



The Once-Only Principle Project

Generic Federated OOP Architecture (2nd version)

Eric Grandry, Paul Brandt, Jerry Dimitriou, Sander Fieten, Carmen Rotuna, Jaak Tepandi, Ermo Täks, Jack Verhoosel, Dimitrios Zeginis



Submitted to the EC on 28/02/2018

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

Generic Federated OOP Architecture (2nd version)

Deliverable Id:	D2.2
Deliverable Name:	Generic federated OOP architecture (2 nd version)
Version:	V1.0
Status:	Final
Dissemination Level:	Public
Due date of deliverable:	M12 (December 2017)
Actual submission date:	28/02/2018
Work Package:	WP2
Organisation name of lead partner for this deliverable:	Tallinn University of Technology
Author(s):	Eric Grandry Paul Brandt Jerry Dimitriou Sander Fieten Carmen Rotuna Jaak Tepandi Ermo Täks Jack Verhoosel Dimitrios Zeginis
Partners contributing:	All beneficiaries

Abstract:

This document presents the second official version of the generic federated OOP architecture. It develops further and extends the deliverable “D2.1. Generic federated OOP architecture (1st version)” (D2.1). The architecture supports interconnection and interoperability of national registries at the EU level, is in line with existing EU frameworks (EIRA, EIF), takes into account the forthcoming regulation about the Single Digital Gateway (SDGR), and uses results of the e-SENS European Interoperability Reference Architecture. It provides support for future developers of OOP projects and is based on the Connecting Europe Facility (CEF) Digital Service Infrastructures (DSIs), the Building Blocks consolidated by the e-SENS project, and in justified cases, on the new building blocks.

Compared to the first version D2.1, this deliverable develops the architecture further, aligns it with the provisions of the forthcoming regulation about the Single Digital Gateway, and focusses on the motivation, domain, and business views of the architecture. Summaries of the main characteristics of the applicable Building Blocks provided in D2.1 establish a starting point for the technology architecture. Detailed description of changes is provided in the section “Changes between D2.1 and D2.2”.

The architecture description in the current deliverable is organized along the business view, concerned with the business operations of the TOOP system. As the project is itself defining the Cross-Border Once Only and is required to support the development of the SDG Regulation, two preliminary views are added: the domain view, concerned with the definition of the Once Only domain (the problem domain), and the requirements view, concerned with the objectives, needs, legal obligations and principles driving the architecture. The architecture is oriented towards reusing existing frameworks and building blocks provided by CEF, e-SENS, and other initiatives.

The key concepts underlying the architecture, including the main principles of the Generic Once-Only Principle Reference Architecture (GOOPRA) are analysed in Ch 2. Chapter 3 presents the domain view, concerned with the definition of the Once-Only domain in which the TOOP project is situated. Requirements to the architecture, including the requirements stemming from the Single Digital Gateway Regulation, are proposed in Ch 4. The business view is designed in Ch 5, focussing on the description of the business operationalization of the Once Only Principles by the business actors. Summaries of the main characteristics of applicable Building Blocks provided in Ch 6, including rationale for their inclusion in the architecture, usage, maintenance, gap analysis, and need for further development, form a basis for the Technology Architecture to be developed further deliverable D2.3.

This deliverable is a work in progress. The next steps are to develop the architecture in more detail, to provide the information system architecture, to complement the technology architecture with how the BB are actually used to support the IS architecture and potential new BBs or extensions, as well as to continue the exploratory and agile approach, together with cooperation with the TOOP pilots and other TOOP tasks. The forthcoming official deliverables are D2.3 (M21, September 2018), and D2.4 (M30, June 2019).

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.

This is a preliminary version of the deliverable, pending review and approval by the European Commission.

Changes between D2.1 and D2.2

Modification	Details
Reworking and restructuring the methodology, architecture, and deliverable	Reworking the methodology, introducing provisions related to the SDGR, redesigning the architecture, restructuring and reworking all chapters of the deliverable, transforming the D2.1 Building Block chapters into summaries in D2.2
Improvements for readability	Added abbreviations, Glossary, summarizing sections and adding 'connecting' texts, made changes throughout the whole text of the deliverable
Update of work methodology	Modified Chapter 1.3. Methodology of Work with respect to reviewer comments, updates to the methodology used, and readability
Changes to Chapter 2 of D2.1 (Key Concepts and Principles)	Added subchapters on Purpose, Scope, and Status of the OOP Architecture, as well as on Generic Once-Only Principle Reference Architecture (GOOPRA)
Changes to Chapter 3 of D2.1 (Requirements)	Reworking and restructuring the requirements section as requested by the reviewers. Added requirements stemming from SDGR
Changes to Ch 4 of D2.1 (existing Building Blocks)	Chapter 4 of D2.2 comprises the domain architecture. Analyses of Building Blocks in Ch 4 and 5 of D2.1 have been transferred into summaries of the main characteristics of applicable Building Blocks in Ch 6 of D2.2, including rationale for BB inclusion in the architecture, usage, maintenance, gap analysis, and need for further development
Changes to Ch 5 of D2.1 (Views, Building Blocks)	Chapter 5 of D2.2 describes business architecture of GOOPRA. Analyses of Building Blocks in Ch 4 and 5 of D2.1 have been transferred into summaries of the main characteristics of applicable Building Blocks in Ch 6 of D2.2, including rationale for BB inclusion in the architecture, usage, maintenance, gap analysis, and need for further development. Added a subchapter with conclusion and summary table of the BBs selected for GOOPRA

Table of contents

LIST OF FIGURES	7
LIST OF TABLES	8
LIST OF ABBREVIATIONS	9
GLOSSARY	11
EXECUTIVE SUMMARY	12
1. INTRODUCTION	14
1.1. SCOPE AND OBJECTIVE OF DELIVERABLE	14
1.2. WP2 GENERAL OBJECTIVES AND VISION	14
1.3. METHODOLOGY OF WORK	15
1.3.1. ASPECTS OF THE WORK METHODOLOGY	15
1.3.2. ARCHITECTURE DESCRIPTION FRAMEWORK	16
1.4. RELATIONS TO INTERNAL TOOP ENVIRONMENT	18
1.5. RELATIONS TO EXTERNAL TOOP ENVIRONMENT	19
1.6. LEGAL ISSUES	19
1.7. STRUCTURE OF THE DOCUMENT	19
2. MOTIVATIONS FOR TOOP REFERENCE ARCHITECTURE	20
2.1. SINGLE DIGITAL MARKET INITIATIVE	21
2.2. FOSTERING THE BEST POSSIBLE USE OF THE POTENTIAL OF DIGITAL DATA	22
2.3. MODERNISING PUBLIC SERVICES AND E-GOVERNMENT	24
2.4. IMPLEMENT TOOP	26
3. DOMAIN DEFINITION AND DESCRIPTION	29
3.1. DOMAIN ROLES	29
3.2. ROLE COLLABORATIONS	31
3.3. DOMAIN PRINCIPLES	32
4. REQUIREMENTS DRIVING THE ARCHITECTURE DESIGN	36
4.1. ARCHITECTURE REQUIREMENT FRAMEWORK	36
4.2. ARCHITECTURE REQUIREMENT INCEPTION	38
4.3. ARCHITECTURE REQUIREMENT ANALYSIS	38
4.4. ARCHITECTURE PRINCIPLES SPECIFICATIONS	38
4.5. ARCHITECTURE REQUIREMENTS SPECIFICATIONS	42
5. BUSINESS ARCHITECTURE	48
5.1. BUSINESS DESIGN DECISIONS	48
5.2. BUSINESS ACTOR MODEL	50
5.3. BUSINESS COLLABORATIONS	50
5.3.1. CROSS-BORDER DATA RETRIEVAL	50
5.3.2. CROSS-BORDER DATA NOTIFICATION	53
5.4. BUSINESS CAPABILITY MODEL	54

5.5.	TOOP COMMON SEMANTIC MODEL	57
6.	TECHNOLOGY ARCHITECTURE	59
6.1.	EDELIVERY	59
6.2.	EID	60
6.3.	ESIGNATURE	61
6.4.	ETRANSLATION	62
6.5.	TRACEABILITY AND NON-REPUDIATION	64
6.6.	TRUST ESTABLISHMENT	65
6.7.	EDOCUMENT	66
6.8.	SEMANTICS	68
6.9.	SUMMARY OF THE BUILDING BLOCKS	69
	CONCLUSION	71
	REFERENCES	72
	ANNEX I. LEGAL FRAMEWORK REQUIREMENTS ANALYSIS	75
	ANNEX II. EIF REQUIREMENTS ANALYSIS	85
	ANNEX III. ARCHIMATE GOAL MODEL NOTATION	92
	ANNEX IV. CONTRIBUTORS	93

List of Figures

Figure 1: Context of TOOP Architecture Design	16
Figure 2: Generic Reference Architecture Description Framework	17
Figure 3: Activities within the TOOP architecture development process	18
Figure 4. Single Digital market initiative goal model.....	21
Figure 5. Fostering the best possible use of the potential of digital data	23
Figure 6. “Modernising public services and e-government” goal model	25
Figure 7. “Implement TOOP” goal model	27
Figure 8: Domain Role Model	29
Figure 9: Domain Collaboration.....	31
Figure 10: Data Retrieval Collaboration.....	51
Figure 11: Data Retrieval - DC Process	51
Figure 12: Data Retrieval - DP Process	52
Figure 13: Data Provider Capability Publication Process.....	52
Figure 14: Data Notification Collaboration	53
Figure 15: Data Consumer Subscription Process	54
Figure 16: Data Provider Notification Process	54
Figure 17: Business Capabilities Map.....	55
Figure 18: Snapshot of the TOOP Common Semantic Model	58
Figure 19: Example of a TOOP CSM concept to a national member state concept.....	58

List of Tables

Table 1 - Relevant Quality Attributes	36
Table 2 - Architecture Principles	38
Table 3 - Architecturally Significant Requirements	42
Table 4 - Business ADR's	48
Table 5: Business Capabilities	55
Table 6: TOOP Common Concepts	57
Table 7: Summary of the BB Analysis	70
Table 8. Goal model elements description	92
Table 9. Goal Model Relationships	92

List of Abbreviations

Acronym	Explanation
ABB	Architecture Building Block
ADL	Architecture Description Language
AI	Artificial Intelligence
AT	Automated Translation
BB	Building Block
BPMN	Business Process Model and Notation
BRIS	Business Registers Interconnection System
CCTF	Common Components Task Force
CEF	Connecting Europe Facility
CEF DSI	the DSI financed by CEF
D2.1	TOOP deliverable “D2.1. Generic federated OOP architecture (1st version)”
D2.2	TOOP deliverable “D2.2. Generic federated OOP architecture (2nd version)”
DC	Data Consumer
DP	Data Provider
DSI	Digital Service Infrastructure
EC	European Commission
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
GOOPRA	The Generic Once Only Principle Reference Architecture
IS	Information System
IT	Information Technology
JTF	Joint Technical Taskforce

JTG	WP3/WP2 Joint Technical Group
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
SDGR	Single Digital Gateway Regulation
TOOP	The Once-Only Principle Project
WP	Work Package

Glossary

Term	Explanation
Application Architecture	A description of the structure and interaction of the applications as groups of capabilities that provide key business functions and manage the data assets (source: The Open Group 2011)
Architecture	Fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution (source: ISO/IEC 42010:2011)
Architecture description	Work product used to express an architecture (source: ISO/IEC 42010:2011)
Architecture framework	Conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders (source: ISO/IEC 42010:2011)
Architecture view	Work product expressing the architecture of a system from the perspective of specific system concerns (source: ISO/IEC 42010:2011)
Architecture viewpoint	Work product establishing the conventions for the construction, interpretation and use of architecture views to frame specific system concerns (source: ISO/IEC 42010:2011)
Business Architecture	A description of the structure and interaction between the business strategy, organization, functions, business processes, and information needs (source: The Open Group 2011)
Information System Architecture	A description of the realization of the Business Architecture with IT components, and more specifically the existing building blocks, as well as a description of the principles guiding the design of the IS architecture
OOP architecture	A complex comprising the Generic Once Only Principle Reference Architecture and associated components, resulting from the TOOP project
OOP system	System based on the Once-Only Principle as applied in the TOOP project
Scenario	One typical way in which a system is used or in which a user carries out some activity.
Technology Architecture	The Technology Architecture describes the logical software and hardware capabilities that are required to support the deployment of business, data, and application services. This includes IT infrastructure, middleware, networks, communications, processing, standards, etc. (source: The Open Group 2011)
TOOP T2.1	TOOP Task 2.1, Federated Technical Architecture. This task focuses on three main activities: 1. defining a generic federated OOP architecture, 2. proposing a framework for development of specific architectures and applications for OOP, and 3. profiling of the common building blocks on specification level
Use case	A specification of one type of interaction with a system. One use case may involve several scenarios (usually a main success scenario and alternative scenarios)
User story	Informal description of one or more system features from the user perspective

Executive Summary

The eGovernment Action Plan 2016-2020 presents the Once Only Principle (OOP) - the public administrations should ensure that citizens and business supply the same information only once to a public administration. The Once-Only Principle Project (TOOP) is about exploring, demonstrating, and enabling the once-only principle in the European Union. The achievement of this objective is supported 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 legal landscape, OOP drivers and barriers, and sustainability.

TOOP focus area within OOP is on information related to business activities and on cross-border sharing of this information. The Generic Once-Only Principle Reference Architecture (GOOPRA) 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. As the TOOP project is required to support implementation of the Single Digital Gateway Regulation (SGDR), the architecture has been aligned with SDGR provisions.

The objective of this document is to present the second version of the OOP architecture, which develops further and extends the deliverable D2.1 “Generic federated OOP architecture (1st version)”. The architecture is aimed at formalizing the description of the designed system that supports interconnection and interoperability of national registries at the EU level. It has been developed using an exploratory and agile approach, in cooperation with the TOOP pilots and other TOOP Work Packages (WPs) and tasks.

Compared to the first version of the deliverable, D2.1, this updated deliverable develops the architecture further, aligns it with the provisions of the proposed Single Digital Gateway Regulation, and focusses on the motivation, domain, and business views of the architecture. Summaries of main characteristics of the applicable Building Blocks provided in D2.1 form a basis for the Technology Architecture to be developed further deliverable D2.3. Detailed description of changes is provided in the section “Changes between D2.1 and D2.2”.

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 (European Commission 2017). 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) (Chou et al. 2015), the CEF Building Blocks, and the e-SENS deliverable D6.6 “e-SENS European Interoperability Reference Architecture”, 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 key concepts underlying the architecture, including the motivation for the Generic Once-Only Principle Reference Architecture (GOOPRA) are analysed in Chapter 2;
- Chapter 3 presents the domain view, concerned with the definition of the cross-border Once-Only domain in which the TOOP project is situated;
- The requirements guiding the architecture design, including the requirements stemming from the Single Digital Gateway Regulation, are proposed in Chapter 4;

- The Business Architecture is designed in Chapter 5, focussing on the description of the business operationalization of the once-only principle by the business actors in terms of required business capabilities;
- Summaries of the main characteristics of applicable Building Blocks, including rationale for their inclusion in the architecture, usage, maintenance, gap analysis, and need for further development, are provided in Chapter 6 and form a starting point for the Technology 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 the European Interoperability Reference Architecture (EIRA), the European Interoperability Framework (EIF) (Publications Office of the European Union 2017), and the SDGR; that this architecture will be 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 new building blocks; and that it will provide support for future developers of OOP projects. Still continuous effort is needed for the regular updating and maintenance of the most mature building blocks, as well as for advancement of the building blocks which are still in the development stage.

This deliverable is a work in progress. The next steps are to develop the architecture in more detail, to add the Information System Architecture dealing with the structure and interaction of the applications that provide key business functions and manage the data assets, to complement the Technology Architecture with potential new Building Blocks and extensions and with the design of the usage of the Building Blocks to support the IS architecture, as well as to continue the exploratory and agile approach, together with cooperation with the TOOP pilots and other TOOP tasks. The forthcoming official deliverables are D2.3 (M21, September 2018), and D2.4 (M30, June 2019).

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 business supply the same information only once to a public administration. 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 business activities and on cross-border sharing of this information (Krimmer et al. 2017). The Generic Once-Only Principle Reference Architecture (GOOPRA) 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. Due to the shift in the TOOP project focus requiring it to support implementation of the Single Digital Gateway Regulation - SGDR (European Union 2017), the current version of the OOP architecture has been aligned with SDGR provisions.

The objective of this document is to present the second version of the OOP architecture, which develops further and extends the deliverable D2.1 “Generic federated OOP architecture (1st version)”. The 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.

Compared to the first version D2.1, this deliverable develops the architecture further, aligns it with the provisions of the proposed Single Digital Gateway Regulation, and focusses on the motivation, domain, and business views of the architecture. Main characteristics of the applicable Building Blocks provided in D2.1 are presented in a summary form. Detailed description of changes is provided in the section “Changes between D2.1 and D2.2”.

Assignments of the TOOP project T2.1 team have been significantly changed during the first year of the project. As agreed during the TOOP WP2 / WP3 meeting on 2-4 Oct 2017 in Rome, the TOOP T2.1 members are simultaneously contributing to several parallel processes: developing further the architecture; delivering T2.1 deliverables in specified deadlines; providing content to populate TOOP wiki; providing specifications for BB and responding to questions from the pilots in the WP3/WP2 Joint Technical Group (JTG), the Common Components Task Force (CCTF), and the Joint Technical Taskforces (JTF). Due to this shift in work orientation, a finalized version of the architecture is expected in the forthcoming versions of the deliverable - D2.3 (M21, September 2018), and D2.4 (M30, June 2019).

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 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 TOOP aims and activities. This project implements three TOOP pilots, develops a generic federated OOP architecture, supports implementation of the Single Digital Gateway Regulation, and explores other aspects of OOP and its supporting infrastructure such as OOP drivers and barriers.

The architecture described in this deliverable is qualified as a

- Generic Architecture, and a
- Reference Architecture.

The architecture is generic and is designed by abstracting domain specificities and identifying the genericities associated with the problem domain (the once only principle). It is part of an architecture continuum, as defined in The Open Group's Architecture Framework (TOGAF)¹ (The Open Group 2011), which allows to move from a generic architecture to a domain-specific and a pilot-specific architecture.

The architecture is a Reference Architecture as opposed to a solution architecture: Reference Architectures "capture the essence of existing architectures, and the vision of future needs and evolution to provide guidance to assist in developing new solution architectures" (Cloutier et al. 2010). Reference architectures are standardized architectures that provide a frame of reference for a particular domain, sector or field of interest (Proper and Lankhorst 2014). Reference models or architectures provide a common vocabulary, reusable designs and industry best practices. They are not solution architectures, i.e. they are not implemented directly. Rather, they are used as a constraint for more concrete architectures. Typically, a reference architecture includes common architecture principles, patterns, building blocks and standards.

The Generic OOP Reference Architecture (GOOPRA) is developed in cooperation with the TOOP pilots and other TOOP Work Packages. The main pilot design activities are done in TOOP WP3, and more specifically in the Common Components Task Force (CCTF), which is responsible for designing the common components to be used in the pilots. The GOOPRA builds on the know-how gained with designing the TOOP pilots and experience of previous Large Scale Pilots (LSP), especially the reusable building blocks constituting the Digital Service Infrastructure (DSI). The GOOPRA also contributes to the TOOP pilot design and to the development of the DSI.

After SDGR was introduced in April 2017, the TOOP project was given the task to provide input to the SDGR Implementing Act. This meant that the architecture had to take into account new requirements emerging from SDGR.

The GOOPRA is therefore developed by combining top-down and bottom-up approaches:

- The legal environment, specifically the draft SDG Regulation, as well as the user requirements from the pilots, guide the design of the architecture;
- The common pilot's solution architecture and the DSI are designed artefacts that are injected within the architecture.

¹ http://www.opengroup.org/public/arch/p3/ec/ec_ac.htm

The Figure 1 graphically represents this combined approach, including the expected outcomes of the GOOPRA: on one hand it should be a blueprint for the SDG implementing acts, and on the other hand it should contribute to both the pilot architecture and the DSI.

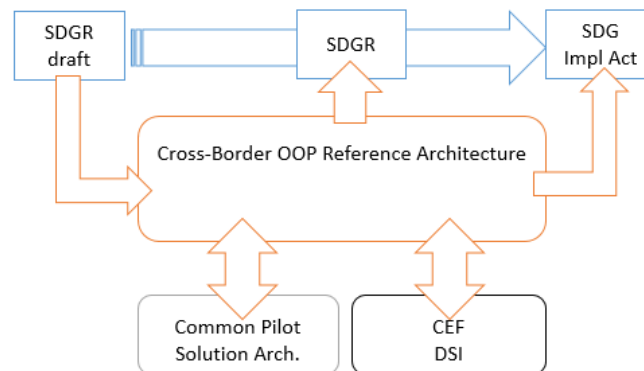


Figure 1: Context of TOOP Architecture Design

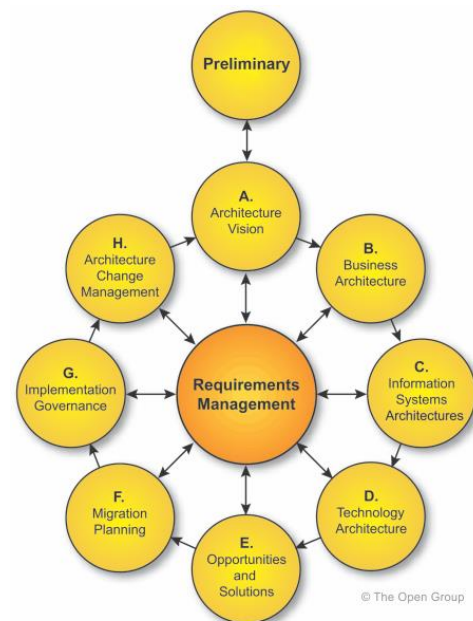
1.3.2. Architecture Description Framework

An architecture description is an artefact describing the architecture for some system of interest. In ISO/IEC/IEEE 4210, system refers to man-made and natural systems, including software products and services and software-intensive systems.

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 TOGAF and Zachman's information systems architecture framework² (Zachman 2008).

For the development process of the generic, federated OOP Architecture, we will use the steps of the Architecture Development Method (ADM) of TOGAF9.1³. 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.

An architecture description language (ADL) may specify one or more architecture viewpoints, but need not have any. The most well-known examples of architecture description languages are: ArchiMate, Business Process Model and Notation (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



² https://en.wikipedia.org/wiki/Zachman_Framework

³ <http://pubs.opengroup.org/architecture/togaf9-doc/arch/>

TOGAF architecture framework, we will make use of the Archimate3.0⁴ specification as architecture description language.

