D2.7 Interoperability Architecture for Cross-border Procedures and Evidence Exchange in light of the Single Digital Gateway Regulation

Document Identification			
Status	Final	**Due Date**	30/03/2022
Version	1.1	**Submission Date**	01/08/2022

Related WP	WP2	**Document Reference**	D2.7
Related Deliverable(s)	WP1, WP3, WP4, WP6, WP7	**Dissemination Level (*)**	PU
Lead Participant	MinBZK/ICTU	**Lead Author**	Alexander Bielowski (MinBZK/ICTU)
Contributors	Harold Metselaar (MinBZK/ICTU), Muhamed Turkanović (UM)	**Reviewers**	Tomaž Klobučar (JSI) Hans Graux (TIME.LEX)

Keywords :
Architecture, Once-Only Principle, Once-Only Technical System, European Digital Identity, Wallet, eDelivery

Document Information

List of Contributors	
Name	Partner
Alexander Bielowski	MinBZK/ICTU
Ana Rosa Guzman Carbonell	MPTFP-SGAD
Thashmee Karunaratne	SU
Harold Metselaar	MinBZK/ICTU
Carl-Markus Piswanger	BMDW
Gérard Soisson	CTIE
Muhamed Turkanović	UM
Alenka Žužek Nemec	SI-MPA

Document History			
Version	Date	Change editors	Changes
0.1	23/02/2022	Harold Metselaar (ICTU)	Instantiated template with content from Miro board
0.2	23/03/2022	Alexander Bielowski (ICTU)	Included patterns
0.3	28/03/2022	Harold Metselaar	Included Application Collaboration descriptions and application architecture diagrams and descriptions per pattern.
0.4	04-11/04/2022	Harold Metselaar	Added text for generic functionalities and interaction patterns. Added diagram and text for Supported User-managed Access Pattern.
0.5	14-15/04/2022	Alexander Bielowski	Draft of 3.1, 3.2 and 3.3
0.5.1	19/04/2022	Alexander Bielowski	Draft of 3.4
0.5.2	20-22/04/2022	Alexander Bielowski Harold Metselaar	Further refinement of 5
0.6	25/04/2022	Alexander Bielowski	Draft of chapter 3
0.61	26/04/2022	Harold Metselaar	Review chapter 3
0.62	28/04/2022	Alexander Bielowski	Draft of 4.1 and 4.2.1 to 4.2.3
0.63	02-16/05/2022	Harold Metselaar	Update Chapter 5
0.64	17-18/05/2022	Alexander Bielowski Harold Metselaar	Complete draft of Chapter 4. Updated all diagrams and propagate changes in document
0.7	23/05/2022	Harold Metselaar	Draft of chapter 1 Updated references Editorial (all sections)
0.8	25/05/2022	Alexander Bielowski Harold Metselaar	Draft of chapter 2 Completion chapter 1

Document History			
0.81	30/05/2022	Muhamed Turkanović (UM)	Technical implementation options section 4.2.6.
0.82	31/05/2022	Alexander Bielowski	Draft of chapter 6
0.83	02/06/2022	Alexander Bielowski Harold Metselaar	Updates to 4.1, Update Figure 8, Executive Summary, Formatting, References, Acronyms
0.9	03/06/2022	Harold Metselaar Alexander Bielowski	Version for internal review
0.10	09/06/2022	Alexander Bielowski Harold Metselaar	Review comments resolved. Pending confirmation of IA publication for reference 3
0.11	12/07/2022	Julia Wells (Atos)	QA for submission
1.0	14/07/2022	Ana Piñuela (Atos)	Final for submission. Submission held on request of editor to better align with publication of IA.
1.1	11/10/2022	Julia Wells (Atos)	Update reference 3 final link to IA

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Alexander Bielowski (MinBZK/ICTU)	09/06/2022
Quality manager	Julia Wells (ATOS)	12/07/2022
Project Coordinator	Ana Piñuela Marcos (ATOS)	14/07/2022

Style Disclaimer

This document is drafted using Oxford English spelling, which is British English spelling in combination with the suffix *-ize* in words like *realize* and *organization*. This choice was made to reconcile the DE4A default UK English spelling convention with the limitations of ArchiMate, where diagrams were labelled in US English (with z instead of s).

References to generic third persons are made by means of the singular '*they*' (and its variants *them, their, themself*).

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
API	Application Programming Interface
ARF	Architecture Reference Framework
AS4	Applicability Statement 4, an open standard for the secure and payload-agnostic exchange of Business-to-business documents using Web services
BPMN	Business Process Model and Notation
BRIS	Business Register Interconnection System
CAAR	Cross-border Access Authorization Registry
DBA	Doing Business Abroad – one of the three DE4A pilots
DC	Data Consumer, consists of the roles DE and DR. A single organization might perform both roles or outsource for example the DR role to another organization and only perform the DE role.
DE	Data Evaluator
DE4A	Digital Europe for All
DID	Decentralized identifier
DO	Data Owner
DP	Data Provider, consists of the roles DT and DO. A single organization might perform both roles or split up in individual roles and outsource for instance the DT role.
DR	Data Requestor
DSD	Data Service Directory
DT	Data Transferor
Dx.y	DE4A formal Deliverable x.y (e.g. D2.7)
EBSI	European Blockchain Services Infrastructure
EC	European Commission
EIF	European Interoperability Framework
EIM	Evidence Interchange Management
EP	Evidence Provider
ER	Evidence Requestor
EUDI	European Digital Identity
eID	Electronic identity
eIDAS	EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. It was established in EU Regulation 910/2014.
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
ID	Identity (document)
IM	Intermediation

Abbreviation / acronym	Description
JSON	JavaScript Object Notation
LKP	Lookup
LoA	Level of Assurance
MA	Moving Abroad – one of the three DE4A pilots
MOR	Multilingual Ontology Repository
MS	European Union Member State(s)
OIDC	OpenID Connect
OOP	Once-Only Principle
OOTS	Once-Only Technical System
PID	Personal Identification Data
PoR	Power of Representation
PSA	Project Start Architecture
(Q)EAA	(Qualified) Electronic Attestation of Attributes
REST	Representational state transfer
RP	Relying Party
S&N	Subscription and Notification
SA	Studying Abroad – one of the three DE4A pilots
SAML	Security Assertion Markup Language
SDG	Single Digital Gateway
SDGR	Single Digital Gateway Regulation
SEMPER	Secure Electronic Marketplace for Europe
SSI	Self-sovereign identity
SUMA	Supported User-managed Access
TL	Task Leader
TLS	Transport Layer Security
Tn.m	DE4A formal project Task n.m (e.g. T2.5)
TOOP	The Once Only Principle Project
UI	User interface
URL	Uniform resource locator
USI	User-supported Intermediation
VC	Verifiable Credential
VIN	Vehicle Identification Number
VP	Verifiable Presentation
XML	Extensible Markup Language

Executive Summary

This document is a deliverable of the Digital Europe for All (DE4A) project and directed at policy makers and architects of the bodies of the European Union and its Member States (MS). It provides architectural advice for the implementation of European public service interoperability solutions in light of the Single Digital Gateway Regulation (SDGR) [18].

Taking the first version of the Once-Only Technical System (OOTS) [18] (due 12.12.2023), as a starting point, a mid-term future, multi-pattern, target architecture is sketched in terms of high-level business processes and application flows. At this time horizon (2025+), the availability of the European Digital Identity (EUDI) Wallet is assumed.

The proposed multi-pattern architecture shows that the infrastructure of the OOTS can relatively easily be leveraged to support additional cross-border interaction patterns. In this way, requirements stemming from state-of-the-art eGovernment procedures at Member State level can be covered in cross-border context, e.g. allowing seamless interoperability and pro-active eGovernment. The addition of a user-centric interaction pattern, supported by the wallet, shows the potential to simplify interactions that need to happen on user initiative and under user-control, while pointing to the opportunity to reuse some elements of the overall architecture.

The interaction patterns included in this mid-term future target architecture are:

1. Intermediation (IM) Pattern: A user-triggered and user-controlled, direct exchange between competent authorities whereby the user only interacts with the eProcedure Portal of the Data Consumer (DC); akin to the pattern piloted by TOOP [23].
2. User-supported Intermediation (USI) Pattern: A variant of the IM pattern that includes a direct interaction between the user and the Evidence Portal of the Data Provider (DP), wherein the user supports the DP in establishing a unique identification, previews the evidence and approves the exchange; akin to the pattern defined in the OOTS implementing regulation [3].
3. Lookup (LKP) Pattern: A direct request-response exchange of evidence between DC and DP without any user involvement.
4. Subscription & Notification (S&N) Pattern: A pattern that allows the DC to subscribe to and get notified about relevant business events (or life events) of a company (or citizen).
5. Push Pattern: In this target time horizon a pattern that allows to push an event signal along a pre-established communication relationship without a prior subscription; with the potential to extend to more general event signalling in the future.
6. Supported User-Managed Access (SUMA) Pattern: A user-centric interaction pattern, making use of the EUDI-Wallet, including a support for the user in identifying and contacting the adequate Data Provider (Electronic Attestation of Attributes provider, in EUDI-terms) directly from the wallet.

Apart from the inclusion of a user-managed element, i.e. the EUDI-Wallet, which is in itself a highly complex challenge, the additions to the basic infrastructure of the OOTS required to support these patterns are rather limited: A Cross-border Subscriptions system and an event handling capability is required for the S&N and Push patterns. For the LKP, S&N, Push and SUMA patterns a formal authorisation control should be included to check whether the Data Consumer (DC) (Relying Party (RP) in wallet-terms) is authorized to request the information. This authorisation control / RP registration should be explored as a potential synergy in the Synergies and Interoperability Contact Group [3].

On a more detailed level, two challenges remain only partially answered, for which no European-level solution is presently available: First, the support for powers of representation in context of the cross-border authentication where experiences from the SEMPER [25] project could be harnessed in the eIDAS revision. Second, the question of unique identification and cross-border record matching. Current solutions are MS specific and rely on the limited mandatory eIDAS dataset and user-provided attributes. The authors expect that the current work on the European Digital Identity Framework and the eIDAS revision will yield a more consistent approach to record matching, not only for the EUDI-Wallet but for cross-border unique identification in general. A fully 100%-match, however, will most probable not be attainable in the foreseeable future.

Concluding, the multi-pattern architecture shows the first version of the OOTS can evolve into a broader infrastructure for cross-border eGovernment interoperability, if two pre-requisites are met. A cross-sectoral governance must be established that guides new requirements towards the common infrastructure. Legal barriers must be broken down and appropriate legal bases should be created on Union or national level to allow, where appropriate, cross-border exchange of data without direct user-involvement in order to allow pro-active eGovernment and security-related use cases, such as fraud prevention or embargo enforcement.

1 Introduction

1.1 Purpose of the document

The main goal of the document is to provide architectural advice for the implementation of European public service interoperability solutions in light of the Single Digital Gateway Regulation (SDGR)[18]. The document projects insight from the DE4A project into the midterm future and makes them accessible in form of a high-level target architecture description to policy makers and architects of the bodies of the European Union and its Member States. The insights in this document are gained from the requirement analysis of the three pilots [7][10][12], worked out in two iterations of the Project Start Architecture (PSA)[6] and first insights from the pilots currently running [8][9][11], combined with additional requirement gathering with Member State representatives, specific to the mid-term future time horizon.

The target architecture description focuses on the application of available technology and builds on the SDG OOTS. We also consider the currently ongoing eIDAS revision, i.e. the EUDI-Wallet.

The deliverable is thus clearly external directed, not to the running pilots, but to external experts. The authors assume that the informed reader has at least basic knowledge of European eGovernment interoperability, e.g. the EIF, the SDGR and more specifically the Once Only Technical System (OOTS) [3], the eIDAS Regulation [21] and the EIDAS network and the proposed revision [19] of that Regulation, including the European Digital Identity Wallet [16].

1.2 Structure of the document

The document follows the following structure:

- Chapter 1 - Purpose and structure of the document (this section)
- Chapter 2 - This chapter outlines the scope of the document as well as some important EU Digitalization Initiatives. The time horizon and some fundamental assumptions made in this document are presented. The relation to the Once-Only Technical System (OOTS) and the currently ongoing eIDAS revision and with it the European Digital Identity Framework is explained.
- Chapter 3 - This chapter summarizes the high-level requirements resulting from workshops with MS representatives and insights from the DE4A Pilots:
  1. Addressing Challenges in Current Functionality
  2. Enable a Roadmap for Semantic eGovernment Interoperability
  3. Formalized Access Management Approach
  4. Empowering the User vs. eGovernment efficiency and ease of use.
  5. Flexibility and Modularity of the Multi-pattern Architecture
- Chapter 4 - This chapter elaborates the Business Architecture. It consists of business process sketches of six interaction patterns of the multi-pattern architecture that jointly cover the requirements described in chapter 3. It focuses on the interaction between the main roles, explaining who does what in each of the pattern along a few key interoperability activities:
  1. Explicit Request
  2. Electronic Authentication
  3. Record Matching
  4. Routing
  5. Preview

- Chapter 5 - This chapter deals with the high-level Application Architecture. At the highest level we have the Application Collaborations. They are aggregations of Application components, Data objects and Interfaces. Together, they implement all Interaction Patterns. First the Application Collaborations are explained. Next the most important Data Objects are presented. Finally, for each of the interaction patterns the application flows are elaborated.
- Chapter 6 – This section deals with the overall conclusions
- References – References to consulted and recommended sources
- Annexes – The annex provides a more detailed example of record matching

2 Scope and relevant EU Digitalisation Initiatives

2.1 Time Horizon and Fundamental Assumptions

The DE4A Architecture Framework [4] defined five distinct time horizons as reference for the architecture definition:

- T=0: The baseline or starting point before the implementation of the Single Digital Gateway (SDG) [18] corresponding approximately to 2019.
- T=1: The situation at the launch of the SDG, in 2020, as information platform that provides access to information on public services across Europe, spanning from a European portal, containing European-level information on rights and obligations of European residents and companies operating in the European single market, to National Portals and Websites of single public service providers, containing information of on specific public services and links to eProcedure portals.
- T=2: The target time horizon for the fully operational SDG in 2023, including cross-border eProcedures and, most relevant for the scope of this deliverable, the first version of the Once Only Technical System (OOTS)[3], that allows the direct, cross-border exchange of evidence between competent authorities in context of these eProcedures. The DE4A pilots focused on this and partly the next time horizon.
- T=3: The mid-term future time horizon where the OOTS is fully adopted and use of the infrastructure extended not only to cover additional procedures, but also to accommodate additional interoperability requirements of public administrations, one could say a "OOTS version 2". We envision the creation of a true multi-pattern architecture that also incorporates fully user-centric interaction patterns supported by the emerging European Digital Identity (EUDI) Wallet at approximately 2-3 years after the first version of the OOTS. The high-level target architecture description in this document focuses on this time horizon.
- T=4: The long-term future time horizon, beyond a full system lifecycle from today where we would expect the emergence of a consistent European Digital Single Market Ecosystem that does cover both public and private sector services and blurs the boundaries of national systems. It is difficult to put a date on this time horizon, but we hope that it can be reached in the next decade, maybe earlier. This time horizon is the focus of another, forthcoming DE4A deliverable.

