The Technical Challenges in OOP Application Across the European Union and the TOOP OOP Architecture

Jaak Tepandi[1], Carmen Rotuna[2], Giovanni Paolo Sellitto[3], Sander Fieten[4], and Andriana Prentza[5](✉)

[1] Information Systems Group, Tallinn University of Technology, Tallinn, Estonia
[2] ICI BUCHAREST, Bucharest, Romania
[3] ANAC, Rome, Italy
[4] Chasquis, Leiden, Netherlands
[5] Department of Digital Systems, University of Piraeus, 18532 Piraeus, Greece
aprentza@unipi.gr

Abstract. The Once-Only Principle requires the public administrations to ensure that citizens and businesses supply the same information only once to the Public Administration as a whole. Widespread use of the Once-Only Principle has the potential to simplify citizens' life, make businesses more efficient, and reduce administrative burden in the European Union. The Once-Only Principle project (TOOP) is an initiative, financed by the EU Program Horizon 2020, to explore the possibility to enable the cross-border application of the Once-Only Principle by demonstrating it in practice, through the development of selected piloting applications for specific real-world use cases, enabling the connection of different registries and architectures in different countries for better exchange of information across public administrations. These piloting ICT systems are designed as a result of a pan-European collaboration and they adopt a federated model, to allow for a high degree of independence between the participating parties in the development of their own solutions. The main challenge in the implementation of an OOP solution is the diversity of organizations, procedures, data, and services on all four main levels of interoperability: legal, organizational, semantic, and technical. To address this challenge, TOOP is developing and testing the TOOP Reference Architecture (TOOPRA) to assist organizations in the cross-border implementation of the OOP. The paper outlines the TOOPRA users, principles, and requirements, presents an overview of the architecture development, describes the main views of TOOPRA, discusses architecture profiling, and analyses the TOOPRA sustainability issues.

Keywords: eGovernment · Interoperability · Reference Architecture

1 Introduction

The Once-Only Principle (OOP) requires the public administrations to ensure that citizens and businesses supply the same information only once to the Public Administration

R. Krimmer et al. (Eds.): The Once-Only Principle, LNCS 12621, pp. 141–163, 2021.
https://doi.org/10.1007/978-3-030-79851-2_8

as a whole. A widespread use of OOP has the potential to simplify citizens' life, make businesses more efficient, and reduce administrative burden in the European Union (EU). The practical application of the OOP requires the set-up of a complex legal, organizational and technical environment to ensure that the information exchanged between public administrations maintains its original validity and meaning even if its expression is changed when used in a different place or context. All these conditions are usually referred to as levels of interoperability between organizations and at the EU level they are clearly explained in the European Interoperability Framework (EIF) [1] and defined in the European Interoperability Reference Architecture (EIRA) [2].

The Once-Only Principle project (TOOP) represents an initiative – financed by the EU Program Horizon 2020 – to explore the possibility to enable the cross-border application of OOP by demonstrating it in practice, through the development of some Information and Communication Technology (ICT) systems to pilot its application to specific real-world use cases, enabling the connection of different registries and architectures in different countries for better exchange of information across public administrations. These piloting ICT systems are designed as a result of a pan-European collaboration and they adopt a federated model, to allow for a high degree of independence between the participating parties in the development of their own solutions.

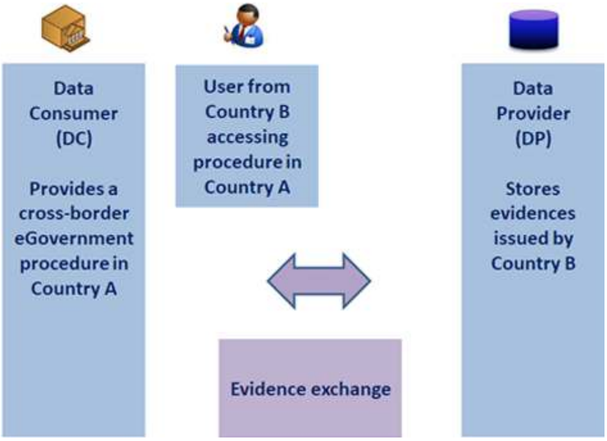
Data Consumer (DC)
Provides a cross-border eGovernment procedure in Country A
User from Country B accessing procedure in Country A
Data Provider (DP)
Stores evidences issued by Country B
Evidence exchange

Fig. 1. A high-level illustration of an OOP exchange.

From a high-level point of view (see Fig. 1), an OOP exchange does not deviate much from the usual interaction between a Data Consumer (DC), where the User accesses a digital public service, and a Data Provider (DP), who acts on behalf of the User. The difference is precisely in the Once Only principle that requires that the Data Provider is the one that from a legal point of view is recognized as trusted, reusable and authoritative source of data for the User (a Base Register, in the European Interoperability Framework terminology).

The main challenge in the implementation of an OOP solution is the diversity of organizations, procedures, data, and services on all four main levels of interoperability: legal, organizational, semantic, and technical [3]. To address this challenge, TOOP is developing and testing the TOOP Reference Architecture (TOOPRA) to assist organizations in the cross-border implementation of the OOP.

An enterprise architecture is typically developed because there are concerns that need to be addressed by the business and Information Technology (IT) systems within an organization. The role of the architect is to address these concerns [4].

A Reference Architecture is a set of standardized Enterprise Architectures that provides a frame of reference for a particular domain, sector, or field of interest [5]. The TOOPRA is driven by the users, architecture principles, and Architecturally Significant Requirements (ASRs). The Architecturally Significant Requirements are "those requirements that have a measurable impact on a software system's architecture" [6]. The architecture is described on four architecture layers (business, data, application, technology), organized in multiple architecture views according to The Open Group Architecture Framework (TOGAF) [7].

One of the main difficulties in designing TOOPRA was related to changing principles and requirements. Therefore, TOOPRA was developed by combining top-down and bottom-up approaches considering also new requirements emerging from the Single Digital Gateway Regulation (SDGR) [8] among others. These issues are presented throughout the paper.

The next section outlines the TOOPRA users, principles, and requirements. An overview of the architecture development is presented in the third section. Main views of TOOPRA are described in the fourth section. The fifth section covers architecture profiling. TOOPRA sustainability issues are analyzed in the sixth section and main conclusions are presented in the last section of the chapter.

2 The TOOPRA Users, Principles, and Requirements

The TOOPRA is intended to provide support in the cross-border implementation of OOP, thus helping to design, assess, communicate, and share digital public services across borders and sectors. The main stakeholders of TOOPRA are those directly involved in the TOOP project, the prospective users of the TOOP Reference Architecture that use it to build OOP services, and finally, the end users of the services that use the OOP services to retrieve their data.