The GOOPRA description is organized along the following architecture views, adopted from TOGAF framework: the business view (**Business Architecture**), concerned with the business operations of the TOOP system, the IS view (**IS Architecture**), concerned with the realization of the business operations with information systems, and the technology view (**Technology Architecture**), concerned with the reuse of the DSI to support the IS architecture. However, as the project is itself defining the Cross-Border Once Only and is required to support the development of the SDG Regulation, two preliminary views are added: the domain view (Reference Model), concerned with the definition of the Once Only domain; the motivation view, concerned with the objectives, needs, legal obligations and principles driving the architecture of the system.

The description framework is illustrated in Figure 2. The environment and the context of the Once-Only domain, affects the architecture by providing relevant knowledge and information that guides the design of the architecture. The political and legal environment, the pilot (and other relevant) requirements, as well as the architecture patterns and other elements of the architecture and design body of knowledge are the main external elements considered.

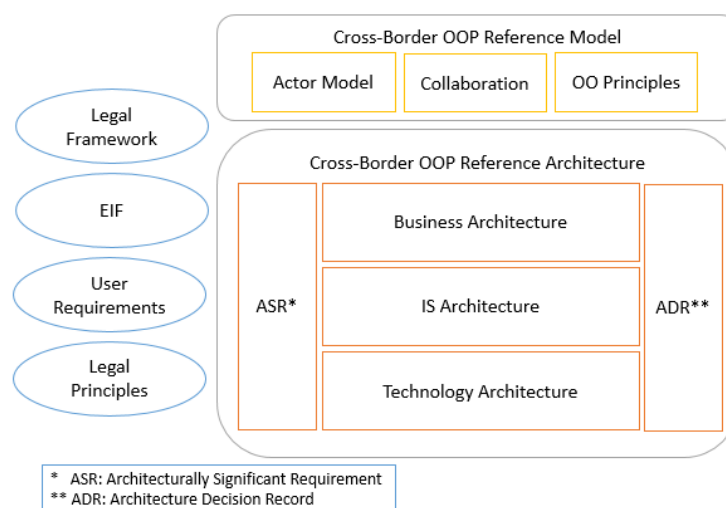


Figure 2: Generic Reference Architecture Description Framework

Besides the 3 architecture views, the reference architecture also contains the Architecturally Significant Requirements (ASR) and the Architecture Decision Records (ADR). The ASRs abstract the various driving forces into requirements that are relevant in the design of the architecture. The ADRs log the various design decisions that are taken during the architecture design process.

Figure 3 shows the principal activities within the TOOP architecture development process together with their outputs and associated deliverable components.

⁴ <http://pubs.opengroup.org/architecture/archimate3-doc/>

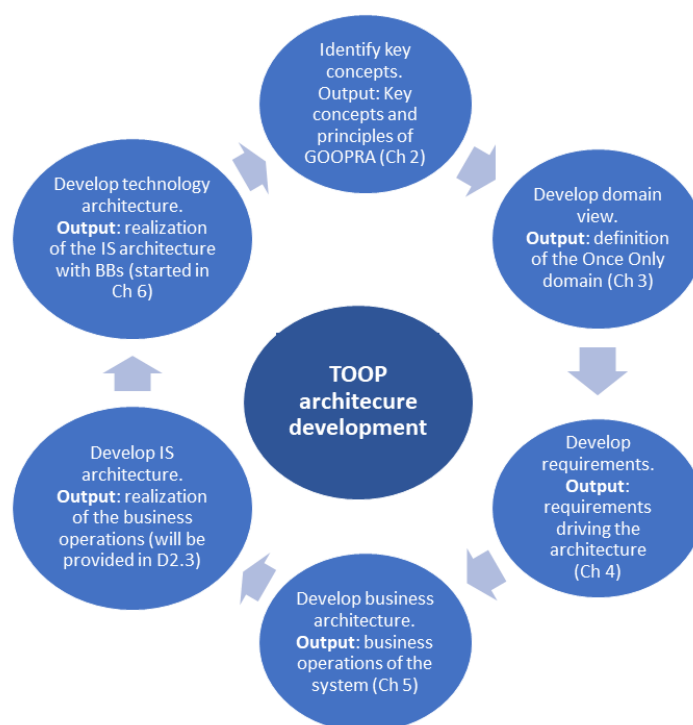


Figure 3: Activities within the TOOP architecture development process

The architecture deliverable development follows an incremental approach, involving four official versions (D1.1, D2.2, D2.3, D2.4) and two interim versions. The current document is the second official version and will be developed further in the subsequent editions. In each consecutive version of the architecture deliverable, some components from the previous versions may be added, some components may be developed further or modified, some components may be left unchanged.

1.4.Relations to Internal TOOP Environment

The current deliverable presents the OOP architecture and demonstrates its standpoints. 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.

Inputs to this deliverable were received from the EU official sources, from CEF Building Blocks, from eSENS deliverables and wikis, from TOOP WP3, from desk research, from architecture guidelines, frameworks, and standards, as well as from other sources.

The output of this deliverable is the OOP architecture, which develops further and extends the deliverable “D2.1. Generic federated OOP architecture (1st version)”. This architecture is aimed at designers and developers of pilot applications in WP3, as well as on stakeholders who will develop applications that support interconnection and interoperability of national registries at the EU level and provide implementation of the Single Digital Gateway Regulation.

1.5. Relations to External TOOP Environment

This deliverable reports the results produced by TOOP WP2. These results represent the main technological innovation of TOOP - the generic federated OOP architecture. The architecture supports the interconnection and interoperability of national registries at the EU level, is in line with existing EU frameworks (EIRA, EIF), and takes into account the e-SENS European Interoperability Reference Architecture. It provides input for SDGR implementation, is oriented towards reuse of the CEF DSIs and the Building Blocks consolidated by the e-SENS project, and proposes new BBs where necessary.

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 (see TOOP Deliverable D2.5, 2017) 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 Single Digital Gateway Regulation, the CEF Building Blocks, and the e-SENS Building Blocks, among others.

1.7. Structure of the Document

The first chapter of the deliverable, introduction, states the deliverable scope, methodology, relations to TOOP internal and external environments, quality and risk management, and other issues.

The key principles motivating the design of the Generic Once-Only Principle Reference Architecture (GOOPRA) are analysed in the second chapter.

The third chapter presents the domain view, concerned with the definition of the Once-Only domain in which the TOOP project is situated.

The requirements to the architecture - including the requirements stemming from the Single Digital Gateway Regulation - is proposed in the fourth chapter.

The business view is designed in the fifth chapter, focussing on the description of the business operationalization of the Once Only Principles by the business actors.

Summaries of the main characteristics of applicable Building Blocks, including rationale for their inclusion in the architecture, usage, maintenance, gap analysis, and need for further development, are provided in the sixth chapter. This chapter is therefore the first version of the technology view.

The information system view of the generic architecture is the focal point of the next deliverable, including how it bridges with the business and technology architectures.

2. Motivations for TOOP Reference Architecture

The TOOP project is part of the EU eGovernment Action Plan 2016-2020. The Action Plan presents the Once Only Principle (OOP) - the public administrations should ensure that citizens and business supply the same information only once to a public administration (European Commission 2016)⁵. TOOP focus area within OOP is on information related to business activities and on cross-border sharing of this information (Krimmer et al. 2017).

When the TOOP project was started, the intended purpose of the OOP architecture was to aid development of specific information systems architectures supporting the Once-Only Principle.

Due to the shift in the TOOP project focus requiring it to support implementation of the Single Digital Gateway Regulation - SGDR (European Union 2017), the current version of the Generic Once-Only Principle Reference Architecture (GOOPRA) has been aligned with new requirements emerging from the SDGR. These requirements have also motivated introduction of the European Commission as one of the main stakeholders in the model, in addition to public administrations, businesses, and citizens.

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 (European Commission 2017)⁶.

As the TOOP project is required to support implementation of the Single Digital Gateway Regulation (SGDR), it has been aligned with its provisions.

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)⁷, the CEF Building Blocks⁸, and the e-SENS deliverable “D6.6 e-SENS European Interoperability Reference Architecture”⁹, among others. It takes these frameworks into account, adding aspects specific to OOP, developing relevant architecture views, and analysing the building blocks with respect to their applicability in OOP applications.

The Generic Once-Only Principle Reference 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 OOP architecture as such does not comprise software components.

The requirements resulting from the OOP architecture must be applied by default to all OOP systems. Different solutions need to be justified and their rationale documented.

The Generic Once Only Principle Reference Architecture is developed following an incremental approach throughout the TOOP Task T2.1 deliverables, starting from D2.1 and finalizing in D2.4.

In the following sections, ArchiMate goal models are used to describe political motivation behind the TOOP project, linking it up to the highest abstract reasoning level. The notation used in the goal models is described in Appendix III.

⁵ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0179>

⁶ http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF

⁷ https://joinup.ec.europa.eu/catalogue/distribution/eira_v1_1_0_overviewpdf

⁸ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home>

⁹ <https://www.esens.eu/deliverables?page=3>

2.1. Single Digital Market Initiative

The TOOP project will contribute towards increasing the efficiency of the Digital Single Market Initiative, which aims to open up digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy (European Commission 2018a)¹⁰.

Single Digital Market initiative contains several activities; Figure 4 shows selection of TOOP related EC policies in the highest abstraction level.

The main identified stakeholders of the Single Digital Market initiative are:

- (i) citizens,
- (ii) businesses/ private organisations,
- (iii) public administrations as enablers of the initiatives, driven by the wish to make life and business easier across the Europe,
- (iv) public and private service providers: research centres, academic institutions, standardisation organisations and businesses supplying services to public administrations, but also by developing enabling technologies and standardizing initiatives.

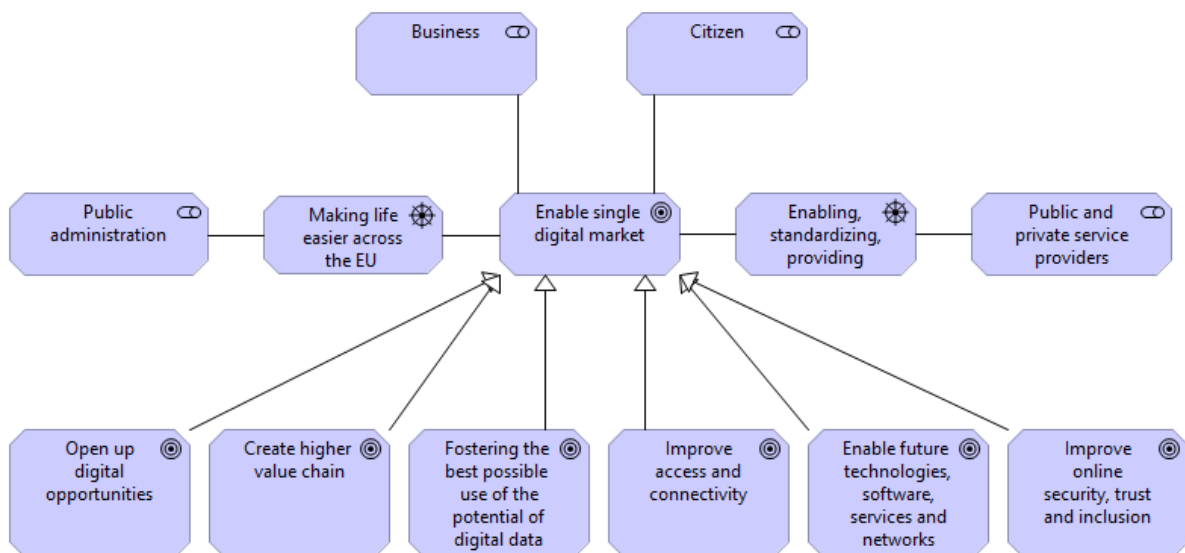


Figure 4: Single Digital market initiative goal model

- The sub-goal “Open up digital opportunities” is the Digital Single Market strategy of the European Commission to ensure access to online activities for individuals and businesses under conditions of fair competition, consumer and data protection, removing geo-blocking and copyright issues. It is meant for people and businesses and enhance Europe's position as a world leader in the digital economy.¹¹
- The sub-goal “Create higher value chain” is aiming toward boosting up European digital industry and aims at ensuring that businesses, SMEs and non-tech industries can benefit from digital innovations to create a higher value chain. This strategy links national & regional initiatives and boosts investment.¹²

¹⁰ <https://ec.europa.eu/digital-single-market/en/news/once-only-principle-toop-project-launched-january-2017>

¹¹ <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market>

¹² <https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry>

- The sub-goal “Fostering the best possible use of the potential of digital data” is Single Market strategy initiative aiming at fostering the best possible use of the potential of digital data to benefit the economy and society. It addresses the barriers that impede the free flow of data and other emerging challenges to achieve a European digital single market.¹³ This initiative forms the main policy basis for TOOP project.
- The sub-goal “Improve access and connectivity” is a set of initiatives and legislative proposals to place the EU at the forefront of internet connectivity.¹⁴
- The sub-goal “Enable future technologies, software, services and networks” is set of Single Digital Market initiatives that enable future technologies, software, services and networks. 5G, the Internet of Things (IoT) and cloud computing are drivers for a Next Generation Internet delivery more to people and the economy.¹⁵
- The sub-goal “Improve online security, trust and inclusion” refers to initiatives aiming to improve online security, trust and inclusion. Trust and security are at the core of the Digital Single Market Strategy.¹⁶

As these initiatives do not give clear link to TOOP project and justify only partly the very existence of the project, several next level goal models have been developed in order to see links between higher level goals and TOOP level goals.

In particular, the sub-goal “Fostering the best possible use of the potential of digital data” of the Single Digital market initiative goal model is in its turn supported by its sub-goal “Modernising public services and e-government” - a logical connection between TOOP project and Single Digital market initiative. These sub-goals are analysed in the next sections.

2.2. Fostering the best possible use of the potential of digital data

The goal “Fostering the best possible use of the potential of digital data” is modelled further to describe related initiatives and policies. Digital data is considered to be an essential resource for economic growth, competitiveness, innovation, job creation and societal progress in general. The value of the EU data economy was more than €285 billion in 2015, representing over 1.94% of the EU GDP. If favourable policy and legislative conditions are put in place in time and investments in ICT are encouraged, the value of the European data economy may increase to €739 billion by 2020, representing 4% of the overall EU GDP.

¹³ <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>

¹⁴ <https://ec.europa.eu/digital-single-market/en/policies/improving-connectivity-and-access>

¹⁵ <https://ec.europa.eu/digital-single-market/en/policies/investing-network-technologies>

¹⁶ <https://ec.europa.eu/digital-single-market/en/policies/strengthening-trust-and-security>

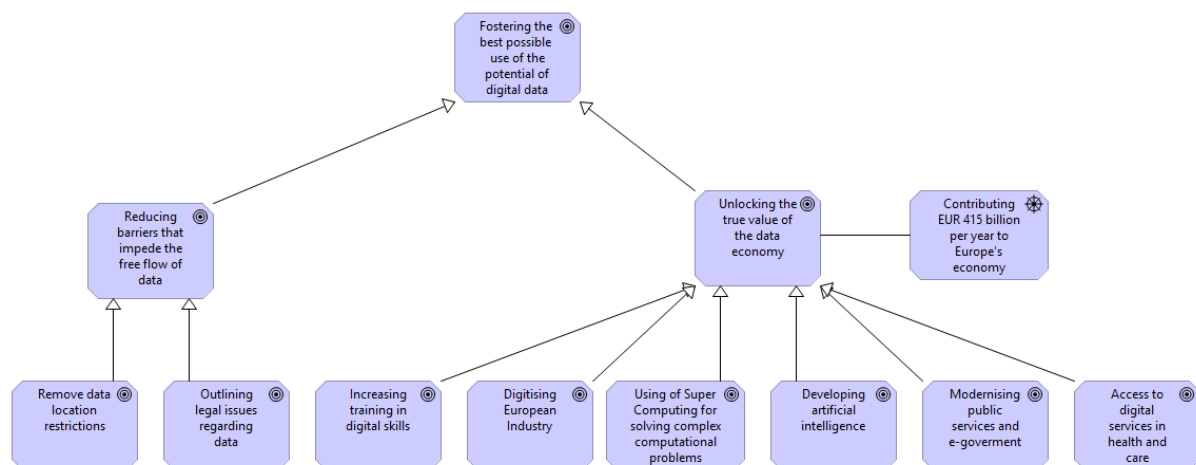


Figure 5: Fostering the best possible use of the potential of digital data

The goal “Reducing barriers that impede the free flow of data”. In order to harness digital data embedded value, EC looked at the rules and regulations impeding the free flow of data and present options to remove unjustified or disproportionate data location restrictions, and outlined legal issues regarding access to and transfer of data, data portability and liability of non-personal, machine-generated digital data (European Commission 2018a).¹⁷

The goal “Unlocking the true value of the data economy” is divided into next sub-goals in order to achieve the target:

- The sub-goal “Increasing training in digital skills” is aiming toward promoting various initiatives aimed at increasing training in digital skills for the workforce and for consumers; modernising education across the EU; harnessing digital technologies for learning and for the recognition and validation of skills; and anticipating and analysing skills needs.¹⁸
- The sub-goal “Digitising European Industry” contains measures to Digitise European Industry will help companies large and small, researchers and public authorities to make the most of new technologies. They will link up national & regional initiatives and boost investment through strategic partnerships and networks.¹⁹
- The sub-goal “Using of Super Computing for solving complex computational problems” focuses on the use of super computers and parallel processing techniques for solving complex computational problems. In the digital era, it is a strategic resource for Europe's future. High Performance Computing, enabling the processing of large amounts of data, is at the core of major advances and innovation in the digital age.²⁰
- The sub-goal “Developing artificial intelligence”. This initiative is still in formulation process. AI has the potential to drive productivity, competitiveness and innovation and to improve human life significantly. AI can boost GDP growth and productivity by enabling companies to automate complex tasks and gain efficiency, as well as developing new business models, products and services.²¹

¹⁷ <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>

¹⁸ <https://ec.europa.eu/digital-single-market/en/policies/digital-skills>

¹⁹ <https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry>

²⁰ <https://ec.europa.eu/digital-single-market/en/high-performance-computing>

²¹ https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Main%20findings%20of%20the%20Policy%20Seminar%20FINAL2_0.pdf

- The sub-goal “Modernising public services and e-government” can provide a wide variety of benefits including more efficiency and savings for governments and businesses, increased transparency, and greater participation of citizens in political life. The potential cost savings are massive. In Denmark, for example, electronic invoicing saves taxpayers €150 million and businesses €50 million a year. If introduced across the EU, annual savings could exceed €50 billion. In Italy alone, e-procurement systems cut over €3 billion in costs.²²
- The sub-goal “Access to digital services in health and care”. Digital technologies such as 4G/5G mobile communication, artificial intelligence or supercomputing offer new opportunities to transform the way we receive and provide health care services. They enable new approaches to independent living or integrated health and social care. Health data and advanced data analytics can help accelerate scientific research, personalised medicine, early diagnosis of diseases and more effective treatments.²³

The sub-goal “Modernising public services and e-government” is a logical connection between TOOP project and the Single Digital market initiative, therefore this sub-domain is analysed further.

2.3.Modernising public services and e-government

ICTs are already widely used by government bodies, as it happens in enterprises, but eGovernment involves much more than just the tools. It also involves rethinking organisations and processes, and changing behaviour so that public services are delivered more efficiently to people. Implemented well, eGovernment enables citizens, enterprises and organisations to carry out their business with government more easily, more quickly and at lower cost. Figure 6 models the goal relations and dependencies within this domain.

²² <https://ec.europa.eu/digital-single-market/en/public-services-egovernment>

²³ <https://ec.europa.eu/digital-single-market/en/policies/ehealth>

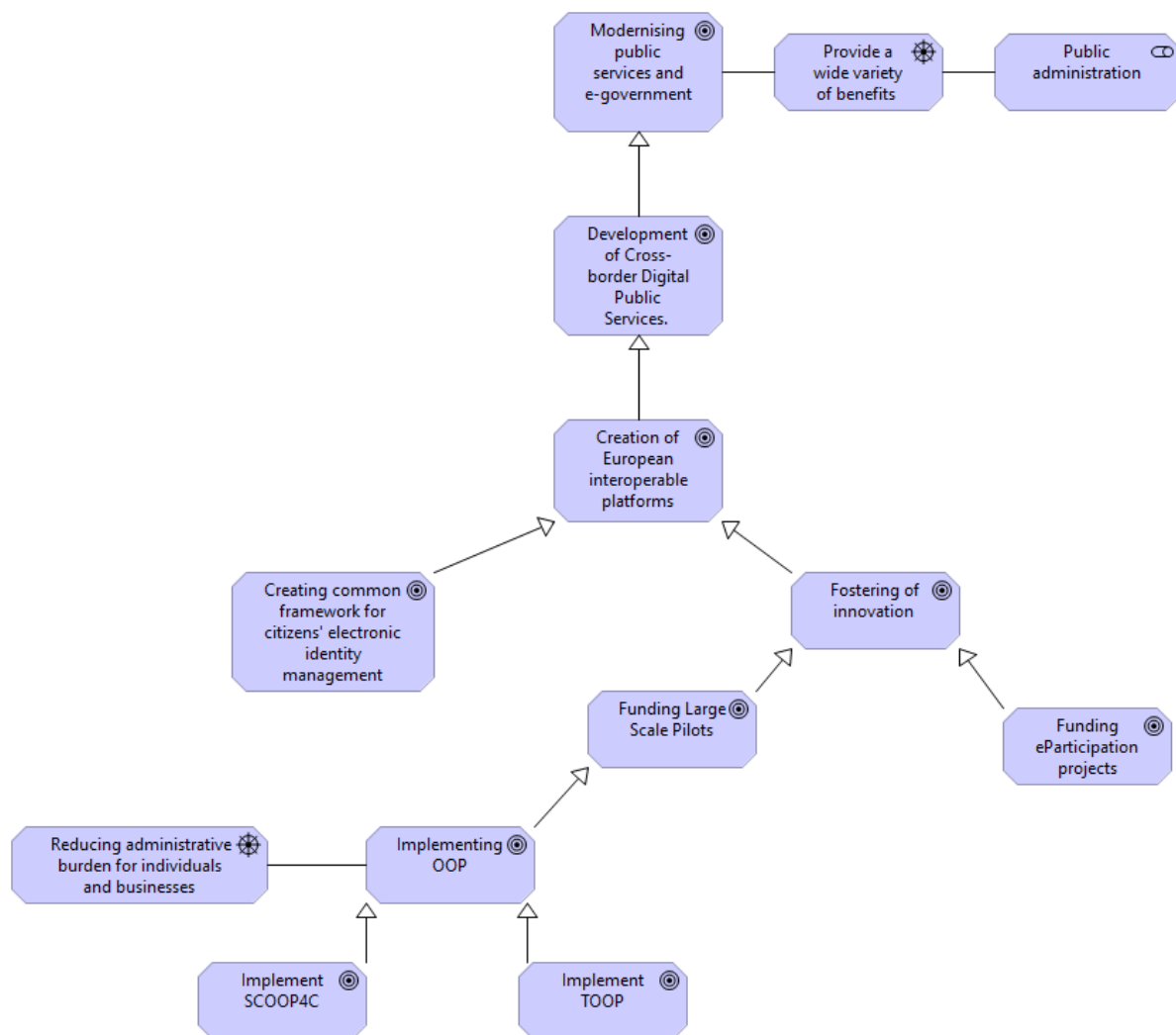


Figure 6: “Modernising public services and e-government” goal model

The goal “Development of Cross-border Digital Public Services” allow achieving the digital single market: in the European Union’s internal market, people are able to move freely – either for work or for private reasons – so they need to be able to deal easily with public services outside their home country.