This deliverable is directed to policy makers and architects of bodies of the European Union and its Member States. It provides architectural advice for the implementation of European public service interoperability solutions at the time horizon T=3 (i.e. 2025+) building on the stepping stone provided by the first version of the OOTS [3]. Some fundamental assumptions for the resulting system are:

1. Functionally speaking the scope is eGovernment interoperability (G2x). Private sector service providers acting independently are not considered.
2. Application of available technology that can allows a stable operation at the 2025+ time horizon.
3. The system builds on the first version of the OOTS and capitalizes on the investments made.
4. The system can and must take on board the eIDAS revision, and the EUDI-Wallet that is assumed to be fully operational by then.

2.2 Relations with the Once-Only Technical System

This target architecture description builds on the first version of the OOTS in order to capitalize to the largest extent possible on the investments made on European and Member State level. This means that we assume that the OOTS will be implemented in accordance with the specifications laid down in the Implementing Regulation [3] on Article 14 of the SDG Regulation [18]. This first version of the OOTS focuses on the direct exchange of evidence between competent authorities in context of a public service eProcedure started by the user, meaning that the user must explicitly request the use of the OOTS and be able to preview the evidence and approve the exchange. By extending this approach to a multi-pattern architecture, the authors hope to contribute to the development of the OOTS into the core cross-border eGovernment interoperability infrastructure in Europe.

2.3 eIDAS and the European Digital Identity Framework

At the time of writing, a revision of the eIDAS Regulation [21] is underway. This revision [19] shall include the creation of a European Digital Identity Wallet. The first version of the Architecture Reference Framework [ARF] [16] was published on February 22, 2022. Even though the detailed operational and technical specifications will only be completed in the course of the next year, the basic concept is clear enough to include it in this high-level architecture description as basis for a user-centric interaction pattern.

3 High-Level requirements

Chapter II of the European Declaration on Digital Rights and Principles states: *Everyone should have access to all key public services online across the Union. Nobody is to be asked to provide data more often than necessary when accessing and using digital public services.* [15] The results of requirement gathering for the target architecture for the mid-term time horizon could not be better summarized in a single sentence.

In addition to the requirement definition of the DE4A Pilots [7][10][12] and the insights gained from the ongoing interaction with the pilot architects in regular meetings, the high-level requirements were collected in several workshops with Member State representatives. In a collaborative brown paper approach, using a large online white-board application, a shared picture of the desired mid-term solution was developed, based on the structure provided by the interdisciplinary questioned drawn from the project start architecture [6] and the broader set of possible interaction patterns defined in the initial architecture framework [4].

This chapter summarizes the result of the workshops and preliminary insights from the DE4A Pilots following five main aspects. Where appropriate, quotes from Member State representatives are provided in *"italic"*.

3.1 Addressing Challenges in Current Functionality

As of today, with the recently published Implementing Regulation of the SDG OOTS [3] and the European Digital Identity Framework being developed, some functional challenges remain either unresolved or the sole responsibility of Member States. For a sustainable, long-term solution these challenges should be addressed at European level.

The first challenge is commonly referred to as **'record matching'** and defined as 'unique identification' in Article 3.55 of the proposed eIDAS revision [19]: *Unique identification means a process where person identification data or person identification means are matched with or linked to an existing account belonging to the same person.* It should be mentioned that, although it is not explicitly mentioned in this definition, record matching is also relevant for the identification of legal persons, which is, however, much less complex owing to the creation of a European unique company identifier [13] in the context of BRIS.

As expressed during the requirement workshop a European unique identification is needed *"to avoid identity matching uncertainties regardless the country responsible of the eID, the procedure portal or the evidence source"*.

The second major challenge concerns the cross-border handling of **Powers of Representation** (PoR), which is essential for company use cases, where the user is a legal person, represented by an authenticated, natural person. Without a European solution to communicate powers of representation as part of an authentication process, most cross-border business use-cases are not implementable.

In addition to the requirement to define and communicate powers as a function of the multi-level architecture, the semantic challenge to define fine-grain powers needs to be addressed. This means that next to the "full-power" of e.g. the legal representative of a company, a European classification of more detailed mandates need to evolve over time, which is not trivial as one Member State representative expressed during the requirement workshop, cross-border powers of representation should "be based on a common EU framework (probably in the context of eIDAS) that takes into account and enables the national specificities."

The challenge is, however, not limited to legal person representation. In context of the Moving Abroad pilot the requirement to *"move whole families, including e.g. dependent children"* was discussed and helped to make clear that a European Solution for Powers of Representation should take the representation of natural person into account from the start. This is also important from an inclusion point of view, as expressed in the European Declaration on Digital Rights and Principles for the Digital Decade: *[Digital transformation] should notably include elderly people, persons with disabilities, or marginalised, vulnerable or disenfranchised people and those who act on their behalf. [15]*

Finally, an exception worth mentioning, because it is only partly addressed by the first version of the Once-Only Technical System [3] is the need to support **interrupted procedures**, or as one Member State representative stated: *"[The architecture] must be able to support interrupted procedures as such situations will be unavoidable in reality. This means that some interaction patterns should be able to timewise decouple the requesting, the sending/issuing and the receiving/submitting of evidence."*

3.2 Enable a Roadmap for Semantic eGovernment Interoperability

The complex topic of legal and semantic eGovernment interoperability needs to consider several interrelated aspects: The legal validity of the exchanged information (i.e. evidence) including the need for legally authoritative translations, the structuredness of the data, the existence of a common definition of meaning of the data. The optimal situation, from an interoperability point of view, are fully structured, harmonized data definitions, i.e. canonical evidence definitions, as they are called in DE4A. One statement from the requirement workshop summarized this optimum: *"The common structured data format is the only solution to the requirement of legal translations and automatic processing of evidence"* and hence enable proactive eGovernment automation.

The sub-group the SDGR Gateway Coordination Group for *evidence standardisation and OOTS data models* [3] that is planned to cooperate closely with the eIDAS Expert Group is a good step in this direction. It is also very welcome that this sub-group is expected to work closely with other DGs experts from sectoral networks to fully capitalize on the knowledge and agreement that were developed over the last decades in these sectoral collaborations.

Taken together, this means that first canonical evidences need to be agreed in a harmonization effort, second attribute definitions need to be translated in order to create multi-lingual labels and third the resulting multi-lingual, canonical evidence needs to be given legal validity. This means that the journey towards harmonization and deep semantic interoperability also demands from national legislators to reduce existing form requirements in national legislation. After all, even a fully harmonized data format does not provide the expected value, if legal validity is tied to one specific, national format.

European harmonization will by no means be completed for all relevant datasets, at the focal time horizon (t=3) for this target architecture advise. Hence, *"even if the goal should be to exchange progressively more and more standardised structured data, this cannot be achieved in a few years. In order to be useful and to be [actually] used, the interoperability architecture has to take into account reality"*. *"Based on the subsidiarity principle and on the principle of national administrative autonomy, the interoperability architecture has to propose a flexible approach and not to try to impose a complete standardisation."* This means to support a) unstructured, digitized documents, b) structured, yet non-standardized data and c) the inclusion of digital copies of documents that carry legal validity (i.e., usually in the language of the country of origin), in addition to d) fully harmonized, structured data.

This dichotomy of the harmonized and unharmonized results in two additional requirements to guarantee the functioning of the system and to *"simplify for users and authorities the location of proper cross-border evidence"*. First, the automated matching of unharmonized, yet generally equivalent

evidence types must be supported. Second, if such a matching results in alternative, potentially overlapping or even conflicting evidence types being identified as generally equivalent, the user must be able to disambiguate the evidence types in order to request the most appropriate one. As an example, one Member State might have a specific proof of citizenship evidence type, whereas in another Member State several evidence types could be used to provide a proof of citizenship. The user must be able to identify these evidence types and choose (i.e. based on the additional information contained in them) the one they want to use.

In a nutshell, the interoperability architecture should support a flexible roadmap towards increased harmonization, allowing everything from unstructured evidences to fully harmonized, canonical data sets to exist side by side. In this way harmonization efforts in specific sectoral context can gradually add value to eGovernment interoperability without the need of additional infrastructure investment, while the scope of the interoperability architecture can be flexibly extended to additional sectors and evidence types, without the need to prior harmonization.

3.3 Formalized Access Management Approach

In the first version of the OOTS [3], the trust model is essentially based on a 'closed network approach' similarly to the DE4A User-supported Intermediation Pattern [6], as explained in the DE4A Trust Management Models [5]. In addition, trust in the rightfulness of the data exchange is furthered by the inclusion of the authentication of the user at the Evidence Provider side and the preview of the evidence and user approval of the exchange before the data leaves the control of the Evidence Provider. This approach is generally considered appropriate; however, it faces certain functional limitations when it is applied in a complex multi-pattern architecture that needs to cater for additional exchange needs (see 3.5 below), which partially do not include direct user interaction or include additional actors and trust service providers.

This gives rise to the need to further formalize the trust relations between actors in the interoperability architecture, akin to the definition of Providers of Registries of Trusted Sources in the European Digital Identity Architecture Framework [16]. The Data Service Directory (DSD) of the OOTS is the first such registry, provided by the Commission and jointly maintained by the Member States. Apart from the operational need to be able to locate the correct data source for an evidence type, the DSD also provides the assurance that the data service is provided by a trusted, competent authority.

The multi-pattern interoperability architecture must additionally enable the evidence provider or user (depending on the pattern) to validate that the Evidence Requester or Relying Party is indeed a competent authority that is authorized to request the evidence/data in question in order to *"guarantee a secure and lawful exchanges*". This is a specific case of the more general requirement that the interoperability architecture should *"implement [..] security-by-design and privacy-by-design, i.e. find technical solutions and design choices that guarantee [..] a maximum of security and privacy and only [resort to purely] organisational or legal measures if [..] unavoidable."*

3.4 Empowering the User vs. eGovernment efficiency and ease of use

The requirements workshop confirmed the existence of two partially opposing requirements in the context of eGovernment interoperability, which, amongst other requirements, indicated the need for a multi-pattern architecture: On the one hand the drive to more user-centric approaches that empower the individual and increase the control they have over their own data. On the other hand, the drive to more efficient and pro-active public service processes, that diminish the administrative burden for the user to the maximum extent possible: *"The interoperability architecture should, as far*

as legally possible and in compliance with the Charter of fundamental rights, avoid preview and approval, but rather prefer an approach of automated and pro-active back-office exchange of evidence without any intervention of the user. […] This is also the best way to really comply to the OOP principle."

The drive to put the user in the centre of the exchange cannot be ignored and is engrained in recent policy developments on European level, as exemplified by the European Declaration on Digital Rights and Principles for the Digital Decade [15] and the revision of the eIDAS Regulation, proposing the European Digital Identity Wallet [19]. A multipattern-architecture must make such an exchange possible to support this policy requirement. It should be seen as a steppingstone for broader (private sector) adoption, as the bottom-up requirement analysis showed some preference for the back-end exchange between competent authorities (without any user involvement) within the scope of eGovernment as explained in section 3.4 above. This is required to provide the same level of pro-active eGovernment cross-border as is provided already today on national level by many Member States: *"To achieve automated pro-active eGovernment and hence true Once Only, we will need more back-office exchange of data without any user intervention."*

Another requirement that is also exhibited by the DE4A DBA pilot is the need to get updated on significant changes in the situation of the subject of the data exchange (i.e. the company). An additional underlying reason for this requirement is fraud prevention. Recent developments, however, also move use-cases like embargo into focus. With or without prior subscription, signals should be transmitted between competent authorities of different Member States, alerting them of relevant business events (e.g. merger, bankruptcy, embargo) or life events (e.g. change of name and/or marital status, change of address, change of employment status, death). In the citizen domain, this would require the removal of legal barriers that exist today, through bilateral agreement or Union law.

Which of these two requirements should be prevalent for each single exchange depends on several aspects: the use-case/procedure and the data exchanged (publicly available data vs. personal data and special categories), the choice of the user, the trust in the correctness of the data (where bilateral or multilateral agreements can play a role). It is also worth mentioning in this context that data quality measures do expand beyond the cross-border exchange of data and the exchange as such should not be seen as a primary point to improve of control data quality.

3.5 Flexibility and Modularity of the Multi-pattern Architecture

An overarching demand from the Member States that is sustained by the preliminary insights from the DE4A Pilots is the call for flexibility and modularity of the architecture. The architecture and its components should be designed to run different interaction pattern interchangeably with a maximum of reuse, even allowing the integration of new or adapted interaction patterns as the need arises. The User-transferred Data Pattern [4], for example, that combines a direct request message from Data Consumer (DC) to Data Provider (DP) with a response routed via the user (i.e. a Wallet) was considered not immediately relevant. However, this pattern should be possible to be implemented with minimal effort, based on the components of the architecture.

The underlying idea is that the multi-pattern architecture should be flexible enough to accommodate different or changing exchange needs mostly through configuration changes, rather than the need to implement new systems: *"The architecture has to be designed in a way that it allows for simple, flexible, fast and easy extension and addition of interaction patterns or document types."* The requirements stemming from different underlying public service processes, national regulatory frameworks, different criticality of personal information exchanges, different national baseline

infrastructures and different data quality in registries represent a diversity that impairs a “one pattern fits all”-approach.

