D2.5 Project Start Architectures (PSA), second iteration

Document Identification			
Status	Final	**Due Date**	30/06/2021
Version	1.0	**Submission Date**	31/07/2021

Related WP	WP2, WP3, WP5	**Document Reference**	D2.5
Related Deliverable(s)	D2.1, D2.4	**Dissemination Level (*)**	PU
Lead Participant	MinBZK/ICTU	**Lead Author**	Harold Metselaar (MinBZK/ICTU)
Contributors	Alexander Bielowski, Mavi Cristache (MinBZK/ICTU), Tomaž Klobucar (JSI), Ivar Vennekens, Bart van Bekkum (RVO), Patrick Öberg (SKV), Hans Graux (TimeLex), Malin Norlander (BVE)	**Reviewers**	Alberto Crespo (ATOS) Carl-Markus Piswanger (BMDW)

Keywords:
Project Start Architecture, PSA, Reference Architecture, Once-Only Technical System, Interaction Patterns, ABB, Intermediation, User-supported Intermediation, Verifiable Credential, Subscription and Notification, Lookup, API, Interdisciplinary

This document is issued within the frame and for the purpose of the DE4A project. This project has received funding from the European Union's Horizon2020 Framework Programme under Grant Agreement No. 870635 The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

The dissemination of this document reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains. **This deliverable is subject to final acceptance by the European Commission.**

This document and its content are the property of the DE4A Consortium. The content of all or parts of this document can be used and distributed provided that the DE4A project and the document are properly referenced.

Each DE4A Partner may use this document in conformity with the DE4A Consortium Grant Agreement provisions.

(*) Dissemination level: PU: Public, fully open, e.g. web; CO: Confidential, restricted under conditions set out in Model Grant Agreement; CI: Classified, Int = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

Document Information

List of Contributors	
Name	Partner
Alexander Bielowski	MinBZK/ICTU
Harold Metselaar	MinBZK/ICTU
Mavi Cristache	MinBZK/ICTU
Tomaž Klobucar	JSI
Ivar Vennekens	RVO
Patrick Öberg	Skatteverket
Hans Graux	TimeLex
Malin Norlander	Bolagsverket (BVE)
Bart van Bekkum	RVO

Document History			
Version	Date	Change editors	Changes
0.0	01/11/2020	Alexander Bielowski, Harold Metselaar, Mavi Cristache	PSA 2nd iteration Table of Contents
0.05	01/04/2021	Alexander Bielowski, Harold Metselaar, Mavi Cristache	Consolidation of PSA on wiki
0.1	20/04/2021	Mavi Cristache	Start of migration of PSA content from wiki to deliverable document
0.11	20/04/2021	Mavi Cristache	• Added Wiki links • Added contribution to DBA chapter from RVO
0.12	7/06/2021	Harold Metselaar	• Moved Lookup section to Wiki • Added new collaborations for Subscription/Notification pattern
0.13	15/06/2021	Mavi Cristache	• Added contribution to SA chapter from JSI • Added contribution to MA chapter from Skatteverket • Added wiki links in Reference Application Architecture
0.2	29/06/2021	Mavi Cristache	Migration of patterns and application architecture from wiki to document

© 870635 DE4A Project Partners

Document History			
Version	Date	Change editors	Changes
0.3	30/06/2021	Alexander Bielowski, Harold Metselaar	Added introduction (chapter 1)
0.4	01/07/2021	Alexander Bielowski, Harold Metselaar	• Added background (chapter 2) • Added draft conclusion (chapter 6)
0.5	05/07/2021	Harold Metselaar	• Added introductions to chapters 3 and 4 • Editorial, typos, cross-references etc.
0.6	06/07/2021	Alexander Bielowski, Harold Metselaar, Mavi Cristache	• Completion of Conclusions (chapter 6) • Review and editing
0.7	07/07/2021	Alexander Bielowski, Harold Metselaar, Mavi Cristache	• Adding Annexes • Review and editing
0.8	08/07/2021	Alexander Bielowski, Harold Metselaar, Mavi Cristache	• Review and editorial • Executive Summary
0.9	14/07/2021, 21/07/2021	Carl-Markus Piswanger, Alberto Crespo	Internal review
0.91	21/07/2021-27/07/2021	Harold Metselaar, Mavi Cristache	• Incorporating feedback internal review • Version for QA
0.92	29/07/2021	Harold Metselaar	• Incorporating feedback • Closing final comments
0.93	30/07/2021	Mavi Cristache	Version for submission
1.0	30/07/2021	Atos	Final QA for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Alexander Bielowski (MinBZK/ICTU)	30/07/2021
Quality manager	Julia Wells (ATOS)	30/07/2021
Project Coordinator -acting	Alberto Crespo (ATOS)	30/07/2021

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*).

© 870635 DE4A Project Partners

Table of Contents

List of Tables 7
List of Figures 9
List of Annexes 11
List of Acronyms 12
Executive Summary 15
1. Introduction 17
1.1. Purpose of the Document 17
1.2. Structure of the Document 18
1.3. Relation to other DE4A Deliverables 18
2. Background 20
2.1. Functional Scope of the DE4A Pilots 20
2.2. Relation to the Once-Only Technical System 21
2.3. Interdisciplinary Questions 24
2.3.1. Orchestration / Choreography 24
2.3.2. Complementary, Overlapping or Conflicting Evidence Equivalents 24
2.3.3. Interrupted vs. Uninterrupted Exchange 25
2.3.4. Explicit Request and Transitivity Between Actors 25
2.3.5. Preview & Approval UI 25
2.3.6. Identity and Record Matching 26
2.3.7. Transitivity of User Identity 26
2.3.8. Hand-over of User Interface Between Actors 26
2.3.9. Mandate and Proxy 26
2.3.10. Encryption Gap 27
2.3.11. Structured Data vs. Unstructured Data 27
2.3.12. Automated Re-use of Data 27
2.3.13. Production System and Real-life Cases 28
2.3.14. EESSI Integration 28
2.3.15. BRIS Integration 28
2.3.16. eIDAS and National Authentication Systems 29
2.3.17. Non-notified eIDs 29
2.3.18. Payment for Evidence 29
2.3.19. Trust Management 29
2.3.20. Legal Basis for SSI and Block Chain Technology 30
2.3.21. Explicit Scope of Article14 30
2.3.22. Matching Evidences between Member States 30
2.3.23. Multi-evidence Cases 31
2.3.24. Stateless DE4A Connector 33

© 870635 DE4A Project Partners

2.3.25. Highly Distributed, Cross-border System 33
3. Reference Business Architecture 35
3.1. Intermediation Pattern 36
3.1.1. Working Hypotheses and Implementation Principles 36
3.1.2. Business Process Collaboration 42
3.1.3. Process Realization 50
3.2. User-supported Intermediation Pattern 54
3.2.1. Working Hypotheses and Implementation Principles 54
3.2.2. Business Process Collaboration 58
3.2.3. Process Realization 68
3.3. Verifiable Credentials Pattern 72
3.3.1. Working Hypotheses and Implementation Principles 72
3.3.2. Business Process Collaboration 75
3.3.3. Process Realization 86
3.4. Subscription and Notification Pattern 90
3.4.1. Functional Variants of the Subscription and Notification Pattern 90
3.4.2. Working Hypotheses and Implementation Principles 92
3.4.3. Legal Considerations 94
3.4.4. Business Process of the Event Subscription and Notification Pattern 95
3.4.5. Process Realization 105
3.5. Lookup Pattern 113
3.5.1. Functional Variants of the Lookup Pattern 113
3.5.2. Working Hypotheses and Implementation Principles 114
3.5.3. Legal Considerations 117
3.5.4. Business Process of the Evidence Lookup 117
3.5.5. Process Realization of the Evidence Lookup 122
3.5.6. Future Extension: Attribute Lookup Using API 124
4. Reference Application Architecture 127
4.1. eProcedure Portal 127
4.2. Information Desk 135
4.3. Evidence Interchange Management 142
4.4. Trust Architecture 147
4.5. Data Logistics 153
4.6. Evidence Portal 154
4.7. Evidence Retrieval 158
4.8. Authority Agent 160
4.9. User Agent 162
4.10. Cross-border Subscriptions 164
4.11. eProcedure Back-office 167

© 870635 DE4A Project Partners

5. DE4A Pilots 169
5.1. Studying Abroad 169
5.2. Doing Business Abroad 170
5.3. Moving Abroad 172
6. Conclusions 174
References 179
Annexes 181

© 870635 DE4A Project Partners

List of Tables

Table 1 Reasons for Multi-evidence Cases 31
Table 2 Intermediation Pattern Working Hypotheses and Implementation Principles 36
Table 3 Business Activities of the Intermediation Pattern 43
Table 4 Intermediation - Conversation between User and Data Consumer 49
Table 5 Intermediation - Conversation between Data Consumer and Data Provider 50
Table 6 User-supported Intermediation Pattern Working Hypotheses and Implementation Principles 54
Table 7 Business Activities of the User-supported Intermediation Pattern 60
Table 8 User-supported Intermediation - Conversation between User and Data Consumer 66
Table 9 User-supported Intermediation - Conversation between Data Consumer and Data Provider 68
Table 10 User-supported Intermediation - Conversation between User and Data Provider 68
Table 11 Verifiable Credentials Pattern Working Hypotheses and Implementation Principles 72
Table 12 Business Activities of the Verifiable Credentials Pattern 77
Table 13 Verifiable Credentials Pattern Conversations 84
Table 14 Business Requirements for Subscription and Notification 90
Table 15 Subscription and Notification Pattern Working Hypotheses and Implementation Principles 92
Table 16 Business Activities of the Event Subscription Pattern 97
Table 17 Business Activities of the Event Notification Pattern 103
Table 18 Message Exchange of the Evidence Lookup 113
Table 19 Message Exchange of the Attribute Lookup 113
Table 20 Lookup Pattern Working Hypotheses and Implementation Principles 114
Table 21 Business Activities of the Lookup pattern 119
Table 22 Application Components of the eProcedure Portal 131
Table 23 Application Services Realized by the eProcedure Portal Front-end 132
Table 24 Application Services Realized by the eProcedure Portal Back-end 133
Table 25 Application Services Realized by the Procedure Management 133
Table 26 Application Services Realized by the eProcedure Rules Engine 133
Table 27 Application Services Realized by the Logging/Archiving 134
Table 28 Application Components of the Information Desk 138
Table 29 Application Services Realized by the Data Service Lookup 140
Table 30 Application Services Realized by the Authorization Controller 140
Table 31 Application Services of the Evidence Type Translator 141
Table 32 Application Components of the Evidence Interchange Management 145
Table 33 Application Services of the Evidence Interchange Front-end 146
Table 34 Application Services of the Evidence Interchange Back-end 146
Table 35 Application Components of the Trust Architecture 150
Table 36 Application Services Realized by the Trust Service Provisioning 151
Table 37 Application Services Realized by the Identity Management 151
Table 38 Application Services Realized by the Record Matching 151
Table 39 Application Services Realized by the Data Encryption / Decryption 152

© 870635 DE4A Project Partners

Table 40 Application Components of the Data Logistics *153*
Table 41 Application Services Realized by the Data Exchange *154*
Table 42 Application Components of the Evidence Portal *156*
Table 43 Application Services Realized by the Evidence Portal Front-end *157*
Table 44 Application Services Realized by the Evidence Portal Back-end *157*
Table 45 Application Components of the Evidence Retrieval *159*
Table 46 Application Services Realized by the Evidence Query *159*
Table 47 Application Components of the Authority Agent *160*
Table 48 Application Services Realized by the SSI Cloud Agent Back-end *161*
Table 49 Application Components of the User Agent *162*
Table 50 Application Services Realized by the SSI Edge Agent Front-end *163*
Table 51 Application Services Realized by the SSI Edge Agent Back-end *163*
Table 52 Application Components of Cross-border Subscription *165*
Table 53 Application Services Realized by the Subscription System *165*
Table 54 Application Services Realized by the Cross-border Event Handler *166*
Table 55 Application Services Realized by the Notification Front-end *166*
Table 56 Application Components of eProcedure Back-office *167*
Table 57 Application Services Realized by the eProcedure Back-office Backend *168*
Table 58 Application Services Realized by the eProcedure Back-office Front-end *168*

© 870635 DE4A Project Partners

List of Figures

Figure 1 Business Process Collaboration View of the Intermediation Pattern 42
Figure 2 Process Realization of the User Process 51
Figure 3 Process Realization of the DC Process 52
Figure 4 Process Realization of the DP Process 53
Figure 5 Business Process Collaboration View of the User-supported Intermediation Pattern 59
Figure 6 Process Realization of the User Process 69
Figure 7 Process Realization of the Data Consumer Process 70
Figure 8 Process Realization of the Data Provider Process 71
Figure 9 Business Process Collaboration View of the Verifiable Credential Pattern 76
Figure 10 Process Realization of the User Process 87
Figure 11 Process Realization of the Data Consumer Process 88
Figure 12 Process Realization of the Data Provider Process 89
Figure 13 Event Subscription Business Process Collaboration View 96
Figure 14 Business Process Collaboration View of the Notification Process 102
Figure 15 Subscription Process Realization of the Data Consumer 106
Figure 16 Subscription Process Realization of the Data Provider 108
Figure 17 Notification Process Realization of the Data Provider 110
Figure 18 Notification Process Realization of the Data Consumer 112
Figure 19 Evidence Lookup Business Process Collaboration 118
Figure 20 Process Realization of the Data Consumer 122
Figure 21 Process Realization of the Data Provider 123
Figure 22 Graphic Representation of the eProcedure Portal Application Collaboration in the IM Pattern 128
Figure 23 Graphic Representation of the eProcedure Portal Application Collaboration in the USI Pattern 129
Figure 24 Graphic Representation of the eProcedure Portal Application Collaboration in the VC Pattern 130
Figure 25 Graphic Representation of the eProcedure Portal Application Collaboration in the Lookup Pattern . 131
Figure 26 Graphic Representation of the Information Desk Application Collaboration in the IM and USI patterns 135
Figure 27 Graphic Representation of the Information Desk Application Collaboration in the VC Pattern 136
Figure 28 Graphic Representation of the Information Desk Application Collaboration in the S&N Pattern 137
Figure 29 Graphic Representation of the Information Desk Application Collaboration in the Lookup Pattern .. 137
Figure 30 Graphic Representation of the Evidence Interchange Management Application Collaboration in the IM Pattern 142
Figure 31 Graphic Representation of the Evidence Interchange Management Application Collaboration in the USI Pattern 143
Figure 32 Graphic Representation of the Evidence Interchange Management Application Collaboration in the VC Pattern 144
Figure 33 Graphic Representation of the Evidence Interchange Management Application Collaboration in the Lookup Pattern 145
Figure 34 Graphic Representation of the Trust Architecture Application Collaboration in the IM Pattern 147
Figure 35 Graphic Representation of the Trust Architecture Application Collaboration in the USI Pattern 148