The goals “Creation of European interoperable platforms”, “Fostering of innovation”, “Funding Large Scale Pilots” and “Funding eParticipation projects” are all aiming the same target. As part of its strategy, the European Commission is taking concrete actions for the development of Cross-border Digital Public Services. These include, but are not limited to, the creation of European interoperable platforms such as a common framework for citizens' electronic identity management ([eID](#)), and the fostering of innovation through the Competitiveness and Innovation Programme (funding Large Scale Pilots and eParticipation projects) (European Commission 2018b).²⁴

The goal “Implementing OOP” is derived from Single Digital Market action plan. The Digital Single Market Strategy adopted a set of targeted actions. It is built on three pillars: (1) better access for consumers and businesses to digital goods and services across Europe; (2) creating the right conditions

²⁴ <https://ec.europa.eu/digital-single-market/en/public-services-egovernment>

and a level playing field for digital networks and innovative services to flourish; (3) maximising the growth potential of the digital economy.²⁵ TOOP project follows the third pillar: Maximising the growth potential of the digital economy.

The goal “Implement SCOOP4C” is a sister project to TOOP project. This Once-Only Principle project aims at eliminating the administrative burden when citizens are required to provide the same information again and again to public administrations.²⁶

The goal “Implement TOOP” is aimed to explore and demonstrate the once-only principle on a cross-border scale with the aim to reduce the administrative burden of businesses and public administrations.²⁷

2.4. Implement TOOP

TOOP implements multiple sustainable pilots by using a federated IT architecture on cross-border, pan-European scale. Its aim is to connect registries and e-Government architectures in 21 countries across Europe. The solutions will be based on already existing systems in Member States and Associated Countries. Businesses will benefit from the solutions developed by TOOP as they will be able to fulfil legal obligations by reduced administrative burden, time- and cost-savings. At the same time, the data that have been provided to public administrations will always remain under full control and consent of the businesses involved, in line with EU data protection legislation.

Administrations will achieve time and cost savings through administrative efficiency and will be able to offer improved service quality to businesses. Thus, administrations will profit from a better-functioning digital single market with increased customer satisfaction and a better image of public authorities.²⁸

The TOOP project supports implementation of SGDR and the European Commission has become one of the main stakeholders in the model, in addition to public administrations, businesses, and citizens.

The goal “Implement TOOP” is specified further on Figure 7. There are several drivers for this project, mainly represented from better public service point of view: reduce administrative burden for stakeholders and increase time and cost efficiency of processes. There are also several constraints present to influencing the outcome of the project.

Constraints “Remain data under full control and consent of the businesses involved” and “Remain in line with EU data protection legislation” are in place in order to guarantee the data given to public administrations will always remain under full control and consent of the businesses involved, in line with EU data protection legislation.²⁹

²⁵ http://europa.eu/rapid/press-release_IP-15-4919_en.htm

²⁶ <https://www.scoop4c.eu/>

²⁷ <http://www.toop.eu/>

²⁸ Ibid

²⁹ Ibid

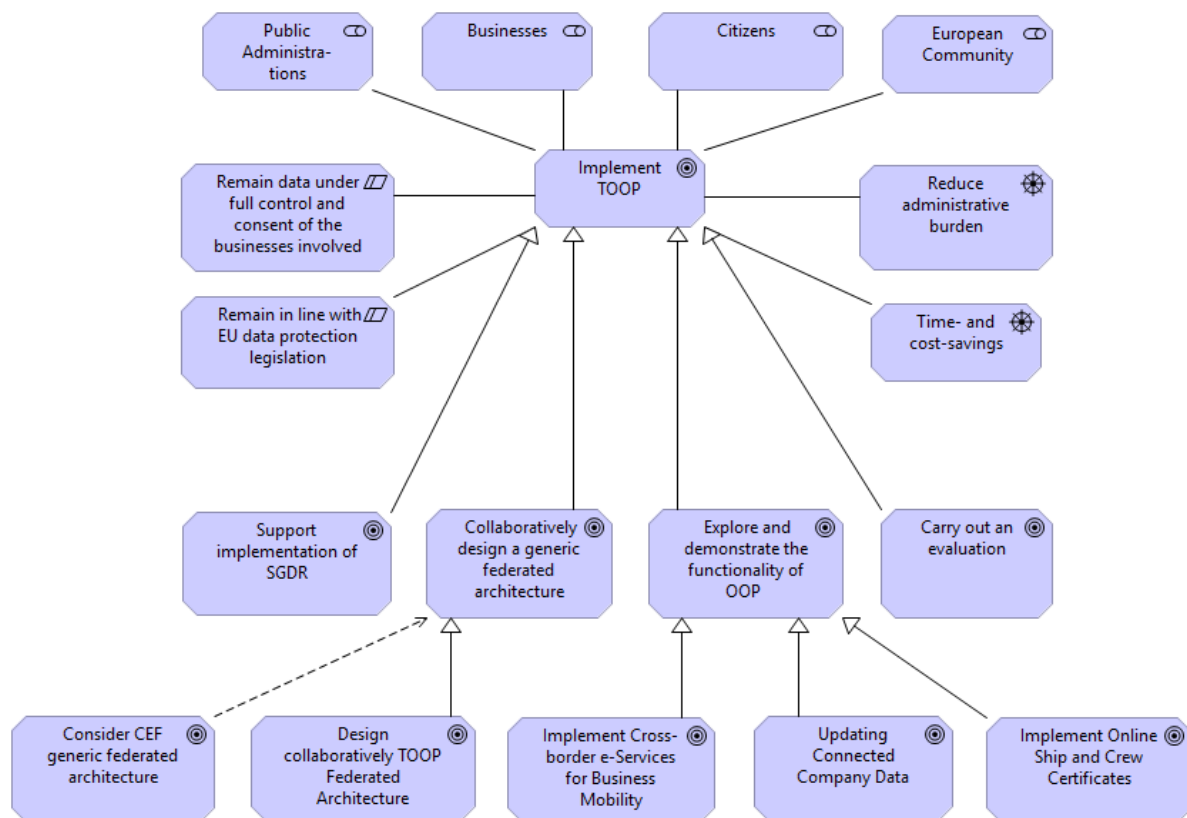


Figure 7: “Implement TOOP” goal model

The goal “Collaboratively design a generic federated architecture” is one of the main activities within the project in order to design collaboratively the generic federated architecture implementing OOP that is able to connect different registries containing base data and e-Government architectures in different countries employing standards, re-using and/or extending existing building blocks.³⁰ This goal has two sub-goals:

- The sub-goal “Analyse CEF generic federated architecture” serves the purpose to align TOOP specific architecture with CEF approach in order to establish direct links with existing architecture principles and ensure update and service of TOOP architectural elements.³¹
- The sub-goal “Design collaboratively TOOP Federated Architecture” One of the innovative solutions developed within the TOOP is a generic federated architecture, developed in collaboration between different Member States. TOOP approach to federated architecture and building blocks reuses existing building blocks and components and integrates new elements in the European and participating States’ ecosystem, develops them further and applies them to new areas, using innovative and flexible methods and putting a strong emphasis on subsequent proliferation, extension and facilitation.³²

The goal “Explore and demonstrate the functionality of OOP” aims to collaboratively design a generic federated architecture implementing OOP that is able to connect different registries containing base

³⁰ Krimmer, R., Kalvet, T., Toots, M., Cepilovs, A. and Tambouris, E., 2017. Exploring and Demonstrating the Once-Only Principle: A European Perspective. In Proceedings of the 18th Annual International Conference on Digital Government Research (pp. 546-551). ACM. DOI: <http://dx.doi.org/10.1145/3085228.3085235>

³¹ Ibid

³² Ibid

data and e-Government to explore and demonstrate the functionality of OOP through multiple cross-border pilots of e-services (e-Government Services) for at least 12 months in real conditions.³³ Three sub-goals specify implementation of next pilot projects:

- The sub-goal “Implement Cross-border e-Services for Business Mobility” refers to the first pilot area - Cross-border e-Services for Business Mobility. This is versatile and composed of different usage scenarios that are of interest to the participating states. It is based on the Exploring and Demonstrating the Once-Only Principle: assumption that government administrations from different countries expose e-services directed at Economic Operators from various countries. During the respective service provision, company-related information is needed. The pilot will show how such information can be automatically retrieved from the Economic Operators’ country of origin without the business representative having to enter it again.³⁴
- The sub-goal “Updating Connected Company Data” refers to the second pilot area – Updating Connected Company Data – foresees a central role for the Business Registers. Now, company data are officially stored in the Business Register within individual Member States according to requirements of relevant EU regulations and directives as well as national legislation. However, the same (or part of the same) data are also stored for other purposes by various public administrations in the same and other MS.³⁵
- The sub-goal “Implement Online Ship and Crew Certificates” refers to the third pilot area – Online Ship and Crew Certificates – addresses the need for simplification in the area of ship and crew certificates, which are currently issued and maintained in paper format, while certificate data is stored by national Maritime Administrations. TOOP aims at connecting the databases of national Maritime Authorities and make the information available to all interested parties, as well as providing a possibility of online certificates, which will substitute paper-based or electronically-signed certificates that have to be carried on board. Once TOOP is implemented, the flag state's Maritime Authority will be able to issue the online ship or crew certificates, while all other interested parties, such as port authorities, police and border guard and the like, will be able to view and check the online certificates, thus reducing the risks and the amount of paperwork.³⁶

The goal “Carry out an evaluation” refers to activity to carry out an evaluation, including identification of drivers & barriers and conducting a cost-benefit analysis of the pilots, to identify the benefits and impacts, both tangible and intangible, and generate insights on the European value in order to facilitate the wider use of OOP.³⁷

³³ Ibid

³⁴ Ibid

³⁵ Ibid

³⁶ Ibid

³⁷ Ibid

3. Domain Definition and Description

The Domain Model represents the vocabulary and key concepts of the problem domain and it identifies the relationships among all of the entities within the scope of the domain, i.e. the Cross-Border Once-Only Principle for Businesses.

The **roles and actors** represent both the responsibilities and the physical and/or legal bodies endorsing these responsibilities. The **Collaboration Model** identifies the flow of activities and information across the actors/roles. The **TOOP principles** represent the rules governing the Once-Only Principle, and providing guidance for decision-making in the design of the supporting system.

These various aspects of the TOOP problem domain are further detailed in the following subsections.

3.1. Domain Roles

Consider an OO-operations space as a 3-dimensional structure $\langle LoU, D, DC \rangle$ with:

- *LoU* referring to the Legislation that applies to the use of Data, i.e., the purposes for which the Data is to be used;
- *D* referring to the Data about the Data Subject (DS)

A *Data Application Envelope (DAE)* refers to the subspace in the operations area within which the use of the Data has been approved by the Data Subject (DS). An application envelope is defined by a single Data and at least one purpose of use as identified by the applicable legislation.

The role model provides for separation of responsibilities into coherent and complementary roles. An overview of the roles, the most important classes they address, and their interrelationships are depicted in Figure 8.

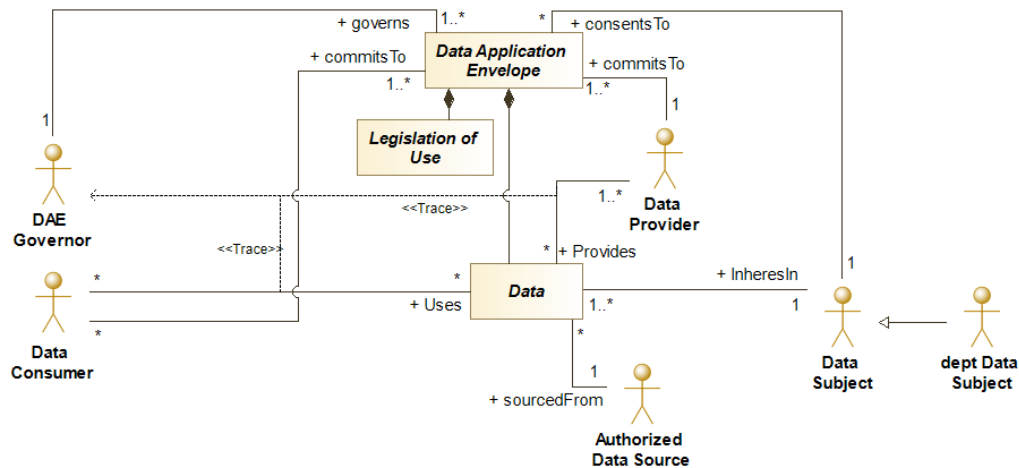


Figure 8: Domain Role Model

The roles and responsibilities are specified in Table 1.

Table 1: Roles and responsibilities

Role	Abbr.	Definition	Responsibilities
Data Subject	DS	The legal entity the data is about. The Data refers to properties, activities, status, etc. which inheres on the legal entity. The Data are therefore dependent on the existence of the DS: when the DS ceases to exist, the Data has become irrelevant except for historical purposes. Furthermore, Data should embody an asset to DC-enabled services that leads to the DS's benefit; data about the DS that lacks support to a clear benefit for the DS is considered out of scope. When referring to Data with a capital D, we imply to refer to the Once-Only Data that has been registered about a particular DS.	<p>to assure the veracity of the data throughout their life cycle, including provenance (when applicable);</p> <p>to assure that any requirement that a particular use of the Data may put on the Data is met and maintained throughout the Data life-cycle;</p> <p>to decide about and consent to the (current and future) use of the Data for specific purposes as admitted by the legal framework;</p> <p>to provide legal proof of identity.</p>
Deputy Data Subject	dDS	The legal entity that has got mandate to act on behalf of the Data Subject.	<p>to provide legal proof of her identity;</p> <p>to provide legal proof of identity of the Data Subject;</p> <p>to realize the responsibilities that belong to the Data Subject in the TOOP context.</p>
Authoritative Data Source	ADS	The authoritative source to the Data on a Data Subject	to provision all-time referral to the Data throughout their life-cycle: No matter how often the Data has been duplicated, in case differences between Data from the ADS or any of its duplicates are identified, the Data from the ADS prevails.
DAE Governor	DG	The legal entity that manages the DAE, and, fulfils a watchdog role that monitors the DAE boundaries during the use of the Data. The DG role only facilitates the enforcement of the DAE boundaries / legal framework during operational use of the Data.	<p>to register and manage each Data Application Envelope;</p> <p>to maintain a register of use of the Data against its DAE;</p> <p>to flag any unauthorized use of the Data, i.e., use of Data by a DC which falls outside the agreed Data Application Envelope;</p> <p>as a facilitating role, it could endorse additional responsibilities</p>
Data Provider	DP	The legal entity that is in charge of the Data deployment	<p>to receive Data requests from DCs and verify their compliance with national legislation;</p> <p>to adhere to the terms of use for which a consent has been admitted;</p> <p>to manage outstanding requests and incoming Data;</p> <p>to provide Data to DC's under authorized conditions only;</p>

Role	Abbr.	Definition	Responsibilities
			<p>to log the events of use of the Data to the DG, e.g., request incl. time stamp, purpose, DS, DAE, and, Data provisioning incl. time stamp, purpose, DC, DAE</p> <p>to maintain a register of available Data with their conditions of use, throughout their life cycle;</p> <p>to facilitate the maintenance a register of (context of) use of Data;</p> <p>to ensure the security of its registers against unauthorized access and use of Data</p>
Data Consumer	DC	The organization/administration that is in demand of the Data in order to fulfil its mission to society or industry.	<p>to generate Data requests;</p> <p>to log Data requests to DG;</p> <p>to assure that Data request comply with international legislation;</p> <p>to state the purpose of use for which the Data is requested;</p> <p>to accept/approve or reject/disapprove the provided Data against the request, and log this to the DG.</p>

3.2.Role Collaborations

The collaboration between the identified roles is represented in Figure 9.

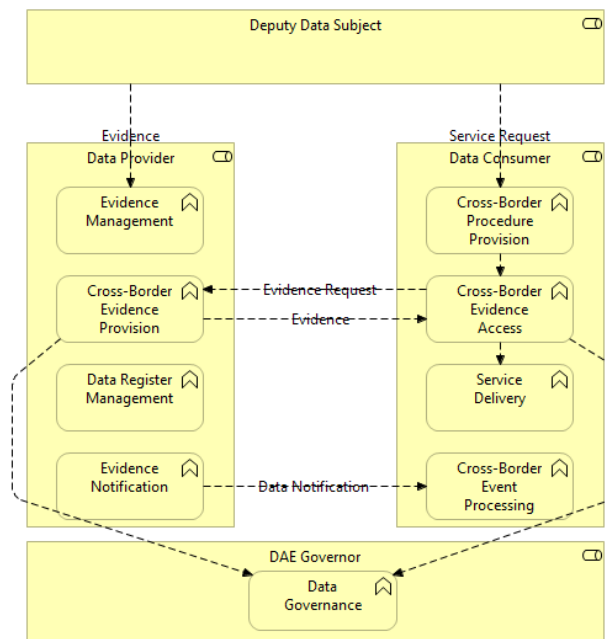


Figure 9: Domain Collaboration

3.3.Domain Principles

A principle is a normative principle on the design of an artefact, thus normatively restricting the design freedom (Greefhorst and Proper 2011). The principle itself is the agreed codification of rules associated with a subject domain. The value of principles should not be underestimated and is an important outcome of pilot projects (sometimes more valuable than actual implementation), especially as a foundation for the design of legislative instruments regulating a domain: the principles of data protection are first class citizens of the GDPR, establishing the set of rules applicable in the domain of data protection.

The principles applicable in the Once-Only domain are listed below. Principles are identified by consecutive numbers, preceded by a single “P”, and represented by a set of attributes, selected from (Greefhorst and Proper 2011):

- *A Title*, in the form of a statement that succinctly present the fundamental rule that is to be followed;
- *A Rationale*, which should highlight the business benefits of adhering to the principle (incl. a reference to the Once-Only Objectives that have been specified in Chapter 2), describing the reasons why this principle applies;
- *Its Implications*, describing the impacts of this principle on the architecture being designed; drives the behavior that is expected from people in order to comply to the architecture principle, and also considers the undesired behaviour that is an implication of the architecture principle (what people should not do), or the negative consequences (the disadvantages of choosing for the architecture principle);
- *Type of Information* classifies the principle to the relevant view (of the architecture) where this principle applies;
- *Quality Attributes* are to provide for an indication on the quality characteristics that this principle contributes to meet, improving the clarity about the intended effect of the principle as well as a suggestion towards its validation.

We intend to specify the attributes that represent the principle as SMART as possible³⁸. To that end the principle and/or its representation have been evaluated to be: (i) *specific* enough to understand its intention and its purported effect on the design decisions; (ii) *measurable* by providing sufficient detail and/or criteria to determine success or failure of its application; (iii) *achievable* in that its application is without any significant impediment; (iv) *relevant* enough that when following its direction it will lead to significant improvement in terms of efficiency, efficacy or simplicity of the resulting design; and (v) *time-bound* in bearing its validity over context and time. Finally, the set of principles have been validated not to be (partially) in conflict with each other, because contradicting rules cannot guide towards meaningful or valuable decisions.

P.1 Citizens and business supply, by the DG, the same Data only once to a public administration, which remain available for authorised use, by the DC, throughout their life cycle.

- **Type of information:** Business view
- **Quality attributes:** Usability (user-friendliness, operability), Maintainability (manageability, reusability), Reliability (availability)
- **Rationale:** This represents the single one purpose of the TOOP project; without its application the project does not deliver on its intrinsic value, and no improvement on European society will be achieved.

³⁸ https://en.wikipedia.org/wiki/SMART_criteria

- **Implications:** On the positive side, the burden on European business that results from interaction with national and European administrations, i.e., governmental organisations, will reduce significantly since those administrations can base their operations on reuse of Data that has been collected previously. On the negative side, the implied connectedness of registers between each and every European administrations will bring the privacy of the Data into a more vulnerable position. Furthermore, due to the necessarily more centralised system approach, the continuity of administrative services will be more dependent on Data availability, which becomes more vulnerable to threats that resemble DDOS-attacks and Trojan horses, and Data integrity, which can suffer more from ransomware holding data hostage and other attempts to cripple data.

P.2 Data can only be used by the DC in the context of a specified purpose, when the DC has a legal basis for data access and satisfies the requirements set for the DC to reach the data.

- **Type of information:** Business view
- **Quality attributes:** Functionality (compliance, security), Usability (user-friendliness),
- **Rationale:** The prime users of the OOP, i.e., European business, will only trust OOP-enabled services once it proves (i) secure, and (ii) transparent. Therefore, the DOs must be eligible to set requirements (for example assurance/security level) for DCs to reach data. DCs must have a legal basis to use the data.
- **Implications:** Trust from the individuals representing the DS will grow, and transparency of its operation will be high.

P.3 Data access and their use should be prohibited for use outside the Data Application Envelope the consent admits to.

- **Type of information:** Business view
- **Quality attributes:** Functionality (security, compliance, maturity)
- **Rationale:** The success of the eGovernment Action Plan is directly related to the efficacy and maturity of the security measures against abuse of Data. This Principle can be considered as partial realization of Principle P.2 where the latter enforces external behaviour of the OOP platform while this principle enforces its internal behaviour. By token of its strict control this enables the use of the OOP platform for distributing the Data to the public sector as well
- **Implications:** On the positive side, this principle will ensure that the OOP platform will enforce secure operation on the Data.

P.4 Despite possible duplication of Data, only one authoritative DG exists to dispute Data correctness.