In view of this, the main categories of TOOPRA users are: architects responsible for the design of cross-border solution architectures; business analysts responsible for assessing and studying the impact of changes in the IT systems; developers responsible for design, development and implementation of software solutions for interoperable digital public services (across borders and sectors); as well as portfolio managers responsible for maintaining the catalogue of assets related to the design and implementation of eGovernment solutions and for making investment decisions on these assets.

The architecture principles are the underlying general rules and guidelines for the use and deployment of IT resources and assets. The principles underlying TOOPRA include the following, among others:

- Give preference to open specifications and standards.
- Develop TOOP architecture as a reusable solution, reuse Building Blocks (BB) when possible.
- Integrate the requirements for and contribute through the TOOP Solution Architecture to the development of the High-level Reference Architecture for SDGR [8].
- Put in place processes to select relevant standards and specifications, evaluate them, monitor their implementation, check their compliance, and test their interoperability.
- Establish interoperability agreements in all layers.
- Clarify and formalize organizational relationships between the participants in the Once-Only processes.
- Decide on a common scheme for interconnecting loosely coupled service components and design the necessary infrastructure for establishing and maintaining European public services.
- Design a shared infrastructure of reusable services and information sources that can be used by all public administrations.
- The TOOP architecture should use trust services according to the eIDAS Regulation [9] that ensure secure and protected data exchange in public services.
- The information exchanged between the participants of the system should be limited to the data required to complete the process for which the information is requested.
- The information exchanged between the participants of the system should only be used for the explicitly agreed purpose.
- When the consent of the user is necessary for data protection purposes, it shall be obtained in accordance with Regulation (EU) 2016/679 [10] and Regulation (EU) 45/2001 [11].
- 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.

A typical information system has many requirements. Some of these - for example, those related to efficiency or reliability - influence the system architecture, but many requirements, for example, related to specific reports, do not. For TOOPRA, over forty ASRs that have an essential impact on the architecture were highlighted. The requirements were structured according to the standard Software/System Product Quality Model (ISO/IEC 25010) and Data Quality Model (ISO/IEC 25012). Some examples follow:

- DC must be informed about the conditions and terms of use of the retrieved information (Functional Suitability).
- DP should communicate the expected level of service associated with the processing of the request for data from the DC (Performance Efficiency).
- DP must be able to automatically process requests for evidence from DC (Interoperability).
- The transmission of an evidence from DP to DC must guarantee the confidentiality of the exchanged evidence (Security).
- The level of availability of the exchange process must comply with the legal requirements (Reliability).

- 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 (Usability).
- The legal value and meaning of data should not be altered crossing a national border (Data Accuracy).
- The User has the possibility to preview the evidence to be used by the DC and to check the validity of the retrieved information (Data Consistency).
- The User may be able to add information not provided by the DP(s) (Data Completeness).
- The authenticity of the data transmitted by DP must be trusted by DC (Data Credibility).

3 Development of the Architecture

The architecture follows the TOGAF Architecture Development Method (ADM) cycle in a continuous development process integrating new requirements emerging from pilots, stakeholders, and EU regulations. The first version of the architecture addressed mainly the initial pilot requirements and the regulations in force at that point in time. Along the development process, the architecture incorporated the requirements derived from SDGR [8] and the new pilot requirements resulting from the extension of business use cases.

The architecture requirements comprise requirements from several areas: pilot requirements, General Data Protection Regulation (GDPR) [10], EIF, legal requirements, as well as the SDGR and the Guidelines for the implementation of the SDGR [12]. The SDGR is the main driver for OOP implementation at the EU level as it provides the legal context to achieve the desired goals. This Regulation has the objective of reducing administrative burden on citizens and businesses, in compliance with national legislation and procedures while ensuring the functioning of the internal market. SDGR states that it is mandatory for Member States (MS) to provide 21 digitized administrative procedures in an interoperable and secure way.

The TOOP architecture requirements include Article 14 of SDGR which, among others, states that the technical system for the cross-border automated exchange of evidence and application of the OOP should enable the processing of requests for evidence at the explicit request of the user, the transmission of the evidence between competent authorities and the possibility for the user to preview the evidence to be used by the requesting competent authority. Also, it states that the evidence made available to the requesting competent authority shall be limited to what has been requested and shall only be used by that authority for the purpose of the procedure for which the evidence was exchanged.

The TOOP Architecture team cooperates and seeks to align its work with other relevant EC Initiatives, especially within the ISA^2 program [13].

4 The TOOPRA Views

The TOOP Architecture embodies in its components the principles and requirements guiding its design and evolution. The overall architecture description contains a collection of artifacts that document the TOOP architecture. The architecture views are the key artifacts in the architecture description.

As an Architecture Description Language (ADL), ArchiMate® [4], has been used starting from the very first version of the architecture. The goal was to describe the layers of an enterprise (business, information systems, technology). Also, the architecture was developed taking into consideration interoperability concerns and is compatible with EIRA [2].

4.1 Introduction

The architecture is described along the business, information system and technology dimensions.

The Business Architecture is a representation of business concerns through capabilities, end-to-end value delivery, information, and organizational structure, and the relationships among these business elements.

The Information System (IS) Architecture describes how the Business Architecture is realized by the Information Systems. The IS architecture includes the data and application architecture and describes (1) the structure of an organization's logical and physical data assets and data management resources, and (2) the individual application systems to be deployed, their interactions, and their relationships to the core business processes of the organization.

The Technology Architecture describes the logical components and services that are required to support the deployment of business capabilities and deployment components described in the IS Architecture. This includes IT infrastructure, middleware, networks, communications, processing, standards, etc.

Specific views addressing cross-cutting quality concerns, such as Security Architecture and Trust Architecture, and Management aspects complement the TOOPRA.

4.2 Business Architecture

The Business Architecture is a description of the structure and interaction between the business strategy, organization, functions, business processes, and information needs [7].

The TOOPRA Business Architecture is presented via the operational processes (process model, capabilities views (capability map), and business interactions.

The Process Model is useful to get a basic overview of the TOOP Business Architecture. It gives an overall upper-level view of the TOOPRA Business Architecture processes. There are two kinds of processes: operational and managerial. The operational processes specify end-to-end processes of executing Once Only Principle. The management processes are responsible for management of the resources required in the operational processes.

The Capability Map diagrams are useful to understand required capabilities and responsibilities of each actor participating in the cross-border Evidence exchange.

The Business Interaction diagrams enable identifying and understanding the major organisational interoperability issues connected with the TOOP Business Architecture. The diagrams in this group specify the collaboration between the actors involved in cross-border Evidence exchange.

The goal of the OOP activities is to retrieve already existing information which is needed for completion of the existing process. The exchanged information is therefore, in alignment with the definition used in the SDGR [8], labelled "evidence" as it is used to fulfill requirements of the current process.