One example from the DE4A Pilots is the flexibility in the location of the preview. The OOTS [3] adopts in its first version an exchange pattern similar to the User-supported Intermediation (USI) pattern (authentication and preview on the DP-side). The USI pattern is used in both the DE4A Moving Abroad (MA) and Studying Abroad (SA) pilot. The DE4A Doing Business Abroad (DBA) pilot, contrastingly exhibited a clear preference for the Intermediation pattern (preview at the DC-side). Reasons can be found in the relatively long-term cooperation between the national registers (i.e. BRIS) that yielded a harmonization of the evidence, simplifying preview on the DC-side. The existence of a unique, European subject identifier simplifies record matching and diminishes the need for an authentication on the DP side. The (company) data exchanged does not contain special categories of personal data [20]. The same is true for other exchanges as was found, for example, during the work on the EUCARIS OOTS Non-Paper [22]. The exchange of vehicle data is also based on a far-reaching semantic harmonization and on the existence of the VIN as unique vehicle identifier and does not contain special category personal data.

4 Business Architecture

The business architecture consists of business process sketches of six interaction patterns of the multi-pattern architecture that jointly cover the requirements described in chapter 3. To keep the business architecture concise, it focuses on the interaction between the main roles, explaining who does what in each of the patterns along a few key interoperability activities

4.1 Key Interoperability Activities

We identified five (5) key interoperability activities that are required, either for legal or organisational/technical reasons.

4.1.1 Explicit Request

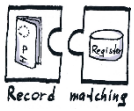
Exchanges that are voluntary for the user and require to be executed under user control either need to be routed via a component that is under direct user control (i.e. a Wallet) or need to be based on an explicit request as stipulated in SDGR Article 14.4 [18]. A competent authority needs to inform the user of the voluntary nature of the exchange and collect their explicit and specific request to start the exchange

4.1.2 Electronic Authentication (eID Authentication or EUDI-Wallet Identification)

Electronic authentication makes sure that the user logs in with notified electronic identification means according to the eIDAS regulation [21]. This can be done either using the eIDAS infrastructure for cross-border authentication or the national eID infrastructure using a notified eID means with the appropriate Level of Assurance (LoA). As an alternative to the authentication using a notified eID means, the identification function of a valid EUDI-Wallet may be used to perform this activity. In any of these three cases, it must support the control of Powers of Representation (PoR) if a natural person is authenticated but acts on behalf of another natural person or a legal person.

Strictly speaking, PoR is not part of authentication as such, however, from a process view it makes sense to combine the two functionalities as they establish either directly or indirectly the relation between the authenticated user and the data subject of the exchange. The experiences gained in the SEMPER[25] project, especially with regards to the question of fine-grain powers validation, could for example be picked up in the current eIDAS revision.

4.1.3 Record matching



In simple terms, record matching describes the process of relating an unknown electronic identification (or an EUDI-Wallet) from a (foreign) eID scheme to an existing record in a public registry (cf. 'unique identification' as defined in Article 3.55 [19]). Current record matching is specific to each Member State and usually directly related to the eIDAS authentication. It is recognized as a crucial functionality in the development of the EUDI-Wallet Toolbox and is expected to yield a European standard solution. It must, however, be considered that no fully automated solution will enable an unambiguous match in 100% of the cases, requiring manual exception procedures to create the first match. Therefore, the record matching activity, when performed for the first time for any given user, can result in a rejection of the user and the exchange not being possible. From an organisational perspective, record matching lends itself to be made a generic Member State service.

4.1.4 Routing

Routing in this context means collecting the metadata needed to address the data services of the Data Provider (DP). This means identifying the correct data/evidence to be requested, the correct participant (DP), the correct data service and its technical address. In case a Wallet is used, the address must lead to a provider of (Qualified) Electronic Attestation of Attributes ((Q)EAA). This means that even if the routing activity must always result in a technical address, i.e. URL, the type of service and the exchange format can vary between patterns. From an organisational perspective, provision of routing information can best be made a central EU responsibility, irrespective of the solution being centralized or federated.

One complicating aspect that one would not directly relate to routing has to do with the degree of harmonization and structuredness of data. In the optimal, most simple case of fully harmonized, structure data being exchanged, e.g. canonical evidence, the required evidence at the DC and the provided evidence at the DP are just the same thing and routing is really only about identifying the right end-point service. If evidence is not harmonized and in the most difficult case only available in a domestic, unstructured format (i.e. a scanned paper document), routing is considered to include also an element of discovering evidence that can be provided by a DP that is, to varying degree, equivalent with the evidence required in the eProcedure of the DC. A lack of predefined semantic interoperability should not automatically result in a lack of technical interoperability. It is well understood that the lack of semantic interoperability remains and must then be resolved after the exchange in the context of the DC's legal and administrative framework and usually involving the informed judgment of public servants.

4.1.5 Preview

If the exchange is to be executed under user control, a preview of the exchanged data needs to be provided to the user for their approval. This is for example required by SDGR Article 14.5 [18]. This can be accomplished by providing the evidence, i.e. as (Q)EAA, to the wallet under direct control of the user, or by providing a preview functionality in a platform controlled by the DC or DP as explained in the patterns below, or by a separate data processor that performs this service, e.g. on a national level.

4.2 Interaction Patterns

This section provides a high-level business process description of the six interaction patterns comprising the multi-pattern architecture. For the graphical descriptions, we adopted a simplified version of BPMN Collaboration Diagrams [2] with black-box pools containing only the pictograms of the key interoperability activities described above and arrows representing the business messages. All purely technical messaging, e.g. confirmation messages, are omitted for the sake of simplicity. For some patterns, namely the Intermediation pattern, the User-Supported Intermediation patter, the Lookup-pattern and the Subscription and Notification pattern, detailed BPMN Collaboration Diagrams are included in the PSA [6].

4.2.1 Intermediation Pattern

The Intermediation (IM) pattern describes a relatively straight forward, direct interaction between DC and DP under control of the user. It is largely similar to the interaction described in TOOP and was the starting point for the design of the OOTS. This pattern is piloted by the DE4A Doing Business Abroad (DBA) pilot. The specific properties of the company data use case, explained in this section, make it the interaction pattern of choice. The preview is located at the DC, which means that the DC must provide

previews for evidence from 26 different Member States, which is simplified by the existing harmonization of company data. The handling of the evidence request at the DP is essentially a back-office response without user interaction, which is facilitated by the existence of a European unique company identifier.

This makes the pattern also a good basis for the integration of existing, sectoral exchange systems through the creation of a bridge between these networks and the OOTS. The underlying assumption is that the DP trusts the evidence request from the DC without an additional control through the user (cf. User-supported Intermediation pattern). This assumption is more likely to hold if the exchanged data does not contain personal data or at least no personal data of special categories, as it is the case for company data. The relative simplicity of the IM pattern and the properties of use cases that fit this pattern makes these use cases also the most likely candidates for the creation of a legal basis for exchange without any preview (cf. SDGR Article 14.5).

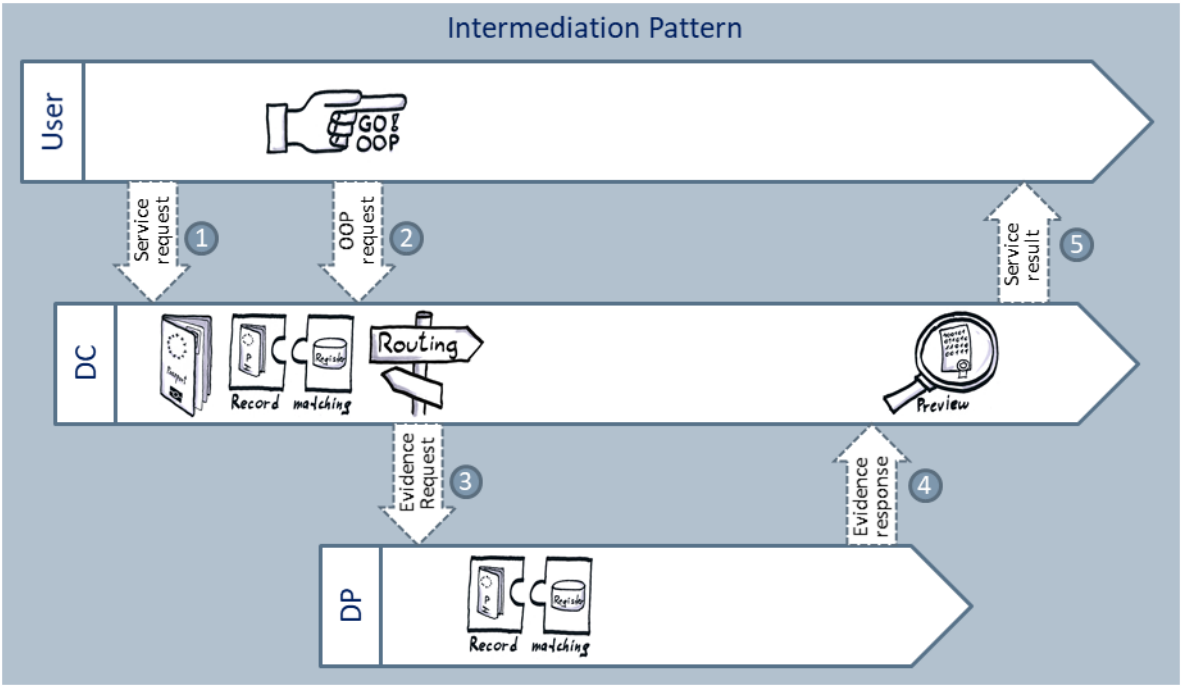


Figure 1: Collaboration Diagram of an Intermediation Pattern

The DC fulfils the central role in the IM pattern, i.e. handling all user interaction, including save and resume functionality of the eProcedure. Additionally, the DC process is the parent process for the DP process, which indirectly remains under control of the DC who coordinates the overall interaction pattern. The collaboration typically starts with the User requesting a service in eProcedure Portal of the DC country (1). Authentication & record matching takes place at DC and the requirements for the eProcedure are determined. The user issues an explicit request to fetch the required evidence(s) making use of the OOTS (2). A lookup of the routing information is performed by the DC and the DC sends an evidence(s) request to the DP (3).

The DP performs record matching, based solely on data contained in the evidence request; as mentioned above, this record matching is simplified for example by the existence of a European unique company identifier. The existence of a Vehicle Identification Number (VIN) could play a similar role in the exchange of vehicle data. The DP retrieves the requested evidence(s) and sends the evidence response message back to the DC (4). Next, the DC prepares the preview for the user and after their

approval can use the evidence in the eProcedure. Finally, the DC can provide the service result to the user (5).

4.2.2 User-supported Intermediation Pattern

The User-supported Intermediation (USI) pattern is the pattern most similar to the interaction proposed for the SDGR OOTS [3] and it is piloted by both the DE4A Moving Abroad and Studying Abroad pilot. The fact that the user for both life events is a natural person, i.e. citizen, is also the underlying reason for the differences between the USI and the IM pattern described above. Whereas these patterns are largely similar, and hence can share large parts of the underlying infrastructure, the USI adds a direct interaction between the user and the DP in order for the user to support the DP in making an unambiguous match and to approve the exchange of the evidence while the data resides still in the sphere of control of the DP. This addition increases the transparency of the exchange and serves to increase the certainty and hence trust at the part of the DP that the data is indeed to be shared cross-border.

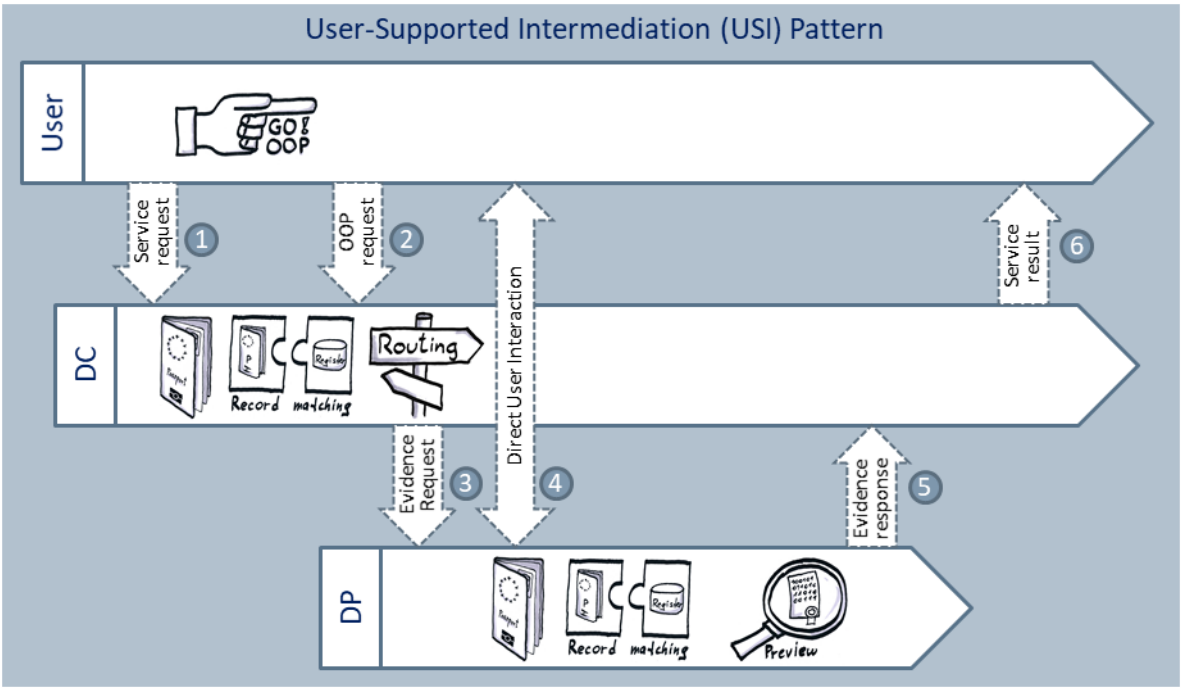


Figure 2: USI Pattern

Identical to the IM pattern, the User navigates to the eProcedure Portal of the DC and requests a public service (1). Authentication & record matching takes place at DC and the requirements for the eProcedure are determined. The user issues an explicit request (2) to fetch the required evidence(s) making use of the OOTS. A lookup of the routing information is performed and the DC sends an evidence(s) request to the DP (3).