- **Type of information:** Business view
- **Quality attributes:** Functionality (accuracy, suitability, manageability), Efficiency (time behaviour), Reliability (fault tolerance)
- **Rationale:** The core ramification of the OOP platform, i.e., reuse of Data, is only effective once guarantees about appropriateness and accuracy of the Data, particularly when being reused, can be guaranteed. Without such guarantees, the OOP platform will fail in achieving its main objectives
- **Implications:** Enforcing an explicit balance between Data correctness and scalability. Any DC must be able to verify who the DG is, for example this may be listed in some sort of catalogue.

P.5 Despite possible duplication of Data, ownership and IPR remains with the DS.

- **Type of information:** Business view, IS view
- **Quality attributes:**
- **Rationale:**
- **Implications:**

P.6 Despite one authoritative DG, once authorisation of use is granted, access to Data is absolute and independent from time and location, and without further delay.

- **Type of information:** IS view
- **Quality attributes:** Maintainability (reusability), Efficiency (time behaviour)
- **Rationale:**
- **Implications:**

P.7 Data cannot be combined or adapted without an explicit regulatory provision.

- **Type of information:** Business view, IS view
- **Quality attributes:** Maintainability (manageability, changeability), Functionality (accuracy)
- **Rationale:**
- **Implications:** Data remains in correspondence with the state of affairs about the DS.

P.8 All organisations that take on an OOP role must comply with the rules of engagement that reflect the essentials of the OOP.

- **Type of information:** Business View, IS view, Technology view
- **Quality attributes:** Functionality, Reliability, Usability, Efficiency, Maintainability, Portability
- **Rationale:** This essentially reflects the need that any collaborative administration in the OOP realm should commit to these Principles. Otherwise, the technical as well as the business interoperability will be hampered or cease to emerge, resulting in a failed OOP realm
- **Implications:** Interoperability on all enabling dimensions, i.e., social and political, regulatory, organisational, technical, semantic, and financial, and on all levels of collaboration, i.e., local, regional, national and international. Together with P.10 it implies that in any given ecosystem there must be a governing authority who supervises that rules of engagement are followed. This role must be clearly defined.

P.9 Use of Data shall be transparent and open

- **Type of information:** Business view, IS view
- **Quality attributes:**
- **Rationale:**
- **Implications:**

P.10 Any handling on Data, in particular but not limited to their Use, shall practice organisational, technical, and other methods and tools in support of auditing and accountability

- **Type of information:** IS view, Technology view
- **Quality attributes:**
- **Rationale:** Within the OOP realm, privacy of Data represents a concern that should be considered a commodity. Therefore, the very basic and integral ability to trace back any abuse of Data is a necessary condition for an operational OOP platform. In information systems,

organisational, technical, and other methods and tools are used to support auditing and accountability. Examples of such methods include, but are not restricted to: division of responsibilities and separation of functions, user authentication and authorisation, logging different activities, use of cryptographic procedures, timestamping, and others³⁹. These methods and tools are used to introduce two OOP-dimensions that reflect, at the one hand, legislation and authorisation events, and, at the other hand, events about transport and use of Data. Based on registration of these events, abuse of Data can be detected throughout the life-cycle of Data

- **Implications:** Introduction of needed organisational, technical, and other methods and tools requires a non-repudiation transaction model that forms a fundamental and integral part of the OOP platform.

P11. Data security

- **Type of information:** Business view, IS view, Technology view
- **Quality attributes:**
- **Rationale:** Data Subject's data transferred, stored in any service used within the TOOP Project must be protected against misuse, manipulation or fraud.
- **Implications:** Data must be stored in the system, which include security and authenticity mechanisms. Neglecting security and authenticity of data may lead to unsuccessful project implementation.

³⁹ https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzHome/itgrundschutzhome_node.html

4. Requirements Driving the Architecture Design

This chapter specifies the requirements driving the design of the reference architecture for Cross-Border Once Only Principle.

First the requirements engineering framework is described. Then each activity belonging to the requirements engineering process are explained, and the architecture requirements are specified.

4.1. Architecture Requirement Framework

The requirements of interest in designing TOOP Reference Architecture are the **Architecturally Significant Requirements** (ASR's), i.e. "those requirements that have a measurable impact on a software system's architecture" (Chen, Babar, and Nuseibeh 2013). Significant is a key term in this definition, and is ultimately measured by high cost of change in the designed architecture.

The ASR's are specified by referring to concepts and elements of the domain model: the requirements are indeed guiding the solution to be designed to solve the problem domain. ASR's will therefore refer to an actor/role's capability, as captured in the domain model.

Besides the ASR's, **architecture principles** are also captured: they are "underlying general rules and guidelines for the use and deployment of all IT resources and assets across the enterprise" (TOGAF). They reflect a level of consensus among the various elements of the enterprise, and form the basis for making future architecture decisions.

A principle differs from a requirement by its scope: it is a general rule applied to any element of the designed architecture. Some architecture principles might be the source from which architecture requirements are derived. The architecture principles however remain key guidelines driving the architecture decisions, and might be referred to at any stage of the architecture design (from business architecture to technology architecture).

Both the ASR's and the Architecture Principles are structured according the standard Software/System Product Quality Model (ISO/IEC 25010) and the related Data Quality Model (ISO/IEC 25020), both part of the Software Quality Requirements and Evaluation (SQuaRE) family of standards. Adopting a standard structure contributes to ensuring all relevant architecture concerns are integrated, and to identifying potential lack of expressed needs from the stakeholders: a relevant quality attributes that is not associated with any requirement might represent a gap in the requirements engineering process, seen from the viewpoint of the architect.

Table 2 identifies the relevant quality attributes in the context of TOOP: these are the concerns for which requirements and/or principles should be specified.

Table 2: Relevant Quality Attributes

Quality Attribute	Relevance and specific goals in TOOP
	System Quality
Functional Suitability	The domain model (actors/roles and collaboration model) is the baseline for the functional suitability dimension. It is complemented with functional requirements associated with the capabilities of each domain participant.
Performance Efficiency	The performance is mainly relevant from the time-behaviour perspective (i.e. the degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements), associated with the end-to-end

Quality Attribute	Relevance and specific goals in TOOP
	processing time of the user request. The capacity might also be relevant, in terms of size of data to exchange, as well as in terms of transaction throughput
Compatibility	The compatibility quality dimension is concerned with interoperability , from the perspective of both exchange of information and use of information exchanged. The coexistence attribute is relevant in terms of integration with existing MS systems.
Usability	The operability of the system is the main concern: it especially relates to the cross-border exchange. Moreover, accessibility is a compulsory requirement, especially in terms of European languages.
Reliability	The reliability is mainly concerned with the availability of the system, and specifically of the cross-border exchange.
Security	Security is a main concern in TOOP, as the system deals with the exchange of authenticated data, and authorized access to the data. The requirements are associated with confidentiality, integrity, availability (of the information), nonrepudiation, accountability, auditability, authenticity/trustworthiness , as well as privacy .
Maintainability	Although modularity and reusability are of paramount importance to ensure maintainability, they are not directly concerned with the architecture of the system (but with the detailed design of the solution).
Data Quality	
Accuracy	Syntactic and semantic accuracy of the exchanged data are particularly important in TOOP.
Completeness	The completeness of data cannot be guaranteed by the system as it does not include the collection and validation of data about the data subject from the data owner.
Consistency	The consistency of data is ensured by the systems that TOOP relies on. TOOP in itself cannot therefore ensure the data consistency.
Credibility	The authenticity of data is a major concern in the cross-border exchange of evidence. TOOP should ensure that the authenticity is maintained during the exchange.
Currentness	Evidence can be updated during its lifecycle. TOOP has to integrate this and provide a mechanism to ensure the use of current data.

The ASR's and Architecture Principles specifications are the outcome of a standard requirements engineering process, composed of the following activities:

- Requirements inception
- Requirements analysis
- Requirements specifications

- Requirements validation

The activities are contextualized, both to the scope of the project, and to the goal of designing a reference architecture (as opposed to an application architecture). The contextualized activities and their outcomes are described in the following sections.

4.2. Architecture Requirement Inception

During the inception phase, the needs of the stakeholders are captured: they are the baseline for the specifications of the requirements. In TOOP, the needs are issued from the following sources:

- The legal environment, and specifically the draft SDGR;
- The interoperability principles and recommendations, extracted from the EIF;
- The pilot needs.

The needs of the stakeholders are captured by other WP and/or tasks, and the main sources of these needs are:

- Legal principles and requirements (D2.5)
- Draft SDGR (<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0256>)
- EIF Principles and Recommendations (https://ec.europa.eu/isa2/eif_en)
- User requirements issued by each pilot, and available on the pilot wiki (<http://wiki.ds.unipi.gr/display/TOOPPILOTS/>)

4.3. Architecture Requirement Analysis

In this phase, the requirements from each source is analysed, and its impact on the architecture is assessed. The result of this assessment might be that

- The requirement is not relevant in terms of architecture
- The requirement is either generalized or specialized in an architecture principle
- The requirement is generalized in an architecture requirement

0 describes the outcome of the legal framework analysis, while 0 describes the outcome of the EIF analysis.

4.4. Architecture Principles Specifications

In this phase, the identified architecture principles are formulated and associated with the quality model. The specified architecture principle is traced back to its source.

Table 3: Architecture Principles

ID	Name	Description	Rationale	Quality	Implications
PRINC-01	Open specifications/ standards	Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support and innovation	EIF-04	IOP	If a new component is to be designed, give preference to open specifications and standards
PRINC-02	Reusable solutions	Reuse and share solutions, and cooperate in the development of joint solutions when	EIF-06	Reusability	Develop TOOP architecture as a reusable solution;

		implementing European public services			reuse BB when possible
PRINC-03	Reusable data	Reuse and share information and data when implementing European public services, unless certain privacy or confidentiality restrictions apply	EIF-07	Reusability	Reuse and share information and data in compliance with the Once Only principle, improving quality, as well as saving money and time
PRINC-04	Technological neutrality	Develop architecture that supports technological neutrality	EIF-08	Replaceability	Technological neutrality minimizes technological dependencies, avoids imposing specific technical implementations, and enhances adaptation to changes of technological environment
PRINC-05	Data portability	Develop architecture that supports data portability	EIF-09	Portability	Data portability helps to avoid lock-in and to support the free movement of data.
PRINC-06	Once Only Principle	Adhere to the Once Only Principle	EIF-13	Operability	The Once Only Principle helps to meet the users' requirement to provide only the information that is absolutely necessary to obtain a given public service
PRINC-07	Standards and specifications process	Put in place processes to select relevant standards and specifications, evaluate them, monitor their implementation, check compliance and test their interoperability	EIF-21	IOP	Standards and specifications are fundamental to interoperability. Their management process needs to be established

					together with architecture development
PRINC-08	Standards and specifications selection	Use a structured, transparent, objective and common approach to assessing and selecting standards and specifications	EIF-22	IOP	A structured, transparent, objective and common approach to the standards and specifications process should be developed
PRINC-09	Interoperability agreements	Establish interoperability agreements in all layers, complemented by operational agreements and change management procedures	EIF-26	IOP	Interoperability agreements in all layers, complemented by operational agreements and change management procedures, are needed to implement TOOP architecture and should be foreseen
PRINC-10	Organisational relationships	Clarify and formalise organisational relationships for establishing and operating European public services	EIF-29	IOP	Clarification and formalization of organisational relationships between stakeholders are needed to implement TOOP architecture and should be foreseen
PRINC-11	Data and information as a public asset	Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved	EIF-30	IOP	Common principles for data and information generation, collection, management, sharing, protection and preserving should be developed

PRINC-12	Open technical specifications	Use open specifications, where available, to ensure technical interoperability when establishing European public services	EIF-33	IOP	Open technical specifications should be evaluated and used
PRINC-13	Infrastructure for European public services	Decide on a common scheme for interconnecting loosely coupled service components and put in place and maintain the necessary infrastructure for establishing and maintaining European public services	EIF-35	IOP	Infrastructure for establishing and maintaining European public services should be decided, developed, and put in place
PRINC-14	Reusable services and information sources	Develop a shared infrastructure of reusable services and information sources that can be used by all public administrations	EIF-36	IOP	The infrastructure for establishing and maintaining European public services should comprise reusable services and information sources that can be used by all public administrations
PRINC-15	Cost-based Efficiency and Effectiveness	Effectiveness and efficiency requirements should be evaluated and established, balanced by considering of costs and benefits	EIF-19	Efficiency	
PRINC-16	eIDAS Trust Services	The TOOP architecture should use trust services according to the Regulation on eID and Trust Services as mechanisms that ensure secure and protected data exchange in public services	EIF-47	Security	
PRINC-17	Data Minimization	The information exchanged between the participants of the system should be limited	Privacy-by-Design	Privacy	

		to the data required by the processing			
PRINC-18	Purpose Limitation	The information exchanged between the participants of the system should only be used for the explicitly agreed purpose	Privacy-by-Design	Privacy	
PRINC-19	Consent Management	When the consent of the user is necessary for data protection purposes, it shall be obtained in accordance with Regulation (EU) 2016/679 and Regulation (EU) 45/2001	Privacy-by-Design	Privacy	
PRINC-20	Multilingualism	Use information systems and technical architectures that cater for multilingualism when establishing a European public service. Decide on the level of multilingualism support based on the needs of the expected users.		Usability	

4.5. Architecture Requirements Specifications

In this phase, the identified requirements are formulated and associated with the quality model. The specified ASR is traced back to its source.

Table 4: Architecturally Significant Requirements

ASR	Description	Source
SYSTEM/SW QUALITY CONCERNS		
Functionality		
ASR-FUNC-01	The Data Consumer can request Data on the Data Subject from the Data Provider	SDGR.Art12.4 PA1.1-REQ4 PA1.2-REQ-4 PA1.2-REQ-5 PA1.3-REQ-4
ASR-FUNC-02	The Data Consumer must be informed about the conditions and terms of use of the retrieved information	PA1.1-REQ-8 PA1.2-REQ-11 PA1.3-REQ-8

ASR	Description	Source
ASR-FUNC-03	Where the completion of a procedure requires a payment, users are able to pay any fees online through cross-border payment services, including, at a minimum, credit transfers or direct debits as specified in Regulation (EU) No 260/2012 of the European Parliament and of the Council <u>40</u>	SDGR-Art.11.1.e EIF-45 PA1.1-REQ-18 PA1.2-REQ-21 PA1.3-REQ-18 PA2.1-BUSINESS-1 PA2.2-BUSINESS-1
ASR-FUNC-04	The Data Consumer may use the system to send messages to the Requester	PA1.1-REQ-15 PA1.2-REQ-18 PA1.3-REQ-15
ASR-FUNC-05	The Data Provider may provide data services for verification of specific conditions, i.e. DP replies True/False to specific statement.	PA2.1-PULL-1 PA2.2-PULL-1
Performance Efficiency		
ASR-PERF-01	The DP should not unnecessarily delay the process of transmitting the Data to the DC	PA1.NiceToHave
ASR-PERF-02	The DP should communicate the expected level of service associated with the processing of the request for Data from the DC	
Compatibility		
Interoperability		
ASR-IOP-01	The Data Provider must be able to understand the request from the Data Consumer and automatically serve it	SDGR-Art12.2 PA1.1-REQ-7 PA1.2-REQ-9 PA1.2-REQ-10 PA1.3-REQ-7
ASR-IOP-02	The Data Consumer must be able to unambiguously understand and process the information retrieved from the Data Provider	SDGR-Art12.2 PA1.1-REQ-9 PA1.2-REQ-12 PA1.3-REQ-9 PA2.1-DATA-2 PA2.2-DATA-2
ASR-IOP-03	The Data Consumer and the Data Provider must be technically able to exchange information	SDGR-Art12.2 PA1.1-REQ-3 PA1.2-REQ-3 PA1.3-REQ-3
ASR-IOP-04	Each service provided by the Data Consumer has to specify set of data required from the Data Provider for a specific purpose.	PA2.1-DATA-5 PA2.2-DATA-5

ASR	Description	Source
ASR-IOP-05	Existing Registries should provide web service interfaces for requesting information and subscribing to information changes	PA2.1-ARCHITECTURE-2 PA2.2-ARCHITECTURE-2 EIF-05
Coexistence		
ASR-COE-01	The Competent Authorities must be able to reuse existing national or EU infrastructure, including the BRIS infrastructure	PA1.1-REQ-19 PA1.2-REQ-22 PA1.3-REQ-19 PA2.1-ARCHITECTURE-1 PA2.2-ARCHITECTURE-1
Security		
ASR-SEC-01	The transmission of an Evidence from DP to DC must guarantee the confidentiality of the exchanged Evidence	SDGR-Art12.2 PA1.1-REQ-16 PA1.1-REQ-17 PA1.2-REQ-19 PA1.2-REQ-20 PA1.3-REQ-16 PA1.3-REQ-17 PA2.1-SECURITY-3 PA2.2-SECURITY-3
ASR-SEC-02	The transmission of an Evidence from DP to DC must guarantee the integrity of the exchanged Evidence	SDGR-Art12.2 PA1.1-REQ-16 PA1.1-REQ-17 PA1.2-REQ-19 PA1.2-REQ-20 PA1.3-REQ-16 PA1.3-REQ-17 PA2.1-SECURITY-3 PA2.2-SECURITY-3
ASR-SEC-03	The DC must be informed about the level of availability of Data provided by the DC.	PA1.1-REQ-8 PA1.2-REQ-11 PA1.3-REQ-8
ASR-SEC-04	The Evidence provided by the DP must be available according to the legal requirements	
ASR-SEC-05	The Data Consumer is responsible for ensuring that the request for Evidence from the Data Provider was initiated by the User, unless not legally required	SDGR.Art12.4

ASR	Description	Source
ASR-SEC-06	The Data Provider is responsible for transmitting the requested Evidence in accordance with the confidentiality and integrity requirements,	SDGR.Art12.4
ASR-SEC-07	The DP should not provide the evidence if the request does not conform to the legal requirements of the DP	
ASR-SEC-08	If the Data Provider cannot transmit any evidence, the data provider must give reasons for this.	LEG-GA-03
ASR-SEC-09	Appropriate audit and logging measures must be implemented to ensure that any exchange of evidence organised under the OOP can be verified by competent authorities in case of disputes (including the identification of the sending and receiving competent authorities, the time of the exchange, and the integrity/authenticity of the exchanged data itself).	LEG-CTRL-02
ASR-SEC-10	The Data Consumer must authenticate the User before requesting Evidence from the Data Provider when authentication is required	PA1.1-REQ-1 PA1.2-REQ-1 PA1.2-REQ-2 PA1.3-REQ-1
ASR-SEC-11	The DC must identify the DS associated with the User.	LEG-CTRL-01 PA1.1-REQ-2 PA1.2-REQ-2
ASR-SEC-12	The DP must validate that the User is authorized to retrieve information about the Data Subject	LEG-CTRL-01 PA1.1-REQ-2 PA1.2-REQ-2
ASR-SEC-13	The participants to the Evidence exchange process must be identified, specifically the DC and the DP	PA2.1-SECURITY-1 PA2.2-SECURITY-1
ASR-SEC-14	The DP must verify that the data consumer is an authorized digital public service before transmitting the required data	PA2.1-SECURITY-2 PA2.2-SECURITY-2
ASR-SEC-15	The Data Consumer must be able to prove that the User explicitly requested the retrieval of Evidence from the Data Provider	SDGR.Art12.4 PA1.1-REQ-5 PA1.2-REQ-6 PA1.2-REQ-7 PA1.3-REQ-5
ASR-SEC-16	The Data Provider must be able to prove the reception of the transmitted data by the Data Consumer	PA1.1-REQ-11 PA1.2-REQ-14 PA1.3-REQ-11
ASR-SEC-17	The Data Consumer must be able to prove the reception of the data request by the Data Provider	PA1.1-REQ-10 PA1.2-REQ-13 PA1.3-REQ-10

ASR	Description	Source
ASR-SEC-18	The Evidence transmitted by the Data Provider to the Data Consumer shall be limited to what has been requested	SDGR.Art12.6 PRINC-17
ASR-SEC-19	The Evidence transmitted by the Data Provider to the Data Consumer shall only be used for the purpose of the procedure for which the evidence was exchanged	SDGR.Art12.6 PRINC-18
ASR-SEC-20	When the consent of the user is necessary to retrieve Evidence from the Data Provider, it shall be obtained in accordance with Regulation (EU) 2016/679 and Regulation (EU) 45/2001	SDGR.Art12.6 PRINC-19
ASR-SEC-21	Data provided by the Data Provider to the Data Consumer may not be provided by the Data Consumer to third parties, <i>except where third parties are required to achieve the communicated purpose, or unless it has been consented by the User</i>	LEG-GA-04 PA2.1-LEGAL-2 PA2.2-LEGAL-2 PRINC-18
Reliability		
ASR-REL-01	The level of availability of the exchange process must comply with the legal requirements	
Usability		
ASR-USA-01	It must be possible to operate the Evidence exchange process according to various deployment models: component on premise, service on premise, mutualized and centralized service	
DATA QUALITY CONCERNS		
Data Accuracy		
ASR-ACC-05	The legal value and meaning of data should not be altered crossing a national border	PA2.1-DATA-1 PA2.2-DATA-1
Data Consistency		
ASR-CONS-01	The User has the possibility to preview the evidence to be used by the Data Consumer, and check the validity of the retrieved information	SDGR-Art12.2 PA1.1-REQ-6 PA1.2-REQ-8 PA1.3-REQ-6
Data Completeness		
ASR-COMP-01	The User may be able to add information not provided by the data provider(s)	PA1.1-REQ-13 PA1.3-REQ-13
Data Credibility		

ASR	Description	Source
ASR-CRED-01	The authenticity of the data transmitted by the DP must be trusted by the DC	
Data Currentness		
ASR-CURR-01	The Data Consumer can subscribe to change events associated with the Data life cycle	PA2.1-PUSH-4 PA2.2-PUSH-4
ASR-CURR-02	Modification of data are asynchronously notified, on a predefined schedule, to the Data Consumer that have subscribed to the notification service. A Data consumer has the possibility to unsubscribe to the notification service	PA2.1-PUSH-1 PA2.1-PUSH-2 PA2.1-PUSH-3 PA2.2-PUSH-1 PA2.2-PUSH-2 PA2.2-PUSH-3

5. Business Architecture

The business architecture is concerned with the capture of the business operations of the system. It includes the specifications of the business actors, roles and responsibilities, as well as the specifications of the business collaborations between the business actors, and associated business capabilities.

When designing the business architecture, design decisions are taken and transform the domain model into the business architecture, guided by the architecture principles and the ASRs relevant from the business perspective: the design decisions are formulated as **Architecture Decision Records (ADRs)** in section 5.1.