© 870635 DE4A Project Partners

Figure 36 Graphic Representation of the Trust Architecture Application Collaboration in the VC Pattern 148

Figure 37 Graphic Representation of the Trust Architecture Application Collaboration in the S&N and Lookup patterns 149

Figure 38 Graphic Representation of the Data Logistics Application Collaboration in the IM, USI, S&N and Lookup patterns 153

Figure 39 Graphic Representation of the Evidence Portal Application Collaboration in the IM and Lookup patterns 154

Figure 40 Graphic Representation of the Evidence Portal Application Collaboration in the USI Pattern 155

Figure 41 Graphic Representation of the Evidence Portal Application Collaboration in the VC Pattern 156

Figure 42 Graphic Representation of the Evidence Retrieval Application Collaboration in the IM, USI and Lookup patterns 158

Figure 43 Graphic Representation of the Evidence Retrieval Application Collaboration in the VC Pattern 159

Figure 44 Graphic Representation of the Authority Agent Application Collaboration in the VC Pattern 160

Figure 45 Graphic Representation of the User Agent Application Collaboration in the VC Pattern 162

Figure 46 Graphic Representation of the Cross-border Subscriptions Application Collaboration in the S&N Pattern 164

Figure 47 Graphic Representation of the eProcedure Back-office Application Collaboration in the S&N Pattern 167

Figure 48 Mapping of SA Use Cases to Interaction Patterns 170

Figure 49 Mapping of DBA Use Cases to Interaction Patterns 171

Figure 50 Mapping of MA Use Cases to Interaction Patterns 173

© 870635 DE4A Project Partners

List of Annexes

Annex 1 Business Process Collaboration View of the Intermediation Pattern *181*
Annex 2 Business Process Collaboration View of the User-Supported Intermediation Pattern *182*
Annex 3 Business Process Collaboration View of the Verifiable Credential Pattern..... *183*
Annex 4 Event Subscription Business Process Collaboration View *184*
Annex 5 Business Process Collaboration View of the Notification Process *185*
Annex 6 Evidence Lookup Business Process Collaboration..... *186*

© 870635 DE4A Project Partners

List of Acronyms

Abbreviation / acronym	Description
ABB	Architecture Building Block
API	Application Programming Interface
AS	Application Service
AS4	Applicability Statement 4, an open standard for the secure and payload-agnostic exchange of Business-to-business documents using Web services
AT	Austria
BB	Building Block
BPM	Business Process Model
BPMN	Business Process Model and Notation
BRIS	Business Register Interconnection System
CCCEV	Core Criteria and Core Evidence Vocabulary
CEF	Connecting Europe Facility
(DG) Connect / (DG) CNECT	The European Commission's Directorate-General for Communications Networks, Content and Technology
CRUD	Create Read Update Delete
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
(DG) DIGIT	The European Commission's Directorate-General for Informatics
DO	Data Owner
DoA	Description of Action
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.
DPIA	Data Protection Impact Assessment
DR	Data Requestor
DSI	Digital Service Infrastructure
DSM	Digital Single Market
DT	Data Transferor
Dx.y	DE4A formal Deliverable x.y (e.g. D2.5)
E2E	End-to-end
EAI	Enterprise Application Integration
EBSI	European Blockchain Services Infrastructure

© 870635 DE4A Project Partners

Abbreviation / acronym	Description
EC	European Commission
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.
EIRA	European Interoperability Reference Architecture
EESSI	Electronic Exchange of Social Security Information
ENIC-NARIC	ENIC: European Network of Information Centres in the European Region NARIC: National Academic Recognition Information Centres in the European Union
ES	Spain
ESSIF	The European Self-Sovereign Identity Framework
EUID	European Unique Identifier
FIDO 2	World Wide Web Consortium's (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance's corresponding Client-to-Authenticator Protocol (CTAP)
GAIA-X	Federated Data Infrastructure for Europe Project
GDPR	General Data Protection Regulation
HLA	High Level Architecture
HTTP	Hypertext Transfer Protocol
ICT	Information and communications technology
ID	Identity (document)
IM	Intermediation
IMI	Internal Market Information System
ISA(^{2})	Interoperability Solutions for Public Administrators programme
IT	Information technology
JRC	Joint Research Centre
JSON	JavaScript Object Notation
LKP	Lookup
LSP	Large scale pilot
MA	Moving Abroad – one of the three DE4A pilots
MS	European Union Member State(s)
MVP	Minimal Viable Product
NFC	Near Field Communication
NL	The Netherlands
NRT	Near real-time
OOP	Once-Only Principle
OOTS	Once-Only Technical System
PhD	Doctor of Philosophy

© 870635 DE4A Project Partners

Abbreviation / acronym	Description
PKI	Public Key Infrastructure
PSA	Project Start Architecture
PT	Portugal
Q&A	Question and answer
(Q)ERDS	Qualified Electronic Registered Delivery Service
QR	Quick response code
REST	Representational state transfer
RO	Romania
SA	Studying Abroad – one of the three DE4A pilots
SAML	Security Assertion Markup Language
SBB	Solution Building Block
SDG	Single Digital Gateway
SDGR	Single Digital Gateway Regulation
SE	Sweden
SEMPER	Secure Electronic Marketplace for Europe
SI	Slovenia
SLA	Service level agreement
SMTP	Single Mail Transfer Protocol
S&N	Subscription and Notification
SSI	Self-sovereign identity
TBP	To Be Provided
TIR	Trusted Issuer Registry
TL	Task Leader
TLS	Transport Layer Security
Tn.m	DE4A formal project Task n.m (e.g. T2.3)
TOOP	The Once Only Principle Project
U	User
UC(#)	Use case of the DE4A pilots
UI	User interface
URL	Uniform resource locator
USI	User Supported Intermediation
VC	Verifiable Credential
VP	Verifiable Presentation
WP	Work Package
XML	Extensible Markup Language

© 870635 DE4A Project Partners

Executive Summary

The DE4A Project Start Architecture (PSA) employs a structured analysis, based on the Architecture Framework laid out in D2.1[2]. It started with the Intermediation pattern, which is highly aligned with the current proposal for an Implementing Regulation for Article 14 of the SDGR[17] concerning the Once-Only Technical System (OOTS). Working hypotheses for 25 interdisciplinary questions (section 2.3) are made explicit and were used to align the interaction pattern with Pilot and Member State requirements. The most prominent interdisciplinary topics are:

- Transitivity of User Identity (section 2.3.7) and Identity and Record Matching (section 2.3.6) are closely related topics; a user must be unequivocally identified by both Data Consumer (DC) and Data Provider (DP); and related to data stored in a registry, which is not trivial in the absence of a European unique ID for citizens. The challenge is aggravated if the record matching is separated from the eIDAS authentication process (Intermediation).
- Explicit Request and Transitivity Between Actors (section 2.3.4) is related to the above in so far that a user, authenticated by the DC, issues an explicit request that is a legal prerequisite for the DP to transmit data related to that user.
- Preview & Approval UI (section 2.3.5) - and especially the moment of the preview in the process (i.e. before, during or after the transfer from DP to DC) - has important implications for privacy-by-design and compliance with national legal frameworks.
- Mandate and Proxy (section 2.3.9), i.e. a natural person representing a legal person or another natural person, is a must-have for all business use cases, but is also increasingly relevant for citizen use cases.
- eIDAS and National Authentication Systems (section 2.3.16) deals with the question of which means and systems can be used for the user authentication and has an impact on the groups that can or cannot use the system.
- Matching Evidences between Member States (section 2.3.22) and questions of semantic interoperability in general. Different approaches lend themselves for sectors that are or are not harmonized yet. The reference Architecture caters to both (canonical evidence and evidence type matching), while the DE4A pilots are focussed on the use of canonical evidences.

This approach has yielded detailed reference architecture descriptions for five different interaction patterns, consisting of interaction pattern-specific business architectures (see chapter 3) and a unified application architecture (chapter 4), serving all patterns employed by the use cases of the DE4A pilots (chapter 5):

1. Intermediation Pattern (IM): Message exchange-based pattern with the DC handling all user interactions, including authentication and preview. This pattern is chosen for the Doing Business Abroad pilot.
2. User-supported Intermediation (USI) Pattern: A variant of the Intermediation pattern that includes a direct interaction of the User with the DP. The User supports the DP in creating a secure and legally valid match between authenticated User and the evidence that they are requested to send. Also, the preview is moved to the DP, prior to the data transfer. This pattern is preferred by the pilots dealing with citizens, rather than companies: Moving Abroad and Studying Abroad pilots.
3. Verifiable Credentials (VC) Pattern: Investigates the potential of decentral identifiers and distributed ledger technology for eGovernment interoperability. The User takes centre-stage between DC and DP. There is no direct interaction between DC and DP, however, the User is guided by the DC in identifying the correct DP (VC issuer), similarly to the two patterns above.

© 870635 DE4A Project Partners

This pattern is piloted in one use case of the Studying Abroad pilot (as early adopter of EBSI[24]).

4. Event Subscription and Notification (S&N) Pattern: This pattern has no User interaction. The DC subscribes to a list of business or life events of a subject and receives event notifications if the situation of the subject changes. This pattern is applied by the Doing Business Abroad pilot to receive event notifications for changes in companies that are relevant across borders.
5. Evidence Lookup Pattern: This pattern has no User interaction. The DC requests an evidence from the DP, which requires a legal basis to do so, and receives the evidence in return. This pattern is used by the Doing Business Abroad pilot in conjunction with the Event Notification mentioned above, in order to receive updated evidence as result of a business event.

We conclude that a multi-pattern architecture for European eGovernment interoperability is indeed needed to cover the large diversity of use case-specific requirements, the heterogeneity of Member State OOP solutions, and the differences in their legal and administrative frameworks. What became especially apparent is that the nature of the user/subject, i.e. the difference between company and citizen/student use cases, is highly significant and exerts influence on most of the interdisciplinary questions and consequently the applicable interaction patterns. Nevertheless, the application services supporting the different patterns exhibit considerable overlap and can be integrated into a unified application layer. This holds even for the VC pattern, which introduces a new paradigm, based on decentral identifiers and distributed ledger technology.

© 870635 DE4A Project Partners

1. Introduction

1.1. Purpose of the Document

The main goal of the document is to provide a consolidated view of the DE4A start architecture and provide architectural guidance for the Pilot Solution Architectures. WP2 - Architecture Vision and Framework, is assisting in this process in the context of a special Technical Task Team involving pilot architects and pilot leaders as well as the pilot's coordinator and the technical coordinator.

However, the effective pilot implementations and setup from the piloting organisations in DE4A can vary to some extent from the technical findings, concepts and depictions in this deliverable.

This document is the formal public delivery D2.5. It is a new, restructured, and shortened version of the PSA, considering recent developments and new insights in addition to two new interaction patterns. It is an extension of D2.4 (PSA first iteration) and defines the updated start architectures for the second iteration of the Pilots. Its content is also integral part of the deliverable D2.6 'Service interoperability solutions toolbox' that is being compiled on the DE4A Wiki. Further insights and subsequent updates will be reflected there.

The start architecture was developed in close collaboration with the Architects from the pilot teams (WP4 – Pilots for Citizens and Business), WP3 – Semantic Interoperability Solutions and WP5 – Common Components Design & Development. In a joint effort, a total of five reference interaction patterns were elaborated, of which the last two are only applicable for the second iterations of the pilots. First lessons learned from pilot development were incorporated in this way, e.g. in updates and extension of the intermediary questions and related working hypotheses per pattern. Insights from the pilot running phase are not yet available.

This document follows the Architecture Framework proposed in D2.1 Architecture Framework [2] and contributes content to this framework, being extended by the technical work packages with specifications in increasing levels of detail throughout the project. Reference interaction patterns are worked out top-down in the conceptual/functional level of abstraction, according to the proposed metamodel. We apply industry standard modelling languages BPMN [20] and ArchiMate [19] to the challenges of cross-border evidence exchange between competent authorities. This exercise helped to shed light on some of the most pressing, interdisciplinary questions (see 2.3) and provides a structured context to further elaborate them in the DE4A Technical Working Group that comprises all technical work packages.

The Business Process Collaboration views provide the end-to-end overview of the (public) service processes with a focus on the OOP exchange of evidence and are the central communication views for stakeholder alignment. Process Realization views zoom in on the single process of each participant and define the Application Services required for each of the Business Activities to be executed. The resulting Service classification is aligned with EIRA and is a major input to the Backlog of the technical work packages (e.g. D5.1[13], D3.3[5], D3.5 [6], D5.3[14], and D5.5 [15]). Each Application Service is realized by an Application Collaboration, which in terms is detailed in an Application Collaboration view, comprised of interacting Application Components and Interfaces. These views are meant as bridge to and as the context for the specification of the Pilot solutions.

Together with the pilot's architects "pattern matching" was performed, finding a best fit per pilot use case:

- Doing Business Abroad: Intermediation, Subscription & Notification and Lookup Patterns
- Moving Abroad: User-supported Intermediation Pattern and Intermediation Patterns
- Studying Abroad: User-supported Intermediation and Verifiable Credentials Patterns

© 870635 DE4A Project Partners

Together with the pilots and WP3 and WP5 an Architecture Log is maintained to document deviations and implications as a means to uncover and document barriers to interoperability. In addition to the future Initial Running Phase and Evaluation reports from WP4, it provides a valuable input for WP6 - Sustainable impact and new governance models and WP7 - Legal and ethical compliance and consensus building.

1.2.Structure of the Document

Chapters 1 and 2 jointly give the wider background of the Project Start Architecture, including an account of the problem area in form of interdisciplinary questions on which guidance is provided. Chapters 3 and 4 constitute the core of the document, the DE4A reference architecture. Chapter 3 defines the multi-pattern Business Architecture and the required Application Services to actually run all of the five reference interaction patterns. Chapter 4 describes the Reference Application Architecture in more detail, which is meant to provide a unified set of components, supporting all reference interaction patterns. Chapter 5 contains the pilot sections for all three pilots. Chapter 6 presents the conclusions.