At this point, the USI pattern deviates from the IM pattern with the addition of a direct interaction between the User and DP (4). Technically, the DP responds to the DC with a redirect URL. The DC redirects the User to the DP using this URL. At DP the User authenticates for the second time and assists the DP in record matching. The DP retrieves the requested evidence(s) and prepares the preview for the User. After approval, the evidence(s) can be provided to the DC. The DP sends the evidence response message (5) containing the requested evidence(s). The DC can now directly use the approved evidence(s) in the eProcedure. Finally, the DC provides the service result to the user (6).

4.2.3 Lookup Pattern

The Lookup (LKP) pattern is planned to be piloted by the DE4A DBA pilot to enable repetitive requests for previously shared evidence. It is in essence a back-office lookup of data, without any user interaction, triggered by the internal needs of a public service process. This means that the LKP pattern could be used in all cases where the need for (additional) evidence emerges after the public service was requested by the user, hence at any point of the public service process.

Different options were considered, including an 'attribute lookup' via direct API calls, however, the complexities related to attribute-level authorization and the need to include an API framework specifically for this pattern led to the decision to focus on 'evidence lookup', therefore reusing the evidence type definitions and the underlying infrastructure of the IM and USI patterns. Applying the lookup pattern requires the existence, or rather creation, of a legal basis for the exchange. In context of the DBA this need was mediated by soliciting user consent during the initial exchange of evidence (linked to the explicit OOP request in the IM pattern).

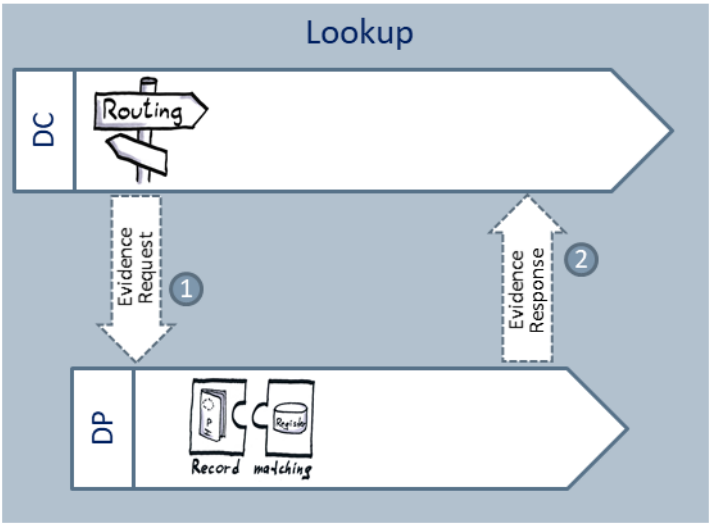


Figure 3: Lookup Pattern

As stated above, the trigger of the pattern resides in a public service process at the DC side. The required cross-border evidence is determined, and the relevant routing information is looked up. The DC then sends an evidence request to the DP (1). In contrast to the patterns explained above, there is no user control over this exchange process. This means that the DP needs to be able to check whether the DC is actually authorized to request the evidence. There are different solutions possible, e.g. a central (or rather hierarchical) register of authorities that are authorized to request such information could be maintained similar to the concept of a register of Relying Parties (RP) in the architecture framework of the EUDI-Wallet [16]. The DP performs record matching and retrieves the evidence. If the DC is authorized to request the evidence, the DP sends the evidence response back to the DC (2).

In the use case piloted in DE4A, record matching without a direct link to an authentication is simplified by the existence of a European unique company identifier. This cannot be easily generalized for the citizen domain, based on the current eIDAS infrastructure. One option that could be considered for the EUDI-Wallet toolbox is to create a two-way match during the first matching process, meaning that the match is documented both on the DP and the DC side, allowing the DC to issue unambiguous evidence requests.

4.2.4 Subscription and Notification Pattern

The Subscription and Notification (S&N) pattern is created with pro-active eGovernment in mind and is planned to be piloted in the DBA pilot. The assumption in the pilot is that the DC has previously received evidence pertaining to one subject (i.e. a company) and needs to be updated of any significant change in the situation of the company. One of the reasons for this are long-running services, like recurring subsidies, that could be affected by company events. In pilot context this is considered purely as an additional service to the user, however, one often cited requirement for the S&N pattern is fraud prevention. For such a use case, the consent-based approach of the DBA would not work and a separate legal basis would need to be created, which could also open the possibility of subscriptions to business or life events independently of a previously shared evidence. Especially in this last case, the DP would also need a possibility to check for the authorization of the DC to actually request a subscription, similar to the LKP pattern explained above in 4.2.3 .

The DE4A pilots did not consider the subscription to life events of citizens, however, there are several good use cases that are implemented on national level in some Member States that would also make perfectly sense in a cross-border setting. Think for example of change of address, change of employment status, or death. Such application would, however, require both a solid legal basis, which is today not in place, and a European solution for the record matching problem for citizens.

The research done in context of the DBA pilot resulted in a clear focus on what we call 'event notification'. A list of harmonized business events can relatively easily be drawn up without the need to harmonize the actual data structures that are used to register and document the event on national level. Once an event is registered, every subscriber is notified about the event with a notification containing the event type and the company identifier. One of the reasons for this approach, apart from data minimization, was that some events fall outside of the data set of the company data evidence or cannot be identified unambiguously from changes in that data set. If the DC determines, based on an event that they would want to receive a new, updated evidence, they can use the LKP pattern described in section 4.2.3 above. It can depend on the DC whether such an update is required and whether that includes a single or multiple evidence types.

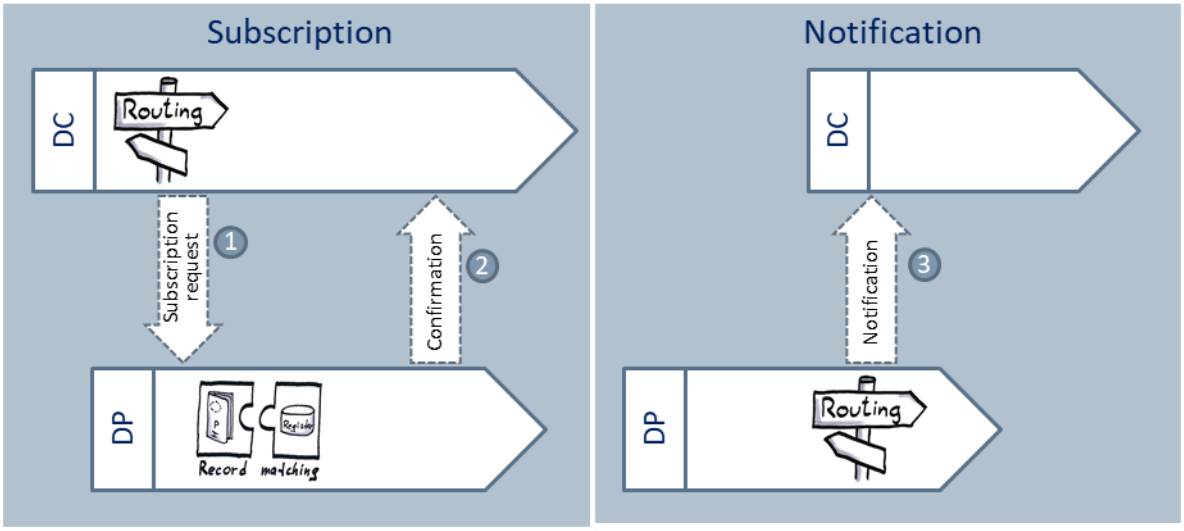


Figure 4: Subscription and Notification Pattern

The S&N pattern consists of two separate processes with different timing. The first one, the subscription process is performed only once for the creation of a subscription and only repeated if the

subscription needs to be changed (e.g. prolonged or cancelled). The notification is performed for every single business event of a company for which at least one subscription exists.

Subscription

The subscription process is triggered by the DC if the need for a subscription is identified. The DC looks up the routing information and sends a subscription request to the DP (1). If the subscription is not linked to a previous exchange of evidence under user control, i.e. using the IM or USI pattern, the DP needs to check whether the DC is authorized to issue such a request. The DP performs record matching, registers the subscription in its system and ends a confirmation back to the DC (2), who maintains their own log of active subscriptions.

Notification

The DP identifies a cross-border event to which subscriptions are registered. Although the subscriber is known at this point, the DP still queries the technical routing information and then sends a notification to all DCs that subscribe to that event (3). We assume here that the DP receives a technical confirmation message via eDelivery that the notification message was received by the DC access point. We do not foresee a business-level conformation that the event was indeed processed at the DC-side. The subscription system should, however, allow resending events for a particular DC on request of that DC.

The S&N pattern could reuse the majority of the infrastructure of the other patterns described above. Apart from adding the subscription and notification functionality, the routing information of these new data services needs to be registered as well.

4.2.5 Push Pattern

The Push pattern caters primarily for the requirement to allow a more proactive eGovernment. We encounter two different flavours of this pattern that differ substantially in legal basis and authorization requirements: one triggered by the user in course of a public service encounter and one triggered by the public authority without any user interaction. Because of the legal implication of the second case, we would not consider this to be part of the target architecture at the mid-term time horizon.

The first flavour, triggered by the user during a service encounter came about in the MA pilot under the term of “deregistration use case”: The citizen registers a new residential address in a Member State. In order to do so, the competent authority (the DC in this exchange) requests the present residential address from a competent authority in another Member State (the DP in this exchange) and offers the user to inform the first competent authority of the fact that a new residential address is registered, i.e. the citizen has moved. Please note that the roles of DC and DP are reversed in that second interaction, using the Push Pattern. This and similar cases are relatively straight forward as they are based on the request and consent of the user, both participants and the user are already known.

The second flavour, triggered proactively by the competent authority itself, would need not only a legal basis, but the routing would need to include the discovery of the DC. This would amount in a lookup of the same type of register of DCs (or relying parties in EDI terms) that would be required for the authorization check in LKP and S&N pattern. Valid use cases for this second type of Push pattern are fraud preventions and, given the current geo-political situation, the enforcement of embargoes. If a legal or natural person is recognized to fall under the embargo, the component authority could push a message to competent authorities in other Member States to alert them of the fact that that person is to be excluded from economic activity. This example shows that such a Push would not be one-to-one, but one-to-many. The fact that a company falls under embargo would need to be communicated not to one, but to all business registers in the Union. As stated above, the legal and technical (Lookup

of DCs) implications of this second type of Push are deemed too complex to include it in the target architecture for t=3, however, it is worthwhile mentioning that, if the need and legal basis for such use cases should arise, they can relatively easily be integrated in the overall interoperability architecture without substantial infrastructure investment.

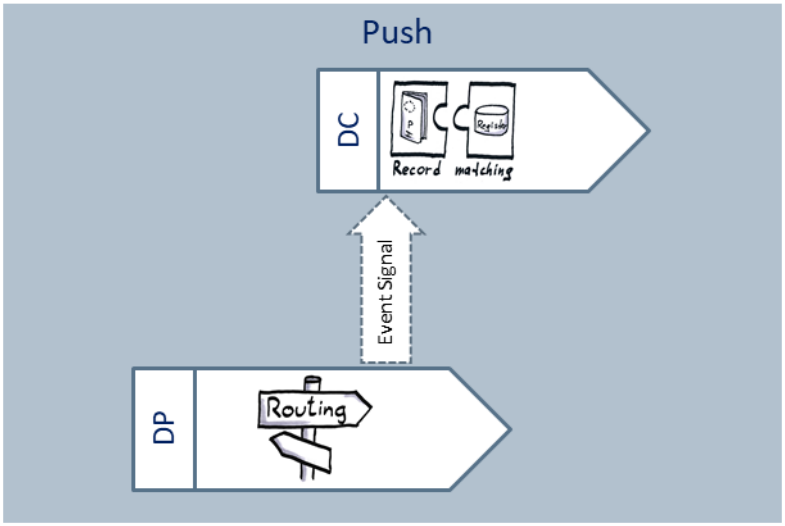


Figure 5: Push Pattern

From a process point of view, the Push pattern is essentially a Notification without prior Subscription. This means that it is again an event notification or rather an event signal that contains only the event type and identifying information of the subject.

As shown in Figure 5, the need for the notification of a DC is identified at the DP side, i.e. in context of the address registration process as explained above which created the need to potentially deregister the old address of the citizen. The participant, the DC in this pattern is already known at this point. The DP looks up the technical routing information and sends an Event signal to the DC. The DC performs record matching and can determine the appropriate follow-up action, i.e. to deregister the old address.

4.2.6 Supported User-managed Access Pattern

The Supported User-managed Access (SUMA) pattern takes a very different approach to the patterns explained above. The user takes central stage and manages the exchange of evidence which is largely in line with the concept of an EUDI-Wallet that can be used for identification and exchange of data, called (Qualified) Electronic Attestation of Attributes. This means that this pattern also departs from the use of message infrastructure between competent authorities as explained in section 5.3.2.

Please not that we retain the DC and DP terminology as synonyms for relying party / verifier and attribute provide / issuer. The table below gives an overview of this terminology.

Table 1: Terminology across different projects and standards

DE4A and TOOP	SDGR OOTS	EUDI-Wallet	W3C Verifiable Credentials
Data Provider (DP)	Evidence Provider (EP)	(Q)EAA Provider	Issuer
Data Consumer (DC)	Evidence Requestor (ER)	Relying Party (RP)	Verifier

DE4A and TOOP	SDGR OOTS	EUDI-Wallet	W3C Verifiable Credentials
Evidence	Evidence	(Qualified) Electronic Attestation of Attributes ((Q)EAA)	Verifiable Credential (VC) / Verifiable Presentation (VP)

Another interesting aspect in which this pattern differs from the other patterns above is that they are all fundamentally designed to support cross-border evidence exchange. In the Supported User-managed Access pattern, the location of the DC and DP is of secondary importance. They could reside in the same Member State, in different Member States, or in associated states outside the Union if they comply to the same interface and certification requirements.