The operational processes specify the end-to-end processes of executing the OOP as part of the delivery of a public eService. It must be noted that the once-only process of retrieving an evidence from another competent authority as shown in the diagram is only a small part of the complete business process that is executed to meet the requirements of the public service that is being provided to the user.

The main actors involved in the cross-border evidence exchange business process are the following:

- User: the entity, which can be either a natural or legal person, that initiates the execution of a procedure.
- Evidence Subject: the entity, whose data is needed to complete the procedure initiated by the User. The Evidence Subject may be a legal entity or a natural person. This is often the same entity as the User, but it can also be an entity related to the User, for example the legal representative of a company which needs to prove a clean criminal record in a procurement procedure. In case the Evidence Subject is a natural person, they may be referred to as a Data Subject and their consent may be necessary for data protection purposes in accordance with GDPR [10] and Regulation (EU) 45/2001 [11].
- Data Consumer (DC): the public organization that executes a procedure for a specific User and which needs to obtain data on one or more Evidence Subjects for the proper execution of the procedure. This data can be provided directly by the User or retrieved from another organization to which the required data has already been provided.
- Data Provider (DP): a public (e.g., Base Registry) or a private organization (e.g., Aggregator, Maritime Recognized Organization) able to provide data about an Evidence Subject, upon request from a DC.

Due to being a reference architecture, TOOPRA is generic in design and therefore does not describe an actual business process but shows what activities are required to integrate the once-only principle in a broader business process.

The process starts from a procedure, offered through a Public Service by a Competent Authority (DC) located in MS A, which has some requirements to be fulfilled by the User who triggers this procedure. The fulfillment of requirements needs to be supported by evidence, which are to be provided by a DP in MS B, to which the User has earlier provided the required information. Per request of the User, the Competent Authority can retrieve the evidence from the DP and as such acts in the role of DC.

As part of the normal business process of executing the procedure, the DC authenticates the user, identifies the required evidence (including identification of the Evidence Subject), asks for confirmation to retrieve the evidence, finds and retrieves evidence from the DP and continues the main process with the retrieved evidence. The DP checks legitimacy of the evidence request, extracts the data for the Evidence Subject, and issues the evidence.

Figure 2 presents an upper level view of the TOOPRA Business Architecture operational processes. For readability, the diagram omits administration processes like data set registration. At this highest level, the specifics of implementation are hidden.

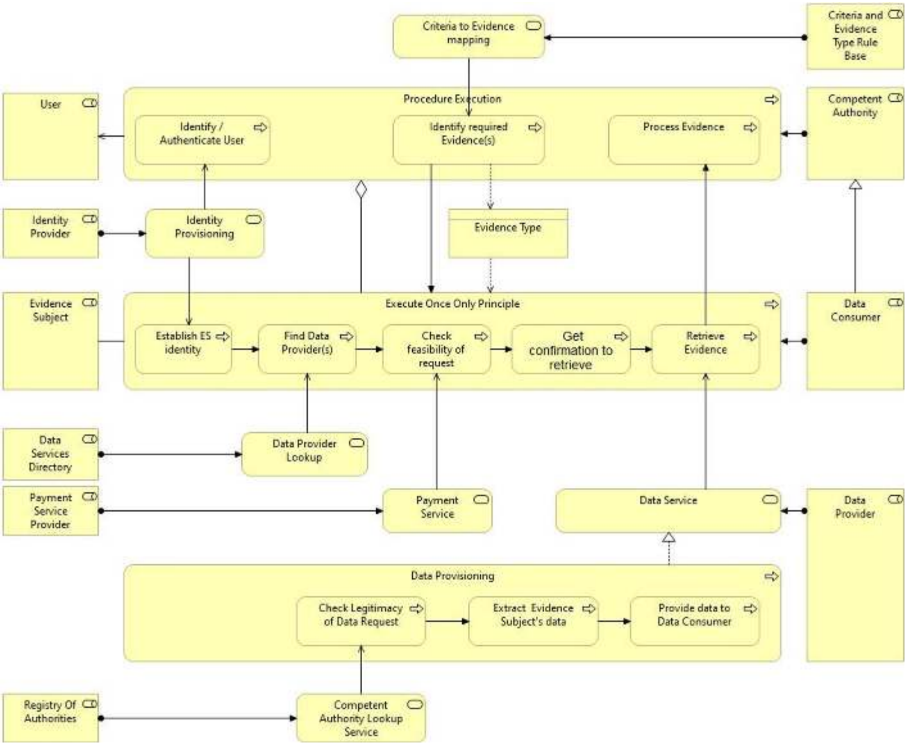

Fig. 2. Upper-level view of the TOOPRA Business Architecture operational processes.

Depending on the requirements of the actual business processes in a domain, several variations can exist in the way the individual process steps are executed.

For example, the DP that can supply the required evidence may be pre-defined in a domain. Also, the actual evidence exchange may vary and can be a two-step process where the DP first provides meta-data on the available Evidence and the actual Evidence is retrieved later in a second step. The retrieval of the actual Evidence data can even be done by another Competent Authority than the one making the original request.

As shown above, several shared services need to be available for the operational processes to function. It is evident that these shared services need to be managed as well, therefore in the model roles have been assigned to these services.

How these services are managed, and as such how these roles will be implemented, will however depend on the domain and the governance agreements made within that domain or even across domains. The definition of these processes is left to the domains. From an architectural point of view, the shared services in the TOOPRA require an underlying governance process, but the choice of the model for these processes is left to the domains and, consequently, they are not presented here.

In the second view component of the Business Architecture, TOOPRA uses the concept of capability – the ability to execute a specified course of action. The business capabilities are identified from the business processes and logically grouped by resources required in their deployment. They are mapped to the Information System level functions. This view of the business architecture is compliant with EIRA ArchiMate representation of the Organizational View Concepts in the Business Architecture.

A capability map identifies business capabilities from the business processes and groups them logically by resources required in their deployment. This architecture view specifies each business role's responsibilities when participating in a TOOP Network. It generically should be interpreted in the following way: to participate in a TOOP Network in a certain Business Role, the organization must have the capability to execute the assigned business functions. The Capability Map enables the participants in a TOOP Network to efficiently and easily identify the required business capabilities associated with the role they will play. It is also a valuable tool for architects and designers to support gap analysis when transitioning to a TOOP environment.

