshot at the time of publishing, for information purposes, since WP3 has not produced any deliverables yet. This inclusion is an exception for the first iteration and not the rule for the next iterations of the Architecture.

Annex I. Cross-border e-Services for Business Mobility Pilot (PA1)

The pilot of Cross-border e-Services for Business Mobility includes the following motivational scenarios[202]:

- European Single Procurement Document (ESPD);
- Mandates (consuming);
- Licenses and Permissions.

The following requirements have been identified.

Number	Requirement
1.	The system must provide authentication
2.	Direct connection between participating systems can be established
3.	Pilot Area/ Economic Operator Representative / Legal Person's Representative / Professional can request ESPD, Basic Company information and information about the mandates and profession qualification form the country of origin
4.	Application for a tender/ cross-border service provision/ in the destination country is provided
5.	PA retrieve and verify the validity of the information
6.	Authorization for sending the information is provided
7.	Semantic mapping of information eCERTIS/EPC is provided

Table 3: Requirements for PA1

[201] https://tools.ietf.org/html/rfc2119

[202] TOOP Alignment workshop WP2 / WP3. WP3.1 Cross-border e-Services for Business Mobility. 18 Apr 2017. Antonis Stasis, Loukia Demiri

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Annex II. Updating Connected Company Data Pilot (PA2)

The Updating Connected Company Data Pilot implements an Event Notification service from the Business Registers towards any other Public Administrations at the European level. This could reduce the burden for the companies, ensuring at the same time the administrations of any MS of the correct, timely and complete update of the relevant company data. The pilot will take note of the timelines and technical implications of possible future integration and deployment into Business Registers Interconnection System (BRIS).

The following requirements have been identified.

Requirement ID	Requirement (specifies what should happen or hold or what should not happen or hold)	IT System, Registry or DB concerned	Goal to be achieved	Type of scenario
SECURITY-1	The system must authenticate participating organisations that access the system	eService, BR, BRIS	All the participants must be authenticated	Push & Pull
SECURITY -2	The system must verify that the data consumer is an authorized digital public service	Public digital service	The data consumer must be an authorised public eService to use the system	Push & Pull
SECURITY -3	Legal value of official public information must be maintained	eService, BR, BRIS	Information must be exchanged in a secure way	Push & Pull
BUSINESS-1	The system must provide a payment mechanism for data consumers to pay for the BR information and service, as required	PA eService, BR, BRIS	The BR has a business policy that must be applied to the information and service provided	Push & Pull
DATA-1	The legal value and meaning of data should not be altered crossing a national border	BRIS, BR	There must be a clear meaning of the information provided by the BR to the foreign service providers' technical-legal definitions beyond the everyday meaning of the words (e.g., "registration date", "limited liability company", etc.)	Pull & Push
ARCHITECTURE-1	Requests for and provision of BR data should take advantage of the BRIS, EBR and other existing infrastructures where requested by member states	PA eService, BRIS	Maximise the reuse of BRIS, EBR and other existing infrastructures, service agreements, organisations and governance rules	Push & Pull
ARCHITECTURE -2	The BRs must provide web service interfaces to push & pull requests for information and subscription management	BR (, BRIS)		Push & Pull
PUSH-1	The change in BR data notification must be an "alert" and not contain the actual changed data	BR		Push

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

PUSH-2	There must be a mechanism to unsubscribe from the change monitoring service	PA eService, BR	Either the subscription automatically expires after a certain time or there must be a way for the public eService to stop monitoring the change of a specific legal entity	Push
PUSH-3	The BRs will send change notifications asynchronously, based on a predetermined schedule (i.e., changes are not notified in real-time)	BR		Push

Table 4: Requirements for PA2

Annex III. Online Ship and Crew Certificates Pilot (PA3)

Currently ship and crew certificates are issued and maintained in paper format, resulting in delays in delivery to the vessel and extra costs. Certificate data exists in national Maritime Administrations (MA), which possess databases where certificate data are retained. The project will connect these databases and make the information available to the concerned parties. When this TOOP pilot is implemented, the flag state's MA and a recognized organisation issue the ship certificate and Port State Control (PSC), or any other interested party (e.g., Port Authority, Police and Border Guard Board, Charter Company), can view or check the certificate data online. Regarding the crew certificate, the seafarer's national MA issues a crew certificate, the ship flag state's MA checks the validity and authenticity of the crew certificate and the ship flag state's MA issues the endorsement of the certificate. Again, PSC or any other interested party (e.g., Port Authority, Police and Border Guard Board, Charter Company etc.) can view and check the certificate data online.