The ADRs introduce **business roles and responsibilities** that complement the domain actors and roles: they are specified in section 5.2.

The business roles collaborate to meet the business objectives: the associated **business collaborations** are described in section 5.3. The actual specifications of the business processes is of less interest in the development of a reference architecture: they are indeed very specific to each industry and integrate specificities of each participant's environment. The business processes are however useful for identifying the business capabilities required to support the business collaborations, and they are also described in section 5.3.

The business collaborations require **business capabilities** to be deployed by each actor: they are specified in section 5.4.

5.1. Business Design Decisions

Architecture decisions are taken at the business level, transforming the conceptual domain collaboration into actual business operations. The architecture decisions are documented as Architecture Decision Records (ADRs) and formulated in Table 5.

Table 5: Business ADR's

ID	Name	Decision	Status	Consequences
ADR-01	Cross-border identification business	A separate entity, with the role of Identity Provider operates the cross-border identification of the DS	Accepted	IdP is a new role in business ops. Requires the authentication of User (ADR-02)
ADR-02	Cross-border User Authentication operations	The Identity Provider operates the cross-border authentication of the User	Accepted	IdP is a new role in business ops
ADR-03	Dynamic Location of DP	The DP capable of providing the required evidence is dynamically located	Accepted	New Capability: DP Capability Management, including DP Discovery
ADR-04	Semantic Capability	The semantics heterogeneity of Evidence across DC's and DP's is managed	Accepted	New Capability: Evidence Semantic Management, including Semantic Mapping
ADR-05	Evidence Exchanger	DP Discovery and Evidence Semantics Management capabilities are both operated by the same entity, with the role of Cross-Border Evidence Exchanger (shared resources)	Accepted	Cross-Border Evidence Exchanger is a new business role

ID	Name	Decision	Status	Consequences
ADR-06	Evidence Exchanger operations	The Evidence Exchanger role is operated by a separate entity than DC and DP	Delayed	New entity potentially operating the Evidence Exchange responsibilities for both DC and DP
ADR-07	DP Capability Registration	The Evidence Exchanger has the capability to manage the DP capabilities publications	Accepted	New capability: DP Capability Registration, included in DP Capability Management
ADR-08	Cross-border Evidence Exchange	The DC and DP rely on the Evidence Exchange Management capability	Accepted	New capability: Evidence Exchange Management
ADR-09	Evidence Exchange deployment	Evidence Exchange Management is operated by the Evidence Exchanger	Accepted	Capability assigned to Evidence Exchanger
ADR-10	Evidence Notification deployment	Data Notification capability is operated by the Evidence Exchanger (shared resources)	Accepted	Data Subscription required (ADR-09)
ADR-11	Data Subscription capability	The DC controls the notification through a subscription to Data changes	Accepted	New capability: DC Data Subscription
ADR-12	Data Subscription deployment	The Evidence Exchanger operates the DC Data Subscription capability	Accepted	
ADR-13	Provisioning Capability Publication	The Data Provider has the capability to publish to the Evidence Exchanger its capabilities to provision Data	Accepted	New capability: Provisioning Capability Publication, part of Provisioning Capability Management

The DS identification (required by the security concerns) is a capability assigned to the cross-border Identity Provider (ADR-01). It requires the authentication of the User, also assigned to the cross-border Identity Provider (ADR-02).

The dynamic location of the Data Provider requires a DP Discovery capability (ADR-03), while the cross-border semantic heterogeneity requires a Semantic Management capability (ADR-04). Both capabilities require access to shared resources, such as a registry of Data Provider and associated provisioning capabilities, and a registry of semantic mapping of Evidence across MS and administrations. For governance reason, the resources cannot be managed by either the DC's or the DP's. The DP Discovery capability and the Semantic Management capability are therefore assigned to another role, the Evidence Exchanger (ADR-05). Although it is recommended that a separate entity operates the Evidence Exchanger role according to the brokerage business model (Board of Innovation 2018)⁴⁰, it is not decided at this stage (ADR-06). As a broker, the Evidence Exchanger acts as a proxy for both the Data Consumer and the Data Provider.

In order for the Evidence Exchanger to operate the DP Discovery capability, the Data Provider has to publish its Data Provisioning Capabilities: it therefore requires the capability Provisioning Capability Publication, part of Provisioning Capability Management (ADR-13). The Evidence Exchanger has the

⁴⁰ <https://www.boardofinnovation.com/business-revenue-model-examples/the-broker/>

capability to process the publication from the Data Provider: DP Capability Registration (ADR-07), part of its Data Provider Capability Management.

The communication between the Cross-Border Evidence Access at DC, and the Cross-Border Evidence Provision at DP (see domain model) requires an Evidence Exchange Management capability (ADR-08). It is operated by the Evidence Exchanger as it relies on shared resources (ADR-09).

The Evidence Notification capability of the DP also requires shared resources: an additional capability is introduced and operated by the Evidence Exchanger (ADR-10). The DC controls the notification of Data through the use of a Data Subscription capability (ADR-11), also operated by the Evidence Exchanger (ADR-12).

5.2. Business Actor Model

According to the architecture decisions, the following roles are added to the domain actor model, as they have responsibilities in the business operations:

Evidence Exchanger (EE): The Evidence Exchanger role acts as a central point for the deployment of the cross-border evidence exchange process. It can be deployed according to various operations models: a supra-national actor, a network of actors, each Data Consumer and Data Provider. The main responsibilities are:

- (i) Manage the capabilities of the Data Providers
- (ii) Locate the Data Provider responsible for a specific Data on a Data Subject
- (iii) Manage the semantic heterogeneity of the Data across DCs and DPs
- (iv) Manage the cross-border exchange of Data
- (v) Register the subscription of data consumers to data change events
- (vi) Notify the relevant data consumer (subscribers) when an actual data change event occurs

Identity Provider (IDP): refers to the entity providing identity and authentication services. The main responsibilities are:

- (i) Identify and authenticate natural persons acting on behalf of a legal entity
- (ii) Identify legal entities

5.3. Business Collaborations

There are two main collaborations identified in TOOP:

- The cross-border data retrieval
- The cross-border data update

5.3.1. Cross-Border Data Retrieval

This collaboration realizes the objective of the Data Consumer retrieving Data from the Data Provider in the context of a cross-border procedure delivery.

Figure 10 describes the collaboration in terms of business actors, business roles and associated business capabilities, as well as the main operational flows. The Data Consumer, Data Provider and Identity Provider roles are assigned to specific actors. The Evidence Exchanger role is not yet assigned to any specific actor at this stage, and various operational models are possible. The next version of the business architecture will specifically address this question, by assessing the operational models according to the governance and sustainability dimensions.

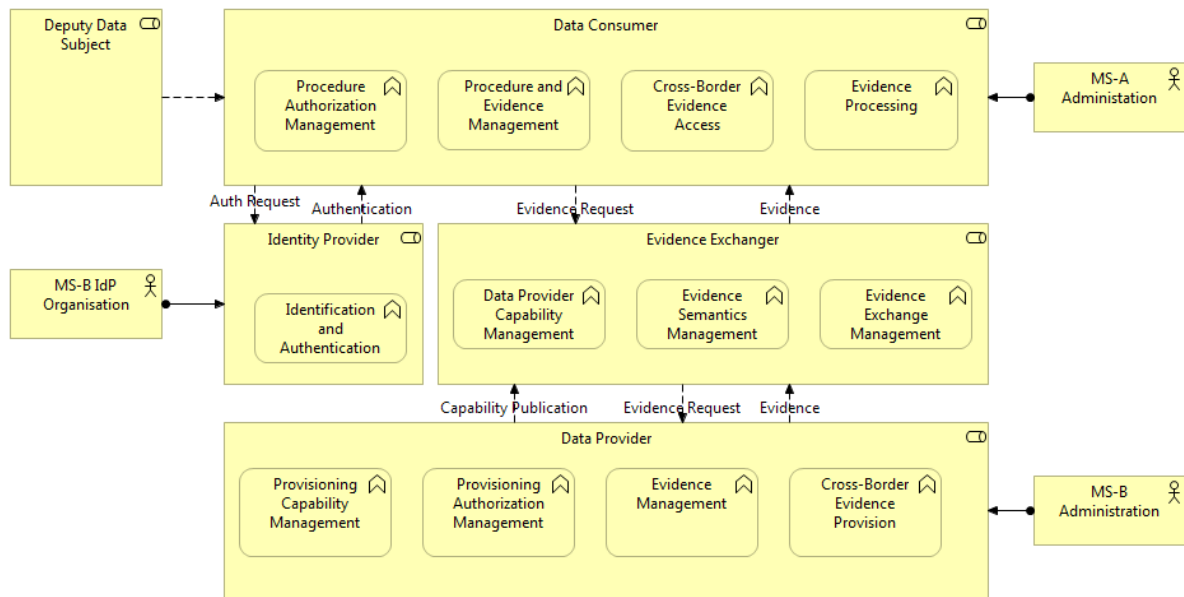


Figure 10: Data Retrieval Collaboration

The business processes associated with the participants of the collaboration illustrate how each role's capabilities are deployed in the business operations context.

Figure 11 describes the business process at Data Consumer, while Figure 12 describes the business process at Data Provider. The business processes are described at a generic level of abstraction, to support the goal of developing a generic reference architecture. The various business capabilities introduced with the architecture decisions are leveraged to support the deployment of the business processes.

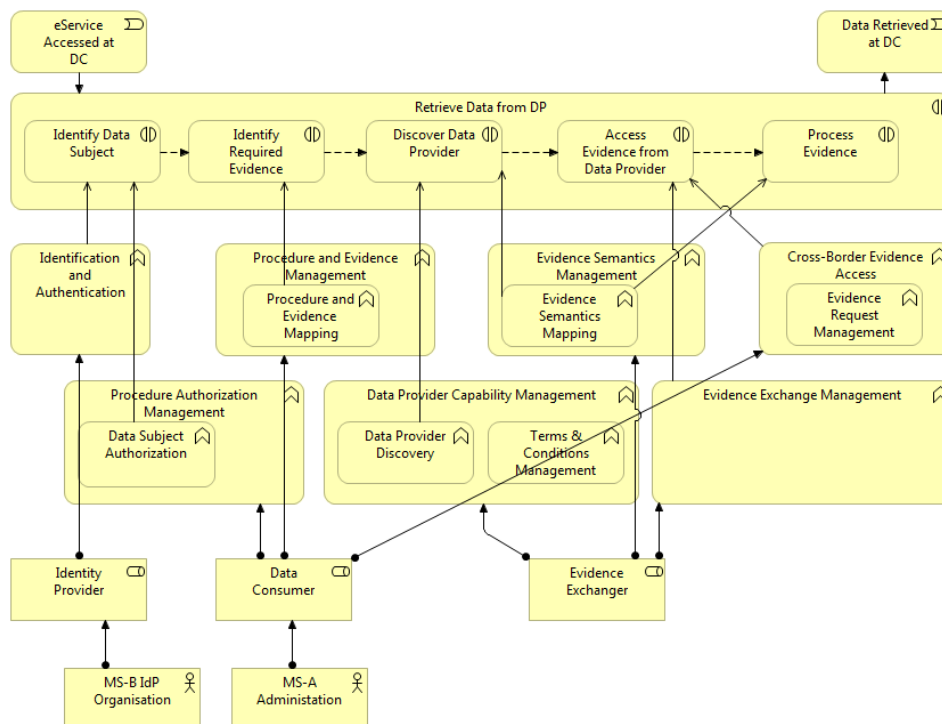


Figure 11: Data Retrieval - DC Process

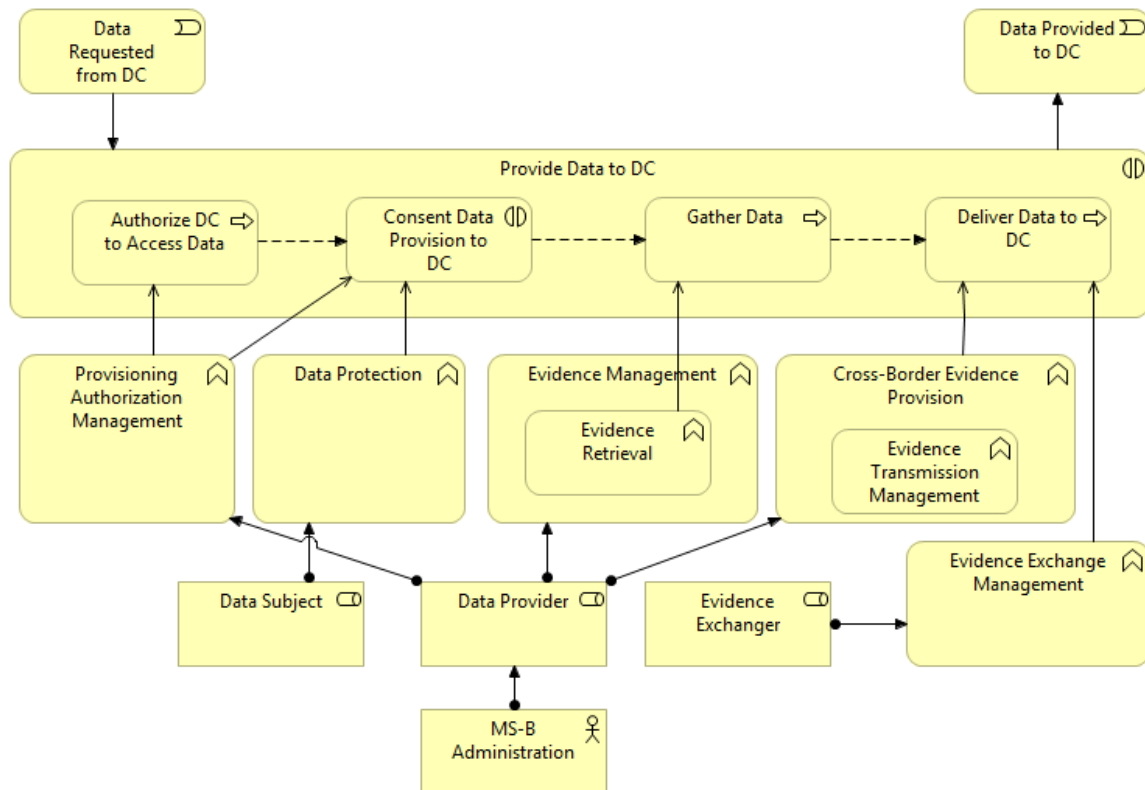


Figure 12: Data Retrieval - DP Process

Figure 13 describes the Data Provider Capability Publication business process. This is a supporting process that ensures that the Evidence Exchanger knows about the actual provisioning capabilities of the Data Providers.

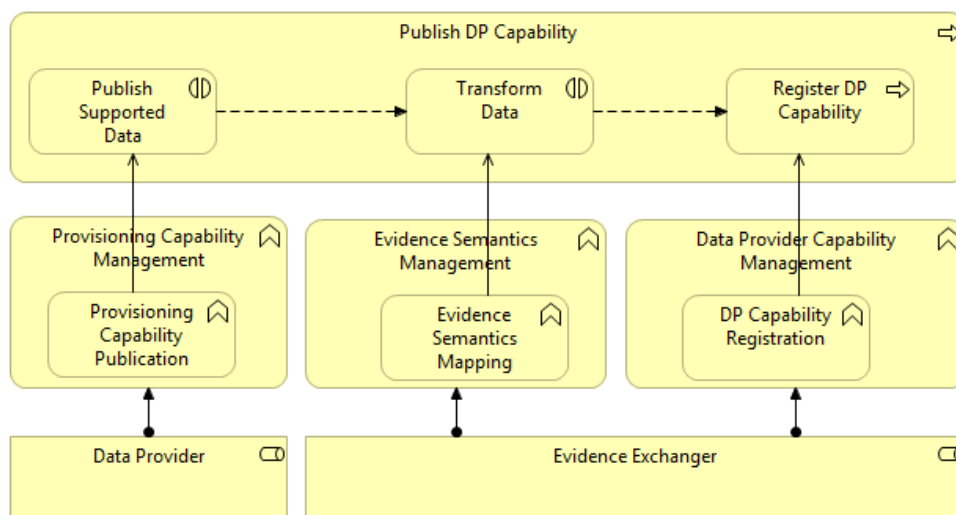


Figure 13: Data Provider Capability Publication Process

5.3.2. Cross-Border Data Notification

This collaboration realizes the objective of the Data Provider notifying the Data Consumers registered to such a notification. Figure 14 describes the collaboration in terms of business actors, business roles and associated business capabilities, as well as the main operational flows. The business processes associated with the participants of the collaboration illustrate how each role's capabilities are deployed in the business operations context.

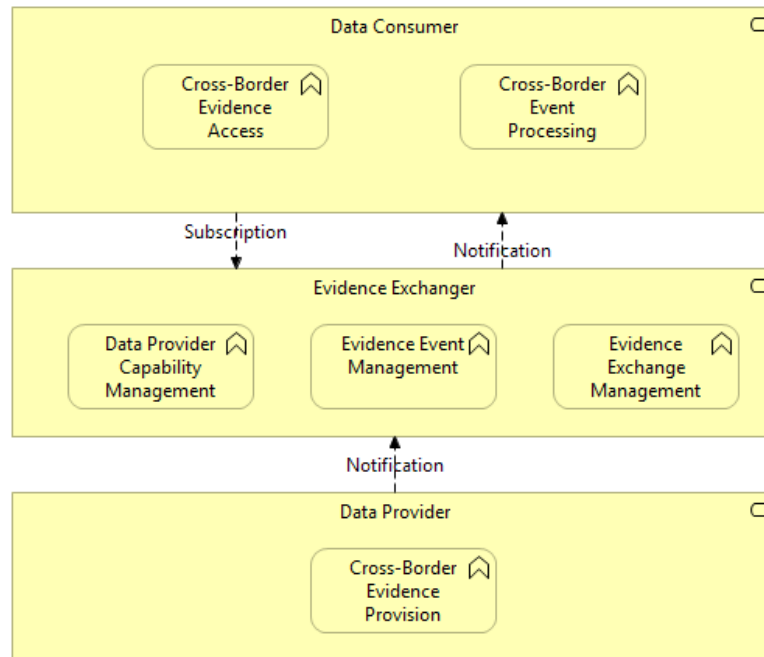


Figure 14: Data Notification Collaboration

Figure 15 describes the Data Consumer Subscription business process, while Figure 16 describes the Data Provider Notification business process. The business processes are described at a generic level of abstraction, to support the goal of developing a generic reference architecture. The various business capabilities introduced with the architecture decisions are leveraged to support the deployment of the business processes.

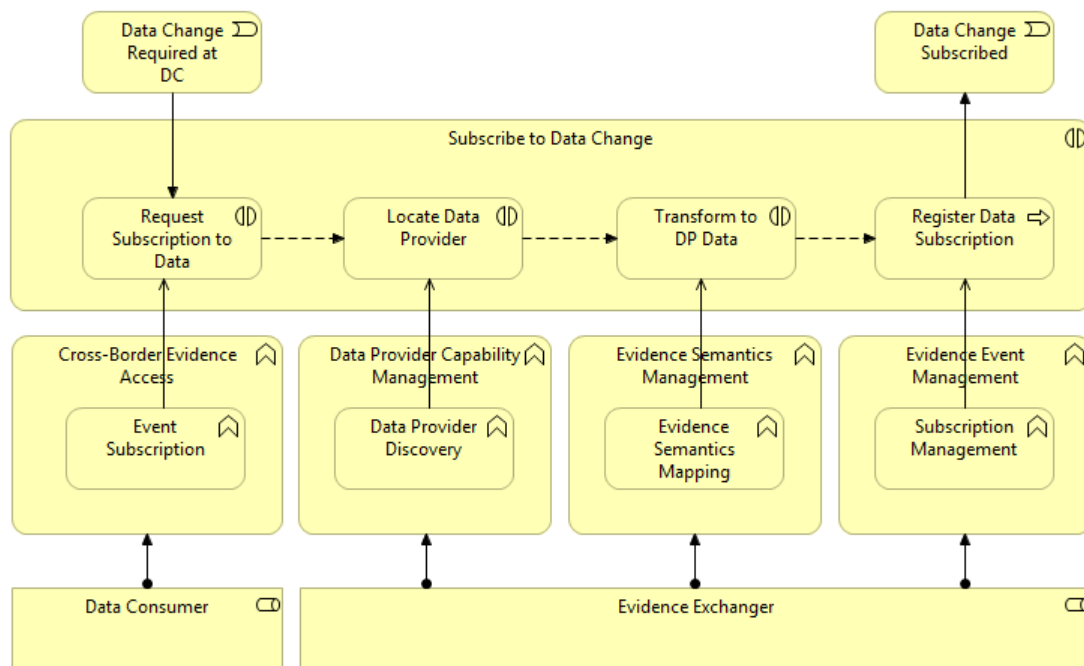


Figure 15: Data Consumer Subscription Process

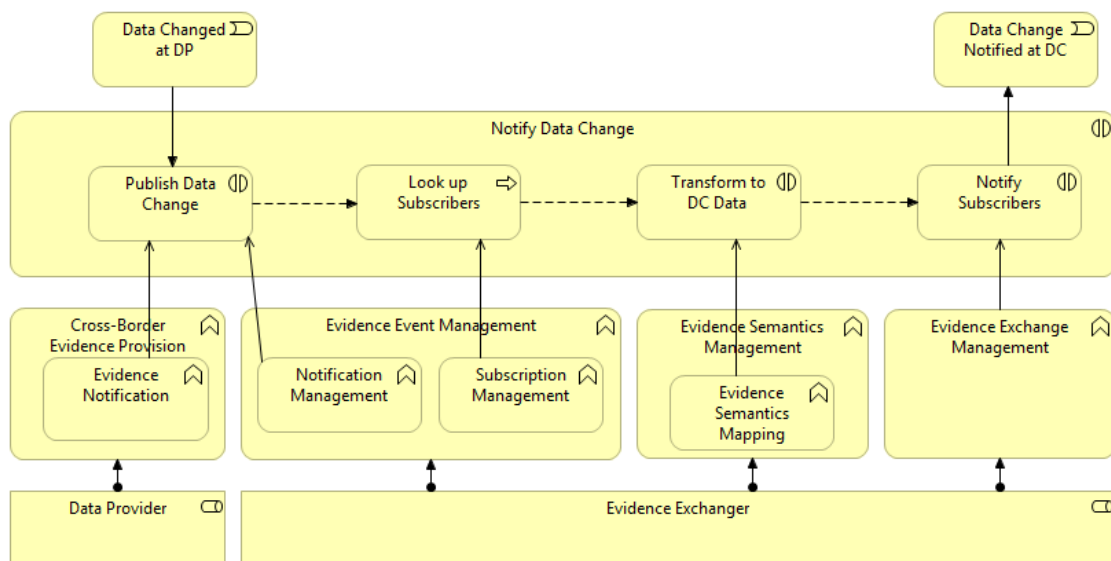


Figure 16: Data Provider Notification Process

5.4. Business Capability Model

A business capability abstracts the capacity and ability of an actor to realize its responsibilities. It deploys resources to meet the associated business goal. Each role's business capabilities are deployed in the business collaborations described in the previous section. This section specifies the business capabilities in terms of purpose, outcomes and required resources.