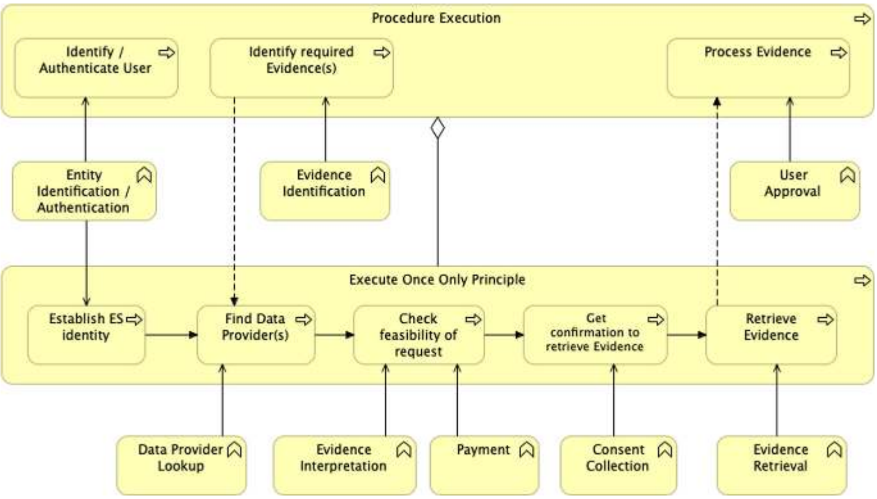

Fig. 3. Archimate model of the capability mapping for the DC process.

In the capabilities view of the Business Architecture, the processes are mapped to functions which the actors need to be able to perform to be capable of executing the processes. In TOOPRA development, only those capabilities are included that would be implemented as functions. In addition, the requirements from TOOPRA on an actor acting in a certain role are on a more detailed level than strategy. So to avoid duplication, capabilities are presented using the function notation.

Figure 3 shows this capability mapping for the processes executed by the DC, described at a generic level of abstraction, to support the goal of developing a generic reference architecture. The various business capabilities introduced are leveraged to support the deployment of the business processes.

The following Table 1 shows the DC capabilities and describes the purpose, outcomes, and required interaction.

Figure 4 shows how the DP capabilities are deployed in the evidence provisioning business process.

The following Table 2 shows the DC capabilities and describes the purpose, outcomes, and required interaction.

The third view component of the Business Architecture is focusing on the interactions between the actors involved in the OOP process. The models in this view show how the different functions of the actors work together, and which data is exchanged between them to enable the execution of the OOP process. It is in these interactions where the actors need to agree on common semantics and specifications to ensure interoperability.

A Business Interactions diagram enables architects and designers to identify efficiently and easily the major organisational interoperability points, as each Exchange of Business Information must be addressed from an interoperability perspective.

Figure 5 represents the most significant exchanges of business information between the main roles participating in an OOP system. It generically should be interpreted in the following way: as part of a Business Capability deployed by a Business Role, an Exchange of Business Information takes place with another Business Role. This view of the business architecture is compliant with EIRA.

Figure 6 presents the model of the interaction between DP and the Data Services Directory to update the DP's service offering.

The actor in charge of Data Services Directory role operates a business service to provide functionality to competent authorities to update their meta-data on the service offered by the authority. The business service is used by the service offering exchange so DPs can manage their dataset meta-data.

4.3 Information System (iS) Architecture

The IS Architecture is a description of the realization of the Business Architecture with IT components, taking into account the ASRs (top-down approach), reuse of Digital Service Infrastructure (DSI) BBs [14], and the TOOP Solution Architecture implemented for the TOOP pilots (bottom-up approach). The IS Architecture can therefore be seen as composed of 2 layers: i) reusable generic BBs, and ii) a TOOP specific layer, leveraging the generic building blocks to realize the TOOP functionalities.

The focal points in the IS architecture description are the following:

Table 1. DC capabilities, purpose, outcomes and required interaction.

Capability	Purpose	Outcomes	Required interaction
Entity identification/Authentication	Establishes the identity of the user and the evidence subject	The identity is known	Identity exchange
Evidence identification	Identifies the required evidence according to the criterion and the special context of the evidence subject	Evidence type corresponding to the criterion is identified	Evidence identification data exchange
Data provider lookup	Find a provider for an evidence related to a legal entity	Data providers identity is established	Data provider information exchange
Evidence interpretation	Links evidence to its business context	Information contained in the evidence is established	Evidence exchange
Payment	Payment for retrieving the evidence when required	Payment is negotiated, if needed	Evidence request exchange
Consent collection	Collects the consent of the user to retrieve the required Evidence	User consent is collected	Evidence request exchange
User approval	Manage the approval of the user to reuse the retrieved Evidence	User approval is collected	Evidence request exchange
Evidence retrieval	Request evidence from a (set of) data provider(s)	Evidence is retrieved	Evidence exchange

- Mapping of the business roles capabilities onto the operational capabilities utilised to operate the Once Only Evidence Processing and identifying the TOOP specific components, candidates for TOOP Building Blocks.
- Interoperability in the exchange of information.
- Reuse of Digital Service Infrastructure (DSI) Building Blocks (BB) to realize the application functions.

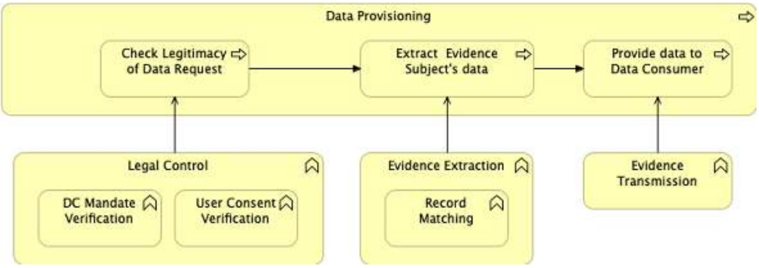
Data Provisioning
Check Legitimacy of Data Request
Extract Evidence Subject's data
Provide data to Data Consumer
Legal Control
DC Mandate Verification
User Consent Verification
Evidence Extraction
Record Matching
Evidence Transmission

Fig. 4. Archimate model of the capability mapping for the DP process

Table 2. DP capabilities, purpose, outcomes and required interaction.

Capability	Purpose	Outcomes	Required interaction
Legal control	Checking the legitimacy of the evidence request	Evaluation of the legitimacy of the evidence request	Identity exchange, data provider information exchange, evidence request exchange
DC mandate verification	Data provider checks the mandate of the DC to request evidence	DC mandate is verified	Identity exchange, data provider information exchange, evidence request exchange
User consent verification	Checking that the requesting user authorized the access to the evidence	Evidence request is authorized	Identity exchange, data provider information exchange, evidence request exchange
Evidence extraction	Extracting the evidence from the providing competent authority	Evidence is retrieved	Evidence request exchange, evidence exchange
Record matching	Record matching is performed by the data provider based on identification attributes provided by the DC	The evidence subject record is found	Evidence request exchange, evidence exchange
Evidence transmission	Transmit the evidence to the requesting competent authority	Evidence is transmitted	Evidence request exchange, Evidence exchange

The TOOP IS Architecture description addresses these focal points by means of the following components:

- The *operational capabilities of the DC and DP* utilised to operate the Once Only Evidence Processing.