Chapter 1	–	Introduction to the Project Start Architecture
Chapter 2	–	Background, Functional Scope of the DE4A Pilots, Relation to the Once-Only Technical System, Interdisciplinary Questions
Chapter 3	–	This section contains the Reference Business Architecture. A total of five interaction patterns are elaborated: Intermediation, User Supported Intermediation, Verifiable Credentials, Subscription & Notification and Lookup. The first three are updated with respect to D2.4 [4] and the last two are completely new. Per pattern the following topics are addressed: Working Hypothesis and Implementation Principles, Business Process Collaboration view, Process Realization
Chapter 4	–	Reference Application Architecture. Application Collaborations with their Application Components and realized Application Services.
Chapter 5	–	DE4A Pilots ▪ Studying Abroad Pilot: choice of interaction pattern ▪ Doing Business Abroad Pilot: choice of interaction pattern ▪ Moving Abroad Pilot: choice of interaction pattern
Chapter 6	–	Conclusions
References	–	References

1.3.Relation to other DE4A Deliverables

This PSA is delivered in two iterations and is set up according to the Architecture Framework of D2.1[2] and extends from the work represented in D2.4[4]. For the three existing patterns small changes to the diagrams and improvements for consistency only. The scope of D2.5 was extended with two new interaction patterns and also reduced with some sections removed to avoid overlap with other

© 870635 DE4A Project Partners

deliverables from WP3 and WP4 as indicated below. The BB chapter containing the initial BB assessment has been moved to the Wiki and is also no longer included.

Next to external references, the pilot use case and requirements documents D4.1[7], D4.5 [9] and D4.9[11] were most important input on the development of the reference architecture. Close cooperation with WP1 and WP7 in compiling D2.4 made sure that the PSA was fully aligned with their deliverables that were developed in parallel, especially D1.7[1] and D7.1[16]. References to D1.7 are now included in this document.

D2.2 Trust Management Models [3] and D3.3 Semantic Framework [5], which were also developed in parallel with D2.4, were considered so important for the pilots that D2.4 included short previews as separate sections. With these deliverables now being available, as well as D3.5 [6] these preview sections are not anymore included in D2.5.

D2.4 PSA (first iteration) was an important input into D5.1[13] and was the basis for the definition of the pilot solutions in the Technical Task Team formed by WP2, WP3, WP4 and WP5. The outcome of this work is documented in greater length in the Pilot Planning deliverables D4.2[8], D4.6[10] and D4.10[12]. The pilot chapter 5 of this document needs to be considered in relation with these deliverables and is kept to a minimum to reduce overlap between deliverables. Deviations between the PSA and the common component design in D5.3, which also builds on D4.2, D4.6 and D4.10 are being documented in an architecture log included in the DE4A Wiki.

Finally, D2.6 Service interoperability solutions toolbox should be mentioned, which is being developed on the DE4A Wiki. The complete Reference Architecture, as well as the Building Block assessment will be made available in this online repository together with more detailed specifications and documentation from WP3, WP4 and WP5. New insights will be represented in updates on the Wiki.

© 870635 DE4A Project Partners

2. Background

Disclaimer: most of this chapter remains unchanged with respect to D2.4 Project Start Architecture (PSA), first iteration. Apart from the usual minor changes to fix errors etc. relevant changes include elaborating the support to SDG and the update of the Interdisciplinary Questions taking into account recent development, as well as the addition of three new topics.

2.1. Functional Scope of the DE4A Pilots

DE4A pilots aim to develop and demonstrate interoperable, scalable, high-impact and viable administrative services in real-life environments to validate DE4A framework of interaction patterns, common specifications, technical and semantic interoperability infrastructure and components and services (c.f. Service Interoperability Solutions Toolbox), re-using to the maximum extent existing and emerging CEF Building Blocks and extending OOP to fully online procedures in the context of Life Events in the SDGR, with citizen and business participation.

In its piloting approach, DE4A is not focusing on a single “one size for all” solution, but takes as starting points a selection of interaction patterns - the Project Start Architectures described in this deliverable as well as in the first iteration PSA - which align with fundamental (i.e. User Centricity and User Empowerment) and derived principles (i.e. OOP Principle) as described in D2.1 Architecture Framework [2], and put them to the test of real-life use cases selected by the DE4A Member States. The pilots represent a secure, privacy-preserving, and trustworthy realization of those principles in the context of cross-border procedures that directly relate to Life Event of the SDGR for citizens (including students) and businesses.

DE4A also puts specific focus on assessing the applicability, benefits and cost effectiveness of innovative technologies with transformative impact like blockchain technology, putting it to active use in pilots in order to create true evidence of the value and the technical and non-technical challenges and benefits it represents for Public Infrastructures and Services delivery. This is above all a practical endeavour: the transformative impact aims to be demonstrated as much as possible in real life.

Furthermore, by combining insights from real-life pilots (inductive approach), including on understanding barriers and ways to resolve them on all four levels of interoperability - legal, organizational, semantic and technical - with an analysis of governance models (cf. WP6 ‘Sustainable Impact and new governance models’), thus enabling a deeper and better understanding of the roles and responsibilities as well of public authorities and other actors delivering public services. The pilots, through intense multi-stakeholder collaboration and involvement across participating Member States support as well establishing a culture of co-creation, transparency, accountability and trustworthiness, that will result in specific recommendations for overcoming existing legal, cultural and managerial barriers and with guidelines for realizing necessary changes to enable Member States to apply the accumulated experience towards their integration with the Once-Only Technical System.

Of even more fundamental importance, the DE4A pilots develop and demonstrate the potential for sharing common public services with different actors to achieve efficiency and effectiveness in these collaborations, demonstrating the multi-sectorial and multi-domain applicability of standards and solutions. It does so sharing the same ambition of previously successful Large Scale Pilots, that is, the three broad DE4A pilots covering different sectors (Studying Abroad, Doing Business Abroad and Moving Abroad) take SDGR[17] life events and procedures related to them (encompassing both citizen and business cross-border needs) as starting point for defining their specific use cases c.f. D4.1[7],

© 870635 DE4A Project Partners

D4.5[9], D4.9[11] "Use Case definition and requirements" and involving real Member State users in real life production environments using real users of pre-defined target groups.

All the pilots in DE4A have a focus on tangible benefits realization and impact creation for different stakeholders i.e. involving by default real users using operational environments (citizens, students, businesspersons and public servants), through an agile and iterative process that includes tight relationship with other technical work packages. DE4A pilots aim to:

- Unleash multiple measurable positive impacts to real users (citizens, students, businesspersons and public servants) in terms of efficiency gains and reduction of current administrative burden and costs and barriers for cross-border public services
- Facilitate Public & Private sector collaboration through sustainable benefits realization.
- Support strategic EC & MS priorities (SDGR esp. Art.14, Tallinn Declaration, eGov Action Plan, DSM).

In order to realize every one of the pilot use cases, the Project Start Architectures defined in this deliverable represent a joint effort between WP2 architects and architects from each of the pilots working together in 'PSA teams', bringing necessary, domain-specific knowledge from the pilots: in particular, on the already defined pilot functional and non-functional requirements (in the context of pilot functional boundaries and specific technical and business goals, pilot success criteria, etc.), user journeys from user perspective and initially defined pre-conditions/main flows and post-conditions, and other pilot-relevant context (e.g. external systems and initiatives like EBSI-ESSIF, BRIS and EESSI).

2.2.Relation to the Once-Only Technical System

The DE4A architecture is built around the need to support different service patterns that are based on a standard set (or toolbox) of capabilities/Application Services, therefore designing and evaluating multiple service patterns is at the core of DE4A. Also, DE4A pilots are essential in providing *Evidence of the benefits of the full implementation of the once-only and digital-by-default principles and user centricity and the transformative impact of new technologies such as blockchain* [16] and will therefore test these patterns and innovative technologies generating valuable knowledge for the EC and the Member States. This perspective of the DE4A project is consequently broader (in terms of applicable use cases and functional scope beyond the OOP exchange of evidence) and wider (extending beyond the legal requirements and timeline of the SDGR[17] Article 14 entering into force on December 12th 2023) than the Once-Only Technical System (OOTS) for which the aforementioned Article constitutes its legal basis. This broader scope is especially valuable considering that 12 December 2023 only marks the start, the initial go-live, of the OOTS and should *constitute a well-balanced step towards the emergence of a European Governmental Interoperability Platform[1], in order to be sustainable* [21].

Although this H2020 Action is not a formal part of the process of further specifying the SDG-Regulation [17], i.e. the Implementing Act on Article 14, or the efforts of implementing the Once-only Technical System, it is important to understand that DE4A is related to and can contribute to the SDG efforts in multiple ways:

- Pilot important concepts that may be reused in the SDG context and beyond
- Producing detailed technical specifications following MS-specific requirements before SDG technical specifications will be ready

[1] This term was chosen in the DoA (Description of the Action) while different terms are used in for example in context of the Digital Europe Programme.

© 870635 DE4A Project Partners

- Investigate requirements beyond the scope of the OOTS blueprint (i.e. patterns like Subscription & Notification, Lookup and Verifiable Credentials and procedures/evidences beyond SDGR Annex II as well as on topics like powers and mandates (SEMPER) and deferred responses)
- Develop reusable common components (semantic and technical) that are not yet fully covered by existing BBs (e.g. CEF and ISA[2]) and LSPs (i.e. TOOP)
- Aid in building consensus on important concepts like "Explicit request" or "Preview/approval"
- Uncover detailed challenges, such as identity and record matching or cross-border transitivity of user identity (i.e. transmitting of user identities across borders) and identify/catalogue important interdisciplinary questions and try out potential solutions to them
- Provide insight in implementation challenges and discover impediments and barriers that can also impact the SDG OOTS implementation, including the different aspects of the underlying trust model and leveraging and extending valuable lessons previously learned e.g. eIDAS approach and which can also be contributed towards the Technical System
- Integrate and use existing BBs, furthering their maturity, and helping in their wider acceptance (e.g. SEMPER)
- Increasing the awareness of OOP in MSs through hands-on experience and dissemination activities
- Provide recommendations to national and Union policy makers for the evolution of OOP beyond 2023, allowing to keep the focus of the SDG OOTS implementation on the task at hand

This is fully in line with the DoA [21] that includes the motivation that *Citizen and business-oriented pilots shall highlight chosen aspects of the technical ecosystem available for the SDG implementation on European and Member State level, prove their technical viability and gauge the performance and degree in which non-functional requirements can be accommodated* and includes the objective of the *development of high quality and optimized common services and components, fully aligned with upcoming milestones foreseen in the SDG roadmap -in particular to assist Member States to realize OOP Technical System.*

DE4A takes the reality as its starting ground - the needs and the capacities of the Member States [21] and has to meet the challenge to have pilots operational as early as second semester of 2021 with the aspiration of running them on production systems as much as possible in order to create immediate business value. This more bottom-up approach can harmonize well with the top-down approach of the CEF Preparatory Action that starts from the stipulations of Article 14 towards creating a consensus for the technical and operational specifications in the (still draft) Implementing Act where the European Commission and each of the Member States will "be responsible for the development, availability, maintenance, supervision, monitoring and security management of their respective parts of the technical system" (Art. 14, paragraph 11)[17].

Given that this paragraph entered into force in October 2018, it is reasonable to assume a keen interest both on the part of the EC and of the Member States that mechanisms for cross-border exchange of evidences are demonstrated (even if at a limited scale and for piloting purposes) in real-life scenarios as this will largely benefit the authorities in the run-up for 12 December 2023 and beyond. To ensure good alignment, as far as possible and appropriate, with the SDGR, WP2 was closely cooperating with WP7 on this topic during the development of the PSA. Additionally, the TOOP [23] Reference Architecture and the High-level Architecture of the CEF Preparatory Action for the OOTS were analysed as starting point for the Intermediation Pattern (see 3.1).

DE4A has strong alignment on:

- Intermediation Pattern (verified in technical workshop of November 2020)
- Major BBs (eIDAS, eDelivery), Core Vocabularies, standards (RegRepv4)

© 870635 DE4A Project Partners

- Re-use of the TOOP code base for core components of DE4A (Connector)

In the last months alignment with EC was achieved through:

- Regular alignment teleconferences with the CEF Preparatory Action team
- SDG WGs attendance
- The Technical Workshop confirmed good alignment between our PSA on the Intermediation Pattern and OOTS Blueprint
- The EC plans to address new topics in the SDG Technical Design WG (interrupted procedures, registration/deregistration, late/deferred responses) which are also addressed in DE4A
- DE4A can provide inputs on "Alternative Patterns", i.e. direct user interaction with the evidence issuer

Legal and organizational limitations uncovered by DE4A will require pragmatic choices to allow the pilots to be implemented successfully. These also generate inputs from the DE4A Action that can feed into the Implementing Act discussions process, thereby aiding timely consensus building. Incompatibilities of the current legal and administrative frameworks and technical baseline of MS with SDG Article 14 and its elaboration in the Implementing Act may either require (legal) changes on national level or may hamper the successful implementation of the SDG OOTS.

This means that DE4A and its pilots must strike a delicate balance between direct contribution to the SDG –– *in particular to assist Member States to realize the OOP Technical System* [meant here is the Once Only Technical System (OOTS)] – and exploring *different ways these* BBs *[CEF, ISA, ISA² and different LSPs, i.e. TOOP] can be combined to provide a flexible ecosystem that allows governments, public administrations and other actors to collaborate and innovate openly with each other, as a stepping stone towards a European Governmental Interoperability Platform* [21], while exploring *the transformative impact of new technologies such as blockchain* [22], all awhile remaining practical and implementable within the project timelines.

In order to manage this balance in a transparent and collaborative way, DE4A sets up regular alignment meetings with the CEF Preparatory Action and participates in the SDG coordination group and working group meetings as observer.

DE4A is also building on the SDG and providing added value beyond it:

- Innovative technologies (Blockchain) and user-supported evidence exchange patterns (User Supported Intermediation and Verifiable Credentials) to demonstrate benefits of alternative way to realize Once-Only (reduced verification costs, high user control of exchange process, increased transparency and trust, now very well set for alignment with new proposal for revision of eIDAS Regulation published by the EC in June 2021
- Realizing synergies with EBSI-ESSIF ('Early adopters')
- Deliver better, interoperable, digital public services
- Accelerate adoption of cross-border services
- Open collaboration and innovation platforms supported by ICT ("government as a platform") to ensure modular services quality ("government as a service")
- Potential to regroup resources under common infrastructures at European level
- Reinforced trust in public institutions (certified transactions, decentralized trust, eIDAS Revision)
- Paving the way to a longer-term time horizon (steps towards an EU Government Interoperability Platform)

© 870635 DE4A Project Partners

2.3.Interdisciplinary Questions

https://wiki.de4a.eu/index.php/Interdisciplinary_Questions

This section introduces 25 interdisciplinary challenges, three more compared to D2.4, in the context of creating an OOTS on European level. These questions are taken from DE4A's own analysis (i.e. Pilot requirements) and from numerous external interactions and sources, e.g. discussions with MS representatives, the SDG OOP working groups, CEF Preparatory Action on OOP and the TOOP LSP. The PSA attempts to provide preliminary guidance on these questions as a starting point for the DE4A pilot development. The collection of topics represents the current state of discussion and are being extended as we progress with the pilots.