Figure 17 is a map of the capabilities associated with each business role. This representation is specifically useful for a participant to understand what capability it needs to deploy in order to participate to the system.

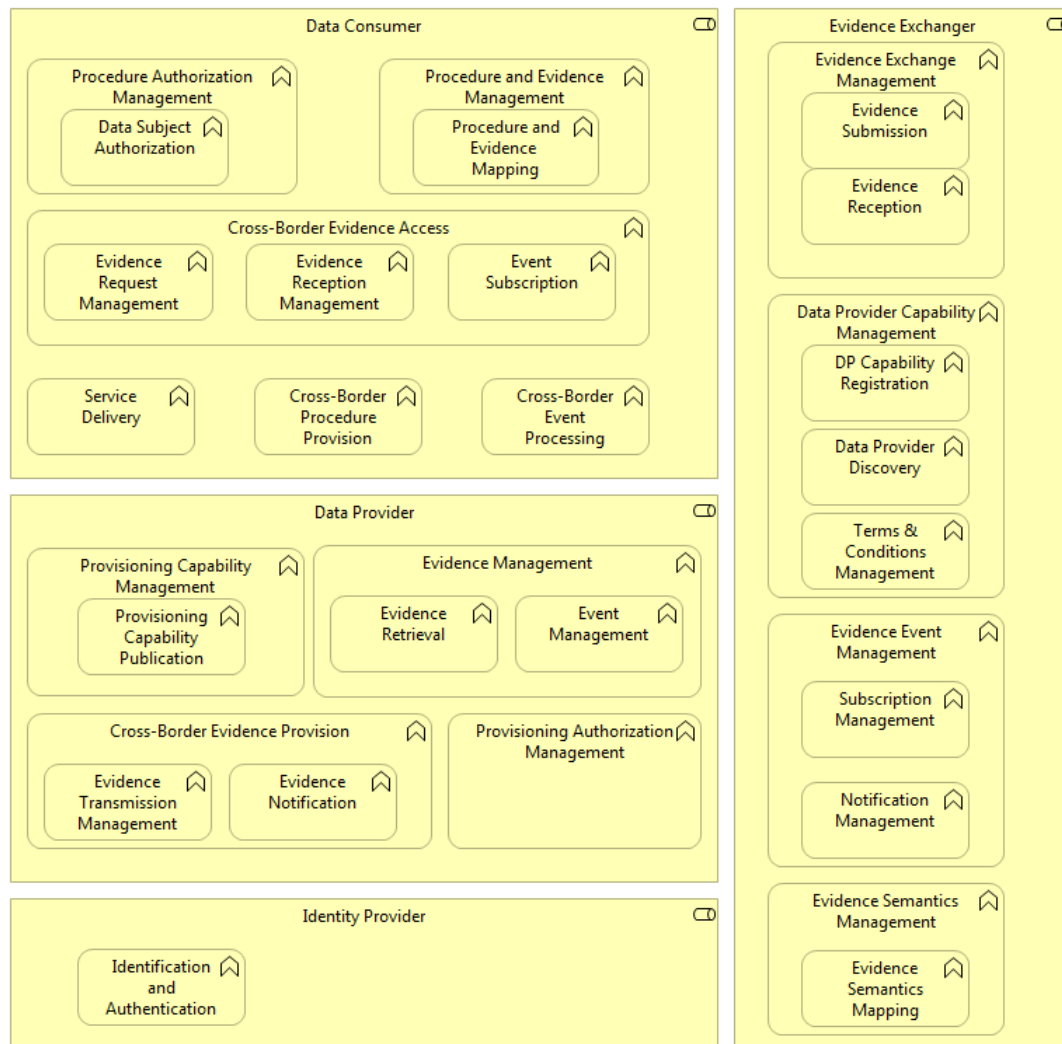


Figure 17: Business Capabilities Map

Table 6 describes the business capabilities associated with each business role. The capabilities are organized in 2 levels: the first level business capabilities represent the business domains of the organisation, while the second level business capabilities are the actual organization's capacity to successfully perform a unique business activity.

Table 6: Business Capabilities

Level 1	Level 2	Purpose
Data Consumer		
Procedure Authorization Management	DS Authorization	Authorize the DS to Access the Procedure
Procedure Evidence Management	Procedure Evidence Mapping	Identifies Evidence associated with Procedure

Level 1	Level 2	Purpose
Cross-border Evidence Access	Evidence Request Management	Manages the request for Evidence to Data Provider
	Evidence Reception Management	Manages the reception of Evidence from the Data Provider
	Event Subscription	Subscribe to events associated with an Evidence
Service Delivery		Delivers the procedure when the required Evidence is retrieved
Cross-border Procedure Provision		Provides access to the procedure for cross-border consumers
Cross-border Event Processing		Processes the event associated with an Evidence
Data Provider		
Provision Capabilities Management	Provisioning Capabilities Publication	Publishes the capabilities in terms of data provisioning
Evidence Management	Evidence Retrieval	Retrieve the Evidence from the Authoritative Data Source
	Event Management	Manages the events associated with the Evidence
Cross-Border Evidence Provision	Evidence Transmission Management	Manages the transmission of the Evidence
	Evidence Notification	Notifies the events associated with an Evidence
Evidence Exchanger		
Provisioning Authorization Management		Manages the authorization associated with the provisioning of Evidence
Evidence Exchange Management	Evidence Submission	Submit the Evidence to the requesting Data Consumer
	Evidence Reception	
Data Provider Capability Management	DP Capability Registration	Register the provisioning capabilities of the Data Providers
	Data Provider Discovery	Locate the Data Provider able to provide the required Evidence
	Terms and Conditions Management	Manages the terms and conditions associated with the retrieval and usage of Evidence
Evidence Event Management	Subscription Management	Manages the subscription to Evidence Events from Data Consumers
	Notification Management	Manages the notification of the Evidence Events received from the Data Providers
Identity Provider		
Identification and Authentication		Authenticates a cross-border user

5.5. TOOP Common Semantic Model

In the previous sections, the various actors, roles, processes, capabilities and services are described that are part of the TOOP business architecture. The actual data or information that is provided only once by businesses and stored, exchanged and requested afterwards is not described yet. In order to capture the information and its semantics that TOOP is concerned with, we define a TOOP Common Semantic Model. This model:

- defines common TOOP concepts in the scope of the project, i.e. business and company information.
- capture the semantics/meaning of these concepts in terms of clear definitions/labels and the formal relations between these concepts in terms of RDF and OWL constructs.
- contains formal mappings between TOOP concepts and national member state concepts in order to transform data requests/responses between member states and the TOOP platform.

In a first version of the TOOP CSM, we focus on basic company data and define the following TOOP concepts:

Table 7: TOOP Common Concepts

TOOP Concept	Short definition
CompanyCode	The unique company identifier
CompanyName	The official current company name as stored in the business register
CompanyType	The legal type of the company
LegalStatus	The legal status of the company (active, ended,...)
MainSite	Aggregation of the address, telephone number, email of the main (physical) site of the company
CompanyAddress	The physical address of the company
CompanyTelephoneNumber	The telephone number of the company
CompanyEmail	The email address of the company
LegalRepresentativeFamilyName	The surname of the legal representative for the company
LegalRepresentativeFirstName	The first name of the legal representative for the company
LegalRepresentativeDateOfBirth	The data of birth of the legal representative for the company
LegalRepresentativeInfo	The type of representation the legal representative is granted

These concepts and their relations have been modelled in the form of an ontology that is constructed using the W3C RDF, RDFS and OWL specifications. In addition, existing vocabularies and ontologies have been reused as much as possible, especially the core vocabularies of ISA2 and ontologies registered at W3C. A first diagrammatic view of the TOOP:RegisteredOrganization concept and the subclasses and properties it uses can be found in the diagram below.

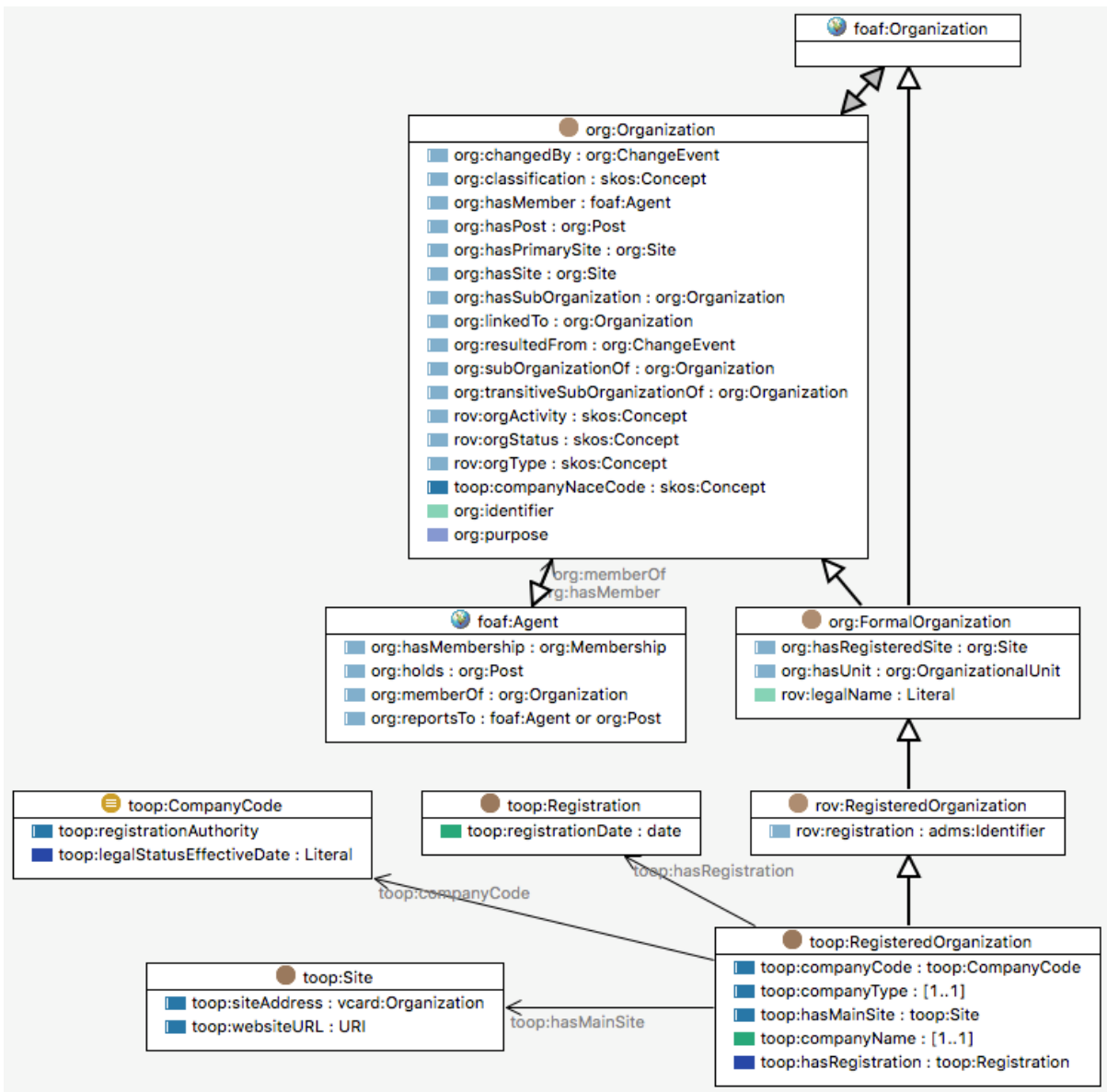


Figure 18: Snapshot of the TOOP Common Semantic Model

The TOOP concepts are mapped to national member state concepts via an ontological mapping using RDF, RDFS and OWL constructs. An example of the mapping between the `toop:CompanyCode` and the Dutch `nh:KvK-nummer` is given in the figure below. The `owl:equivalentClass` construct from the OWL language is used to express the equivalence or similarity of the two concepts.



Figure 19: Example of a TOOP CSM concept to a national member state concept.

For more details on the definition of the TOOP concepts, please see the TOOP CSM page on the wiki: <http://wiki.ds.unipi.gr/pages/viewpage.action?spaceKey=TOOP&title=TOOP+Common+Semantic+Model>.

6. Technology Architecture

Designing the Technology Architecture - the logical software and hardware capabilities that are required to support the deployment of business, data, and application services - requires an overview and thorough analysis of the available building blocks. A first version of this analysis has been provided in the deliverable “D2.1. Generic federated OOP architecture (1st version)”. The current chapter presents the analysis summaries for selected building blocks. In the forthcoming deliverables, the Technology Architecture will be complemented with potential new Building Blocks and extensions and with design of how the Building Blocks will be used to support the IS architecture.

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 4;
- 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.

6.1.eDelivery

Overview and references

The CEF eDelivery Digital Service Infrastructure (DSI) Building Block defines an interoperability architecture to implement the technical components needed to exchange electronic data and documents between entities in an interoperable, secure, reliable and trusted way. The building block was first developed in the e-SENS project and later the governance and maintenance was taken over by CEF.

The eDelivery building block is based on a distributed model, where each participant is a node in the network, using standard transport protocols and security policies. 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.

Besides this basic *Message Exchange* building block the eDelivery architecture includes the *Dynamic Service Location* and *Capability Lookup* building blocks which enable the dynamic configuration of the network nodes. This reduces the complexity of managing participants in the network because it enables direct communication between participants without the need to set up bilateral agreements.

All eDelivery building blocks build on OASIS specifications which are then further profiled for use within the building block’s architecture. For the *Message Exchange* building block the underlying OASIS specification is the “AS4 Profile of ebMS 3.0” and for the *Dynamic Service Location* and *Capability Lookup* building blocks these are the “Business Document Metadata Service Location Version 1.0” respectively the “Service Metadata Publishing (SMP)” specifications.

Rationale for inclusion in the TOOP architecture

The main goal of TOOP is to enable users to retrieve data they already provided to a public authority for re-use in other business processes, so they don’t need to providing data more than once. This requires that the TOOP architecture includes a mechanism for the exchange of information between the data consumers and data providers. Therefore it is evident that there’s a need for at least the *Message Exchange* building block in the TOOP architecture.

Since data consumers may need to communicate with many data providers also the *Dynamic Service Location* and *Capability Lookup* building blocks will be included in the TOOP architecture to enable the dynamic configuration of network nodes.

Application

Currently there is no single generic implementation of an eDelivery gateway, there are several open source and commercial implementations that are listed in CEF eDelivery pages. Typically, any CEF conformant eDelivery Gateway can be deployed and used for TOOP, with minimal adjustments to their backend interfaces, since TOOP will reuse the Conformance and Interoperability Testing Interface that every CEF Conformance gateway must implement.

Usage, maintenance, and further development

The CEF eDelivery building block is used in multiple production environments, for example in the eJustice and EUCED domain. The OASIS AS4 Profile standard which is the basis for the *Message Exchange* building block is also used within the energy sector and for the communication with the Australian Tax Office but they use their own profiles of the OASIS AS4 Profile. PEPPOL already uses the *Dynamic Service Location* and *Capability Lookup* building blocks in production and is now in the process of full implementation of CEF eDelivery as it is migrating the messaging protocol to AS4.

As owner CEF is responsible for the maintenance and further development of the generic eDelivery building block, including the profiles of the used OASIS specifications.

Gap analysis

In TOOP it is assumed that the data consumer does not know beforehand which data provider can provide certain information. This means that a problem that needs to be solved in TOOP is how the data consumer can determine the data provider it should contact to get the requested information.

When using the *Capability Lookup* building block, data providers will already publish information about the requests they can receive and process in the SMP. By querying the information stored in the SMPs, data consumers could find the data providers they should contact for a specific kind of data. Querying the data available in the SMPs however is neither part of the OASIS SMP specification nor the *Capability Lookup* building block.

As the need to query the data available in the SMP was already recognized in the PEPPOL community they have developed a so-called “PEPPOL directory” that does allow for querying of data stored in the SMPs. This could also be a solution for the TOOP problem of finding the right data provider.

6.2.eID

Overview and references

The CEF eID Building Block⁴¹ (CEF Digital 2018a) is a set of services providing effective and secure cross-border authentication through the mutual recognition of national eID schemes. 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) 910/2014⁴²) 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.

⁴¹ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID>

⁴² http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

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. In particular, this allows a legitimate user to securely access services in a foreign European country through one or more identity attributes.

Rationale for inclusion in the TOOP architecture

To adhere to the Once Only Principle, public administrations need to share data of citizens and businesses, at the same time respecting the data protection rules. This requires secure cross-border authentication into the OOP systems involved, in order to exchange information between public administrations. For this reason, the eID BB will be needed in future OOP applications.

Application

The CEF eID Building Block is a set of services provided by the European Commission. These services include technical specifications, software (eIDAS Node integration package), testing, training, and other services⁴³.

The eIDAS-Node software is a sample implementation of the latest set of eIDAS-compliant technical specifications⁴⁴. It contains the necessary modules to help Member States to communicate with other eIDAS-compliant counterparts in a centralised or distributed fashion. The sample implementation comprises eIDAS-Node, an implementation of the eID eIDAS Profile able to communicate with other nodes of the eIDAS Network, testing tools, as well as additional tools for setting up a demo environment for testing purposes. The sample software is mainly intended for stakeholders that are responsible for setting up and managing the eIDAS-Node in their respective Member States.

Usage, maintenance, and further development

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 eID⁴⁵.

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.

Gap analysis

The main challenges of using the eID Building Block in TOOP are its integration with the other Building Blocks (e.g., eDelivery), its integration in existing e-services, OOP systems, and online platforms in various public or private sectors, as well as design of enabling attributes, mandates and authorities to be associated with electronic identities for cross-border use through the eIDAS node.

6.3.eSignature

Overview and references

Through the CEF eSignature building block⁴⁶ (CEF Digital 2018b), the European Commission supports the use of electronic signatures across European countries. This BB facilitates the mutual recognition and cross-border interoperability of eSignatures between the Member States, allowing the public administrations and business to trust and use eSignatures that are valid and structured in EU

⁴³ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/All+eID+services>

⁴⁴ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Node+integration+package>

⁴⁵ https://ec.europa.eu/info/departments/communications-networks-content-and-technology_en

⁴⁶ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature>

interoperable formats. It helps public administrations and business 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.

Rationale for inclusion in the TOOP architecture

The eSignature BB can be used in OOP systems to ensure that information can be relied upon and is accurate and complete. It also helps to establish traceability and non-repudiation of business transactions. The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation) has applied directly to the EU Member States since 1 July 2016, so the OOP systems must be able to support it. The eSignature BB is a mature building block with sufficient amount of specifications and software available for utilization.

Application

Most Member States have their providers of eSignatures services⁴⁷. In case a service provider is not available, or if a separate service provider is needed, an open-source software library for electronic signature creation and validation (Digital Signature Services⁴⁸, DSS) can be used. It is available for download from the CEF Digital Portal⁴⁹.

Usage, maintenance, and further development

The European Commission maintains an open-source library supporting the creation and validation of electronic signatures in line with European legislation and standards, compliant with the eSignature specifications.

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.

Gap analysis

The OOP applications that need to use the eSignature Building Block must be able to use the Digital Signature Service open-source library to create and/or validate electronic signatures and electronic seals compliant with the eIDAS Regulation and related standards.

6.4.eTranslation

Overview and references

eTranslation is the CEF Automated Translation building block⁵⁰ (CEF Digital 2018c). Its purpose is to provide means of information exchange throughout Europe for national and European administrations, overcoming the existing language barriers within the Union. CEF eTranslation is mainly intended for integration into other digital services, but can also be used as a stand-alone service.

The CEF eTranslation building block utilizes the existing Machine Translation service of the European Commission (MT@EC) developed by the Directorate-General for Translation (DGT). MT@EC is based

⁴⁷ <https://webgate.ec.europa.eu/tl-browser/#/>

⁴⁸ <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pagelD=46992515>

⁴⁹ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS>

⁵⁰ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eTranslation>

on the open source software MOSES, which is a machine translation system, based on a statistical machine translation approach⁵¹ (Koehn et al. 2007). The translation engines of MT@EC are based and trained on the European advanced multilingual information system (Euramis)⁵² translation memories, providing translation capabilities for 24 languages.

Rationale for inclusion in the TOOP architecture

eTranslation is included in the TOOP architecture, because it enables one of the GOOPRA underlying principles, it has been indicated as potentially needed in pilot areas, it provides additional capabilities as compared to other solutions, its application is practically viable, it has been used in other projects, and it is supported and developed further.

eTranslation enables multilingualism - one of the main political and legislative principles underlying the TOOP generic federated OOP architecture, as stated in the Annex 2 to the European Interoperability Framework Implementation Strategy (European Commission 2017)⁵³.

The preliminary mapping of TOOP pilot areas and building blocks has indicated that eTranslation may be needed.

Support for multilingualism can be provided in various ways, but compared to general-purpose web translators, CEF eTranslation provides two important additional 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).

Application

The eTranslation service provided by the European Commission is available for single users or entire public authorities, either through direct access via the existing Web interface or for developers via an API for integration into another system.

Usage, maintenance, and further development

Projects, which have already included the eTranslation service into their architecture are, e.g., the European Data Portal⁵⁴, the e-Justice Portal⁵⁵, or the Online Dispute Resolution Forum⁵⁶.

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-documented⁵⁷ (Koehn 2010).

Gap analysis

Currently there is no public software nor API specification available, and projects, which would like to incorporate the service, have to explicitly request access. Therefore, 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.

⁵¹ <http://www.statmt.org/moses/?n=Moses.Overview>

⁵² <https://ec.europa.eu/jrc/en/language-technologies/dgt-translation-memory>

⁵³ http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF

⁵⁴ <https://www.europeandataportal.eu>

⁵⁵ <https://e-justice.europa.eu/home.do>

⁵⁶ <https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home.show&lng=EN>

⁵⁷ <http://www.statmt.org/moses/manual/manual.pdf>

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.