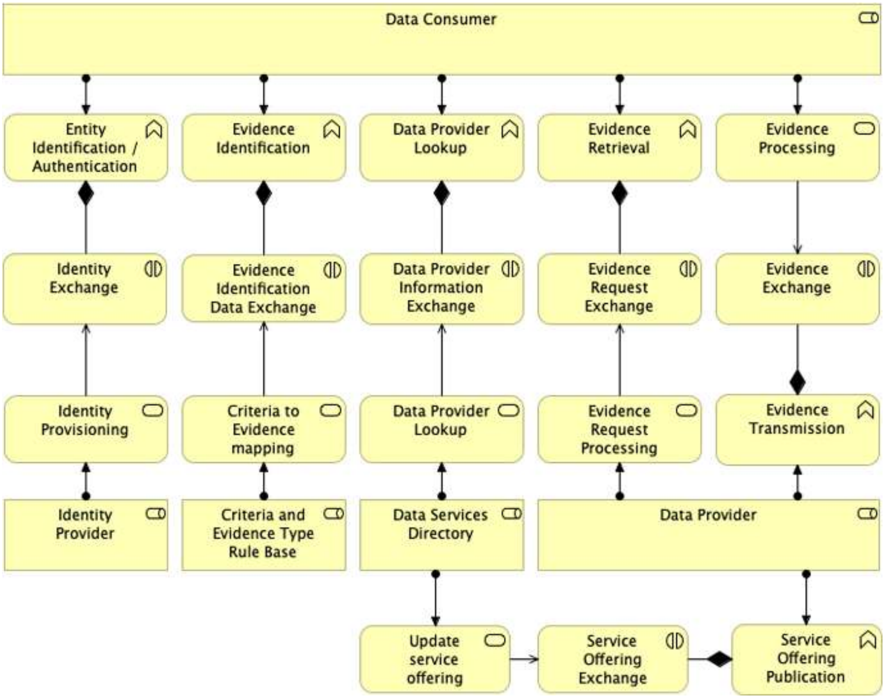
Data Consumer
Entity Identification / Authentication
Evidence Identification
Data Provider Lookup
Evidence Retrieval
Evidence Processing
Identity Exchange
Evidence Identification Data Exchange
Data Provider Information Exchange
Evidence Request Exchange
Evidence Exchange
Identity Provisioning
Criteria to Evidence mapping
Data Provider Lookup
Evidence Request Processing
Evidence Transmission
Identity Provider
Criteria and Evidence Type Rule Base
Data Services Directory
Data Provider
Update service offering
Service Offering Exchange
Service Offering Publication

Fig. 5. Overview of the most significant exchanges of business information between the main roles participating in an OOP system interaction.

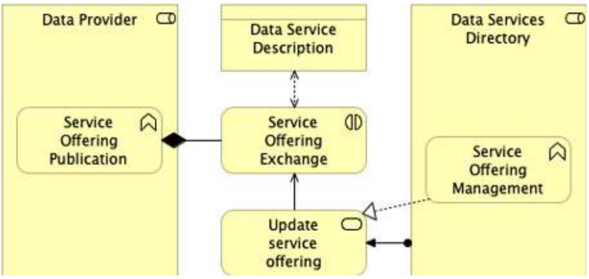

Fig. 6. Model of the interaction between DP and the Data Service Directory to update the DP's service offering.

- The *OOP Interoperability layer*, presenting the generic building blocks to realize the TOOP functionalities.
- The *IS Architecture Interfaces diagram*, depicting the main interactions among architecture building blocks, the way they communicate and the exchanged data.

The operational capabilities are utilised to operate the Once Only Evidence Processing. From an IS perspective, the main target is to generically address the interoperability concerns, i.e., the exchange of business information between participants of TOOP Network. In this section, the most important Business Architecture level capabilities are represented on the IS Architecture level and mapped to the Building Blocks. If a mapping between the Business Architecture and the IS Architecture level for a specific capability is not provided, then this capability is outside the scope of TOOPRA. Figure 7 specifies how the DC operational capabilities are realized and how the existing Building Blocks are leveraged to realize the required functionalities.

The capabilities identified during mapping of capabilities are presented in the OOP Interoperability layer as the generic building blocks that implement TOOP functionalities. For the DC, the following building blocks (shown in Fig. 7) are introduced:

- The *Identification and Authentication* Building Block establishes the identity of the User.
- The *User Consent Management* Building Block handles the consent of the Data Subject.
- The *Evidence Identification* Building Block enables the DC to determine which evidence types are available to the User to prove fulfillment of the requirement.
- The *Semantic Mediation* Building Block establishes semantic interoperability between the services used by the DC and DP.
- The *Data Provider Discovery* Building Block enables to determine the DP that can provide the information to be used as evidence in the procedure executed by the DC.
- The *Routing Metadata Discovery* Building Block provides the details for routing between the services of the participating authorities.
- The *Evidence Exchange* Building Block handles the cross-border exchange of Evidence between the DC and the DP.

In addition to the *Semantic Mediation* Building Block, *Routing Metadata Discovery* Building Block, and *Evidence Exchange* Building Block introduced above, the DP utilises the following building blocks.

- The *Legal Control* Building Block enables checking legitimacy of the data request.
- The *Evidence Extraction* Building Block makes possible to extract data of the Evidence Subject,
- The *Record Matching* Building Block allows to find the relevant record within a data set that applies to the Evidence Subject.

The IS Architecture Interfaces diagram shows the main interactions among architecture building blocks, the way they communicate, and which data is exchanged. The process diagram shows all the steps required in a cross-border Evidence exchange and depicts the entire process from user authentication to Evidence retrieval. There is only one Dynamic Service Location component and it is queried by both DC and DP. The DC discovers the routing metadata by accessing Capability Lookup of the DP and the DP by accessing Capability Lookup of the DC.

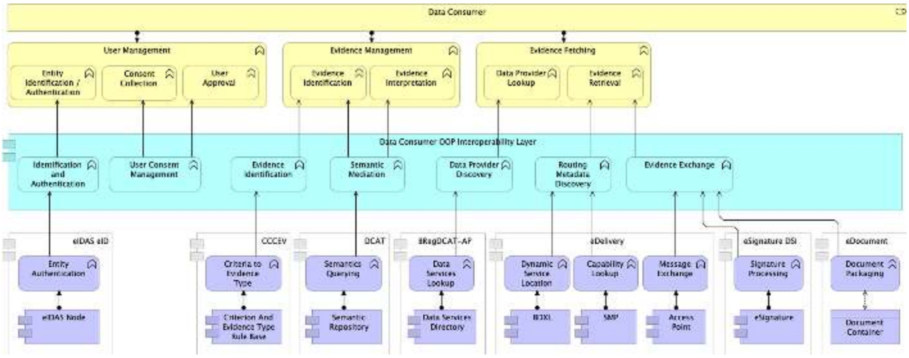

Fig. 7. Information system DC architecture.