We provide preliminary direction concerning the questions mentioned in this section in a structured way, through the description of reference interaction patterns in chapter 3, using the DE4A architecture metamodel. Working hypotheses for the relevant topics are formulated in the sections of the different interaction patterns in chapter 3 (e.g.: 3.1.1 for the Intermediation Pattern). These working hypotheses proved very useful in aligning architecture to pilot requirements and Member States' expectations in preparing for the first DE4A pilot iteration, as well as the alignment with the SDGR OOTS.

2.3.1. Orchestration / Choreography

The automated cross-border exchange of evidence requires many actors and systems to collaborate in an orderly manner, as also identified as barrier in D1.7: T3: The managing and governance of the choreography of distributed components managed by different agents and during a single user session. The sheer number of possible combinations in different procedures means that most combinations cannot be tested prior to first operational use. The more so, a solid concept of coordinating the actions and services required for the OOP exchange of evidence is required, irrespective of it being central orchestration or decentral choreography.

This need is further aggravated in Interrupted scenarios, which might include extended pauses or waiting periods in the overall process (i.e. issuing the evidence needs several days). Restricting the system to only uninterrupted exchange simplifies the challenge somewhat, but essentially, we still need to manage the interaction between User, DC, potentially several DP and several organizations in-between facilitating the exchange (DRs, DTs). In addition, we expect that a purely uninterrupted scenario might be too restrictive to cover the breadth of real-life scenarios.

2.3.2. Complementary, Overlapping or Conflicting Evidence Equivalents

We need to consider that the request for evidence in one country can lead to the identification of a multitude of available equivalents in other countries. This leads to the need for disambiguation: The equivalents can be *complementary*, meaning that several pieces of evidence are needed jointly to be equivalent. They also could be *overlapping*, meaning that several equivalents are available for a required evidence or criterion, yet all are valid; or they could be *conflicting*, which would mean that at least one of them is not correct. The underlying reasons for such situations could be complex real-life cases (e.g. multiple nationalities or complex life journey through several Member States), or the result of poor data quality across unreconciled registries in different Member States. In any case, the Once-Only Technical System will need to be robust against such cases and cannot assume a single request to single evidence case to be the only viable standard situation. Please note that this topic is about disambiguation, as opposed to cases that rightfully and correctly have multiple evidences involved in a single eProcedure (see 2.3.23 below).

© 870635 DE4A Project Partners

2.3.3. Interrupted vs. Uninterrupted Exchange

In the SDG context lives a strong assumption that the complete evidence exchange will be handled in an uninterrupted way within the timelines of a single user session, as part of completing an e-procedure. From Member State experience, we see that there are good practical and technological reasons to also consider scenarios where the evidence exchange is interrupted and can be resumed later (in the SDG context, the term “deferred response” is used at the moment). One practical reason is, for example, that some requested evidence is not immediately available in a format that allows for its automated exchange but can be made available at a later moment. Several Member States have a mechanism to digitize the requested evidence on demand. Including this possibility would increase the volume of evidence that can be made available through the system. Also, in the multi-evidence case, when two or more evidences needs to be collected, it may not be feasible for the user to complete the procedure in one take. In fact, the Moving Abroad pilot intends to pilot such a case. This topic was also recognized as organizational barriers in D1.7 [1]: O1: Data may be not ready for access in real-time without authorization by a civil servant, and OP2: Data may not be ready for access in real-time without following procedures involving batch processing.

Also, a hybrid case appears to make sense, where the resume functionality serves as fall-back to handle exceptions in an a-priori uninterrupted procedure. It must be considered, however, that supporting interrupted procedures (resume functionality) across a multitude of cross-border participants is a very complex challenge involving correlation across highly independent systems and persistence (and consequently clean-up) of process instances.

2.3.4. Explicit Request and Transitivity Between Actors

In the SDGR, the exchange of evidence is generally initiated on explicit request of the user (except where the relevant Union or national law allows for automated cross-border data exchange without an explicit user request). This request is issued to the DC. It remains unclear whether that explicit request needs to be provided as well to the DP, in order for them to check the request prior to actually extracting the evidence back, or the DP can simply trust a request from a DC to be based on an explicit request or applicable law. The Data Protection Impact Assessment (DPIA) of the SDGR Art. 14 Implementing Regulation (version April 2021), for example, expressed that the Explicit Request does not need to be handed over to the DP. Later versions of the (yet to be adopted) Implementing Regulation, however, still explicitly include extensive information about the Explicit Request in the Evidence Request message from DC to the DP.

The political relevance of this topic becomes clear when looking at findings of D1.7 Legal, technical, cultural and managerial risks and barriers[1]: more that 70% of the responding MS expressed that they are 'very cautious' when sharing personal data with other countries and 67% reported that their national OOP approach requires 'Prior request from the user' before sharing data with other administrations within their country.

2.3.5. Preview & Approval UI

A lot of discussion already went into the topic of user preview and approval prior to completing the exchange of evidence. From a legal and data protection standpoint, we consider a preview prepared by the system of the DC as not optimal, because it would require the evidence to be already transferred prior to the preview. From a solution point of view, however, a preview provided by the DP would introduce several additional complexities, e.g. related to the handover of the user session from DC to potentially several DPs. We should consider the need for a user interface for the once-only technical system that is separate from the eProcedures form itself. Consensus on this point between Member

© 870635 DE4A Project Partners

States and the Commission is not yet final and the PSA includes reference interaction pattern for all three cases: preview at the DC, the DP, or the User.

2.3.6. Identity and Record Matching

This is the problem of matching the eIDAS attributes (mandatory and optional) to the national identification numbers required to extract the evidence. Basis for this matching are the mandatory eIDAS attributes, and in some cases the optional ones as well. This issue arises both at the DC in starting the online procedure as well as the DP side for extracting the requested evidence (see 2.3.7 below), as mentioned in D1.7[1]: S5: Identity/record matching when accessing online services cross-border and S6: Identity/record matching of user for data request and data access.

As this match is not 100% an exception flow is required. This still needs discussion as it either leads to the OOTS not being available for the user (a potential solution for the Minimum Viable Product) or might require more complex user interaction, potentially even involving manual work by a civil servant or the provision of additional evidence. In this way this is also related to the topic of interrupted procedures in 2.3.3 above.

Recently some proposals on the way forward were made by the SDG team with respect to the record matching problem. One is adding more attributes on top of the eIDAS minimum dataset, the other is the support for user provided data. The eIDAS review process will look into possible solutions for this.

2.3.7. Transitivity of User Identity

This problem arises in the Intermediation Pattern because the User first authenticates themself vis-à-vis the DC. It is however the DP in another MS that needs to retrieve the evidence related to that User. This often requires a unique identifier, for example that in the population registry, to access natural person information. The identity of the User (e.g. coming from eIDAS) is unfortunately not transitive (i.e. eUniqueness IDs differ between Member States). This topic related directly to the barrier 'L8: Identity transitivity cross border' identified in D1.7[1]

As a result, the DP needs to re-establish the identity of the User, i.e. as described in 2.3.6 above by matching eIDAS attributes to national records. This has again two implications: First, the match can be ambiguous (especially for common names where transliteration and similarity algorithms are needed following language rules specific to each Member State). Second the DC must be legally allowed to transfer the eIDAS attributes to the DP.

In the business domain, this is simpler to resolve as a European Unique Identifier (EUID) for companies exist since 2012. The EUid for Citizens, proposed for the current eIDAS revision should help to resolve this problem as well for natural persons in the Union.

2.3.8. Hand-over of User Interface Between Actors

If the eProcedure including the OOP transfer requires several systems, controlled by different actors in different MS, to interact with the User, then a UI reference would need to be handed on throughout the OOP evidence exchange. The likeliness for such a hand-on to break along a longer procedure is significant, which would giving again rise to the need of supporting interrupted procedure as described in 2.3.3 above.

2.3.9. Mandate and Proxy

The power of representation, either a natural person representing a legal person (i.e. mandate) or a natural person representing a natural person (i.e. proxy) or even a legal person representing a natural

© 870635 DE4A Project Partners

person is a complicating factor in the identification and OOP exchange of evidence that we cannot ignore. It is also identified as one of the most critical barriers in D1.7[1]: S8: Non-harmonized (or mapped) user rights, including powers and mandates.

Whereas a first implementation for citizen procedures might still put this out of scope, it is surely required in the mid-term solution (time horizon t=3 [6]). For business-related procedures, this issue must be tackled from the start, as it is always a natural person representing a legal person. The long-term solution should also consider chaining together 'representation'-relationships or 'intermediaries' (e.g.: an accountant representing an accounting firm that represents a trading company that represents a manufacturer).

Successful piloting might require an eIDAS extension for powers attributes (i.e. SEMPER). Some partners may be hesitant to deviate from using their eIDAS reference software in production.

2.3.10. Encryption Gap

The existence of a national OOP system in many MS means that the roles of Data Requestor (DR) and Data Transferor (DT) will be taken over by central MS organizations that are separate entities or authorities from the Data Owners (DO) and Data Evaluators (DE). These roles are described in D2.1 [2]. This is fully in line with the 4-corner model, see for instance [28]. This means that it is likely that the gateway between the national OOP system and the European cross-border OOTS will need to decrypt and then re-encrypt the evidence using the national and the European standards, respectively. Consequently, the evidence is available at some point in unencrypted form while being processed by the gateway. Real E2E encryption, which would result in nesting encryptions, could theoretically solve this problem on the technological level. It creates, however, two new challenges: one related to managing certificates across many thousands of competent authorities and the second related to the user preview.

2.3.11. Structured Data vs. Unstructured Data

This relates to the extent to which OOTS should support unstructured data. The SDGR is explicitly not making a choice in this regard, however the solutions discussions are often assuming a structured data exchange. The consensus is not yet final, and we expect this to be one of the topics that remain unclear at least until the completion of the implementing act in the course of 2021.

If we refer to structured data, we mean electronic data that is adhering to some defined and known schemas or data models. It is important to note that this means that 'structured data' is not equivalent to data in data bases. Also, a structured data document adhering to a known, domestic schema is perfectly structured data. A document with "some text" or a randomly named image file (of a scanned document) is considered unstructured. Additionally, evidences from different domains might use different data models and schemas, it is important that the data models are defined and known.

This discussion is often confused with the assumption of automated re-use of data after transfer (cf. 2.3.12 below).

2.3.12. Automated Re-use of Data

Related to the structured data discussion (see 2.3.11 above), is the widely held, implicit assumption that data can be automatically reused after exchange in the systems of the DC. Structured data is only one of the prerequisites for automated data re-use. Fully enabling such an automated reuse required not only: 1) Structured data but also 2) established semantic equivalence across MS and 3) compatible data formats and attribute domains that lend themselves to automated transformation and re-use. Without going into the details of different transformation requirements (e.g. reversible vs.

© 870635 DE4A Project Partners

irreversible), it becomes apparent that enabling automated reuse of data is a major challenge across different MS, which is also apparent in the barriers identified in D1.7: S2: Evidence Format and cross-MS Compatibility of Formats and S3: Missing Semantic mapping of data elements.

The way semantic equivalence and data format compatibility can be achieved is a closely related discussion. In simple terms, the two standpoints are:

a) Harmonization of data definitions (semantic standardization and standardization of the syntaxes, i.e. data formats used) through negotiated agreement either by the legislator (e.g. Directive 2016/1191) or by voluntary consensus (i.e. e-Health domain) b) Use of semantic technologies to map different ontologies onto each other, potentially involving machine learning (e.g. used by e-commerce platforms and data aggregators)

2.3.13. Production System and Real-life Cases

The optimal outcome of the DE4A pilots are systems that add real business value to the citizen and enterprises of the participating Member States. There are, however, significant impediments or hard-to-overcome challenges that could make full production go-live impractical or even impossible. Examples are extensions of the eIDAS nodes to support mandates and proxies (see 2.3.9) or the use of non-notified eIDs. These adapted systems would need to run in “acceptance environments” but could still interface with production systems (i.e. identity service providers) and pilots could still be based on real-life cases.

Another example is the availability of a legal basis for issuing evidence to competent authorities in another MS (cf. 2.3.4). Piloting, using real-life cases, can be seen as a required part of developing the OOTS prior to 12.12.2023. Consequently, it is considered to be covered by SDGR Article 14(11). While this interpretation would support piloting, it implies that the pilot solutions can transfer to full production use only after SDG Article 14(1) to (8) and (10) entered into force 12 December 2023. Approaches like signing a Memorandums of Understanding between piloting Member States (authorities) can alleviate this limitation and substantiate a consensus on the interpretation of Article 14 (11).

Pilots and Member States are following strategies to overcome these challenges.

2.3.14. EESSI Integration

Electronic Exchange of Social Security Information (EESSI) is a domain specific, sectoral network that has some overlap with the third use cases in the DE4A Moving Abroad (MA) pilot, i.e. - Request Pension Information & Claim Pension, - both regarding relevant authorities and to exchanged information. Reuse can take different forms, reaching from a full adoption of EESSI for the use case, via a bridge solution that that would use EESSI as a DP on European level, to the adoption of harmonized data models and definitions. The MA pilot has explored the integration with EESSI and concluded we would be overlapping for pensions request as this is already an EESSI use case for which OOTS is not needed. DE4A decided against implementing the pensions request procedure and instead will pilot the pensions info request but with widened scope to include social benefits as well.

2.3.15. BRIS Integration

Business Register Interconnection System (BRIS) is a domain specific, sectoral network that has some overlap with the use cases in the DE4A Doing Business Abroad (DBA) pilot, both in relevant authorities (i.e. business registers) and in exchanged information. Even if BRIS can only be used by (a subset of) business registries themselves, it already provides today an operational exchange of company information across Europe. A reuse of (an extended) BRIS is understandably in the interest of the

© 870635 DE4A Project Partners

participating business registers, however, the possibility of DE4A to create legal and technical changes on the existing BRIS system is very limited. Analysis of the DBA pilot shows that the potential of reuse of BRIS is limited for the pilot, i.e. will remain at the level of the reuse of data definitions.

2.3.16. eIDAS and National Authentication Systems

The question of user authentication in OOP centres around the use of eIDAS, after all this is what eIDAS is there for, to provide cross-border authentication. To focus exclusively on eIDAS might be too restrictive as it would exclude an important user group, namely users that have an eID of the DC country, encompassing own nationals and immigrants. In addition, the current state is that most eProcedures are designed for use by in both national and a cross-border settings and we can safely assume that this will remain the case. This means that the eProcedure offers authentication via the national eID scheme or eIDAS as two alternatives.