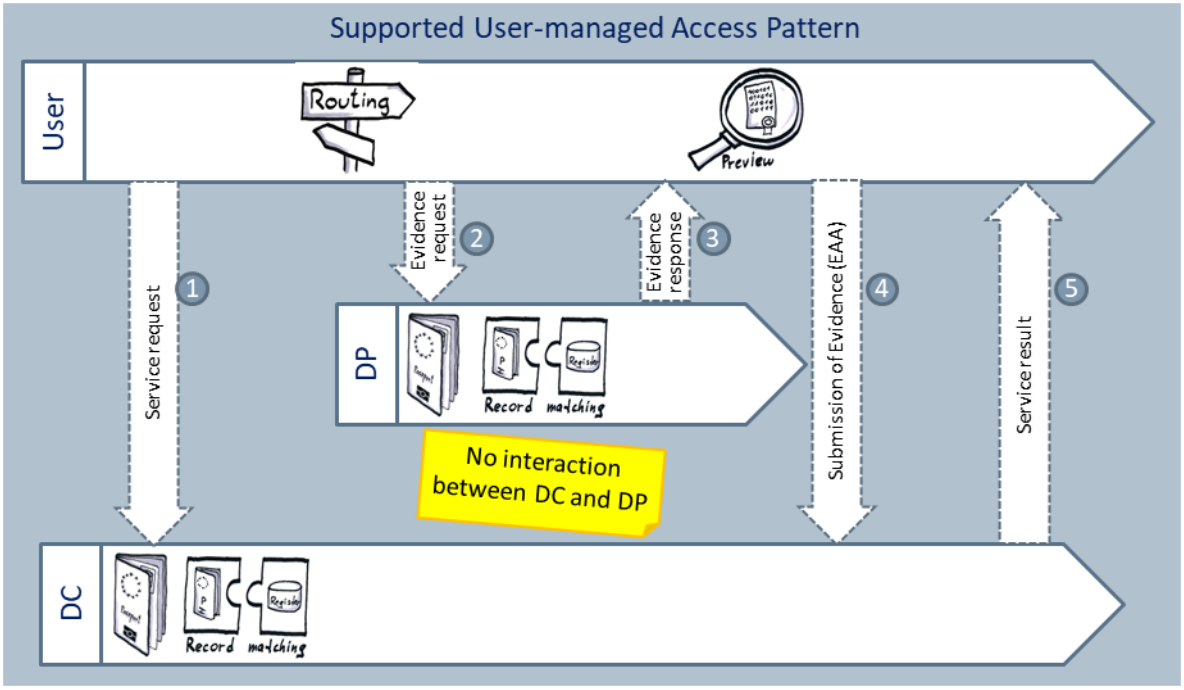


Figure 6: Supported User-managed Access Pattern

Please note that the order of participants (pools) in Figure 6 changed in comparison to the other patterns to represent the user-centric nature of the pattern. The user takes the central role and orchestrates the entire interaction, rather than DC. Stated differently, the user process functions as parent process for both the DC and the DP process. This also creates a bit more flexibility in the flow, as explained below.

In the default flow depicted in Figure 6, the User navigates to the eProcedure Portal in the DC country and requests a public service (1). Authentication & record matching takes place at DC and the requirements for the eProcedure are determined. This results in Evidence(s) that need to be provided to the DC. If the user holds the correct evidence (i.e. EAA) in their wallet, they can directly proceed to step 4 and submit the Evidence to the DC.

The user is supported by the system by helping them to discover where they can obtain the Evidence(s), they are routed to the correct DP irrespective of the Member State the DP resides in. The User then requests the Evidences directly in their wallet, from the DP that can issue them (2). Please

note that, instead of issuing an explicit request for the OOP exchange to the DC, as in the IM and USI patterns, the user explicitly and directly requests the evidence from the DP itself. Authentication & record matching takes place at DP. The DP fetches requested evidence(s), transforms them into the EAA format and provides them to the user (3).

Neither the DP nor DC provide preview functionality, the User can preview the Evidence(s) on their own and choose to make use of it or not. Next, the User provides Evidence(s) to the DC (4) so it/they can be used in the eProcedure. Finally, the DC can provide the service result to the user (5). If the service result can be framed in terms of an EAA, e.g. it being a right or license, this could in turn be done by using the Wallet functionality.

As stated above, this user-centric approach leaves some flexibility to the flow. The user could collect evidences and store them in their wallet long before they start the public service eProcedure, and long after they complete it. The order of the flow would consequently change to (2)(3)(1)(4)(5).

This pattern can be implemented in various ways. In DE4A a very similar pattern was implemented as the “VC pattern”, based on blockchain technology, making use of the European Blockchain Service Infrastructure (EBSI) [14]. This architecture description assumes the use of the EUDI-Wallet [19], which changes the exchange pattern somewhat from the piloted VC pattern. At the time of writing, the technology choice for the EUDI-Wallet is not yet completed. Section 5.3.7 mentioned some implementation options.

5 Application Architecture

The application architecture description adopts the same ArchiMate [1] language used in the DE4A Architecture Framework[4], however, it concentrates on the highest level of elements in the framework, namely the Application Collaborations. Section 5.1 describes each Application Collaboration. Section 5.2 assigns ownership of the main Data Objects to these Application Collaborations, and Section 5.3 contains high-level Application flow diagrams for each of the interaction patterns.

5.1 Main Application Collaborations

Application Collaborations are aggregations of Application components, Data objects and Interfaces. A total of 10 Application Collaborations have been elaborated, together implementing all 6 Interaction Patterns. Figure 7 below contains an overview of all Application Collaborations of the Multi-pattern Architecture, followed by a description of each Application.

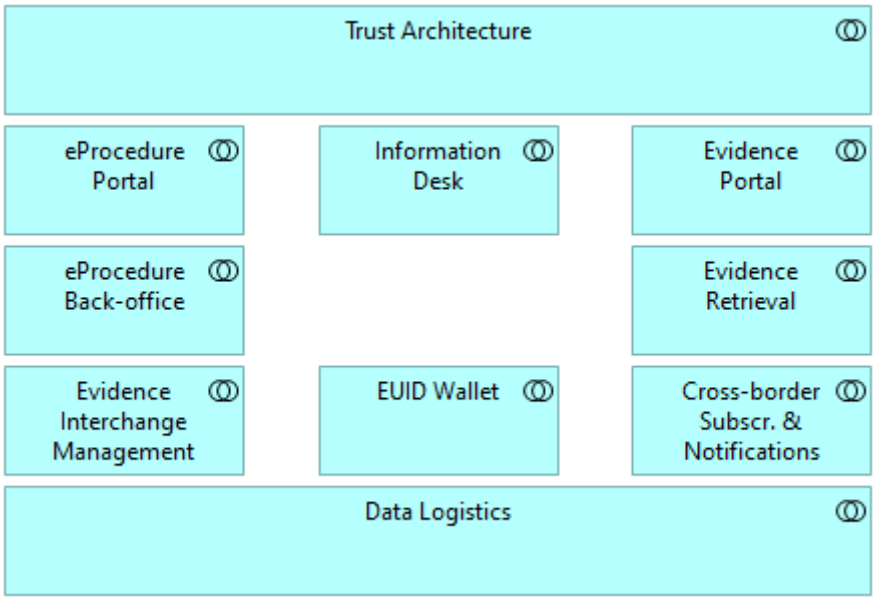


Figure 7: Application Collaborations of the Multi-pattern Architecture

5.1.1 eProcedure Portal

The eProcedure portal Application collaboration resides at the DC and bundles functionality for handling a user requesting a public service. The eProcedure portal application offers a UI for interacting with the user and back-end functionality to support the handling of the eProcedure.

Through this portal the user makes the explicit request for OOP transfer and receives confirmation when all requirements of the eProcedure are met, i.e. all evidences have been received by the DC. Subsequently the user can choose to submit the eProcedure.

The eProcedure Portal should offer functionality for save and resume of eProcedures. This is to avoid that the user must start all over in case of exceptions (e.g. when a piece of evidence is not available or when it takes longer than expected, i.e. interrupted procedures).

5.1.2 Information Desk

The Information Desk (Data Service Lookup) application collaboration is a conceptual component that offers services to facilitate the participants in making use of the OOTS.

It provides information to the DC for helping the user to locate the proper competent authority to provide the required cross-border evidence type and for obtaining the routing information to do the request. The OOTS v1 [3] implements this in form of the Data Service Directory (DSD) and the Evidence Broker. In this multi-pattern architecture, it also helps the user to find the provider of (Qualified) Electronic Attestation of Attributes ((Q)EAA) in case of the Wallet. The DP can consult the information desk to establish that the DC is authorized/allowed to request some evidence type or subscription or to lookup the DC in order to send a push signal. Such a functionality is not foreseen in OOTS v1, however, a register or registers of Relying Parties in context of the EUDI Framework could be a step in that direction.

This Information Desk functionality can be EU centralized. It could also be some federative solution but with a central database like TOOP and DE4A piloted. We advise dynamic routing for the technical addresses (i.e. SML/SMP) in order to have maximum flexibility.

5.1.3 Evidence Interchange Management

The Evidence Interchange Management (EIM) application collaboration manages the interchange of evidence. It keeps track of the requests and status of evidence(s) and provides an evidence status overview for the user.

To execute the IM pattern, it also contains the preview functionality with which the user can preview and approve the evidence. EIM also takes care of the “shredding” of evidence to respect privacy regulations and the proposed OOTS implementing regulation [3]. Evidence Interchange Management application collaboration interfaces with Data Logistics in order to exchange the evidence. It is a good candidate for a generic piece of eGovernment national infrastructure, because it contains much of the functionality required for the exchange of evidences on the DC side in order to keep the impact on the potentially large number of different eProcedure portals to a minimum.

5.1.4 Trust Architecture

The Trust Architecture application provides all needed trust services to support all identified interaction patterns: Identity management based on eID (eIDAS) and the EUDI-Wallet, identity matching based on attributes (Record Matching, see Annex 1) to allow unique identification and the provision of all needed services for data encryption/decryption, electronic signatures, seals, time stamps, certificates and preservation thereof. In case of certificates this also includes transport layer security. The Trust Architecture also provides functionality so that natural persons can represent other natural and legal persons (Powers of Representation).

5.1.5 Data Logistics

The Data Logistics application collaboration realizes the functionality needed to implement all data logistics surrounding the exchange of messages between DC and DP. It offers an interface to expose its functionality to other components, e.g. Evidence Interchange Management.

In the application architecture, we assume each business message is acknowledged on communication layer. This detail is omitted in the architecture descriptions below for the sake of readability.

Building on the first version of the SDG OOTS [3], AS4-based eDelivery messaging is a central, yet not the only element of Data Logistics. Intermediary platforms, e.g. central national implementations of

Evidence Exchange Management and Evidence Portal more likely than not will use different infrastructure and protocols to link to eProcedure portals and Evidence Retrieval, i.e. reusing parts of their current national OOP infrastructure.

5.1.6 Evidence Portal

The Evidence Portal application collaboration provides all functionalities needed to provide evidence either to the DC or to the wallet of the user. It includes transformation functionality, for IM, USI and LKP pattern transformation from domestic evidence formats (received from evidence retrieval) into the Canonical Evidence format and for the Supported User-managed Access pattern into (Q)EAA format, e.g. Verifiable Credentials [24]. The Evidence Portal application collaboration also includes the functionality implementing error handling for the DP. It takes care the interfaces with Evidence Retrieval and Data Logistics.

Specifically, for USI it handles the generation of the persistent URL to enable the redirection of the user from the eProcedure Portal to the Evidence Portal. For USI it also takes care of preview and user approval.

The Evidence Portal is a good candidate for a generic piece of eGovernment national infrastructure. It handles the Preview (USI), evidence responses (IM, USI, LKP) and issuing of EAA (SUMA). This would constitute the creation of a “one stop shop”, however other implementation options down to a single evidence portal instance per competent authority are possible. This to cater for the flexibility required for the diversity of 27 MS.

Note the Evidence Portal doesn’t play a role for the S&N and Push patterns.

5.1.7 Evidence Retrieval

The Evidence Retrieval application collaboration implements the looking up of evidence from an evidence registry.

IM, USI, LKP and SUMA all make use of it. S&N and Push do not.

5.1.8 EUDI-Wallet

The EUDI-Wallet provides various functionalities and combines front-end and backend components.

It supports authentication and identification using the EUDI (including the provision of Personal Identification Data (PID)) [16]. It has functionality to find, obtain, store, view, combine and manage Evidences in form of (Q)EAA in the Wallet with the aim of providing Evidences to Competent Authorities in a secure and privacy-friendly way. We also foresee the Wallet to provide functionality for representing other natural and legal persons.

5.1.9 Cross-border Subscriptions and Notifications

The Cross-border Subscriptions and Notifications application collaboration implements multiple services used by both Notification Process realization and Subscription process realization:

- The full life cycle of subscriptions
- The lookup, creation & update, validation and error handling of subscriptions
- Event handling, i.e. filtering local (national) events for relevant cross-border events
- Notifications of events
- Preparing the list of subscribers and the dispatching of notifications as well as error handling

5.1.10 eProcedure Back-office

The eProcedure Back-office is the collaboration of various systems used by the competent authority in providing the public service. They can have varying degrees of automation but often include user tasks performed by public servants.

The eProcedure Back-office application collaboration encompasses:

- Collecting relevant data in preparation for a subscription request
- Determining an appropriate response to a received event, where several cases can occur:
  - The event is not relevant, i.e. can be dismissed
  - The event requires a new (i.e. updated) evidence (this would trigger the usage of the LKP pattern to obtain the evidence)
  - A business response is required
- Updating the logs
- A UI for user tasks for the public servant to analyse wrong subscriptions

5.2 Main Data Objects

The diagram below (Figure 8) presents the high-level Target architecture with a focus on the most important data objects.