6.5. Traceability and Non-Repudiation

Overview and references

Traceability is the set of tools and techniques aimed at following paths and footprints of *principals*, e.g., users, transactions, and software agents (Cleland-Huang et al. 2007; Cleland-Huang, Gotel, and Zisman 2011; Mason 2012; Zhou 2001). It is also defined by ISO 9000:2005 as the "ability to trace the history, application, or location of that which is under consideration". The ISO 9000:2005 specially focuses on the origin of the artefacts, the processing history, and the distribution of the artefact after the delivery. In order to be authoritative, traceability needs to be coupled with cryptographic techniques such as integrity, electronic signature, namely *evidence tokens*. Such concepts as "history", "application", and "location" need the support of a reliable logging framework and an accurate synchronized clock among the participant of the business transaction under analysis.⁵⁸

Non-repudiation services are mandated to generate, collect, maintain, make available and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. Non-repudiation mechanisms provide protocols for the exchange of non-repudiation tokens specific for non-repudiation service. Non-repudiation tokens shall be stored as non-repudiation information that may be used subsequently in case of disputes by services named Trusted Third Parties (TTP). Different applications and their legal environments motivate the support and usage of specific security policies, and thus, specific non-repudiation policies.⁵⁹

The e-SENS Non-Repudiation and Traceability SAT 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)⁶¹. The SAT builds on two ABB: Timestamping⁶² and Evidence Emitter⁶³. Both building blocks rely directly on standards and have not been profiled in the e-SENS project although for the evidence emitter some recommendations are given how to profile it for specific domains.

Rationale for inclusion in the TOOP architecture

Traceability and non-repudiation are included into TOOP architecture, because these are a much-desired property in any business transaction, both in the real and digital world.

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. Non-repudiation refers to situation where the author of a statement will not be able to successfully challenge the authorship of that statement.

The preliminary mapping of TOOP pilot areas and building blocks has indicated that eTranslation may be needed.

The core functionality of OOP architecture for traceability and non-repudiation will be based on e-SENS Non-Repudiation and Traceability SAT¹⁴⁵. 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

⁵⁸ <http://wiki.ds.unipi.gr/display/ESENS/SAT+-+Non-Repudiation+and+Traceability+1.3>

⁵⁹ Ibid

TOOP software might be necessary in order to strengthen OOP architecture with functional and rigorous tools for traceability and non-repudiation.

Application

The core software modules needed for traceability and non-repudiation are still under the development.

Usage, maintenance, and further development

The core software modules needed for traceability and non-repudiation are still under the development. The Non-Repudiation and Traceability SAT developed by the e-SENS project should be adopted by CEF.

Gap analysis

The core software modules needed for traceability and non-repudiation are still under the 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.

6.6.Trust Establishment

Overview and references

Trust establishment guarantees, that data and documents are secured against any modification (integrity); documents are encrypted during the transmission and the origin and the destination of the data and documents are trustworthy (Cofta 2007; Gaurav, Sarfaraz, and Singh 2014; Winslett 2003).

In order to activate the message exchange, two public administrations' Access Points need to establish trust between each other.⁶⁰ Trust establishment is an important if not essential aspect of data change, which does contain roughly two critical stages: request of data and validation of the data request. This highlights Public Key Infrastructure role within data exchange process. Within CEF framework, Public Key Infrastructure 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.⁶¹

Rationale for inclusion in the TOOP architecture

Trust Establishment is present in both architectural frameworks: e-SENS and CEF. The preliminary mapping of TOOP pilot areas and building blocks has indicated that eTranslation may be needed. e-SENS SAT Trust Establishment is developed in line with the objectives of eIDAS⁶². There is a certain conflict between structures of e-SENS SAT and CEF framework regarding this TOOP related building block. Question is whether Trust Establishment should be handled as integral part of eDelivery⁶³ or should it remain as independent building block as e-SENS SAT.

⁶⁰ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/How+does+eDelivery+work+--+Trust+Establishment>

⁶¹ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service>

⁶² http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

⁶³ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/How+does+eDelivery+work+--+Trust+Establishment>

Application

According to CEF approach, Access Points need to establish trust between each other. This is possible using 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)⁶⁴ and Service Metadata Publishers (SMP)⁶⁵, to ensure confidentiality, integrity and non-repudiation of the data moving across systems.

Usage, maintenance, and further development

Components of Trust Establishment, CEF eDelivery Access Points⁶⁶ and Service Metadata Publishers⁶⁷ are supported by CEF. Same applies for the CEF managed services regarding Public Key Infrastructure⁶⁸ and Service Metadata Locator.⁶⁹

Gap analysis

The overlap between TOOP specific eDelivery expected functionality and e-SENSE Trust Establishment SAT functionality needs to be established and relevant development decisions made before defining the actual gaps in needed functionality.

6.7.eDocument

Overview and references

eDocument (e-SENS 2015), a high-level building block consolidated by eSENS project, provides solution architects with a template to be used in creating interoperable and reusable solutions that support the handling of e-Documents by the public administration. It includes a collection of specifications and standards that can be utilized for specifying and building applications.

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

- Document Provisioning ABB⁷⁰ describing how to produce and consume an e-Documents comprises the following functions: structure, validate, annotate, convert or transform, attach business rules;
- Document Container ABB⁷¹ which 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. It includes document packaging, attaching signatures and timestamps and document encryption. The specification proposed for the Container are ETSI ASiC Specifications (ETSI 2013, 2006).
- Document Business Envelope ABB⁷² which 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. For the routing functionality the recommended standard is *UN/CEFACT Business Document Header SBDH* (GS1 2012).

⁶⁴ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+software>

⁶⁵ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+software>

⁶⁶ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+specifications>

⁶⁷ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+specifications>

⁶⁸ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service>

⁶⁹ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+service>

⁷⁰ <http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Document+Provisioning+-+0.7.0>

⁷¹ <http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Document+Container+-+0.6.0>

⁷² <http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Document+Business+Envelope+-+0.6.0>

Rationale for inclusion in the TOOP architecture

eDocument provides with a common terminology and approach supporting interoperability needs of e-Document services and specifically addresses the semantic interoperability needs.

It promotes a binding contract between the producer and the consumer in which the two parties are agreeing upon the e-Document exchange format, the method of exchanging electronic documents and the methods of assuring the authenticity and non-repudiation of the information.

Through the routing functionality based on SBDH it allows end entities to encode information on business process, business transaction, agreement, and business quality-of- service and facilitates automated machine processing without opening the container structure, thus it may be useful for solutions developed in TOOP pilots.

eDocument introduced the concept of Application Profiling for e-Documents, defined as an e-Document engineering methodology (ISA 2014), along with a set of guiding principles, that may be adopted and followed by any domain in order to create a customized e-Document format.

It supports advanced digital signatures (XML Advanced Electronic Signatures (XAdES) and CMS Advanced Electronic Signatures (CAAdES) for non-repudiation and trusted timestamps for the long-term preservation.

Application

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

Usage, maintenance, and further development

eDocument structuring functionality is covered by the e-Document engineering methodology defined in *Guidelines for public administrations on e-Document engineering methods* (ISA 2014) by ISA.

An open-source validation service is ph-schematron⁷³ a Java library that validates XML documents via ISO Schematron⁷⁴, licensed under Apache 2.0 license.

The document container is recommended to be generated using a software that is known in producing a valid ASiC container. There are several solutions, including European Commission DSS⁷⁵, for producing a valid ASiC container.

SBDH is interpreted by the gateways in order to route documents between member states. A library for producing and consuming various variants of Standard Business Documents according to the UN/CEFACT SBDH TS v1.3 is vefa-sbdh⁷⁶.

Gap analysis

Currently there are several public implementation software tools and libraries available on Joinup and Github developed during PEPPOL and eSENS projects, which could be used for eDocument components generation and integration. Though, the structure of the exchanged documents, the ASiC container and SBDH need to be profiled for each TOOP piloting domain use case. When using eDocument components within the pilots, a profiling must be done, in order to achieve high quality and reliable results (e-SENS 2016).

⁷³ <https://github.com/phax/ph-schematron/>

⁷⁴ <http://schematron.com/>

⁷⁵ <https://joinup.ec.europa.eu/release/dss-470>

⁷⁶ <https://github.com/difi/vefa-sbdh>

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

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 supporting automated processing of documents.

6.8.Semantics

Overview and references

The main role of the semantics building blocks is to enable semantic interoperability between IT systems of different member state governments within the EU. Semantic interoperability is defined 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. The core to the solution is to strive for a loosely coupled semantic architecture that will align the MS-ontologies (i.e. the member states' particular native models) and then will translate the data from the native format of MS A into the native format of MS B, in conformance with the particular alignment that have been established.

The semantics building block utilizes existing services and vocabularies:

- e-SENS Semantic Mapping Service⁷⁷ (e-SENS 2017) translates terms or concepts between different domains or communities or between different levels of abstraction, completing the requestor's knowledge with relevant domain knowledge. The service's conceptual functionality is to provide legal and semantic interoperability, with the provision of legal document equivalence mapping.
- e-CERTIS⁷⁸ is an implementation of the e-SENS Semantic Mapping Service for the eProcurement domain. It has been implemented by DG GROW (European Commission, 2016).
- e-SENS Base Registry Service⁷⁹ is a trusted authentic source of information under the control of an appointed public administration or organization appointed by government. The base registry is managed by a governing administration that, on a legal basis, has the mandate to collect the necessary data to create and maintain over time the register.
- ISA core vocabularies are simplified, re-usable and extensible data models that capture the fundamental characteristics of an entity in a context-neutral fashion. The Core Vocabularies developed are: i) Core Person (ISA specification 2012), ii) Registered Organisation (ISA specification 2012), iii) Core Location (ISA specification 2012), iv) Core Public Service (ISA specification 2013), (ISA specification 2017) v) Core Criterion and Core Evidence (ISA Specification 2016), and vi) Core Public Organisation (ISA specification 2016).

Rationale for inclusion in the TOOP architecture

Semantics is included in the TOOP architecture, because it enables many GOOPRA underlying principles including Interoperability, Reusable Data Model, "Common Semantic Standards and Vocabularies" and Technical Interoperability. Semantics have been indicated as needed at "PA1

⁷⁷ <http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Semantic+Mapping+Service-new>

⁷⁸ <https://ec.europa.eu/growth/tools-databases/ecertis/>

⁷⁹ <http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Base+Registry>

Business Mobility” and at “PA2 Business Registries”. At “PA3 Ship and Crew Certificates” Semantics is indicated as potentially needed.

Additionally, Semantics realizes some business services identified by GOOPRA: i) the Identification of Required Data and ii) the Determination of Terms and Conditions. To achieve this, the Semantics building block generates alignments between different ontologies. This semantic reconciliation process is needed at design-time and results in alignments between ontologies used in different systems in different member states. These alignments are used to perform semantic mediation at run-time when this is asked for by member state systems in the pull and push scenarios in OOP cross-border applications. 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. To guarantee the consistency of the alignment a governance process is necessary.

Application

Currently there is no generic implementation of the Semantic Mapping Service. e-CERTIS provides an implementation of the Semantic Mapping Service but is dedicated only at eProcurement. e-SENS provides only the specification of the service. It also provides documentation for a suggested REST API from the experience of both the PEPPOL European VCD System Requirements and the e-CERTIS use cases. The core vocabularies are implemented and provided by the EU ISA program⁸⁰.

Usage, maintenance, and further development

The core vocabularies are maintained by the ISA program. However, these models do not cover all the TOOP requirements so there is a need to define the “TOOP common semantic model” that re-uses many concepts of the core vocabularies. Additionally, the e-SENS Semantic Mapping Service specification needs to be further extended and make use of existing core vocabularies as developed by ISA program and the “TOOP common semantic model”. The Semantic Mapping Service will be made available in a linked data triple store on a server that is accessible via a REST-API. The API will support SPARQL (Harris and Seaborne 2013) queries to be submitted to the triple store to retrieve the semantics of the TOOP concepts and their mapping to national models.

Gap analysis

Currently there is no generic implementation of the Semantic Mapping Service, while the existing ISA core vocabularies do not fully cover the TOOP needs. Hence, a “TOOP common semantic model” and a generic Semantic Mapping Service should be implemented by TOOP.

6.9. Summary of the Building Blocks

As a start of the technology view, this chapter has provided analysis of selected building blocks with respect to their relevance for inclusion in the TOOP architecture, applicability, sustainability of maintaining and supporting organisation, and gap analysis (need for further development).

The summary of the BB analysis for these properties is provided in the below table. The list of building blocks in the table may be complemented in future versions of the architecture.

⁸⁰ https://ec.europa.eu/isa2/solutions/core-vocabularies_en

Table 8: Summary of the BB Analysis

Building Block	Relevance	Applicability	Sustainability	Need for further development
eDelivery	Needed or maybe needed in all pilots	Specifications and software exist	CEF Building Block	Regular updating and maintenance
eID	Needed or maybe needed in all pilots	Specifications and software exist	CEF Building Block	Three ways for using eIDAS compliant eID BB
eSignature	Maybe or not needed in the pilots	Specifications and software exist	CEF Building Block	Use of cross-border interoperable electronic signatures is supported
eTranslation	Maybe or not needed in the pilots	Specifications and service exist	CEF Building Block	Work In Progress
Traceability and Non-Repudiation	Needed or maybe needed in all pilots	Specifications exist	Should be adopted by CEF	Work In Progress
Trust Establishment	Needed or maybe needed in all pilots	Specifications exist	Should be adopted by CEF	Work In Progress
eDocument	Needed or maybe needed in all pilots	Specifications exist	Should be adopted by CEF	Regular updating and maintenance
Semantics	Needed or maybe needed in all pilots	Specifications, ISA Core Vocabularies exist	The core vocabularies are maintained by the ISA program	Work In Progress

The table allows to conclude that it is possible to build the generic federated OOP architecture 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, and that it will provide support for future developers of OOP projects. Still continuous effort is needed for the regular updating and maintenance of the most mature building blocks, as well as for advancement of the building blocks which are still in the development stage.

Conclusion

This deliverable presents the second official version of the generic federated OOP architecture. Compared to the first official version D2.1, it develops the architecture further, aligns it with the provisions of the forthcoming regulation about the Single Digital Gateway, and focusses on the domain, requirements, and business views of the architecture.

The architecture description in the current deliverable is organized along the business view, concerned with the business operations of the TOOP system. As the project is itself defining the Cross-Border Once Only and is required to support the development of the SDG Regulation, two preliminary views are added: the domain view, concerned with the definition of the Once Only domain (the problem domain), and the requirements view, concerned with the objectives, needs, legal obligations and principles driving the architecture of the system. Main characteristics of the applicable Building Blocks provided in D2.1 form a basis for the forthcoming Technology 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); that this architecture will be 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; and that it will provide support for future developers of OOP projects. Still continuous effort is needed for the regular updating and maintenance of the most mature building blocks, as well as for advancement of the building blocks which are still in the development stage.

This deliverable is a work in progress. The next steps are to develop the architecture in more detail, to add the IS architecture dealing with the structure and interaction of the applications that provide key business functions and manage the data assets, to complement the Technology Architecture with potential new Building Blocks and extensions and with the design of the usage of the Building Blocks to support the IS architecture, as well as to continue the exploratory and agile approach, together with cooperation with the TOOP pilots and other TOOP tasks. The forthcoming official deliverables are D2.3 (M21, September 2018), and D2.4 (M30, June 2019).

References

TOOP Deliverables

- TOOP D2.1: Tepandi, J., Verhoosel, J.P.C., Zeginis, D., Wettergren, G., Dimitriou, J., Rotuna, C., Carabat, C., Albayrak, Ö., Yilmaz, E., Lampoltshammer, T., Täks, E., Prentza, A., Brandt, P., Kavassalis, P., Leontaridis, L., Streefkerk, J.W. (2017) Generic Federated OOP Architecture (1st version). Deliverable D2.1 of the TOOP project. Available at: http://toop.eu/sites/default/files/D21_Federated_OOP_Architecture.pdf.
- TOOP D2.5: Graux, H. (2017) Overview of legal landscape and regulations. Deliverable D2.5 of the TOOP project. Available at http://www.toop.eu/sites/default/files/D25_legal_landscape_and_regulations.pdf.
- TOOP D2.6: Krimmer, R., Kalvet, T., Toots, M., Cepilovs, A. (2017) Position Paper on Definition of the “Once-Only” Principle and Situation in Europe. Deliverable D2.6 of the TOOP project. Available at: http://toop.eu/assets/custom/docs/TOOP_Position_Paper.pdf.
- TOOP D2.7: Kalvet, T., Toots, M., Krimmer, R. (2017) Drivers and Barriers for OOP (1st version). Deliverable D2.7 of the TOOP project. Available at: http://toop.eu/sites/default/files/D27_Drivers_and_Barriers.pdf.

Other references

- Board of Innovation. 2018. “The Broker.” 2018. <https://www.boardofinnovation.com/business-revenue-model-examples/the-broker/>.
- Chen, Lianping, Muhammad Ali Babar, and Bashar Nuseibeh. 2013. “Characterizing Architecturally Significant Requirements.” *IEEE Software* 30 (2):38–45.
- Chou, By Carol C H, By Carol C H Chou, Florida Digital Archive, Florida Digital Archive, Andrea Goethals, and Andrea Goethals. 2015. “An Introduction to the European Interoperability Reference Architecture v0.9.0 (EIRA),” 65.
- Cleland-Huang, J., O. Gotel, and A. Zisman. 2011. *Software and Systems Traceability*. Springer, London.
- Cleland-Huang, J., R. Settimi, E. Romanova, B. Berenbach, and S. Clark. 2007. “Best Practices for Automated Traceability.” *Computer* 40 (6):27–35.
- Cloutier, Robert, Gerrit Muller, Dinesh Verma, Roshanak Nilchiani, Eirik Hole, and Mary Bone. 2010. “The Concept of Reference Architectures.” *Systems Engineering* 13 (1):14–27. <https://doi.org/10.1002/sys.20129>.
- Cofta, P. 2007. *Trust, Complexity and Control: Confidence in a Convergent World*. Wiley.
- e-SENS. 2015. “E-SENS SAT eDocument.” <http://wiki.ds.unipi.gr/display/ESENS/SAT+-+eDocument+-+0.6.0>.
- . 2016. “eSENS D3.7. Sustainability Plans for E-SENS Building Blocks.” https://www.esens.eu/sites/default/files/e-sens_d3.7.pdf.
- ETSI. 2006. “Technical Specification XML Advanced Electronic Signatures and Infrastructure; ETSI TS 101 903 v1.3.2.” http://uri.etsi.org/01903/v1.3.2/ts_101903v010302p.pdf.
- . 2013. “ETSI TS 102 918 v1.3.1 (2013-06) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC).” http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf.
- European Commission. 2016. “EU eGovernment Action Plan 2016-2020 - Accelerating the Digital Transformation of Government.” Communication from the Commission to the European

- Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2016 (179):1–11. <https://doi.org/10.1017/CBO9781107415324.004>.
- . 2017. “European Interoperability Framework – Implementation Strategy.” Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, no. COM(2017) 134 final:9.
- . 2018a. “Digital Single Market.” 2018. <https://ec.europa.eu/digital-single-market/>.
- . 2018b. “eGovernment & Digital Public Services.” 2018. <https://ec.europa.eu/digital-single-market/en/public-services-egovernment>.
- European Union. 2017. “Proposal for a Regulation of the European Parliament and the Council on Establishing a Single Digital Gateway to Provide Information, Procedures, Assistance and Problem Solving Services and Amending Regulation (EU) No 1024/2012, COM/2017/0256 Final - 2017.” 2017. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017%0APC0256>.
- Gaurav, R., M. Sarfaraz, and D. Singh. 2014. “Survey on Trust Establishment in Cloud Computing.” In The Next Generation Information Technology Summit (Confluence), 5th International Conference. Noida, India. IEEE.
- Greefhorst, Danny, and Erik Proper. 2011. Architecture Principles The Cornerstones of Enterprise Architecture. Architecture Principles The Cornerstones of Enterprise Architecture. Vol. 6. <https://doi.org/10.1007/978-3-642-20279-7>.
- GS1. 2012. “Standard Business Document Header (SBDH) Specification.” <https://www.gs1.org/standard-business-document-header-sbdh>.
- Harris, Steve, and Andy Seaborne. 2013. “SPARQL 1.1 Query Language.”
- Ian Sommerville. 2010. “Software Engineering (Ninth Edition).” In Software Engineering (Ninth Edition), 147–75.
- ISA. 2014. “Guidelines for Public Administrations on E-Document Engineering Methods.” <https://ec.europa.eu/isa2/sites/isa/files/miscellaneous/guidelines-for-public-administrations-on-e-document-engineering-methods-en.pdf>.
- ISA specification. 2012. “ISA Interoperability Solution for European Public Administration. ‘Core Vocabularies Specification: Core Business Vocabulary, Core Person Vocabulary, Core Location Vocabulary’ . ISA Specification.”
- . 2013. “ISA Interoperability Solution for European Public Administration. “Core Public Service Vocabulary Specification“. ISA Specification.”
- . 2016. “ISA Interoperability Solution for European Public Administration. ‘Core Public Organisation Vocabulary v1.0.0’. ISA Specification.”
- . 2017. “ISA Interoperability Solution for European Public Administration. ‘Core Public Service Vocabulary Application Profile 2.1’. ISA Specification.”
- ISA Specification. 2016. “ISA Interoperability Solution for European Public Administration. ‘Core Criterion and Core Evidence Vocabulary v1.0.0’. ISA Specification.”
- Koehn, Philipp. 2010. “MOSES, Statistical Machine Translation System, User Manual and Code Guide.” Technical Report, 245. <http://www.statmt.org/moses/manual/manual.pdf>.
- Koehn, Philipp, Hieu Hoang, Alexandra Birch, Chris Callison-Burch, Marcello Federico, Nicola Bertoldi, Brooke Cowan, et al. 2007. “Open Source Toolkit for Statistical Machine Translation.” In Proceedings of the 45th Annual Meeting of the Association for Computational Linguistics (ACL), 177–80. <https://doi.org/10.3115/1557769.1557821>.

- Krimmer, Robert, Tarmo Kalvet, Maarja Toots, and Aleksandrs Cepilovs. 2017. "The Once-Only Principle Project Position Paper on Definition of OOP and Situation in Europe."
- Mason, S. 2012. *Electronic Signatures in Law*. Cambridge: Cambridge University Press.
- Peffers, Ken, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. 2007. "A Design Science Research Methodology for Information Systems Research." *Source Journal of Management Information Systems* 24 (3):45–77. <https://doi.org/10.2753/MIS0742-1222240302>.
- Proper, Henderik A., and Marc M. Lankhorst. 2014. "Enterprise Architecture. Towards Essential Sensemaking." *Enterprise Modelling and Information Systems Architectures* 9 (1):5–21. <https://doi.org/10.1007/s40786-014-0002-7>.
- Publications Office of the European Union. 2017. "New European Interoperability Framework. Promoting Seamless Services and Data Flows for European Public Administrations" 2017:48. <https://doi.org/10.2799/78681>.
- Zachman, John A. 2008. "The Concise Definition of The Zachman Framework." Zachman International, Inc. 2008. <https://www.zachman.com/about-the-zachman-framework>.
- Zhou, J. 2001. *Non-Repudiation in Electronic Commerce*. Artech House.
- The Open Group. 2011. "TOGAF®, an Open Group Standard." Open Group Standard. 2011.
- Winslett, M. 2003. "An Introduction to Trust Negotiation." In *Lecture Notes in Computer Science*, Vol 2692. Berlin, Heidelberg: Springer.