Having both eIDAS and the national eID supported can in some cases resolve the issue if a MS has no eIDAS node operational, although this strictly limits the pilot population to users that have (already) an eID of the DC country. At the moment, Romania has no eIDAS node operational; Netherlands and Slovenia support only eIDAS IN.

An interesting new proposal [29] has been presented by the EC: revising the eIDAS regulation to introduce self-determined wallets for citizens with a broader scope than the current eIDAS framework. The aspect of user authentication will evolve and there will be an impact on the OOTS being currently defined.

2.3.17. Non-notified eIDs

Until now the pilots can only move to production with Member States that notified their eID. Not all partners have notified so far. This might limit the possibility to pilot on production environments with all partners. An upcoming eIDAS node release, supporting the usage of non-notified eIDs might solve this issue to a certain extent. Further research is needed though. Austria, Slovenia, and Romania have not notified yet their identification scheme. Currently it is proposed to use pre-production nodes as they would support notified and non-notified eIDs.

2.3.18. Payment for Evidence

As defined as one of the organizational barriers in D1.7[1] Some competent authorities charge fees for retrieving or issuing evidence. Pricing models usually cater for national data consumers, not for cross-border users. There could be a legal or financial arrangement for the piloting phase (and preferably beyond). It is important to understand that the payments can also be required between DC and DP and not only between User and DP. This is in line with the barrier 'Access to data may be subject to charges' identified in D1.7[1].

2.3.19. Trust Management

A consistent framework is needed that provide trust services across the complete OOTS. Having several PKI, or even different trust systems like white-listings, trust lists, or similar in parallel and different nested encryptions will make the overall system unmanageable. In simple terms: we need to make sure that the OOTS is not drowning in key and certificate management complexities. T2.2 set out to develop this trust architecture, initially based on mature technologies and then extending it to include the capabilities of modern block chain technologies.

© 870635 DE4A Project Partners

Irrespective of the technical representation of trust relationships, there might also be an organizational interoperability barrier related to trust. On the one hand, the question whether a DP in one country trusts the DC in another country to handle the exchanged evidence in a trustworthy way. On the other hand, a DC in one country trusting a DP in another country to provide evidence that is correct, up-to-date, and truthful. This issue is beyond the scope of the DE4A pilots, however, discussions around authorization (which DC is allowed to request what type of evidence) or the discussion whether the DP can rely on an explicit user request issued to the DC or must evaluate such request independently of the DC (see also 2.3.4) are all influenced by the barrier of 'Lack of trust (cultural) across Member States' identified in D1.7[1].

2.3.20. Legal Basis for SSI and Block Chain Technology

There are several legal concerns related to Self-Sovereign Identity and blockchain technology, such as the storage of personal data in distributed ledgers or the validity of a decentral identifier. This led Spain to all but ban blockchain from application in eGovernment. By Royal Decree Law 14/2019 it is forbidden use a blockchain infrastructure to offer any identification or signature process (until a European or national law regulates the use of these technologies). Ongoing research, discussions, and progress in context of EBSI and ESSIF are clearly relevant for DE4A. It cannot be ascertained yet whether piloting use cases applying block chain technology can go live in production or would remain exploratory, running in acceptance environments.

The new proposal for revising eIDAS Regulation explicitly contemplates Distributed Ledgers as a new type of trust services and provides an apparently solid legal basis in case SSI may be chosen as the implementation basis for the EU eID and wallets.

2.3.21. Explicit Scope of Article14

The Blueprint of CEF Preparatory Action on OOP adopted a strict interpretation of Article 14: “this exchange pattern is the pattern specified in Article 14. This will therefore become the default evidence exchange pattern of the OOP technical system”.

This should not restrict DE4A to explore other interaction patterns for several reasons: First, initial discussions show that a translation of the legal text into requirements and further into an optimal solution provides more degrees of freedom than implied by the current blueprint version. Second, the blueprint is focussed on meeting the 12.12.2023 deadline, which is not the end, but the start of the Once-Only Technical system. Third, the scope of DE4A is wider than the scope of the SDG implementation.

2.3.22. Matching Evidences between Member States

Evidences that cater for the same or similar life events or public procedures are very heterogenous across MS, as was confirmed by the Deloitte Study on Data Mapping for the cross-border application of the Once-Only technical system SDG [11] and corresponds to the barriers for Once Only, identified in D1.7[1]: Data incompatibility, and Semantic incompatibility of information systems and datasets. This means that in many cases the evidence type required for a procedure in the DC country is meaningless for an evidence issuing authority in the DP country and vice versa. This extends well beyond the question of different languages into the definition of the evidence type itself, the structure and the semantics of its contents.

There is a considerable difference between domains where harmonized evidence types and corresponding schemas and definitions exist and domains without such prior harmonization, which pose a much larger challenge. The approach for matching required evidences (DC side) and available

© 870635 DE4A Project Partners

evidences (DP side) could consequently also differ between harmonized and non-harmonized sectors. DE4A is designing different data models, services and components in the context of the Semantic Framework of WP3 and is fruitfully providing feedback to the SDG Working established for Data Semantics, Formats and Quality.

A good example of the complexities involved are university degrees. Even if the Bologna Process harmonized the three cycles of higher education in the EU, the equivalence of studies and subjects is not established. Trying to offer equivalence between subjects in different degrees in different universities and different countries may be a titanic effort as it extends from the schema (a degree relates to a specific subject of study) to the definition (is it just the study, or is it more specialized, like a set of five subjects in a degree allows a specific mention in a Master's degree) to the attribute domain (which would be the official list/catalogue of studies and subjects in the EU). Relevant ongoing efforts (e.g. EAR project, ENIC-NARIC Network) will be considered in the Studying Abroad Pilot.

2.3.23. Multi-evidence Cases

A Multi-evidence Case is an interaction between Data Consumer and Data Provider, where the Data Consumer needs to request several pieces of evidence for a single eProcedure from one or more Data Providers in one or more Member States. Multi-evidence Cases implies a more complicated scenario for the involved actors and may require multiple requests, previews, responses as well as aggregating evidences. The implications of Multi-evidence Case depends on the interaction pattern used in the procedure, e.g. Intermediation, User-supported Intermediation or Verifiable Credentials. The Table below shows four distinct reasons for the Multi-evidence Case to arise.

Table 1 Reasons for Multi-evidence Cases

	Multiple Data Providers	Multiple Evidence Types	Multiple Evidences of the same type	Evidences for multiple subjects
Description	Multiple Data Providers, either one or several evidence types for the same subject (one user = single subject)	Single Data Provider, multiple evidences of different types for the same subject (one user = single subject)	Single Data Provider, multiple evidence of same type for the same subject (one user = single subject)	Single Data Provider, multiple evidence of same type for different subjects (one user, multiple subjects)
Example	Example from Moving Abroad Pilot: For change of address, several evidence types are required, such as evidence of birth, place of residence, pension claims	Example from Moving Abroad Pilot: In some MS (i.e. ES, SI), a national data portal consolidates evidences from different Data Owners (e.g. Secondary Education evidence and Higher Education Diplomas) and doing so acts as	Example from Studying Abroad Pilot: A student who has multiple diplomas that can be sourced from the same Data Provider. (This can be either the same University or a	Example from Moving Abroad Pilot: A family is moving abroad. In that case a parent might run a single eProcedure instance requiring evidence (e.g. place of residence) from all their family members

© 870635 DE4A Project Partners

	Multiple Data Providers	Multiple Evidence Types	Multiple Evidences of the same type	Evidences for multiple subjects
	and income, which are for most MS issued by different Data Providers.	a single Data Provider for several evidence types.	national diploma repository, holding diplomas from different education service providers).	(e.g.: partner, kids, dependent).
General approach	Several Evidence Requests, resulting in several Evidence Responses, all holding essentially one single evidence.	The Evidence Request and Evidence Response should include multiple canonical evidence IDs and evidence definitions respectively. The request and response would consequently hold an array of evidences. The number of evidence types in the Evidence Request can differ from the number of evidence types that are actually in the response.	The Evidence Response should include multiple evidence definitions. This means that there is a 1:n relation between requested canonical evidence IDs and issued evidences.	It is left to the Data Provider endpoint to validate the representation relationship, which is the preferred option. This means that the Evidence Requestor needs to collect identification information (e.g.: first name, last name, date of birth) that the Evidence Provider can match with their representation registry. The Evidence Request should allow to specify different subjects for either a single or several different canonical evidence IDs and the Evidence Response should include several evidence definitions related to different subjects. This does **not** mean that here are different users! Using the second, end-point centric, approach does not have any impact on authentication and record matching for the User. It adds a separate record

© 870635 DE4A Project Partners

	Multiple Data Providers	Multiple Evidence Types	Multiple Evidences of the same type	Evidences for multiple subjects
				matching challenge for dependent subjects (i.e. children).

2.3.24. Stateless DE4A Connector

Business Processes are either Stateless or Stateful, depending on the transactions contained in the process.

Stateless: a stateless process or application can be understood in isolation. There is no stored knowledge of or reference to past transactions and also the actual state is unknown. Each transaction is made as if from scratch for the first time.

Stateful applications and processes, however, are those that can be returned to again and again, i.e. keeps track of the state of interaction. Stateful processes are intended to support business scenarios that involve complex, long-running logic and supports reuptakes of IT processes and therefore have specific reliability and recovery requirements.

With respect to cross-border exchange of evidence in the context of the Once-Only Technical System there are complex cases where state needs to be maintained between sessions. Examples include multiple DPs, multi-evidence, delay in digitizing evidence, extensive input from the user required etc. It will not be feasible or is impracticable to perform this in one user session. See also 2.3.3 above).

The main purpose of the DE4A Connector however is to:
- shield business parties from the complexity of using eDelivery and the information desk
- facilitating integration in MSs
- addressing the different roles DE/DR (DC) end DT/DO (DP) which might be performed by different entities.

Irrespective of whether a business process is stateful or stateless, the state should not be maintained in the connector. Instead, this is on the DC/DP for doing so if needed.

2.3.25. Highly Distributed, Cross-border System

D1.7 Legal, technical, cultural, and managerial risks and barriers[1] identified 'Administrative Complexity / Organizational silos' and 'Different OOP levels in other EU MS' as two of the main barriers for cross-border once-only. This points to the formidable integration challenge posed by the level of complexity that needs to be managed for a European cross-border, cross-domain Once-Only system to function properly: Integrating across 27 highly heterogenous national eGovernment architectures, administrative systems and legal frameworks.

This is not a typical Enterprise Application Integration (EAI) effort, it is orders of magnitude more complex, encompassing hundreds of organizations and thousands of applications in each of the 27 Member States. As a consequence, best practices and architecture principles from EAI must be treated with caution, as they are not equally applicable for such highly distributed systems. Even simple things like maintaining case-specific single attribute correlation IDs can require changes in thousands of systems and interfaces.

© 870635 DE4A Project Partners

In the DE4A architecture, we are constantly trying to balance "common EAI sense" with the subsidiarity principle and a 'minimal impact on MS systems'-approach in an attempt to follow up on two of the main findings of D1.7[1]:

- cross-border digitization should build upon national digitalization efforts.
- that digitization initiatives should have a positive return on investment.

With 27 national architectures in the mix, every assumption about their functioning, structure, ease of integration, used technology etc. is essentially wrong by definition, because at least one MS will be different. This is even true for the implementation of European building blocks – for instance, not all eIDAS nodes are the same. Minimal assumptions about the national systems and an attempt to couple them as loosely as possible goes beyond defining clear interfaces, because these very interface requirements can have significant implications on national level: a mandatory cross-border correlation ID for example might already have significant impact that is disproportional to using concatenate keys to correlate request and response. The assumption that a platform can provide a static URL that is stable over time or that can accept a specific parameter might not hold for all eProcedure portals, as does the assumption that a portal can provide a case-specific URL; hence the solution should be able to deal with both.

© 870635 DE4A Project Partners

3. Reference Business Architecture

https://wiki.de4a.eu/index.php/Reference_Architecture

DE4A develops a multi-pattern architecture for eGovernment interoperability with a focus on digital-by default procedures for citizens and businesses and the full implementation of the Once-Only Principle. The DE4A Reference Architecture is based on the Architecture Metamodel described in deliverable D2.1[2] and applies the definitions and description language from ArchiMate and BPMN.

The DE4A Architecture Framework defines five architecture Time Horizons, starting from the pre-SDG baseline (t=0, ~2019) and reaching to a long-term vision (t=4, ~2030+) to place different developments in context. More detail on the Architecture Framework is available in the public deliverable D2.1 Architecture Framework.

The development of the DE4A Reference Architecture started in the context of D2.4 Project Start Architecture (PSA) - First iteration and recognized three distinct Reference Interaction Patterns:

- Intermediation Pattern
- User-supported Intermediation Pattern
- Verifiable Credentials Pattern

The design of the Intermediation Pattern took the Single Digital Gateway (SDG) Once-Only Technical System High Level Architecture (HLA) and insights gained from the TOOP Reference Architecture as starting point and was instrumental in uncovering implicit assumptions (i.e. working hypotheses) concerning the fundamental, Interdisciplinary Questions in context of cross-border exchange of evidence. The User-supported Intermediation Pattern can relax some of these hypotheses by introducing a direct interaction between the User and the Data Provider. These two patterns fall in the Time Horizon t=2 (~end 2023), whereas the third pattern, the Verifiable Credentials Pattern open a perspective to the potential future solution and investigates the transformative impact of new blockchain technologies.

Apart from an update to the above patterns, this version of the PSA introduces two additional Reference Interaction Patterns:

- Subscription and Notification Pattern
- Lookup Pattern

The Subscription and Notification Pattern was introduced especially for the Doing Business Abroad pilot second iteration, i.e. the business domain, but is wider in scope and can potentially be used for citizens as well, for instance Life Event Notification. There are two distinct purposes, or business requirements for Subscription and Notification, both of which are relevant for the DE4A Doing Business Abroad Pilot: Evidence update notification and Event notification. This leads to different flavours of the pattern as well as a hybrid form.

Another pattern was introduced for the business domain, i.e. the Lookup Pattern. The basic logic of the Lookup pattern is a light-weight simple Request-Response interaction between DC and DP without any user involvement. We identified two functional variations: Evidence Lookup and the Attribute Lookup.