Conceptually, the TOOPRA distinguishes between the OOP Core Semantic Model (CSM) (TOOP specific concepts), the core vocabularies (general application related concepts), and Domain Semantic Models (DSM), which are domain specific, e.g., health, public procurement. The OOP CSM describes entities relevant to the application of the OOP. These entities are generic and not affected by the domain where the architecture is applied. The core vocabularies are used in most or all services (e.g., CPSV [15] and CCCEV [16]). The methodology for creating Domain Semantic Models (DSM) is used in the context of OOP in specific domains.

4.4 Technology Architecture

The Technology Architecture provides logical components and services that are required to support the deployment of business capabilities and application components described in the IS Architecture. It comprises both the European infrastructure components and the components within the MS responsibility. The components within the MS responsibility include the components maintained by the MS and by its Competent Authorities. The current Technology Architecture model comprises two views: the *Deployment Topologies* view, and the *Network and Communication* view.

Due to a wide variety of information systems that can be developed using the Technology Architecture, there is no fixed way of how to deploy TOOP services. In the *Deployment Topologies* view we consider three different deployment topologies. Each deployment topology comprises the central European infrastructure components, components deployed on the MS level, and components deployed on a Competent Authority level.

The central European infrastructure components providing the TOOP Network Management are the same in every variation. They comprise the services provided by the Criterion and Evidence Type Rule Base (CERB), the Semantic Repository (SR), the Data Services Directory (DSD), as well as the Business Document Exchange Network Location (BDXL) Server and the DNS Server that are composed to realize the BDXL component.

Components provided on an MS and Competent Authority level can be of three types with respect to the level of their deployment: components deployed only on the

MS level (eIDAS nodes both in the DP and DC MSs), components deployed only on a Competent Authority level (as a minimum, the DP Competent Authority maintains its backend information systems and similar configuration is maintained by the DC Competent Authority), as well as components that can be deployed both on a national or on a Competent Authority level (the Service Metadata Publisher – SMP, Access Point – AP, and the OOP interoperability layer components that support the exchange of Evidence from one participant to another).

The diagram on Fig. 8 shows a variation of how the application components defined in the IS Architecture can be deployed to nodes in the technology architecture. In this variation, the Competent Authority acting as the DC operates its own SMP, AP, TOOP Connector, and backend information system.

Deployment topology depicted on this diagram enforces significant additional workload on the DC Competent Authority, who needs to adjust its business organization, deploy, and maintain all three components: TOOP Connector, SMP, and AP.

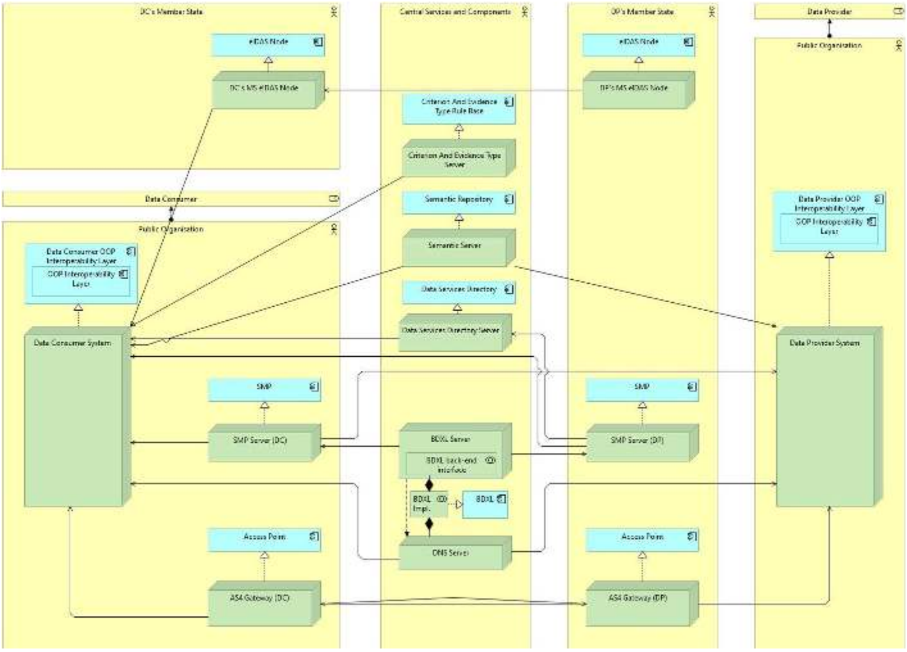

Fig. 8. Deployment of application components defined in the IS Architecture (variation).

On the MS level, the effort required seems minimized at first sight. Still in case of widespread usage of the TOOP architecture by various Competent Authorities, there is a very high probability that implementation of SMP and AP on MS level is needed anyway. So, this option may be not really advantageous form the MS view in the long-term perspective.

As a conclusion, this option may be preferred in the initial phase of introducing TOOP architecture on a MS level, when there is insufficient level of MS infrastructure