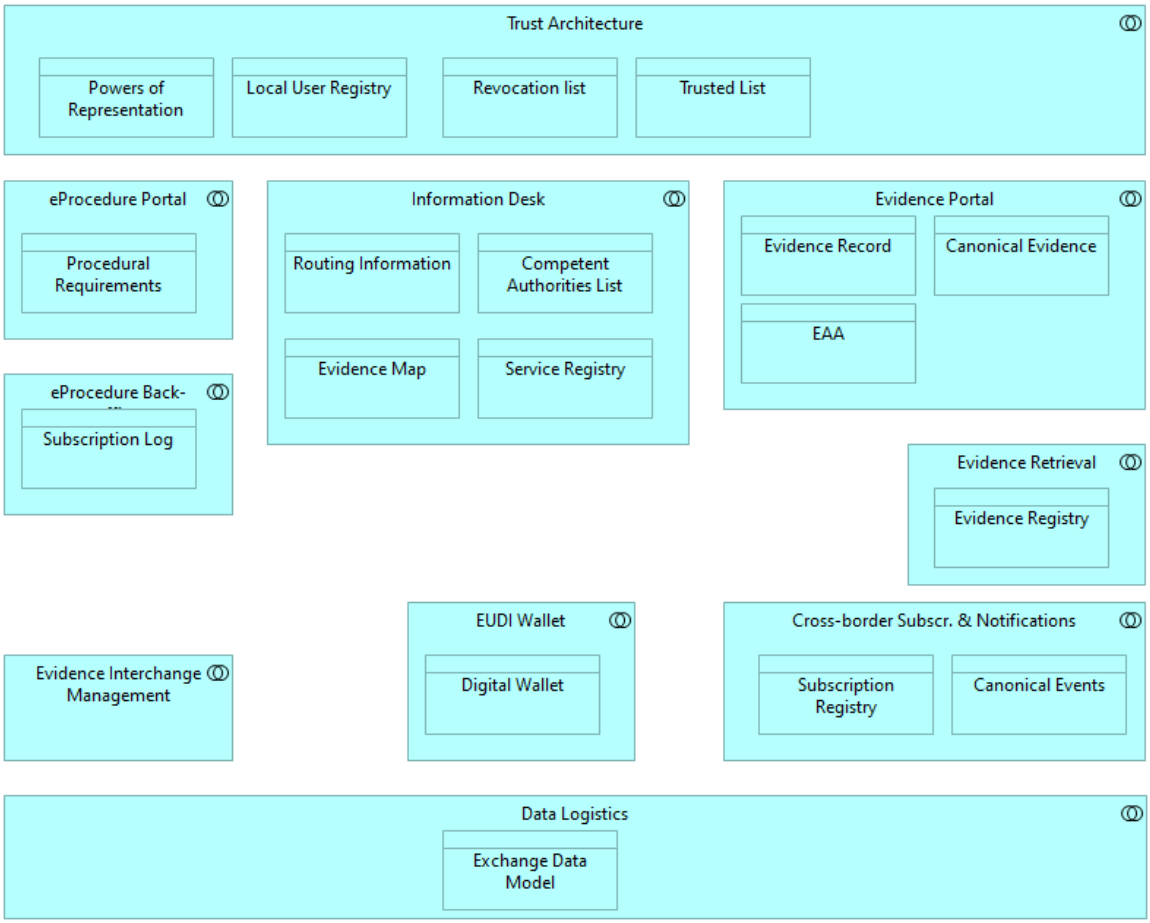


Figure 8: High-level Target Architecture

The table below provides a short description of the main data objects and points to implementations thereof.

Table 2: Main Data Objects Target Architecture

Data Object	Details
Trust Architecture	
Powers of Representation	This represents the information needed for natural persons to represent natural and legal persons as well as the degree to which they can represent, i.e. the assigned powers.
Local User Registry	This embodies the national (e.g. population register) and local registries of users and their IDs. This information is used in the record-matching process (see Annex 1).
Revocation List	This represents for example a certificate revocation list, i.e. a list of untrustworthy digital certificates or revoked attestations (e.g. a list of revoked diplomas, driving licenses etc.)
Trust List	This reflects the various trusted lists of qualified trust service providers..
eProcedure Portal	
Procedural Requirements	A collection of requirements per eProcedure that must be met. From this the need for specific evidence is derived.
eProcedure Back-office	
Subscription Log	This reflects a store where own subscriptions are recorded at the subscriber upon receiving confirmation. It serves as an overview for all active subscriptions.
Information Desk	
Routing Information	This represents routing information of: • The competent authority that can provide the required evidence / the (Q)EAA provider • The data service provided by that competent authority • The technical address(es) needed (cf. DSD [3])
Competent Authorities List	Embodies a list of competent authorities in their role as DC / Relying Party per evidence type. This is used to check if a competent authority can rightfully request a specific type of evidence. In case of requesting a subscription, it is used to verify that the competent authority is allowed to subscribe. This Data Object is not included in the first version of the OOTS [3]. In the DE4A pilots, this is conceptualized as the Cross-border Access Authorization Registry (CAAR). In the EUDI-Wallet Architecture [16] this could take the form of a registry of Relying Parties.
Evidence Map	Represents a mapping between evidence types in the different Member States. Required to identify the correct non-harmonized or especially unstructured evidence.

Data Object	Details
	The SDG OOTS v1 [3] will compile the rule base of the Evidence Broker as a first implementation.
Service Registry	Contains a list of all data services and addresses. It is used to create the routing information.
Multilingual Ontology Repository	Provides the semantics and syntax of canonical evidence types, additional parameters of provisions, and code lists used. The aim is to provide a common understanding of each canonical evidence type and multilingual graphical user interfaces for the explicit request, evidence preview and additional parameters functionalities. The Semantic repository of the first version of the OOTS [3] is a step towards the MOR, however, not yet including (legally valid) multilingual labels for all attributes.
EUDI-Wallet	
Digital Wallet	This encompasses: • The EUDI (PID) • Attributes representing the Evidences • PoR Forthcoming extension of the W3C Verifiable Credentials are expected to be able to support above 3 elements [24].
Evidence Portal	
Evidence Record	The single record of an evidence in domestic format, retrieved from a national registry.
Canonical Evidence	Domestic evidence can be transformed to canonical form. Canonical Evidence is the canonical form of domestic evidence according to a common data structure and format.
(Q)EAA	(Q)EAA are considered a special form of Canonical Evidence that conform to an EAA schema.
Evidence Retrieval	
Evidence Registry	This is the domestic registry that contains evidence. From this evidence can be fetched.
Cross-border Subscriptions and Notifications	
Subscription Registry	This represents the active subscriptions as recorded by the competent authority that sends the notifications.
Canonical Events	Business or Life Events defined in a harmonized way on European level. So only the event and its semantics, not the data definitions used to identify or document the event on national level.
Data Logistics	
Exchange Data Model	The Exchange Data model describes message format and payload specification of the messages to be exchanged between competent authorities.

5.3 Application Flows per Interaction Pattern

The diagrams in the subsequent sections are all based on Figure 7. Per pattern the most important flows that take place between the application collaborations are drawn. The flows are numbered for the sake of reference in the text and in general following the sequence in time. For reasons of simplification the technical acknowledgements are not drawn, the reader can assume however that flows have acknowledgements to confirm successful communication or determination of error situations.

5.3.1 Intermediation Pattern

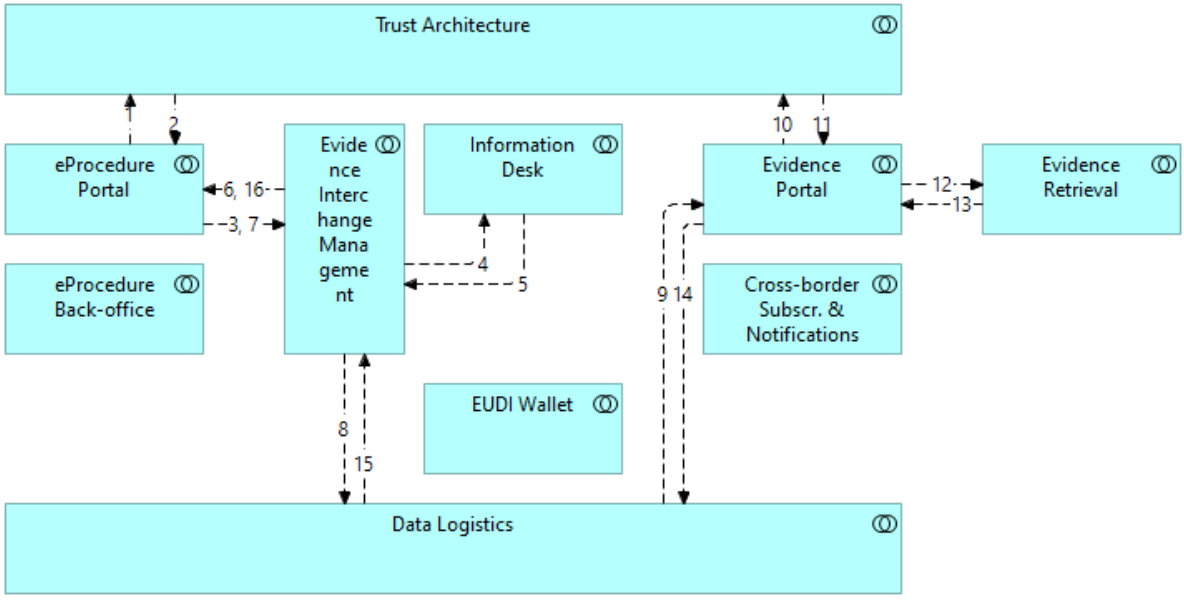


Figure 9: IM Application Architecture

The User requests (or resumes) a public service via the eProcedure Portal. Authentication and record matching takes place through the Trust Architecture (1) and (2). Alternatively, the identification function of the EUDI-Wallet could be used for the authentication, once it is available.

The required cross-border evidence is determined, and the relevant routing information is looked up via Evidence Interchange Management (3) which queries the Information Desk (4). The IDK returns the requested evidence type and routing information (5) to Evidence Interchange Management which returns it to the eProcedure Portal (6) for the explicit user request.

The Evidence is requested via Evidence Interchange Management (7) which uses Data Logistics (8) to send a cross-border evidence request. This request is forwarded to the Evidence Portal (9). Again, record matching takes place using the Trust Architecture (10) and (11).

The Evidence is looked up using Evidence Retrieval (12) and returned to the Evidence Portal (13). Evidence Portal sends the response using Data Logistics (14) which forwards it to Evidence Interchange Management (15). The Preview is prepared and after approval by the user, the Evidence is forwarded to the eProcedure Portal (16).

5.3.2 User-supported Intermediation Pattern

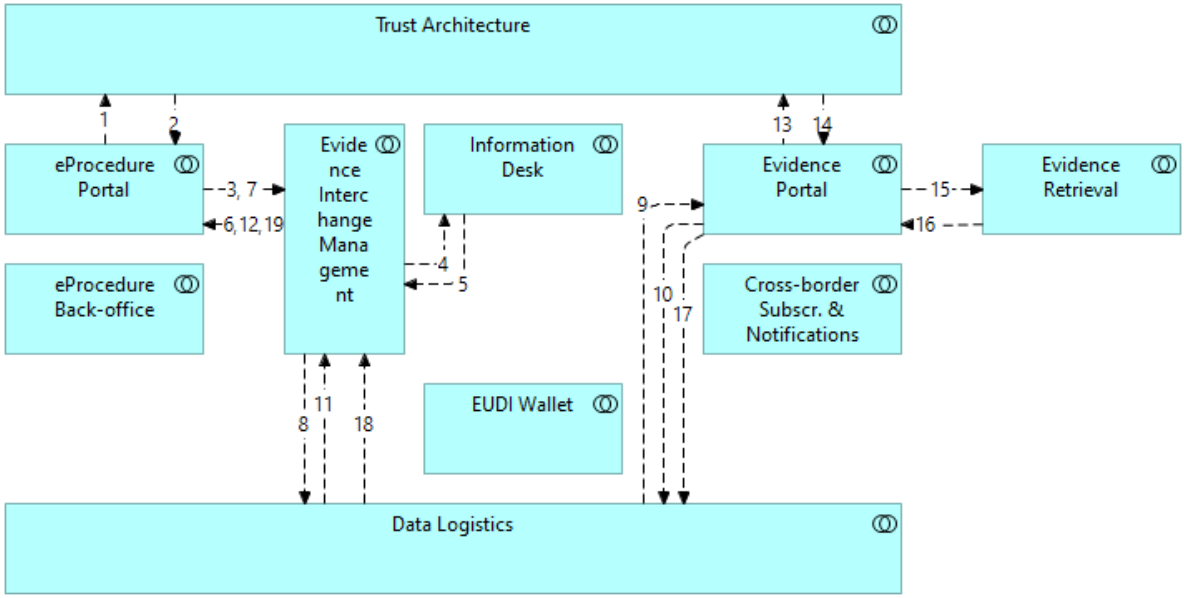


Figure 10: USI Application Architecture

The User requests (or resumes) a public service via the eProcedure Portal. Authentication and record matching takes place through the Trust Architecture (1) and (2). Alternatively, the identification function of the EUDI-Wallet could be used for the authentication, once it is available.

The required cross-border evidence is determined, and the relevant routing information is looked up via Evidence Interchange Management (3) which queries the Information Desk (4). The IDK returns the requested evidence type and routing information (5) to Evidence Interchange Management which returns is to the eProcedure Portal (6) for the explicit user request.

The Evidence is requested via Evidence Interchange Management (7) which uses Data Logistics (8) to send a cross-border evidence request, which includes the return URL, leading back to the user session of the eProcedure Portal. This request is forwarded to the Evidence Portal (9).

The Evidence Portal sends a response containing the URL to redirect the user to the Evidence Portal (10) using Data Logistics which forwards it to Evidence Interchange Management (11). The response arrives at the eProcedure Portal (12), and the user is forwarded to the Evidence Portal using the received redirect URL. From this point onwards, the user interacts directly with the Evidence Portal.