© 870635 DE4A Project Partners

3.1.Intermediation Pattern

https://wiki.de4a.eu/index.php/Intermediation_Pattern

The Intermediation Pattern is one of the cross-border interaction patterns of the DE4A Reference Architecture (cf. D2.1 Architecture Framework [2])**.** It is used by the Use Case "Starting a Business in Another Member State" (DBA UC1; see section 5.2 below). The Intermediation Pattern is largely derived from the High-level technical Architecture presented by the CEF Preparatory Action for the Once-only Technical System (OOTS) for Article 14 of the Single Digital Gateway Regulation [17].

Several alignment meetings and Workshop between DE4A and SDG Team took place, and the conclusions are reflected in an alignment document [2]produced by the WP2 leader. We can summarize here by stating that a high level of alignment was achieved.

3.1.1. Working Hypotheses and Implementation Principles

The Intermediation Pattern is valid under several working hypotheses, which are based on an architecture analysis and is oriented along the Interdisciplinary Questions identified for the field of cross-border eGovernment interoperability (see also section 2.3 above).

Table 2 Intermediation Pattern Working Hypotheses and Implementation Principles

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Orchestration / Choreography	The DC is orchestrating the overall flow. This means that the (potentially multiple) processes on DP side are child processes of the process on the DC side.	This is essential for the intermediation pattern. The DC manages both the interaction with the User and controls the status of all DP evidence retrieval processes. The DC can retain overall control by reacting to responses of the DP (evidence or error) and monitoring that a response is received in a reasonable amount of time (i.e. SLA)
Complementary, overlapping, or conflicting evidence equivalents	Cases of ambiguous evidences must in principle be supported by the technical system. Deep analysis on whether they are jointly valid or are contradicting each other is left to the public service provider and not included as functionality in the cross-border OOP sequence.	The DE4A pilot cases appear not to be affected by this issue and the canonical evidence approach also means that this issue is usually resolved at the DP-side. Ambiguous, multiple evidences are still possible in a three-country case, which could be piloted in the second iteration.
Interrupted vs. Uninterrupted exchange	Once the OOP sequence is started by receipt of an explicit request, the whole OOP exchange is handled in an uninterrupted manner, while the User remains waiting for the	One example of a disrupted procedure is evidence that is not readily available in a digital format, said to be out of scope of the SDGR, however appears to be a frequent case for older

[2] Not a formal public deliverable but available on request to the project reviewers.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
	evidence. This means that any exception during the OOP exchange leads to the termination of this OOP attempt, potentially to be repeated at a later time as a new attempt. Notwithstanding the possibility for the eProcedure portal of the DC to offer a "save and resume" functionality, the OOP request itself needs to be repeated in its entirety upon returning to the eProcedure. In this way we keep the save and resume entirely in the control of the single Procedure portal and "simulate" a disrupted procedure case, without the need to manage persistent process instances across a multitude of highly independent systems.	evidence that still resides in paper archives. We might consider a sub process at the DP that digitizes the requested evidence and informs the User (e.g. via a direct e-mail) about the evidence now being available in a digital format.
Explicit request and transitivity between actors	After 2023 (with SDGR as legal basis), the DP does not need to re-validate the explicit User request, they can rely on the DC to have done so. It is questionable whether this is presently possible in the Pilots, as the SDGR Article 14 enters into force after the Pilot timeline (Article 39). The assumption is, however, that piloting for the SDGR is part of the public authority tasks related to the SDGR (i.e. fall under the application of Article 14 (11)).	We need the MS participating in the pilots to sustain this interpretation and accept the limitation that the pilot solution cannot transition to full production on grounds of this legal basis, before the full Article 14 of the SDGR enters into force on 12.12.2023.
Preview & Approval UI	The preview can be provided, and the User approval collected, by the DC, prior to the evidence being used in eProcedure. It is well understood that the data processing of the evidence on the part of the DC is restricted to providing the preview to the User. This entails the risk that operators of the receiving competent authority could gain, either by accident or (disingenuous) intent,	There are legal, privacy and security concerns with this hypothesis and there are indications that not all MS are prepared to accept these. A preview provided by the DC would for instance break the privacy-by-design principle. It is also noteworthy that the DP does not know about the outcome of a DC-side preview or would need to be explicitly informed about it.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
	access to the evidence data prior to User authorization.	The preview at the DC side must be able to show previews of evidences from multiple countries and must be implemented for every DC. The DC has in any case to implement a solution guaranteeing “the data included in the preview should not be stored longer than is technically necessary” (recital 47 SDGR) [3] if the User decides not to reuse or to submit the data.
Identity and Record Matching	From experience on MS-level we see that a reasonably good match can result from the use of the (mandatory) eIDAS attributes. The working hypothesis is that this insight can be generalized to all pilot MSs. Two consequences of this hypothesis are that a) the User does not need to provide supplementary attributes and b) a second eIDAS authentication at the DP (potentially multiple DP) is not required.	As the unique matching based on eIDAS attributes cannot always be done (e.g. multiple matches or no match at all) it is only considered sufficient from a piloting perspective, where an unsuccessful match could be dropped from the pilot population. Most MS consider current examples of implementation of record matching as insufficiently matured and scalable across all EU MS. A process must be defined, for example, to manage the situations where this automatic matching does not work. The Intermediation pattern has limitations for catching these exceptions especially in case of an unsuccessful match at the DP, as no direct interaction between User and DP is foreseen.
Transitivity of user identity	After 12.12.2023, the SDGR and the legal task of the DC provide the legal basis for the exchange of User or data subject data from DC to DP. We assume that the development in preparation of the SDGR (i.e. piloting) is part of the public authorities’ tasks covered by the SDGR (i.e. Article 14 (11)), hence that the SDGR provides the legal basis for the pilots. Adding a GDPR consent in the explicit request is not a valid legal	If the intermediation pattern is used in in the citizen domain, we need the MSs participating in the pilots adopting the intermediation pattern to sustain this interpretation.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
	basis for the case that the identification does include personal data of other data subjects than the requestor (e.g. change of address for families).	
Hand-on of UI between actors	The DC handles all user interaction of the eProcedure, including the OOP transfer of evidence, thus eliminating the need to hand-over user sessions across MSs.	This means that the pilot cases do not include additional information, other than included in the initial request and (mandatory) eIDAS attributes, to be used by the DP.
Mandate and Proxy	The mandate and proxy challenge can be resolved by an extension of the eIDAS node. A simple solution can be built on the "full powers"-assumption with current eIDAS functionality.	The results from SEMPER can be adopted for piloting. It is expected that solutions based in this approach cannot go production live within the timelines of DE4A, as it would require an adjustment of the eIDAS Regulation.
Encryption Gap	OOP in the public sector does not require true E2E encryption. The exchange between DR and DT must be encrypted and signed, as well as the transfers (if applicable on national level) between DR and DE on DC side and DT and DO on DP side (i.e. using the national OOP layer), but the encryption gap within the systems of the DR and DT is acceptable.	This might not hold for cases where the gateway would be outsourced to a private sector subcontractor, which is not foreseen for the DE4A pilots.
Structured data vs. unstructured data	Evidence is handled as structured data.	This is not contradicting the addition of an unstructured or scanned document/certificate as part of the structured data transfer (hybrid approach) for reasons of legal validity, in line with the legal barrier of 'L4: National requirements for original and /or certified copies of evidence' identified in Deliverable D1.7 [1].
Automated re-use of data	Evidence and its use in public service procedures has legal consequences. We assume that automated re-use without premediated harmonization of evidence data definitions is not	To facilitate automated re-use of data requires establishing canonical evidence definitions.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
	applicable for the OOP transfer of evidence between MS.	
Production system and real-life cases	With reference to SDGR Article 14(11), pilots based on the intermediation pattern can interface with productive systems and use real-life cases (if participants are made aware that they are participating in a DE4A pilot).	Pilots considering the intermediation pattern must align with their participating MS that they accept the interpretation of the Article 14(11) as legal basis of the pilot even before the full Article 14 of the SDGR enters into force on 12.12.2023. The situation in the business domain is different as the company registration data is already publicly available.
Payment for evidence	In the context of the pilots we assume that no payments are required.	This can restrict transition of pilot solutions to production in cases that competent authorities require payment for issuing evidence.
BRIS integration	A technical re-use or bridge to BRIS is not possible because of differences in scope and accessibility by competent authorities other than business registers. The semantic definitions of BRIS can be largely reused.	The pilot system for the Doing Business Abroad Pilot need to be set-up separate from BRIS.
Matching evidences between Member States	The final system should support both harmonized and non-harmonized evidence type, and the architecture is taking account of both bases. In the pilot context, focus will be put on establishing deep semantic interoperability through the definition of canonical evidences	Heterogeneous, national evidence types do not need to be matched in run-time. For all evidence types in DE4A, a canonical form must be defined an agreed between the pilot partners. Each partner needs to implement a transformation from domestic to canonical evidence.
Multi-evidence Cases	The system should support all four multi-evidence cases, which means that an array of evidence types and evidences must be included in a single OOP request/response.	The second iteration should expand the MVP restriction to a single request to single evidence cases, which requires an update of the Exchange Information Model. It is likely that piloting would focus on simpler cases to show the inclusion of multiple evidences in a single evidence response. The multi-evidence cases are likely not relevant for the Doing Business

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
		Abroad Pilot. Theoretically, the 'Multi Evidence Types'-case could be applied in the second iteration to request e.g. company registration evidence and annual financial statement in a single request.

© 870635 DE4A Project Partners

3.1.2. Business Process Collaboration

Figure 1 below models the intermediation pattern in BPM notation. It consists of three interacting processes, one for the User (U) - the user journey -, one for the Data Consumer (DC) and one for the Data Provider (DP). The message flow (dashed lines) shows the interactions – the conversation – between these participants.

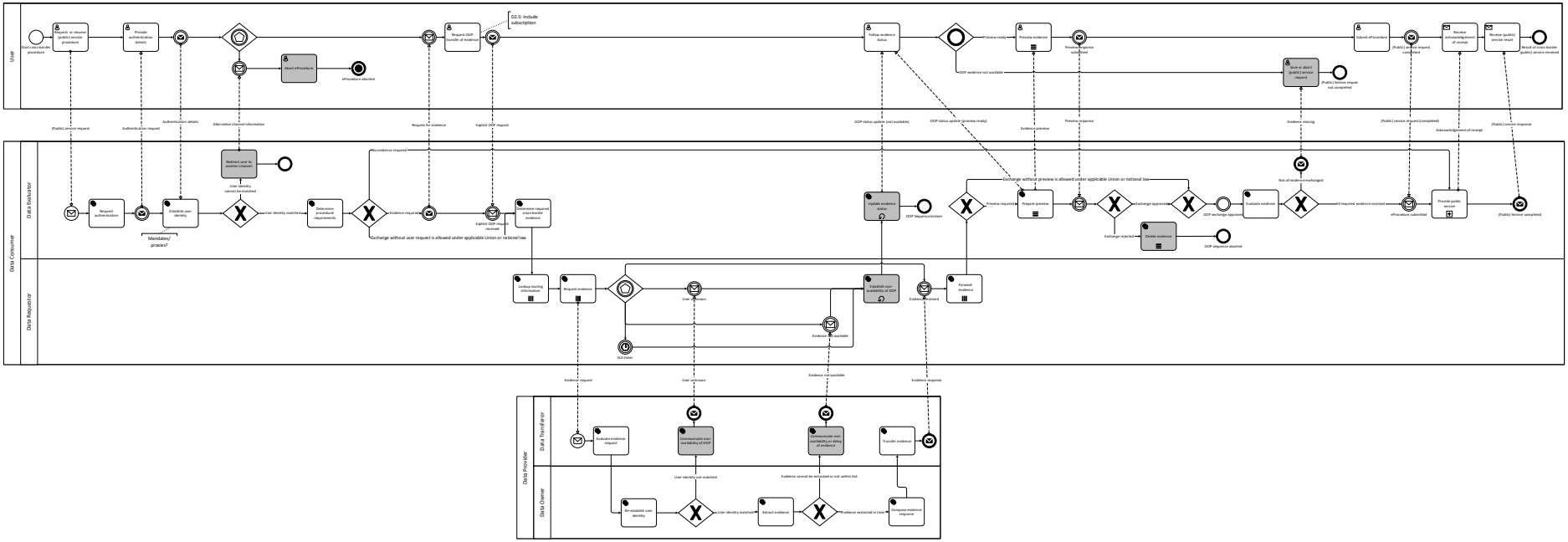


Figure 1 Business Process Collaboration View of the Intermediation Pattern

See also Annex 1 for larger size.

© 870635 DE4A Project Partners

The activities of all participants are listed in roughly chronological order across all three processes in Table 3 below. The conversations between the participants are described in the subsequent two tables ('Conversation between User and Data Consumer' and 'Conversation between Data Consumer and Data Provider').

In this pattern the DC is centre stage, as can easily be seen in the diagram: All user interactions are managed by the DC, acting as the front-office for all other competent authorities involved. The process(es) by potentially several DPs are structurally child-processes of the DC process, which means that the DC needs to retain control of the processes of the DP by tracking their completion, as depicted in the centre of the diagram, using an exclusive event gateway that tracks the desired and alternative DP responses against an SLA timer.

The working hypothesis that the OOP sequence must be executed in an uninterrupted manner is also clearly visible in the diagram: the start (triggered by the explicit OOP request) and end (after User approved preview) are represented by intermediate events all tasks between these two events are fully automated and any exception flows result in the OOP transfer attempt being stopped (after this is communicated via the DC to the User). Consequently, all 'save and resume' functionality is concentrated on the DC Procedure portal and the OOP sequence would need to be repeated in its entirety if unsuccessful on first attempt.

Table 3 lists the business activities of all three processes roughly in chronological order. The first column designates the activities included in the diagram. The second column provides the abbreviation of the responsible role. For a definition of these roles, please refer to Deliverable D2.1 Architecture Framework [2]. The third column contains the task type (see BPMN 2.0 standard specification[20]) as shown in the diagram above. Please consider that the task type 'User' means that it is a Human/Computer interaction task, not that it is in the responsibility of the User (U) as defined in the Architecture Framework or in Article 3(1) of the SDGR. The fourth column describes the business activity in concise language.