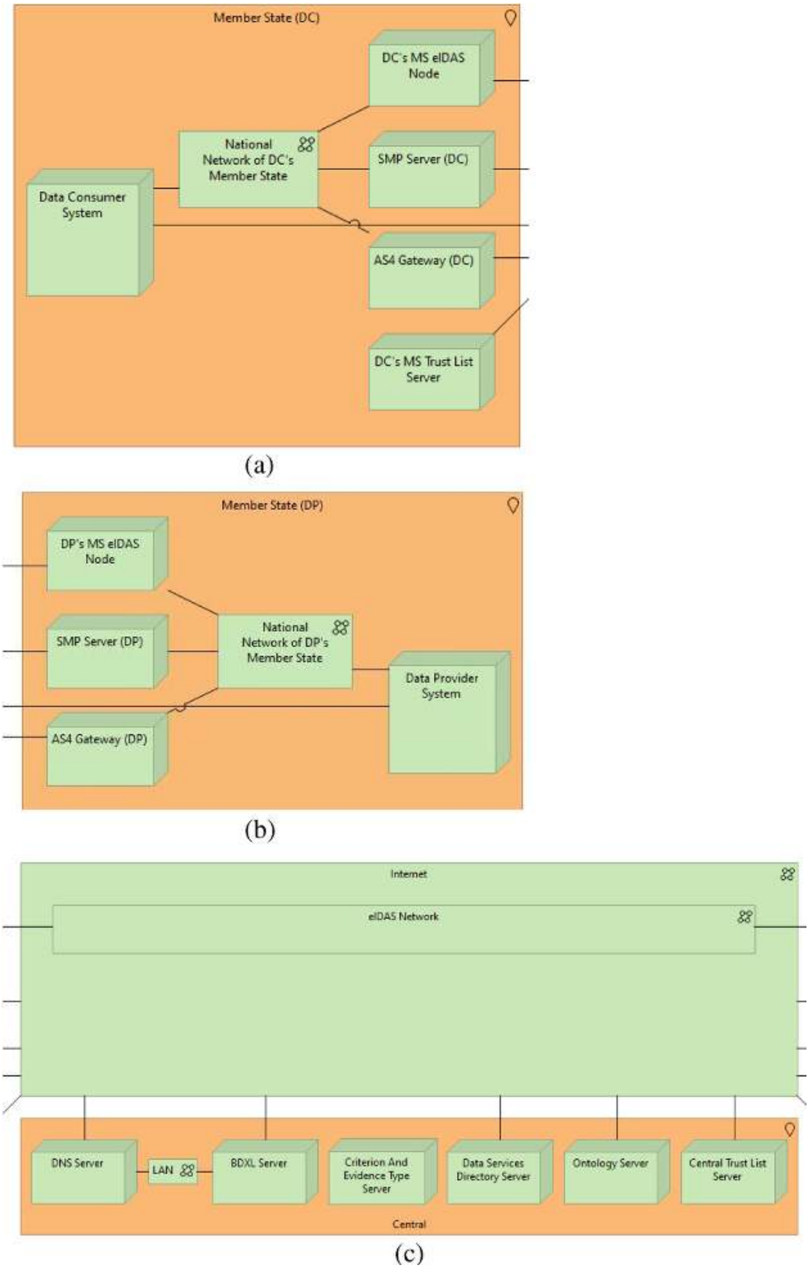

Fig. 9. a. The Network and Communication view (DC part). **b.** The Network and Communication view (DP part). **c.** The Network and Communication view (Internet part between DC on the left and DP on the right).

and some advanced Competent Authorities wish not to be hindered by this insufficiency. Additionally, it may be useful in case of additional requirements to the SMP and AP from some Competent Authorities.

Similar conclusions apply when the DP Competent Authority operates its own SMP, AP, TOOP Connector, and backend information system.

The *Network and Communication* view focuses on how the system is implemented from the perspective of the communications engineer. It helps to assure that within the system, appropriate communications and networking services are developed and deployed by relevant stakeholders.

From the network and communication perspective, a TOOP application uses communication networks in the MSs, the TOOP central communications infrastructure, the eIDAS network, and the Internet (Fig. 9a, 9b, 9c).

The communication networks in the DC MS connect the DC system to the national network of data consumers. Through this national network and the eIDAS node server, the DC connects to the eIDAS network for user identification. The DC also connects to the SMP server for the DP discovery and to an AP for the evidence exchange. Similar connections are used in the DP MS.

The TOOP central communications infrastructure comprises the DNS servers, local area networks, the Business Document Exchange Network Location (BDXL) server, the Data Services Directory server, the Semantic Server, and the Criterion and Evidence Type server.

4.5 Security and Trust Architecture

In view of recent trends in the IS area, security and trust are of primary importance for TOOPRA. At the same time, a project based on such architecture would involve many diverse stakeholders. Therefore, it would be too restrictive to propose just specific security measures to be implemented by all parties. To resolve this conflict, the TOOPRA security and trust view comprises two components: (1) an overall trust and security framework and (2) specific standards and protocols related to security and trust.

The TOOPRA security and trust framework first makes a distinction between information security and trust. Information security is commonly defined as preservation of its attributes - confidentiality, integrity, and availability of information, as in the standard ISO/IEC 27000:2018 [17]. Various other attributes may be needed to further specify the concept of information security, such as trustworthiness, authenticity, non-repudiation, accountability, reliability and traceability.

Trust establishment on the other hand is about the guarantees, that the origin and the destination of the data and documents are authentic (authenticity) and trustworthy (trustworthiness), and that data and documents are secured against any modification by untrusted parties (integrity) [18–20]. Additional trust management can include authorization, accountability, non-repudiation, traceability, and confidentiality. The main difference between information security and trust is the focus on specific concepts. As an example, information security usually does not involve trustworthiness of the data origin. From the other side, trust usually does not involve availability, reliability, and confidentiality.

Using the ISO/IEC 27000 series of standards, the TOOP security and trust architecture introduces the concept of Information Security Management System (ISMS) for all organizations involved in an OOP project. An ISMS comprises policies and procedures together with necessary activities and resources that are used and managed to protect information assets. To establish and maintain its ISMS, the organization needs to identify information assets and information security requirements associated with these assets. Security risks must be assessed and treated, including selection and implementation of controls to manage unacceptable risks. Effectiveness of ISMS must be maintained and improved.

The TOOP security and trust architecture uses the CEF eDelivery AS4 profile for message exchange, the CEF eDelivery profile of the BDXL specification, the OASIS Service Metadata Publishing 1.0 (BDXR SMP) specification, the OASIS RegRep v4.0, the CEF eID BB, and the CEF eIDAS Profile, among other building blocks, standards and interfaces.

5 Architecture Profiling

Based on the reference architecture, different profiles for application domains can be created. Application profiles are collections of variations of the basic TOOPRA model. These variations may be in the form of:

- explications, giving more detailed specifications of an existing TOOPRA component;
- extensions, providing additional functionalities or capabilities to TOOPRA; or
- modifications, introducing changes to TOOPRA structure or components.

To create a profile, it is recommended to i) understand the goals, legal foundations, stakeholders, and specific requirements leading to the profile development; ii) identify components that need to be detailed, extended, or modified; and iii) introduce, test, and document the variations.

The following profiles have been developed from TOOPRA after analysing the goals, legal framework, and specific requirements of the three piloting areas of the TOOP project:

- General Business Mobility
- eProcurement
- Online Ship and Crew Certificates

The goal of the General Business Mobility profile is to facilitate the mobility of companies in terms of doing business within the EU. It demonstrates how information can be automatically retrieved from a company's country of origin, avoiding duplicated effort, and eliminating paperwork and red tape for business management. The use cases covered by this profile are targeting European business needs and are aligned with the SDGR [8], which facilitates online access to information, administrative procedures and assistance services.