The following requirements for PA3 have been identified.

Requirement ID	Requirement (specifies what should happen or hold or what should not happen or hold)	Information System, Registry, or Database	Goal
SECURITY-1	Access to information must be limited to the corresponding role (PSCO, captain, ship owner / manager, general public), i.e. users must be authenticated, unless data is exchanged as open data (no confidentiality or business secret requirements)	Governing Authority Information System	Access information to e.g., Conduct Port State Control
SECURITY-2	Parties to the data exchange layer need to be certified.	Flag State Maritime Administration Database National Single Window (or European Maritime Single Window) RO Ship Certificates' Database Seafarer's State E-health Information System Seafarer's State Maritime Administration Database Inquirer's Information System Governing Authority Information System	Trust between the parties exchanging data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

SECURITY-3	Message Integrity, message authentication: messages should be secured against any modification during transmission. To enable electronic only certificates, non-repudiation is important.	Access Point to the Online Ship and Crew Certificates Pilot system (hereafter "Access Point") to Access Point	
SECURITY-4	Message Confidentiality – confidential messages should be encrypted during transmission	Access Point to Access Point	Confidential messages should be encrypted during transmission. Encryption is not mandatory during transmission of non-confidential data (non-authenticated view)
SECURITY- 5	Sender Identification- The identity of the sender should be verified by the system.	Access Point to Access Point	
SECURITY-6	Recipient / Addressee Identification - Recipient / addressee Identity should be verified before the delivery of the message.	Access Point to Access Point	Identity should be verified before the delivery of the message (not necessarily during transmission of non-confidential data - non-authenticated view)
SECURITY-7	Time – Reference - The date and time of sending and receiving a message should be indicated via a qualified electronic timestamp.	Access Point to Access Point	
SECURITY-8	Proof of Send/Receive - Sender and receiver of the message should be provided with evidence of message sending and receiving.	Access Point to Access Point	Not necessarily during transmission of non-confidential data (non-authenticated view)
FUNCTIONAL-9	The system must enable a trusted information system to locate and request data services from data providers	Inquirer's Information System	Port State Control Officer and other roles are able to request certificates' data
FUNCTIONAL-10	The system must enable certificate data to be provided to trusted parties	Ship Certificates' Database	Port State Control Officer and other roles are able to get ship certificates' data
FUNCTIONAL-11	The system must enable crew list data to be provided to trusted parties	Maritime Single Window (or EMSW)	Port State Control Officer and other roles are able to get the crew list data
FUNCTIONAL-12	The system must enable seafarer's certificate data to be provided to trusted parties	Seafarer's State Maritime Administration Database	Port State Control Officer and other roles are able to get seafarer's certificates' data
FUNCTIONAL-13	The system must enable seafarer's medical certificate data to be provided to trusted parties	Seafarer's State E-health Information System	Port State Control Officer and other roles are able to getseafarer's medical certificates' data
FUNCTIONAL-14	The system must enable discovery of trusted parties and data services		Discoverability of service providers and services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

AVAILABILITY-15	Latency of the result of the request must not be longer than [30 seconds]	Flag State Maritime Administration Database Maritime Single Window RO Ship Certificates' Database Seafarer's State E-health Information System Seafarer's State Maritime Administration Database Inquirer's Information System Governing Authority Information System	Availability of certificates' data for Port State Control Officer and other roles
FUNCTIONAL-16	Data provider must be able to regulate access to data, e.g. by trusted party classes	Flag State Maritime Administration Database RO Ship Certificates' Database Seafarer's State E-health Information System Seafarer's State Maritime Administration Database	Data provider can limit access to data
TECHNICAL-17	Organisations must be allowed to participate in data exchanges with their existing platforms	Architecture	Interoperability of information systems and databases through platform indepencency
ARCHITECTURE-18	Organisations must be able to communicate without intermediaries	Architecture	Decentralised governance
ARCHITECTURE-19	Scalability to global level and participation of non-EU countries must be supported. Participating countries must be able to support their own ecosystems, including central components and member management. Members belonging to different ecosystems must be able to communicate directly with each other.	Architecture	Trust federation, distributed governance
SUISTAINABLE-19	System should be sustainable on international level (who will maintain it)	Sustainability	Components will be maintained after the end of project
BUSINESS-20	Services should be and remain free of charge for participants	Business	Free public service

Table 5: Requirements for PA3

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460