Table 3 Business Activities of the Intermediation Pattern

Activity / UC	Role	Type	Description
Request or resume (public) service procedure	U	User	The User navigates to the eProcedure in the DC country and requests a (public) service. This means they fill in the required information and start the eProcedure. It is specific to the MS and the eProcedure how much information is provided by the User (i.e. which fields to be filled out) in this activity (i.e. prior to authentication) or when submitting the eProcedure later in the process. Email should be included as means to contact the User or provide updates. If the User is returning to a previously started procedure, the eProcedure will return to original instance after authentication.
Request authentication	DE	Service	The DE requests the User to authenticate themself. This can happen in two ways, either using eIDAS (default) or using the eID of the DC MS, in case that the User has the national eID of the DC country available. The DE provides both options to the User.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
Provide authentication details	U	User	The User uses the means available to them to provide the authentication details. This can happen at the User's discretion using the eID of the DC MS or eIDAS. In the second case, the User is forwarded to the authentication service of the identity provider of their means of authentication. If the User is representing another entity (typically a legal person), this relation is also retrieved as part of this authentication.
Establish user identity	DE	Service	The DE establishes the identity of the User in the DC MS environment. In the eIDAS case, this means that the eIDAS uniqueness ID must be linked to the national identification number used to access the MS registries. In the national eID case, this means that the eIDAS attributes (mandatory and optional) must be retrieved for further use in the process. In case of business user, the company identification must be matched. The match of the representing natural person to a population register is not required in all MS.
Redirect user to another channel	DE	Service	Exception handling activity: The User cannot be identified in an automated way by the DC and alternative digital or non-digital channel information (depending on the eProcedure at hand user and potentially dependent on the type of identification error) is collected and provided to the User.
Abort eProcedure	U	User	Exception handling activity: Alternative channel information is displayed to the User and the User exits the e-procedure.
Determine procedural requirements	DE	Service	The DE compares the available information (i.e. in the DC MS registries via the national OOP layer) with the information required by the eProcedure. The result can be a (list of) required evidence, defined in terms of the DC country, which is then displayed to the User as a request to provide the evidence, together with the option for the User to request the evidence via the OOTS. This activity is not trivial and should prevent that we ask a User for evidence that is readily available in the DC MS and might not be available in the OOTS cross-border scope. Example: It would not make any sense for a Dutch DC to ask a German national born in the Netherlands to provide a birth certificate (which he could not get via the OOTS as it is not cross-border). A similar situation would be asking a French national with a Belgian university diploma to provide that diploma in order to be admitted for a PhD in another Belgian university.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
Request OOP transfer of evidence	U	User	The User choses to request the evidence to be fetched for them using the OOTS – the explicit OOP request. The User also indicates – in a guided way – which MS, and possibly lower administrative level, issues the required evidence. Alternatively, the User could provide (i.e. upload) the evidence, but that would not involve the OOTS at all, so we are not considering this case in the reference architecture.
Determine required cross-border evidence	DE	Service	The required evidence type (in terms of the DC country) is translated into equivalent evidence types that are issued in a lawful way in the DP country indicated by the User. This is next to trivial if canonical evidences are agreed.
Lookup routing information	DR	Service	The DR retrieves the technical routing information (e.g. eDelivery rooting identifier or URL of the webservice provider), based on the evidence type (in terms of DP country) and the issuing competent authority (or geographic scope of authority).
Request evidence	DR	Service	The DR encrypts, signs, and sends the evidence request to the identified technical data service interface of (potentially several) DP. The evidence request must include user information that enables the DP to identify for which User or represented company the evidence must be issued.
Evaluate evidence request	DT	Service	The DT receives and decrypts the request and checks whether the request meets formal requirements and can be accepted. It should be checked whether the requesting competent authority can reasonably and rightfully request that specific type of evidence.
Re-establish user identity	DO	Service	The DO matches the information about the User (i.e. eIDAS mandatory and optional attributes) with the DP country's records to identify the User in their systems. This amounts to matching the eIDAS attributes to a national identification number. This is a Data Owner activity, because in a distributed scenario the Data Transferor might not have a legal basis to do so. In some cases, however, DT could have a legal basis (on a national level).
Communicate non-availability of OOP	DT	Service	Exception handling activity: The DT informs the DR that the User cannot be identified unequivocally and the OOTS cannot be used to transfer the evidence.
Extract evidence	DO	Service	The DO extracts the requested evidence from their registry and forwards it to the DT.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
Communicate non-availability of evidence	DT	Service	Exception handling activity: The DT informs the DR that the requested evidence cannot be provided or cannot be provided within the agreed SLA.
Establish non-availability of OOP	DR	Service	Exception handling activity: The DR catches the negative (non-evidence) response from the DT and establishes the reason in terms of the DC country system and language: There are potentially several reasons why an OOP transfer of evidence is not available. The DT communicates these reasons to the DR in all cases that the evidence request cannot be fulfilled (i.e. by sending the digitally available evidence within the agreed SLA as described above). At the moment we expect at least the following reasons for such an exception that should be framed in standard error messages or codes, each one with a corresponding recommendation to the User. • User cannot be uniquely identified – fallback to another channel (i.e. IMI) • Evidence not found – Check whether the request specified the correct geographical scope of authority and contact the DP directly if that was the case • Evidence transfer blocked for legal or authorization reasons – Contact the DP directly • Evidence is not readily available in a digital format now. Expected time for the evidence to be available is x days – return after x days and issue a new evidence request
Update evidence status	DE	Service	The DE updates the status of a requested evidence and provides that update to the User in the evidence overview. Additionally, the update could be sent to the User via email, including a link to the status overview page.
Follow evidence status	U	User	After the User requested the OOP transfer of evidence, they observe the status of the evidence request on an evidence status overview. It essentially shows the progress or the request for each separate requested evidence. These statuses should include: • Evidence requested, expected response in x minutes/seconds • Preview available (click here) • Evidence approved • SLA overrun – please try again later • User identification failed

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			• Evidence not available • Evidence expected to be available in y days – please return If a preview is ready for the User this is shown in the overview, including a link (or similar) that allows the User to navigate to the preview.
Compose evidence response	DO	Service	The DO prepares the extracted evidence to be send as an evidence response. Depending on the level of harmonization of the evidence type this task can differ in complexity. If a canonical evidence definition is agreed, this task includes the translation of the national definitions into the canonical evidence.
Transfer evidence	DT	Service	The DT creates the evidence response message (compliant to agreed message format), encrypts, and signs the message and sends it to the DR.
Forward evidence	DR	Service	The DR registers the receipt, decrypts the message and in many cases encrypts the message in a MS specific format to hand it on to the DE. It must also be established whether the evidence can be used right away, because the exchange is allowed under EU or national law or must be previewed.
Prepare preview	DE	Service	The DE prepares a preview for the User and provides it to UI to be displayed in the User session.
Preview evidence	U	User	The User can view the evidence in a UI or UI component (i.e. widget/frame) separate from the actual eProcedure form (i.e. the preview should not be data auto-filled in the eProcedure form itself. This requires an aligned UI framework in the MS. Alternatively, the Preview could be provided in a second window/tab (with consideration for accessibility requirements). In any case, the User can approve the use of the evidence in the eProcedure or can decline the use of the evidence. The User should be reassured that the evidence is not kept by the DC in case of non-approval.
Delete evidence	DE	Service	Exception handling activity: An evidence that was declined by the User must be deleted permanently from all systems in the DC MS.
Evaluate evidence	DE	Service	The DE checks whether all requested evidences are available and validates that they conform to the evidence type requested. In the positive scenario that all evidences are available, the DE communicates to the User that the procedure can be submitted. In the negative case that not all evidences are received, the DE communicates this

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			back to the User. The Procedure can then not be completed.
Save or abort (public) service request	U	User	Exception handling activity: The User is informed that not all required evidence could be received, hence that there are still missing evidences preventing the eProcedure to be completed. It depends (only) on the functionality of the specific eProcedure portal what options are provided to the User. We expect that in most cases the User can save the procedure in order to return at a later stage, to repeat the cross-border OOP request or to provide the missing evidence themself.
Submit eProcedure	U	User	The User fills the remaining fields required for the eProcedure. It is specific to the MS and the eProcedure which fields to be filled out in this activity or when requesting the eProcedure at the start of the process. Usually, the User is prompted to verify the provided information in an overview before hitting the Submit button.
Receive acknowledgement of receipt	U	Receive	The User is waiting to receive the acknowledgment that their (public) service request is received in order and that the service will be provided, oftentimes incl. an indication of the expected time needed. The acknowledgment can be displayed in the eProcedure portal or sent by e-mail or deposited in a government-hosted, secure message box or a combination of the above.
Provide public service	DE	Sub-process	This is a subprocess that is very heterogeneous in composition and timeline, depending on which public service is provided and by which competent authority. Theoretically, the subprocess could be fully automated in some cases, but typically this is a back-office process involving multiple activities of public servants and might take days to several weeks. In many countries the maximum time for this process is defined by law.
Receive (public) service result	U	Receive	Once the public service is completed, the result is provided to the User. This communication is fully dependent on the functionalities of the eProcedure portal (e.g. e-mail and/or government-hosted, secure message box).

Table 4 describes the conversation between User and DC by listing the exchanged messages in chronological order. Table 5 does the same for the conversation between DC and DP. It lies at the core of the Intermediation pattern that there is no direct conversation between User and DP, in contrast to the User-supported Intermediation Pattern and the Verifiable Credentials Pattern.

© 870635 DE4A Project Partners

Table 4 Intermediation - Conversation between User and Data Consumer

From	Message	To	Description
U	(Public) service request	DC	The choice of public service requested and an initial set of information from the User required for the initiation of the request (breadth and type of information can vary between MS and requested service and can be substantial in some cases. Essentially this includes all information that the User provides prior to the point in the procedure where authentication is required). Inclusion of e-mail could facilitate (additional) messages to the User.
DC	Authentication request	U	Link to UI of the identity service provider, potentially to several alternative eID services
U	Authentication details	DC	Identity information of the User (i.e. uniqueness ID + identification data set)
DC	Alternative channel information	U	Contact information (e.g. email, telephone, or address) of an alternative channel to request the public service or to complete authentication/registration
DC	Request for evidence	U	List of evidences (in terms of the DC country) that are required to complete the eProcedure
U	Explicit OOP request	DC	Information about the geographic scope of authority for identifying the type of evidence and the data service provider (e.g. which MS ministry, region, municipality)
DC	OOP status update (not available)	U	Error message to the User (see activity description) explaining the reason why the evidence could not be retrieved and recommendation of action
DC	OOP status update (preview ready)	U	Status update that the preview is ready to be viewed including the link to the preview page
DC	Evidence preview	U	Rendered preview of the evidence
U	Preview response	DC	Accepting or declining of the evidence exchange
DC	Evidence missing	U	Message to the User that not all evidence could be retrieved and that they can resume the eProcedure once all evidence can be provided (either by the User or via the system)
U	(Public) service request (completed)	DC	Complete and final submission of the (public service request), including all required information
DC	Acknowledgement of receipt	U	Acknowledgement that the eProcedure was submitted and the (public) service can be provided to the User
DC	(Public) service response	U	The result of the (public) service, irrespective of how it is provided (post, email, secure message box, personal appearance.

© 870635 DE4A Project Partners

Table 5 Intermediation - Conversation between Data Consumer and Data Provider

From	Message	To	Description
DC	Evidence request	DP	Must include user identification (eIDAS attributes, mandatory and possibly optional). Could additionally include the User email for direct communication
DP	User unknown	DC	Message that the User could not be identified
DP	Evidence not available	DC	Message that the evidence does not exist or could not be retrieved in time
DP	Evidence response	DC	The evidence in electronic format

3.1.3. Process Realization

The Process Realization viewpoint is adapted from the Service Realization Viewpoint mentioned in the ArchiMate 3.1 specification as was described in the Architecture Framework [2]. It is the bridge between business architecture and application architecture in DE4A, defining which application services are required and which Application Collaboration realize these services in order to execute the business activities derived from the business requirements. The Business Activity objects are occurrences of the activities in the Business Process Collaboration.

© 870635 DE4A Project Partners

Figure 2 below shows how the User process (cf. Figure 1 above, 'Business Process Collaboration View of the Intermediation Pattern') is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by the application collaborations named below.

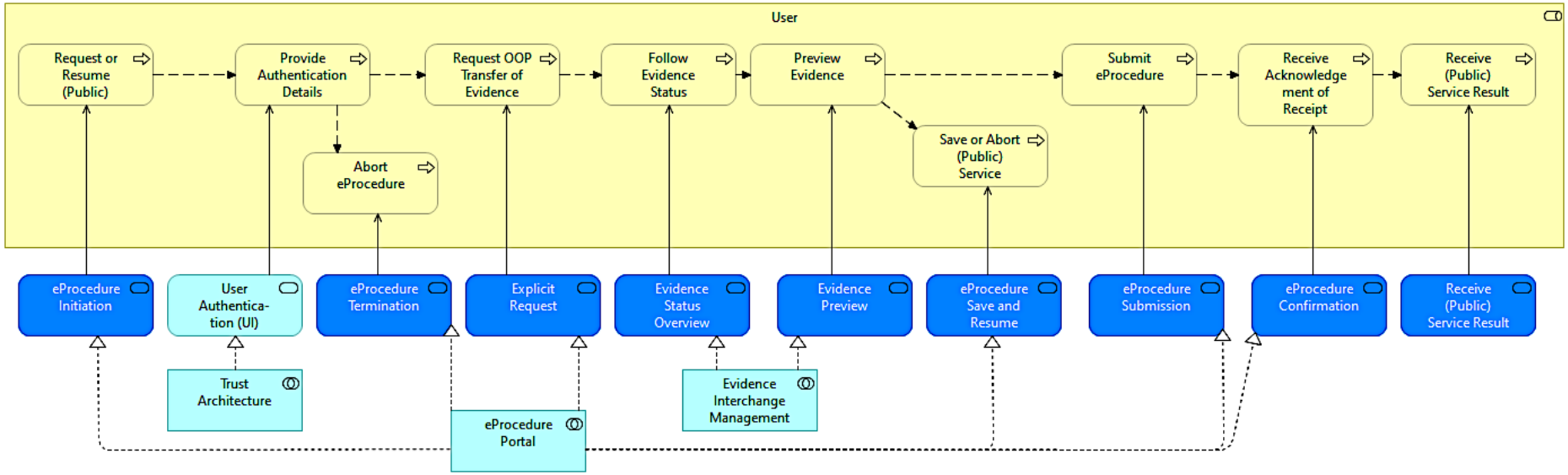


Figure 2 Process Realization of the User Process

The User requests (or resumes) a public service via the eProcedure Portal (see section 4.1 below) and has to authenticate themself through the Trust Architecture (see section 4.4 below). The User can choose to abort the eProcedure, or, if the authentication is successful, request a transfer of evidence via the OOP Technical System (eProcedure Portal).

The User can follow the Evidence Status and preview the Evidence once transferred (Evidence Interchange Management, section 4.3 below). Via the eProcedure Portal the User can save the eProcedure to continue it at a later point in time or abort it altogether if they wish so. Confirmation reception of the evidence by the DC and finally submission of the eProcedure is also provided by eProcedure Portal after which the public service can be offered to the User.