Authentication and record matching take place through the Trust Architecture (13) and (14). Alternatively, the identification function of the EUDI-Wallet could be used for the authentication, once it is available. The Evidence is looked up using Evidence Retrieval (15) and returned to the Evidence Portal (16). The Preview is prepared and after approval by the user, the Evidence Portal sends the response using Data Logistics (17) which forwards it to Evidence Interchange Management (18). The Evidence arrives at the eProcedure Portal (19). In parallel, the return URL is used to facilitate the navigation of the user back to the eProcedure Portal.

5.3.3 Subscription

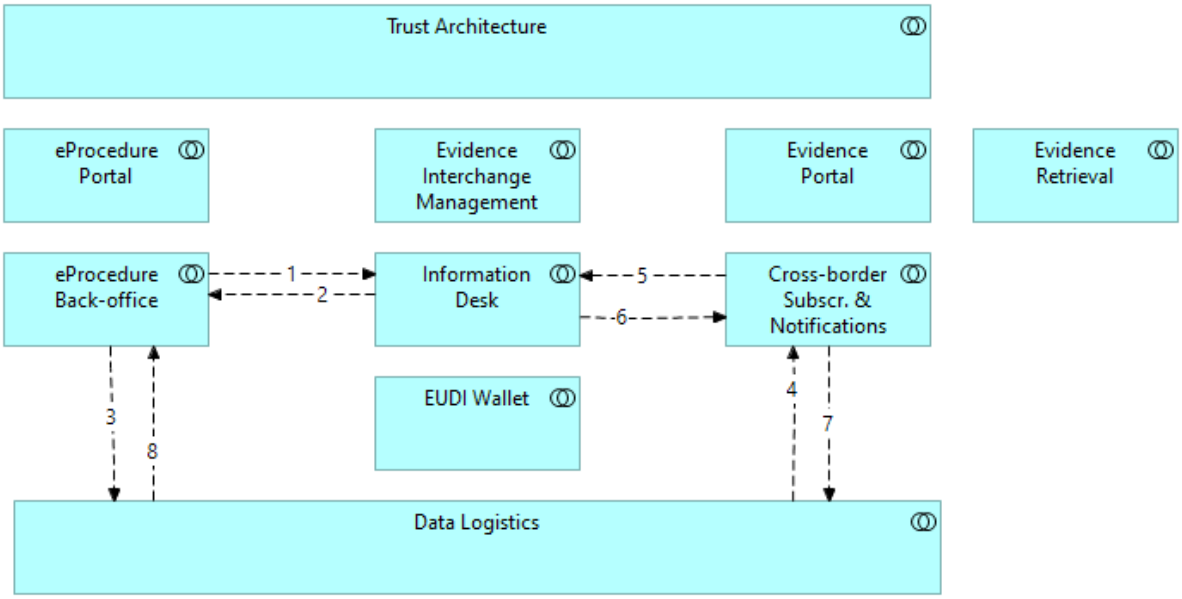


Figure 11: Subscription Application Architecture

A subscription is initiated (or changed) by eProcedure Back-office. The routing information of the event provider is looked up using the Information Desk (1). This is the routing information of the competent authority that facilitates the subscription service. The IDK returns it to the eProcedure Back-office (2).

A subscription request is sent by the eProcedure Back-office using Data Logistics (3) which forwards it to cross-border Subscriptions & Notifications (4). The Information Desk is queried to establish that the authority requesting the subscription is allowed to do so (5). The outcome is returned by the IDK (6).

Cross-border Subscriptions & Notifications validates and registers the subscription after which a confirmation is sent using Data Logistics (7). This in turn forwards it to eProcedure Back-office (8) where a record of active subscriptions is maintained.

5.3.4 Notification

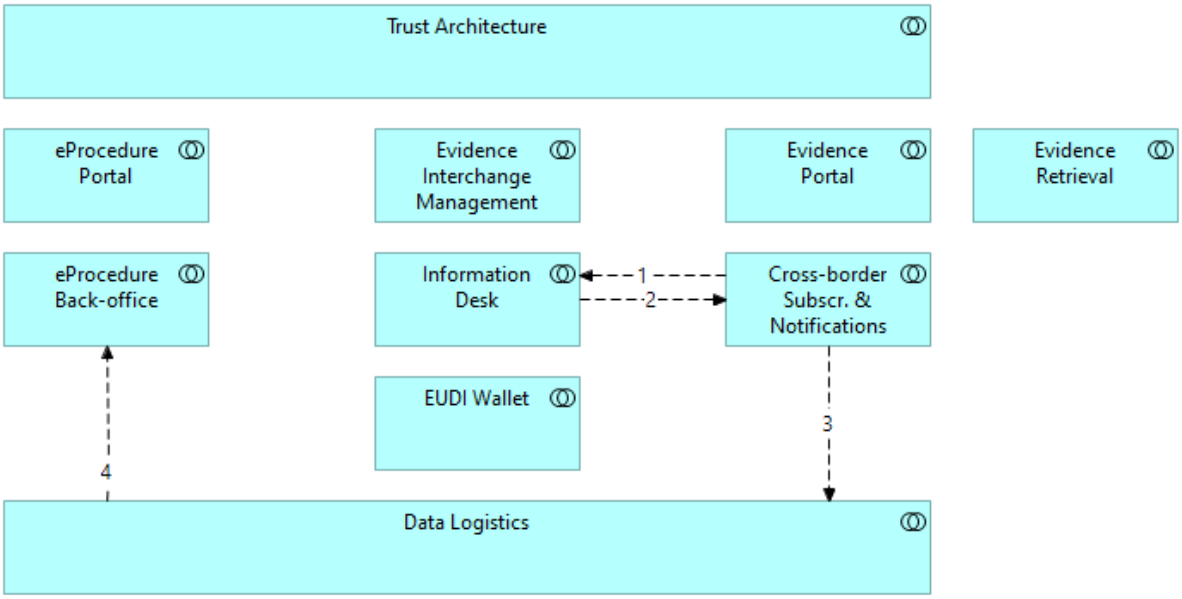


Figure 12: Notification Application Architecture

Cross-border Subscriptions & Notifications identifies a cross-border event for which there is an active subscription. The routing information is looked up using the Information Desk (1) and returned (2). It sends a notification message using Data Logistics (3) which forwards it to eProcedure Back-office (4). At the eProcedure Back-office it is determined how to react to the event, e.g. do nothing or follow it up. In case of problems with receiving or processing events a request to resend events can be submitted. This is a manual process at Cross-border Subscriptions & Notifications.

5.3.5 Lookup Pattern

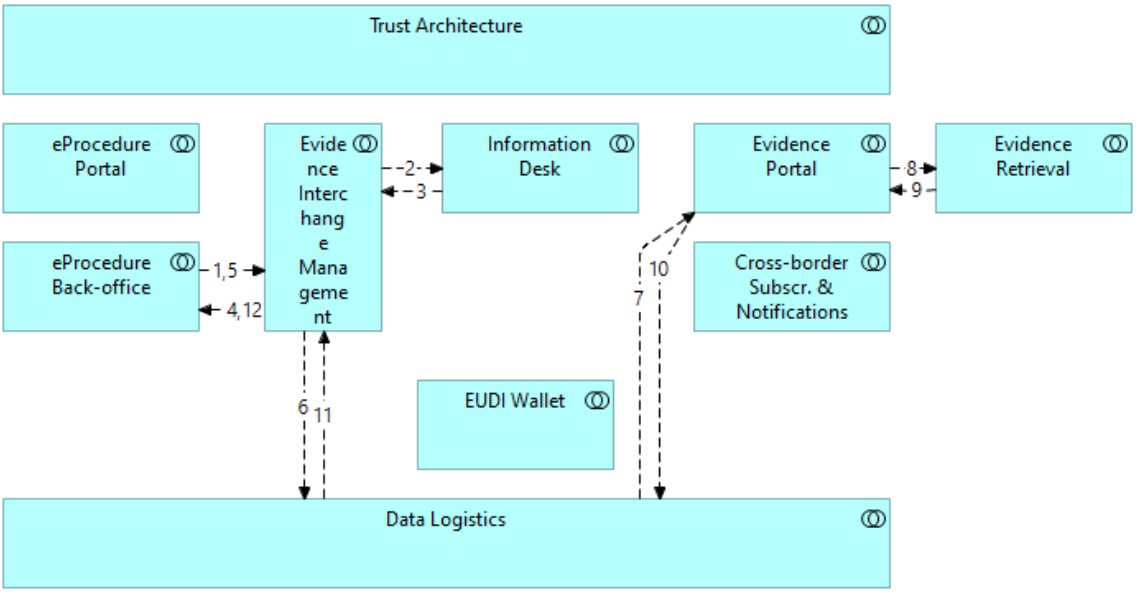


Figure 13: Lookup Application Architecture

The need for an evidence or update thereof is identified in the eProcedure Back-office. The routing information is obtained through Evidence Interchange Management (1) which queries the Information Desk (2). The IDK returns the routing information (3) which is forwarded to eProcedure Back-office (4).

eProcedure Back-office performs a lookup of the evidence via Evidence Interchange Management (5) which uses Data Logistic (6), which in turn sends the evidence request to Evidence Portal (7).

Evidence Portal fetches the requested Evidence using Evidence Retrieval (8) & (9) and returns the Evidence response to eProcedure Back-office travelling the reverse flow: Data Logistics (10), Evidence Interchange Management (11) and finally eProcedure Back-office (12).

5.3.6 Push Pattern

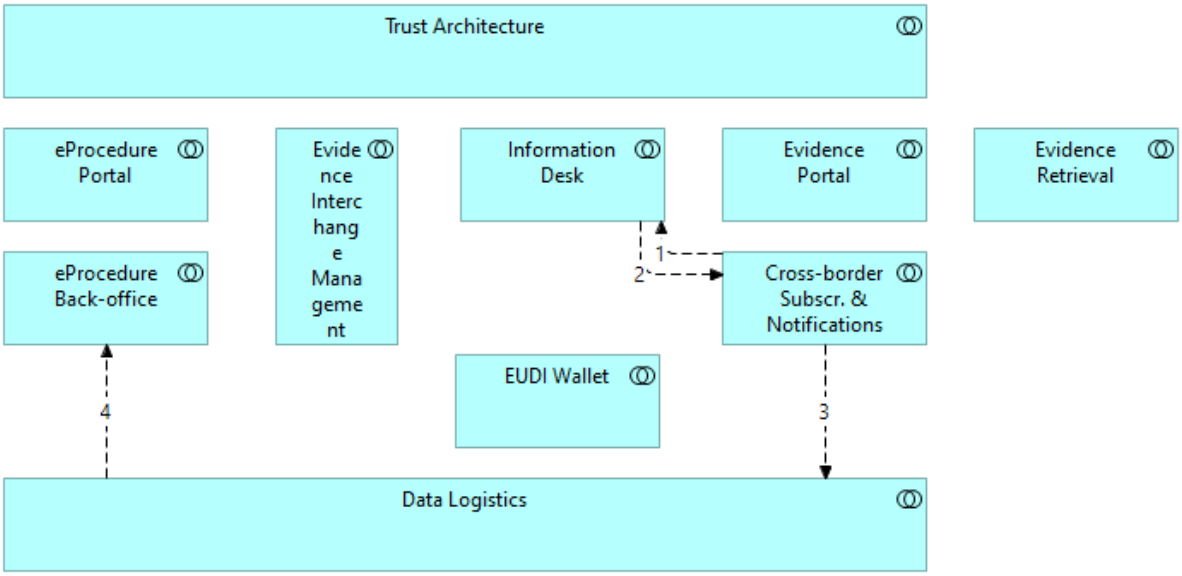


Figure 14: Push Application Architecture

From a business perspective this is in essence a Notification without a Subscription, however the Push relations need to be pre-established, i.e. based on a previous exchange in the opposite direction as described in 4.2.5. Cross-border Subscriptions & Notifications is used to send notification(s).

As discussed before there are two flavours of this pattern. Here we focus on the first flavour, i.e. triggered by the user in course of a public service encounter, and consider the second flavour, i.e. triggered by the public authority without any user interaction out of scope. DC, DP and user are all known at this point.

First, the routing information of the target DC is looked up by the DP using the Information Desk (1). The IDK returns the technical address to send the notification to. Next, Cross-border Subscriptions & Notifications uses Data Logistics (3) to send the notification. This in turn forwards it to the relevant eProcedure Back-office (4) of the DC.

5.3.7 Supported User-managed Access Pattern

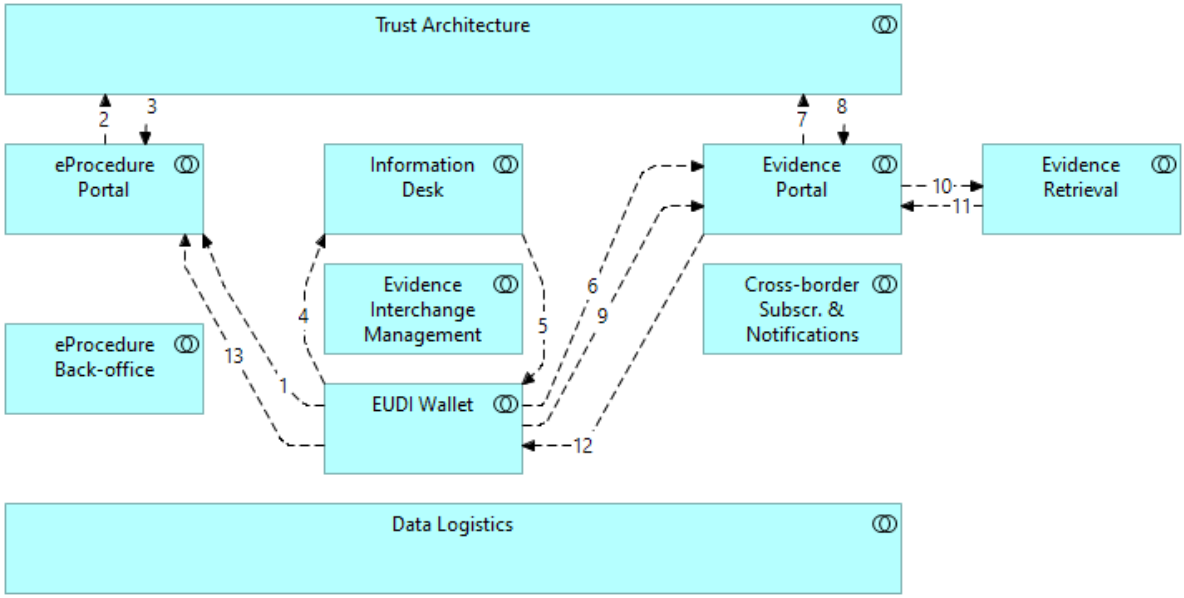


Figure 15: Supported User-managed Access Application Architecture

As explained in 4.2.6 there are various flows possible. To stay in line with the flows of the IM and USI pattern, we assume there that the required Electronic Attribute Attestation is not yet available at the Wallet and that the user starts the process at the eProcedure Portal, there they authenticate with EUID, using the EUDI-Wallet (1)[1]. This triggers record matching using the Trust Architecture (2) and (3). The user learns which evidences they need and uses the lookup function of the Wallet to inquire the right attribute provider from the Information Desk (IDK) (4). The IDK responds with the URL (5) of the competent authority where the evidence as (Q)EAA can be obtained.