Annex I – Legal Framework Requirements Analysis

Project's Legal Assessment Framework

D2.5 identifies and analyses the legal source documents relevant in the legal assessment of the TOOP project. The analysis is summarized as a set of principles.

These legal principles are assessed from the perspective of the architect, and the architecture impacts are identified - as summarized in the below table 9.

Table 9: Legal assessment framework

Legal Principle	Description	REQ-ID	Requirement	Architecture Impact
Good administration	The OOP must be implemented in a way that ensures that affairs are handled impartially, fairly and within a reasonable time.	LEG-GA-01	The OOP must be implemented in a way that ensures non-discrimination: evidence must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving competent authority on the basis of the evidence.	
		LEG-GA-02	The OOP must be implemented in a way that ensures transparency: the evidence to be transferred, the modalities of the transfer (specifically the duration of the accessibility of the evidence and the purposes of the exchange) and the categories of competent authorities involved must be clearly known to the persons concerned prior to the transfer.	
		LEG-GA-03	If no evidence can be transferred, the competent authority must give reasons for this	Auditability
		LEG-GA-04	After the exchange, the receiving competent authority may only use the evidence for the purpose of the procedure for which the evidence was exchanged. as communicated to the persons benefiting from the	Privacy

Legal Principle	Description	REQ-ID	Requirement	Architecture Impact
			OOP, excluding any use that is incompatible with the original purpose and any transfer to third parties (except where those third parties are required to achieve the communicated purposes)	
		LEG-GA-05	The OOP must be implemented in a way that facilitates comprehension: without prejudice to the autonomy of the receiving competent authority, the person benefiting from the OOP should be able to receive information in relation to the evidence transfer process in his/her language of the Treaties	
Accountability	The OOP must be implemented in a way that ensures that responsibilities are clearly allocated between each participant in the exchange of electronic evidence.	LEG-ACC-01	The OOP must be implemented in a way that ensures that all participants are aware of their obligations, and that the persons relying on the OOP have the right to restitution of any damages caused by noncompliance with these obligations insofar as this is possible under applicable law (i.e. taking into account possible exemptions of liability that may apply to the competent authorities under their national laws).	
Justice	The OOP must be implemented in a way that ensures the right to recourse for the persons relying on the OOP, and that contains appropriate	LEG-JUS-01	The OOP must be implemented in a way that safeguards the right of every person to be heard, before any individual measure which would affect him or her adversely is taken on the basis of evidence exchanged via the OOP	

Legal Principle	Description	REQ-ID	Requirement	Architecture Impact
	enforcement mechanisms.	LEG-JUS-02	The OOP must therefore be implemented in a way that provides appropriate contact mechanisms for persons relying on the OOP towards all competent authorities involved as providers or as recipients of the evidence	
Privacy, data protection and confidentiality	The OOP must be implemented in a way that safeguards the fundamental rights to privacy and data protection for natural persons, and respecting the legitimate interests of confidentiality and of professional and business secrecy.	LEG-PRI-01	<p>The evidence exchanged via the OOP may only be processed in accordance with applicable data protection law when it contains any personal data, notably the DPD, or as of 25 May 2018, the GDPR. This includes the principles of:</p> <p>lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.</p>	<p>Confidentiality of the data exchange</p> <p>Privacy of the data exchange when personal data</p> <p>Security- and Privacy-by-design principles</p>
		LEG-PRI-02	When the evidence exchanged via the OOP does not contain any personal data, the competent authorities must still ensure that appropriate measures are taken to ensure an appropriate level of confidentiality of the evidence exchanged. When there is a legitimate confidentiality concern, the same principles as under data protection law can be applied	
Equality and solidarity	The OOP must be implemented in a way that protects the persons	LEG-EQ-01	The OOP must be implemented in a way that ensures non-discrimination: evidence must be transferred	Usability and Accessibility

Legal Principle	Description	REQ-ID	Requirement	Architecture Impact
	concerned against discrimination.		on a neutral basis, without prejudicing any decisions that would be made by the receiving competent authority on the basis of the evidence	
		LEG-EQ-02	The OOP must be implemented in a way that ensures universal accessibility, including to persons with disabilities. Accessible support and communication mechanisms must be provided to ensure that such persons can receive comparable functionality as those persons benefiting from the OOP	
Lawfulness and compliance	The OOP must be implemented in a way that ensures that evidence is only transferred if there is an adequate legal basis for this, and in compliance with any applicable legal requirements.	LEG-LAW-01	Evidence may only be transferred under the OOP between competent authorities if there is a legal basis for this, either the consent of the persons concerned or a separate legal basis such as a legal obligation	Consent Management Rules on what to exchange ?
		LEG-LAW-02	Evidence may only be transferred under the OOP between competent authorities if it has been determined that any pre-existing legal requirements (including sector or context specific legal requirements) are satisfied, including national authorisation procedures, legal agreements on usage restrictions, assurances with respect to security, assurances or exclusions of liability, data or service quality arrangements, etc. During the course of the TOOP project, this will	

Legal Principle	Description	REQ-ID	Requirement	Architecture Impact
			require a case by case assessment; after the entry into force of the SDGR this will likely be facilitated	
Control	The implementation of the evidence exchange mechanism must contain appropriate controls to ensure that the evidence is relevant and to allow incidents to be detected and addressed.	LEG-CTRL-01	Prior to initiating any evidence exchange, the competent authorities participating in the exchange must verify the link between the identity of the person benefiting from the OOP and the corresponding evidence	Identification and authentication Dispute resolution support (end-to-end non-repudiation)
		LEG-CTRL-02	Appropriate audit and logging measures must be implemented to ensure that any exchange of evidence organised under the OOP can be verified by competent authorities in case of disputes (including the identification of the sending and receiving competent authorities, the time of the exchange, and the integrity/authenticity of the exchanged data itself)	
Value, validity and evidence	The legal value and validity of any evidence exchanged under the OOP must be clear to all competent authorities participating in the exchange.	LEG-VAL-01	There must be an understanding between the competent authorities on the legal value and validity of the evidence, including specifically whether the providing authority considers it to be authoritative (originating from and identical to information from an authoritative source or base register, i.e. any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity), or whether it can otherwise be assumed to be genuine. Ultimately, the receiving	Legal value management

Legal Principle	Description	REQ-ID	Requirement	Architecture Impact
			authority will decide whether the evidence is valid and appropriate for its purposes; but at a minimum the receiving authority must know the status of the information in the issuing authority's Member State	
Security	The OOP must be implemented in a way that protects the exchanged evidence against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the evidence, thereby ensuring its integrity and authenticity.	LEG-SEC-01	<p>The competent authorities and any other participants in the evidence exchange mechanism must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:</p> <p>the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing</p>	<p>Integrity and authenticity of the information exchange</p> <p>Availability of the exchange service</p> <p>System monitoring</p> <p>Incident management</p>
		LEG-SEC-02	Incident response measures must be implemented to ensure that the exchange of compromised evidence is avoided and notified to recipients. Requirements	

Legal Principle	Description	REQ-ID	Requirement	Architecture Impact
			under data protection law must at any rate be adhered to	
Quality of data	The OOP must be implemented in a way that provides a clear shared understanding between all competent authorities on the quality of the exchanged evidence.	LEG-QUAL-01	A legal framework must exist that clarifies the obligations of the competent authorities in relation to the quality of the data, including any assurances of its accuracy, factual correctness, and timeliness of updates (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear)	User feedback on accuracy of information
		LEG-QUAL-02	A feedback mechanism must be in place that allows the persons involved to contact the competent authority at the source of the evidence to correct any inaccuracies	
Quality of service	The OOP must be implemented in a way that provides a clear shared understanding between all competent authorities on the quality of the services for the exchange of evidence.	LEG-SLA-01	A legal framework must exist that clarifies the obligations of the competent authorities in relation to the availability and responsiveness of the services (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear)	System monitoring SLA management
		LEG-SLA-02	An evaluation mechanism must be in place that allows noncompliance with this framework to be detected and addressed when necessary	

Legal Principle	Description	REQ-ID	Requirement	Architecture Impact
Interoperability	The OOP must be implemented in a way that ensures semantic and technical interoperability of the evidence exchanged under the OOP.	LEG-IOP-01	Appropriate agreements must be in place with respect to the technical and semantic characteristics of the evidence to be exchanged between competent authorities, taking into account linguistic challenges and diversity of legal systems. Evidence should not be exchanged under the OOP if interoperability is not ensured	

Single Digital Gateway Regulation

The Single Digital Gateway Regulation - [SDGR](#) - proposition was analysed in details, as it will become the legal framework underpinning the cross-border once only principle. Articles 10, 11 and 12 are the most relevant for TOOP as an instance of the SDG.

Table 10: SDGR impact on TOOP architecture

ID	Rule	Architecture Impact
SDGR-Art.10	Deadlines associated with the procedure are respected	
SDGR-Art.11.1.a	users are able to access and receive instructions for completing the procedure in at least one official language of the Union other than the national language or, where applicable, the national languages	web site support multiple European languages
SDGR-Art.11.1.c	users are able to identify themselves, sign and authenticate documents using electronic identification and authentication means, as provided for under Regulation (EU) 910/2014 of the European Parliament and of the Council, where identification and signature are required	Integration with eIDAS infrastructure
SDGR-Art.11.1.d	users are able to provide evidence of compliance with applicable requirements in electronic format	Electronic exchange of evidence
SDGR-Art.11.1.e	where the completion of a procedure requires a payment, users are able to pay any fees online through cross-border payment services, including, at a minimum, credit transfers or direct debits as specified in Regulation (EU) No 260/2012 of the European Parliament and of the Council 40	Integration of cross-border payment service
SDGR-Art.11.3	Competent authorities shall cooperate through the Internal Market Information system (IMI), established by Regulation	Integration with IMI

ID	Rule	Architecture Impact
	(EU) No 1024/2012 of the European Parliament and of the Council, where necessary to verify the authenticity of evidence submitted to them in electronic format by the user for the purpose of an online procedure.	
SDGR-Art.12.1	For the purpose of the exchange of evidence for the online procedures referred in paragraph 0, a technical system for the automated electronic exchange of evidence between different MS ("the technical system") shall be established by the EC in cooperation with the MSs	Online procedure Operated by EC ?
SDGR-Art.12.2	<p>The technical system shall in particular:</p> <ul style="list-style-type: none"> ▪ enable the processing of requests for evidence to be accessed or exchanged ▪ allow the transmission of evidence between actors requesting and issuing it ▪ allow the processing of the evidence by the requesting competent authority ▪ ensure the confidentiality and integrity of the evidence ▪ enable the possibility for the user to preview the evidence to be used by the requesting authority ▪ ensure an adequate level of interoperability with other relevant systems ▪ ensure a high-level of security for the transmission and processing of evidence 	<p>Evidence Exchange capability</p> <p>Security</p> <p>IOP (technical and semantics)</p> <p>Preview capability at requesting side</p>
SDGR-Art.12.4	The competent authorities responsible for online procedures referred to in paragraph 1 shall, upon an explicit request of the user, request evidence directly from competent authorities issuing evidence in other MS through the technical system. The issuing competent authorities shall, in accordance with point d of paragraph 2 (confidentiality and integrity) make such evidence available through the same system	<p>Non Repudiation of user request</p> <p>CI for evidence transmission</p>
SDGR-Art.12.6	The evidence made available to the requesting competent authority shall be limited to what has been requested and shall only be used for the purpose of the procedure for which the evidence was exchanged. When the consent of the user is necessary for data protection purposes, it shall be obtained in accordance with Regulation (EU) 2016/679 and Regulation (EU) 45/2001	<p>Data minimization principle</p> <p>Purpose limitation principle</p> <p>Consent management</p>
SDGR-Art.12.4a	The explicit request of the user does not have to be applied to procedure where the automated cross-border data exchange	

ID	Rule	Architecture Impact
	without such an explicit request is allowed under applicable EU or national law	

Annex II – EIF Requirements Analysis

The 12 principles of EIF are detailed into a list of 47 recommendations. The relevance of each recommendation was analysed and the impacts on TOOP architecture were assessed. The table below summarizes the outcome of this activity.

In the last column of the table, the architecture impact of a recommendation may be characterized as an Architecturally Significant Requirement (ASR), as an architecture principle, or as having no significant architecture impact. In case a recommendation may be characterized both as an ASR or a principle, it is given as ASR.

The ASRs are further elaborated in the section of architecture requirements. The architecture principles are detailed in the architecture principles section. In case a recommendation does not have significant impact on TOOP architecture, the corresponding shell in the Architecture Impact column may be left blank, or it may include a justification for this choice.

Table 11: EIF requirements analysis

ID	EIF Principle	EIF Recommendation	Architecture Impact
EIF-01	Subsidiarity and Proportionality	Ensure that national interoperability frameworks and interoperability strategies are aligned with the EIF and, if needed, tailor and extend them to address the national context and needs.	
EIF-02	Openness	Publish the data you own as open data unless certain restrictions apply.	
EIF-03		Ensure a level playing field for open source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution	
EIF-04		Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support and innovation.	Principle. Open specifications/ standards
EIF-05	Transparency	Ensure internal visibility and provide external interfaces for European public services.	ASR. External interfaces for European public services must be provided
EIF-06	Reusability	Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.	Principle. Reusable solutions
EIF-07		Reuse and share information and data when implementing European public services, unless certain privacy or confidentiality restrictions apply.	Principle. Reusable data

ID	EIF Principle	EIF Recommendation	Architecture Impact
EIF-08	Technological Neutrality and Data Portability	Do not impose any technological solutions on citizens, businesses and other administrations that are technology-specific or disproportionate to their real needs.	Principle. Technological neutrality.
EIF-09		Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible.	Principle. Data portability
EIF-10	User Centricity	Use multiple channels to provide the European public service, to ensure that users can select the channel that best suits their needs.	
EIF-11		Provide a single point of contact in order to hide internal administrative complexity and facilitate users' access to European public services.	
EIF-12		Put in place mechanisms to involve users in analysis, design, assessment and further development of European public services.	
EIF-13		As far as possible under the legislation in force, ask users of European public services once-only and relevant-only information.	Principle. Once Only Principle
EIF-14	Inclusion and Accessibility	Ensure that all European public services are accessible to all citizens, including persons with disabilities, the elderly and other disadvantaged groups. For digital public services, public administrations should comply with e-accessibility specifications that are widely recognised at European or international level.	Inclusion and accessibility mechanisms are provided on an individual Member State level.
EIF-15	Security and Privacy	Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.	ASR. Security and privacy requirement.

ID	EIF Principle	EIF Recommendation	Architecture Impact
EIF-16	Multilingualism	Use information systems and technical architectures that cater for multilingualism when establishing a European public service. Decide on the level of multilingualism support based on the needs of the expected users.	ASR. Multilingualism support may require mechanisms designed on TOOP architecture level.
EIF-17	Administrative Simplification	Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens.	
EIF-18	Preservation of Information	Formulate a long-term preservation policy for information related to European public services and especially for information that is exchanged across borders.	Information preservation policies should be provided by Data Owners and Data Governors.
EIF-19	Assessment of Effectiveness and Efficiency	Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality and balance between costs and benefits.	ASR. Effectiveness and efficiency requirements should be evaluated and established, balanced by considering of costs and benefits.
EIF-20	Interoperability Governance	Ensure holistic governance of interoperability activities across administrative levels and sectors.	
EIF-21		Put in place processes to select relevant standards and specifications, evaluate them, monitor their implementation, check compliance and test their interoperability.	Principle. Standards and specifications process
EIF-22		Use a structured, transparent, objective and common approach to assessing and selecting standards and specifications. Take into account relevant EU recommendations and seek to make the approach consistent across borders.	Principle. Standards and specifications selection
EIF-23		Consult relevant catalogues of standards, specifications and guidelines at national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.	

ID	EIF Principle	EIF Recommendation	Architecture Impact
EIF-24		Actively participate in standardisation work relevant to your needs to ensure your requirements are met.	
EIF-25	Integrated Public Service Governance	Ensure interoperability and coordination over time when operating and delivering integrated public services by putting in place the necessary governance structure.	
EIF-26		Establish interoperability agreements in all layers, complemented by operational agreements and change management procedures.	Principle. Interoperability agreements
EIF-27	Legal Interoperability	Ensure that legislation is screened by means of 'interoperability checks', to identify any barriers to interoperability. When drafting legislation to establish a European public service, seek to make it consistent with relevant legislation, perform a 'digital check' and consider data protection requirements.	
EIF-28	Organisational Interoperability	Document your business processes using commonly accepted modelling techniques and agree on how these processes should be aligned to deliver a European public service.	
EIF-29		Clarify and formalise your organisational relationships for establishing and operating European public services.	Principle. Organisational relationships
EIF-30	Semantic Interoperability	Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved.	Principle. Data and information as a public asset
EIF-31		Put in place an information management strategy at the highest possible level to avoid fragmentation and duplication. Management of metadata, master data and reference data should be prioritised.	
EIF-32		Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and encourage relevant communities to share their results on national and European platforms.	

ID	EIF Principle	EIF Recommendation	Architecture Impact
EIF-33	Technical Interoperability	Use open specifications, where available, to ensure technical interoperability when establishing European public services.	Principle. Open technical specifications
EIF-34	European Public Service Conceptual Model	Use the conceptual model for European public services to design new services or reengineer existing ones and reuse, whenever possible, existing service and data components.	
EIF-35		Decide on a common scheme for interconnecting loosely coupled service components and put in place and maintain the necessary infrastructure for establishing and maintaining European public services.	Principle. Infrastructure for European public services
EIF-36	Internal Information Sources and Services	Develop a shared infrastructure of reusable services and information sources that can be used by all public administrations.	Principle. Reusable services and information sources
EIF-37	Base Registries	Make authoritative sources of information available to others while implementing access and control mechanisms to ensure security and privacy in accordance with the relevant legislation.	This recommendation is largely targeted towards the Data Owners and Data Governors of Base Registries.
EIF-38		Develop interfaces with base registries and authoritative sources of information, publish the semantic and technical means and documentation needed for others to connect and reuse available information.	This recommendation is largely targeted towards the Data Owners and Data Governors of Base Registries.
EIF-39		Match each base registry with appropriate metadata including the description of its content, service assurance and responsibilities, the type of master data it keeps, conditions of access and the relevant licences, terminology, a glossary, and information about any master data it uses from other base registries.	This recommendation is largely targeted towards the Data Owners and Data Governors of Base Registries.
EIF-40		Create and follow data quality assurance plans for base registries and related master data.	This recommendation is largely targeted towards the Data Owners and Data

ID	EIF Principle	EIF Recommendation	Architecture Impact
			Governors of Base Registries.
EIF-41	Open Data	Establish procedures and processes to integrate the opening of data in your common business processes, working routines, and in the development of new information systems.	This recommendation is targeted towards the Data Owners and Data Governors.
EIF-42		Publish open data in machine-readable, non-proprietary formats. Ensure that open data is accompanied by high quality, machine-readable metadata in nonproprietary formats, including a description of their content, the way data is collected and its level of quality and the licence terms under which it is made available. The use of common vocabularies for expressing metadata is recommended.	This recommendation is targeted towards the Data Owners and Data Governors.
EIF-43		Communicate clearly the right to access and reuse open data. The legal regimes for facilitating access and reuse, such as licences, should be standardised as much as possible.	This recommendation is targeted towards the Data Owners and Data Governors.
EIF-44	Catalogues	Put in place catalogues of public services, public data, and interoperability solutions and use common models for describing them.	ASR. Where feasible, the TOOP architecture should put in place catalogues of public services, public data, and interoperability solutions, and use common models for describing them.
EIF-45	External Information Sources and Services	Where useful and feasible to do so, use external information sources and services while developing European public services.	ASR. The TOOP architecture should allow for using external information sources (for example, open data) and services (for example, payment or connectivity services) while developing European public services, where it is useful and feasible to do so.

ID	EIF Principle	EIF Recommendation	Architecture Impact
EIF-46	Security and Privacy	Consider the specific security and privacy requirements and identify measures for the provision of each public service according to risk management plans.	ASR. The TOOP architecture should allow for considering the specific security and privacy requirements and identifying measures for the provision of each public service according to risk management plans.
EIF-47		Use trust services according to the Regulation on eID and Trust Services as mechanisms that ensure secure and protected data exchange in public services.	ASR. The TOOP architecture should use trust services according to the Regulation on eID and Trust Services as mechanisms that ensure secure and protected data exchange in public services.

Annex III – Archimate goal model notation

Short description of the notations used in Archimate goal models is given in the following tables.

Table 12: Goal model elements description ⁸¹


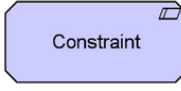


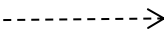

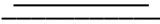
The name of element	Description	Graphical element
Goal	A goal represents a high-level statement of intent, direction, or desired end state for an organization and its stakeholders.	
Constraint	A constraint represents a factor that prevents or obstructs the realization of goals.	
Stakeholder	A stakeholder is the role of an individual, team, or organization (or classes thereof) that represents their interests in the outcome of the architecture.	
Driver	A driver represents an external or internal condition that motivates an organization to define its goals and implement the changes necessary to achieve them.	

Table 13: Goal Model Relationships ⁸²

The name of element	Description	Graphical element
Access Relationship	The access relationship models the ability of behaviour and active structure elements to observe or act upon passive structure elements.	
Specialization Relationship	The specialization relationship indicates that an element is a particular kind of another element.	
Association Relationship	An association relationship models an unspecified relationship. Used in first high-level model where relationships are initially denoted in a generic way.	

⁸¹ <http://pubs.opengroup.org/architecture/archimate3-doc/chap06.html>

⁸² <http://pubs.opengroup.org/architecture/archimate3-doc/chap05.html>

Contributors

Name	Surname	Organisation	Country
Madis	Ehastu	Ministry of Economic Affairs and Communications	Estonia
Giovanni Paolo	Sellitto	National Anticorruption Authority (ANAC)	Italy
Tevriz	Iusupova	University of Koblenz	Germany