The goal of the eProcurement profile is to support businesses in public procurement. By implementing this profile, businesses will no longer have to provide all information they have already delivered in the past during public procurement. The eProcurement profile intends to use the TOOP infrastructure in order to demonstrate how the provision of evidence during an eTendering procedure can be faster and seamless. More specifically, it focuses on the automatic retrieval of the necessary information and qualification documents of tenderers at any phase of the process (pre-award, award or post-award) using the existing national European Single Procurement Document (ESPD) [21], eCertis and available eTendering Services. The main variation to TOOPRA introduced by the eProcurement profile is that the evidence exchanged in the reference OOP process is explicated as a national ESPD. Additionally, there are two different kinds of transactions with the DP: Get Evidence Metadata and Get Evidence. This is a variation mentioned in connection with the TOOPRA Business Architecture operational process model (the exchange of the Evidence information can also be a two-step process where the DP first provides meta-data on the available Evidence and the actual Evidence is retrieved later in a second step).

The Online Ship and Crew Certificates profile addresses problems in the maritime sector, related to accessing Ship and Crew Certificates which are currently issued and maintained in paper format and stored by national Maritime Administrations. The process of validating and checking ships and their crew can be streamlined by making the certificates accessible for Maritime Administrations directly from the issuer, not through the Master of the ship. This approach is fully in line with OOP principle, namely that instead of burdening citizens and businesses with proving compliance, administrations access and re-use information already existing in other administrative bodies. Models in this profile do not use the Criterion and Evidence Type Rule Base, because the Maritime Administrations already know which certificates they need, to perform the inspection. The Data Services Directory is still included to find the Maritime Administrations of other countries.

6 Sustainability of TOOPRA

To stay useful in the long run, components of TOOPRA need to be maintained and sustained. Different components need varying levels of sustainability effort by different stakeholders. First, the TOOPRA itself requires maintenance, including the following components:

- The wiki component of TOOPRA, currently maintained in the TOOP documentation space in Confluence.
- Views of TOOPRA specified by models expressed in ArchiMate, currently maintained in a git repository.
- The support history and open issues of TOOPRA, currently maintained in the JIRA platform.

The BBs and their components needed to implement TOOPRA are currently maintained by CEF. They comprise the CEF eDelivery building block, the CEF eID building block, and the CEF eSignature building block, among others.

The standards and other components needed to implement and maintain TOOPRA are maintained by the organisations driving the development, convergence, and adoption of these standards. It is assumed that the long-term maintenance of these artefacts is outside the TOOP scope. They comprise the AS4 Profile of ebMS 3.0 Version 1.0 OASIS Standard, the ebMS3 OASIS ebXML Messaging Services Version 3.0, the OASIS Business Document Metadata Service Location Version 1.0, the OASIS Service Metadata Publishing 1.0 (BDXR SMP) specification, standards from the ISO/IEC 27000 and ISO/IEC 25000 series of standards, ISO/IEC/IEEE 42010:2011, as well as the TOGAF® Standard, a standard of The Open Group.

7 Conclusions

The main goal of TOOP Reference Architecture is to overcome the main technical challenge in OOP application across the EU – the diversity of organisations, procedures, data, and services on all four main levels of interoperability.

This goal is achieved by using standard solution blocks, by designing the Reference Architecture and standard solution blocks in line with legal requirements, as well as by using tested, mature, inter-connected and interoperable standards and BBs.

TOOP Reference Architecture is developed in cooperation with the TOOP pilots and the TOOP Solution Architecture. It relies on proven Enterprise Architecture methodology, ensuring consistent standards, methods, and communication among Enterprise Architecture professionals.

To ensure sustainability of TOOPRA, its different components still need varying levels of maintenance effort by different stakeholders.

The results of the TOOP architecture 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.

References

1. The New European Interoperability Framework. https://ec.europa.eu/isa2/eif_en, Accessed 26 Aug 2020
2. European Interoperability Reference Architecture. https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/about, Accessed 26 Aug 2020
3. European Commission: 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 (2017)
4. ArchiMate® 3.1 Specification, a Standard of The Open Group. https://pubs.opengroup.org/architecture/archimate3-doc/chap01.html#_Toc10045268, Accessed 12 Oct 2020
5. Proper, H., Lankhorst, M.: Enterprise architecture – towards essential sensemaking. Enterp. Model. Inf. Syst. Arch. **9**(1), 5–21 (2014). https://doi.org/10.1007/s40786-014-0002-7
6. Chen, L., Babar, M., Nuseibeh, B.: Characterizing architecturally significant requirements. IEEE Softw. **30**(2), 38–45 (2013). https://doi.org/10.1109/MS.2012.174
7. The Open Group: TOGAF®, an Open Group Standard. Open Group Standard (2011)

8. European Union: Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Single Digital Gateway Regulation). OJ L 295, 21.11.2018, pp. 1–38 (2018)
9. European Union: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation). OJ L 257, 28.8.2014, pp. 73–114 (2014)
10. European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR). OJ L 119, 4.5.2016, pp. 1–88 (2016)
11. European Union: Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. OJ L 8, 12.1.2001 (2001)
12. European Commission: Commission notice—Guidelines for the implementation of the Single Digital Gateway Regulation—2019–2020 work programme, C/2019/4881. https://op.europa.eu/en/publication-detail/-/publication/877b88c4-b356-11e9-9d01-01aa75ed71a1/language-en/format-HTML/source-105856679, Accessed 26 Aug 2020
13. ISA^2 - Interoperability solutions for public administrations, businesses and citizens Homepage. https://ec.europa.eu/isa2/home_en, Accessed 26 Aug 2020
14. European Union: Regulation (EU) No 283/2014 of the European Parliament and of the Council of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision No 1336/97/EC, OJ L 86, 21.3.2014, pp. 14–26 (2014)
15. Core Public Service Vocabulary Application Profile (CPSV-AP). https://joinup.ec.europa.eu/solution/core-public-service-vocabulary-application-profile, Accessed 26 Aug 2020
16. Core Criterion and Core Evidence Vocabulary (CCCEV). https://joinup.ec.europa.eu/solution/core-criterion-and-core-evidence-vocabulary, Accessed 26 Aug 2020
17. ISO/IEC 27000:2018. Information technology—Security techniques—Information security management systems—Overview and vocabulary
18. Cofta, P.: Trust, Complexity and Control: Confidence in a Convergent World. Wiley, Hoboken (2007)
19. Gaurav, R., Sarfaraz, M., Singh, D.: Survey on Trust Establishment in Cloud Computing. In: 5th International Conference the Next Generation Information Technology Summit (Confluence). IEEE, Noida (2014)
20. Winslett, M.: An introduction to trust negotiation. In: Nixon, P., Terzis, S. (eds.) iTrust 2003. LNCS, vol. 2692, pp. 275–283. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-44875-6_20
21. European Union, Commission Implementing Regulation (EU) 2016/7 of 5 January 2016 establishing the standard form for the European Single Procurement Document, OJ L 3, 6.1.2016, pp. 16–34 (2016)