Next the user authenticates with the EUDI-Wallet (6) at the Evidence Portal. This triggers the record matching (7) and (8) using the Trust Architecture.

After establishing the identity of the user, they can request a (Q)EAA (9) from the Evidence Portal. The requested evidence is looked up in Evidence Retrieval (10) and is provided back to the Evidence Portal (11) which takes care of the transformation into the (Q)EAA schema. This (Q)EAA is returned to the user's wallet where it can be accepted or rejected (12). Assuming the user accepts the (Q)EAA, it can now be provided to the eProcedure Portal (13).

Technical implementation options

The interactions with the EUDI-Wallet can be based on several implementation options considering their architectural backgrounds and technical details. At the time of writing the technology choice for the EUDI-Wallet is yet to be taken. We discuss below several options that essentially leave above explained high-level application flow unchanged.

[1] The possibility to authenticate using notified eID means and the eIDAS network to bootstrap a Decentral Identifier was piloted in using the Verifiable Credential pattern in the DE4A Studying Abroad pilot. This effectively showed the potential to use blockchain technology and SSI concepts in a public service context requiring strong identification, based on eIDAS1[21] and EBSI [14] prior to the concept of an EUDI-Wallet. In the 2025+ time horizon of this target architecture, given the existence of an EUDI-Wallet that combines the identification function with the possibility to present (Q)EAA, the use of a different identification means in combination with the (Q)EAA-functionality is considered to make not much sense.

These implementation options can be divided into four main layers, i.e. (1) identity, (2) authentication, (3) communication, and (4) data layer:

The first layer deals with the identity of the EUDI-Wallet user, which in the sense of the Supported User-managed Access Pattern is the user who is interacting with the eProcedure and the Evidence portals. The identity of the user can be dealt with in two ways, i.e. the legacy-based eID (and eIDAS) or based on decentralized identifiers (DIDs). If the latter are used, the user as the natural person cannot be identified per se, since due to privacy concerns the DID documents are not stored on a publicly accessible endpoint – in the case of DIDs these are naturally publicly available distributed ledgers.

The second layer is the authentication layer, which again can be different based on the first layer implementation choice and based on the verification process used. The authentication can thus be implemented using classical enterprise related SAML protocols or the more novel OpenID Connect (OIDC) protocol, depending on the assurance level required by the process. The former enables higher assurance levels, while the latter lesser. But these options are not the only ones. Should DIDs be used within the first layer, the authentication could thus be dependent on DID documents and/or Verifiable IDs. The former can be enough if the user is a legal entity and their DID documents are thus stored and accessible on a publicly available ledger (i.e. DID registries and possibly other types of registries, as mentioned in the Trust Architecture). The DID documents of legal entities can, beside public keys, hold also other identifiable legal information of the user. However, should the user be a natural person, the authentication process will have to be supported with Verifiable IDs (VID), which are QEAA in the form of Verifiable Credentials (VC), issued by qualified identity providers (QIdP). Nevertheless, it should be noted that implementation options of layer 2 are not necessarily bound to Layer 1 choices.

The third layer is the communication layer, which has two implementation options, i.e. the classical SOAP over HTTP/S based communication, where request and responses are the basis for the communication, while the other option is DID-Communication (DIDComm), which represents a bidirectional channel of communication between two entities that know each other's DIDs.

The last layer is the data layer, which represents the format in which the data is being exchanged between the two parties. In most cases this is XML based on pre-defined XML schemas and aligned with the SOAP/WSDL structures. It is more aligned with the current enterprise-level systems. However, the likely de-facto data format of the future will be the VC in the JSON format, which in itself is more aligned with current novel ICT concepts such as REST, micro-services, etc. The VC itself is a W3C recommendation and can hold many document data types, like the QEAA or others.

The matrix of implementation solutions is not firmly defined, since multiple choices based on the layer options are possible, whereby the probably the most convenient option for now is the combination of eIDs, SAML or OIDC and VC.

6 Conclusions

This document provides architectural advice for the implementation of European public service interoperability solutions in light of the SDGR with a mid-term future time horizon in mind of 2025+.

Together with MS representatives and WP leaders and architects a set of high-level functional requirements was defined in terms of interaction patterns needed, use cases to be supported, and certain aspects of the interdisciplinary questions [4] deemed important. The second requirement base is drawn from the main working hypothesis that the target architecture will build on the OOTS and incorporates the EUDI-Wallet as per the currently ongoing eIDAS revision.

The architecture description shows that different required exchange processes can be projected on a conclusive high-level application architecture with a maximum of reuse, providing a solid basis for the notion of a multi-pattern interoperability architecture consisting of 6 interaction patterns. The target architecture was decomposed in 10 application collaborations jointly providing all functionality for all patterns.

We were able to show that the infrastructure of the Once Only Technical System, designed for the interaction pattern that DE4A calls the User-supported Intermediation Pattern (4.2.2 and 5.3.2) can be leveraged mostly unchanged to support the Intermediation (4.2.1 and 5.3.1) and Lookup patterns (4.2.3 and 5.3.5). With the addition of a Cross-border Subscriptions and Notifications system and an inclusion of an active subscriptions log functionality to the eProcedure Back-office, the Subscription & Notification pattern (4.2.4, 5.3.3 and 5.3.4) and the Push pattern (4.2.5 and 5.3.6) can be supported by the multi-pattern architecture. This means that the OOTS infrastructure can be extended with additional use-cases and requirements beyond the direct context of an eProcedure with relative ease. This should be kept in mind for future interoperability initiatives to leverage the investments made on European and Member State level. Rather than implementing new, separate systems for each new use case, future regulations should explicitly recognize the existence of the multi-sectoral infrastructure and contribute to its stepwise extension to support new patterns. The deliverable does not expand into the need for a European-level governance to steer such a cross-sectoral, long-term development.

In addition, the target architecture description includes a user-centric interaction pattern, the Supported User-Managed Access Pattern (4.2.6 and 5.3.7) which makes use of the EUDI-Wallet. With the ongoing specification of the Wallet, we looked into different implementation choices and assumed a wallet concept that does not use a Self-sovereign Identity (SSI) approach. Though an SSI approach would be technical viable, as shown in one of the DE4A pilots, the ongoing work on the EUDI-Wallet Toolbox shows some level of scepticism towards the maturity of the SSI-approach. Most findings and identified synergies are independent of this choice.

The user-centric approach of the wallet means that the message-based data logistic of the other patterns is not reused. However, other functionalities of the Trust Architecture, i.e. record matching, the Evidence Portal and the Information Desk could be easily expanded for the use of the wallet. This means that the function of the Information Desk to identify the right data service of an Evidence Provider, provided by the Data Service Directory on the first version of the OOTS, could also be used to support the user in identifying and subsequently contacting the right provider of (Qualified) Electronic Attestation of Attribute ((Q)EAA) directly from their wallet.

Some Member States raised concerns that the OOTS and the EUDI-Wallet show a significant functional overlap and questioned whether the value of choice for the citizen would warrant the double investment. It is beyond the scope of this paper to provide advice in this policy question or judgment on the societal value and administrative cost. What the multi-pattern architecture shows, however, is

that the Wallet-based Supported User-managed Access Pattern can only carry transactions based on direct user involvement and full user control. Contrastingly, the User-Supported Intermediation Pattern, i.e. the OOTS version 1, shows a great potential in creating an infrastructure that enables, given the right legal basis, the exchange between competent authorities without user involvement, i.e. the Lookup, Subscription & Notification and Push patterns. This would allow the creation of a more seamless user experience including cross-border pro-active public services, similarly to the situation that we grew accustomed to on the national level in some Member States.

In particular, for the Lookup, Subscription & Notification and Push patterns, there is a need to include an authorisation check to control whether a Data Consumer is allowed to request the information. This requires the extension of the Information Desk functionality and provides a potential synergy with the EUDI-Wallet, where the need for a registry, or registries of Relying Parties is discussed.

On a more detailed level, we find that some remaining challenges exist that need further consideration. First, the question of cross-border representation of Powers of Representation (PoR) both between natural persons and for natural persons representing a legal person needs further investigation. What becomes apparent from the flows is that PoR, though not strictly part of the authentication function, is closely related to it. The advice is to resolve questions of PoR always in direct context of the authentication function. This could for example be picked up in context of the eIDAS revision.

Second, identity and record matching currently remains a MS specific challenge. We expect that the eIDAS revision will bring some improvements to this topic, however, an automated 100% match scenario is and will most likely remain unattainable in the foreseeable future.

Summing it all up, the multi-pattern architecture, based on the first version of the Once-Only Technical System, has the potential to support additional interactions that are required to enable a more seamless and pro-active cross-border eGovernment interoperability. The inclusion of the EUDI-Wallet can lead to a simplification of exchange under direct user control and is able to reuse parts of the overall architecture.

Two important prerequisites for the OOTS to evolve into the multi-pattern target architecture are: First, the creation of a cross-sectoral European governance to guide sector-specific requirements, e.g. stemming from new Directives, towards implementation in a common infrastructure. Second, the creation of adequate legal basis for cross-border exchange without direct user involvement, either in Union law or, based on bi-lateral agreements, in national law.

References

[1] ArchiMate® Standard, Version 3.1, The Open Group

[2] Business Process Model and Notation (BPMN), Version 2.0, Object Management Group

[3] COMMISSION IMPLEMENTING REGULATION (EU) /... setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the "once-only" principle in accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council; C/2022/5628 final; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282022%295628&qid=1658925262468

[4] DE4A Deliverable D2.1 Architecture Framework, submitted 01.04.2020, can be consulted via https://www.de4a.eu/project-deliverables

[5] DE4A Deliverable D2.3 Final DE4A Trust Management Models and Blockchain Support Framework, can be consulted via https://www.de4a.eu/project-deliverables

[6] DE4A Deliverable D2.5 Project Start Architecture (PSA), second iteration, can be consulted via https://www.de4a.eu/project-deliverables

[7] DE4A Deliverable D4.1 Studying Abroad - Use Case Definition & Requirements, can be consulted via https://www.de4a.eu/project-deliverables

[8] DE4A Deliverable D4.10 Moving Abroad - Pilot Planning, can be consulted via https://www.de4a.eu/project-deliverables

[9] DE4A Deliverable D4.2 Studying Abroad - Pilot Planning, can be consulted via https://www.de4a.eu/project-deliverables

[10] DE4A Deliverable D4.5 Doing Business Abroad - Use cases definition and requirements, can be consulted via https://www.de4a.eu/project-deliverables

[11] DE4A Deliverable D4.6 Doing Business Abroad - Pilot Planning, can be consulted via https://www.de4a.eu/project-deliverables

[12] DE4A Deliverable D4.9 Moving Abroad - Use cases definition and requirements, can be consulted via https://www.de4a.eu/project-deliverables

[13] Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law; 30.6.2017; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L1132

[14] European Blockchain Services Infrastructure (EBSI) ; https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi

[15] European Declaration on Digital Rights and Principles for the Digital Decade, COM(2022) 28 final, 27 January 2022; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022DC0028&from=EN

[16] European Digital Identity Architecture and Reference Framework; 22 February 2022

[17] European Digital Identity | European Commission (europa.eu)

[18] European Parliament and the Council, "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", https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1724&from=EN, retrieved on June 8, 2021.

[19] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, 03/06/2021, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A281%3AFIN

[20] 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), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[21] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1990/93/EC (eIDAS Regulation) EUR-Lex - 32014R0910 - EN - EUR-Lex (europa.eu)

[22] Single Digital Gateway Regulation, Once-Only Technical System, EUCARIS OOTS Non-Paper, Version [1.0]; file: (EUCARIS OOTS Non-Paper)(1.0 final).pdf

[23] The Once-Only Principle Project (TOOP) https://toop.eu/

[24] W3C Verifiable Credentials, https://www.w3.org/TR/vc-data-model/

[25] SEMPER - Crossborder Semantic Interoperability of Powers and Mandates (https://www.a-sit.at/en/semper/)

Annexes

Annex I – Record Matching

A very important generic functionality used in all interaction patterns and in some patterns even twice (DC and DP side).

Record Matching tries to match the identity of the user in some national or local system, i.e. a national ID or some local ID, with the identity received as part of the eIDAS or Wallet authentication.

Example: Dutch natural person using eIDAS, e.g. USI after redirect

In case of eIDAS the "eIDAS uniqueness ID" and the mandatory eIDAS attributes are received as part of the authentication. For natural persons these mandatory attributes consist of FamilyName, FirstName and DateOfBirth.

Every MS implements the eIDAS uniqueness ID differently, in some cases it's a hash of some national ID, here for instance NL/ES/123243g13fa$!agqf1, or even a national unique ID. Linking this ID, originating in the DC country, to some national/local ID of the DP under which the Evidence is registered is a challenge. This matching can take place based on the received information from the request message, i.e., the mandatory eIDAS attributes. It turns out that this is not always enough to uniquely identify a person leading to false positives. It would be more than embarrassing to exchange the wrong Evidence belonging to another person!

Possible solutions include to extend the set of mandatory attributes, use the optional attributes or even let the user supply attributes. For instance, adding the place of birth can improve the probability of a unique match, but it still is not 100%.

In case of the Wallet the problem remains, and the solution is similar.