© 870635 DE4A Project Partners

Figure 3 below shows how the Data Consumer process (cf. Figure 1, 'Business Process Collaboration View of the Intermediation Pattern') is served by application services (dark blue: DE4A specific, light blue: EIRA).

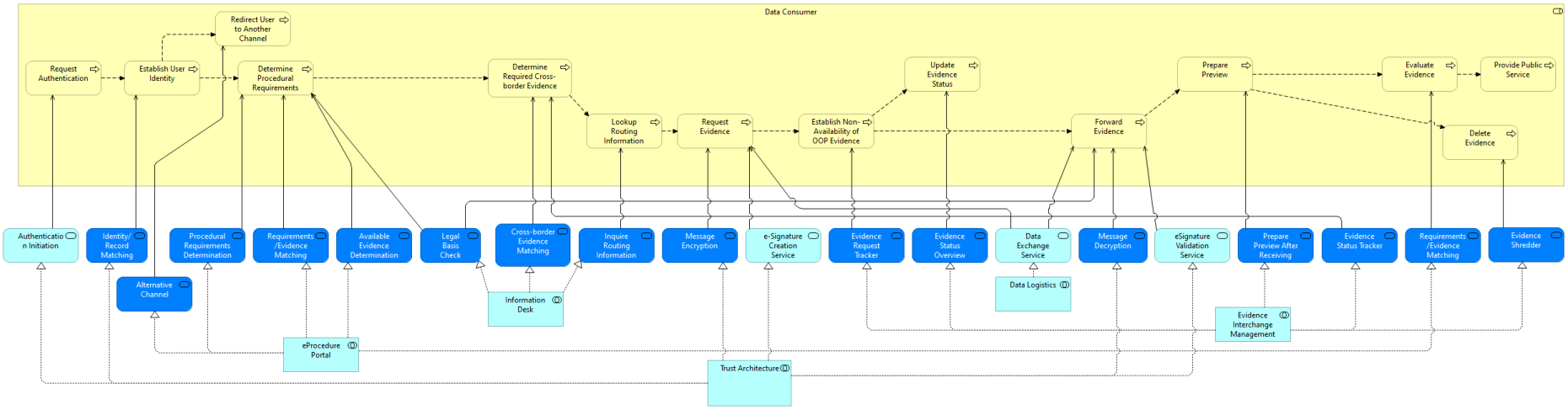


Figure 3 Process Realization of the DC Process

The DC initiates the authentication of the User in order to establish his identity (Trust Architecture, section 4.4 below). If this fails, the User may be directed to an alternative channel via (eProcedure Portal, section 4.1 below). If authentication is successful, the DC has to determine the procedural requirements, match those requirements with the Evidence needed and determine what Evidence is already available (all through the eProcedure Portal).

With the help of the Information Desk (section 4.2 below) the required cross-border evidence is determined, and the relevant routing information is looked up.

Next the Evidence can be requested, the request message is encrypted and digitally signed using the Trust Architecture. The evidence is exchanged using Data Logistics (section 4.5 below) and its status can be tracked via the Evidence Interchange Management (section 4.3 below).

The signature of the received message is validated, and the message decrypted (Trust Architecture). Via Evidence Interchange Management the evidence is prepared for preview. After approval of the User, the evidence can be evaluated by the DC and the public service can be provided to the User. If the User does not approve the evidence, it must be deleted (also Evidence Interchange).

© 870635 DE4A Project Partners

Figure 4 shows how the Data Provider process (cf. Figure 1, 'Business Process Collaboration View of the Intermediation Pattern') is served by application services (dark blue: DE4A specific, light blue: EIRA).

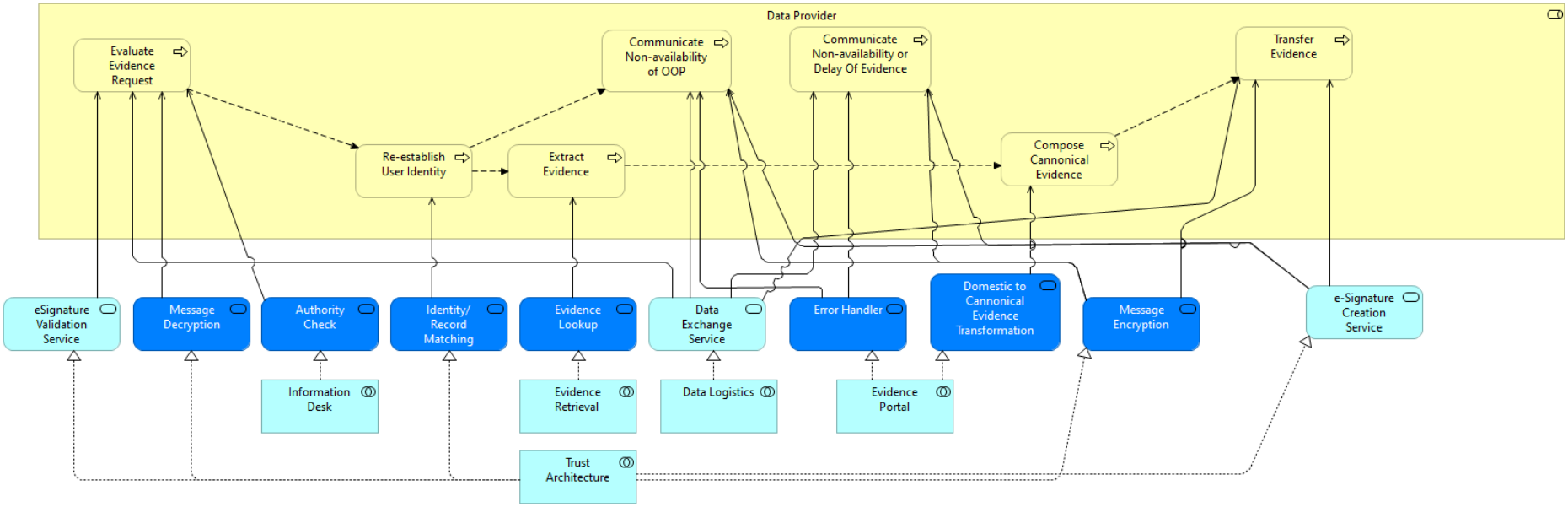


Figure 4 Process Realization of the DP Process

The Evidence request is received via Data Logistics (see section 4.5 below). With the help of the Trust Architecture (section 4.4 below) the DP checks the signature of the request and decrypts it. An Authority check may be performed using the Information Desk (section 4.2 below) establishing that the DC is allowed to request the evidence type. Next the user identity is re-established using Trust Architecture.

If this successful the evidence is extracted by Evidence Retrieval (section 4.7 below) and transformed to canonical form (Evidence Portal, section 4.6 below). Various exceptions like non-availability of OOP or the delay or non-availability of evidence are handled by Data Logistics and Evidence Portal.

If all is well the Evidence is prepared for transfer, encrypted and digitally signed using Trust Architecture and ultimately exchanged using Data Logistics.

© 870635 DE4A Project Partners

3.2.User-supported Intermediation Pattern

https://wiki.de4a.eu/index.php/User-supported_Intermediation_Pattern

The User-supported Intermediation Pattern is one of the cross-border interaction patterns of the DE4A Reference Architecture [2]. It is used by the following use cases:

- "Request Address Change" (MA UC1, see section 5.3 below)
- "Request an Extract or Copy of a Civil State Certificate" (MA UC2, see section 5.3 below)
- "Request Pension Information - Claim Pension" (MA UC3, see section 5.3 below)
- "Application to Public Higher Education" (SA UC1, see section 5.1 below)
- "Applying for Study Grant" (SA UC2, see section 5.1 below)

3.2.1. Working Hypotheses and Implementation Principles

The User-supported Intermediation (USI) reference interaction pattern is valid under several working hypotheses. They can be considered a tool for understanding the implications of applying the USI and should be considered by the partners participating in the use cases mentioned above.

Table 6 User-supported Intermediation Pattern Working Hypotheses and Implementation Principles

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Orchestration / Choreography	The DC is orchestrating the overall flow. This means that the (potentially multiple) processes on DP side are child processes of the process on the DC side.	This is also essential for the User-supported intermediation pattern. The DC manages the interaction with the User in context of the eProcedure and controls the status of all DP evidence retrieval processes. The control of the overall process is thus not transferred to the User.
Complementary, overlapping, or conflicting evidence equivalents	Cases of ambiguous evidences must in principle be supported by the technical system. Deep analysis on whether they are jointly valid or are contradicting each other is left to the public service provider and not included as functionality in the cross-border OOP sequence.	Identical to the Intermediation Pattern (see section 3.1 above). The DE4A pilot cases appear not to be affected by this issue and the canonical evidence approach also means that this issue is usually resolved at the DP-side. Ambiguous, multiple evidences are still possible in a three-country case, which could be piloted in the second iteration.
Interrupted vs. Uninterrupted exchange	The assumption can be slightly relaxed in comparison to Intermediation, as the direct interaction between User and DP makes it easier to communicate delays transparently.	One example of an interrupted procedure is evidence that is not readily available in a digital format said to be out of scope of the SDGR, however appears to be a frequent case for older evidence that resides still in paper archives. We could

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
	In order to prevent that process instances, need to be kept alive across multiple platforms in multiple MS, we treat the interdependencies similar to the Intermediation Pattern. This means that if the evidence is delayed, i.e. because it is not yet available in digital form, a second essentially independent request needs to be issued in a later attempt. A “save and resume” functionality on the side of the eProcedure portal of the DC becomes, of course, more important, because of the higher probability that the eProcedure session hits a time-out during the additional time involved in the direct interaction of the User with the DP in comparison to the Intermediation pattern.	consider a subprocess at the DP that digitizes the requested evidence and informs the User (e.g. via a direct e-mail) about the evidence now being available in a digital format. This is, however, outside of the scope of DE4A piloting
Explicit request and transitivity between actors	The assumption can be relaxed in comparison to the Intermediation pattern.	The User authenticates themself at the DP and explicitly sustains the request issued to the DC.
Preview & Approval UI	The assumption can be relaxed in comparison to the Intermediation pattern: The preview is provided by the DP, prior to the evidence being sent.	The preview is provided by the DP. The preview must only show previews of evidences from the DP themselves. Nevertheless, a national preview solution that is shared by all DP in that country could be considered as an efficient solution.
Identity and Record Matching	The assumption can be relaxed in comparison to the Intermediation pattern: The direct User interaction with the DP makes soliciting additional information easier.	In case of a User authentication at the DP, using an eID of the DP country, record matching is not needed. If eIDAS is used, then the DP can solicit additional information from the User to perform the match as part of the eIDAS authentication session.
Transitivity of user identity	The assumption can be relaxed in comparison to the Intermediation pattern: The user identity does not need to be transferred from DC to DP.	The User authenticates themself at the DP.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Hand-on of UI between actors	The DP messages the URL to the DC that the User can navigate to.	Especially in multi-evidence cases, the DC must display the link to the DP evidence portal to the User. Auto-redirect could only be applicable in single-evidence cases, but the added ease should be balanced with the loss of transparency.
Mandate and Proxy	Identical to Intermediation, however not relevant for the DE4A pilots: The mandate and proxy challenge can be resolved by an extension of the eIDAS node.	The matching of interaction pattern to pilot use cases means that the DBA pilot is not intending to use the User-supported Intermediation pattern, hence mandates and powers are not in scope.
Encryption Gap	Identical to Intermediation: OOP in the public sector does not require full E2E encryption. The exchange between DR and DT must be encrypted and signed, as well as the transfers (if applicable on national level) between DR and DE on DC side and DT and DO on DP side (i.e. using the national OOP layer), but the encryption gap within the systems of the DR and DT is acceptable.	This might not hold for cases where the gateway would be outsourced to a private sector subcontractor, which is not foreseen for the DE4A pilots.
Structured data vs. unstructured data	Identical to Intermediation: Evidence is handled as structured data.	This is not contradicting the addition of an unstructured or scanned document/certificate as part of the structured data transfer (hybrid approach) for reasons of legal validity
Automated re-use of data	Identical to Intermediation: Evidence and its use in public service procedures has legal consequences. We assume that automated re-use without premediated harmonization of evidence data definitions is not applicable for the OOP transfer of evidence between MS.	To facilitate automated re-use of data requires establishing canonical evidence definitions.
Production system and real-life cases	The direct interaction between User and DP allows the pilot to go live in production under current national legal constraints	

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Payment for evidence	Identical to Intermediation: In the context of the pilots, we assume that no payments are required.	This can restrict transition of pilot solutions to production in cases that competent authorities require payment for issuing evidence.
Matching evidences between Member States	Identical to Intermediation: The final system should support both harmonized and unharmonized evidence type and the architecture is taking account of both bases. In the pilot context, focus will be put on establishing deep semantic interoperability through the definition of canonical evidences	Heterogeneous, national evidence types do not need to be matched in run-time. For all evidence types in DE4A, a canonical form must be defined an agreed between the pilot partners. Each partner needs to implement a transformation from national to canonical evidence.
Multi-evidence Cases	Identical to Intermediation: The system should support all four multi-evidence cases, which means that an array of evidence types and evidences must be included in a single OOP request/response. Multiple Data Providers: If Data Providers are not highly integrated on MS-level, then the User needs to re-authenticate on several different platforms and perform a preview in different platforms with potentially different look and feel. Multiple Evidence Types: User needs to authenticate only once at the Data Provider. Data Provider offers Preview for all canonical evidences at the same time. Multiple Evidences of the same type: User previews all canonical evidences at the same time. The User can select a subset of evidences for transfer to the Data Consumer. Evidences for multiple subjects: The multiple-subject case (i.e. parent with children) requires a separate record matching for the representation register. We expect that this can be done appropriately, based on the matched record of the	The second iteration should expand the MVP restriction to include multi evidence cases, which requires an update of the Exchange Information Model. It is likely that piloting would focus on simpler (i.e. single user/subject) cases to show the inclusion of multiple evidences in a single evidence response.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
	User (i.e. parent) and the combination of first name, last name and date of birth of the dependent (i.e. child).	

3.2.2. Business Process Collaboration

Figure 5 models the User-supported Intermediation pattern in BPMN notation. It consists of three interacting processes, one for the User (U) - the user journey -, one for the Data Consumer (DC) and one for the Data Provider (DP). The message flow (dashed lines) shows the interactions - the conversation - between these participants.

In Table 7 Business Activities of the User-supported Intermediation Pattern the activities of all participants are listed roughly in chronological order across all three processes. The conversations between the participants are subsequently described in Table 8, Table 9, and Table 10, listing the messages between the User and DC, between DC and DP, and between User and DP, respectively.

© 870635 DE4A Project Partners

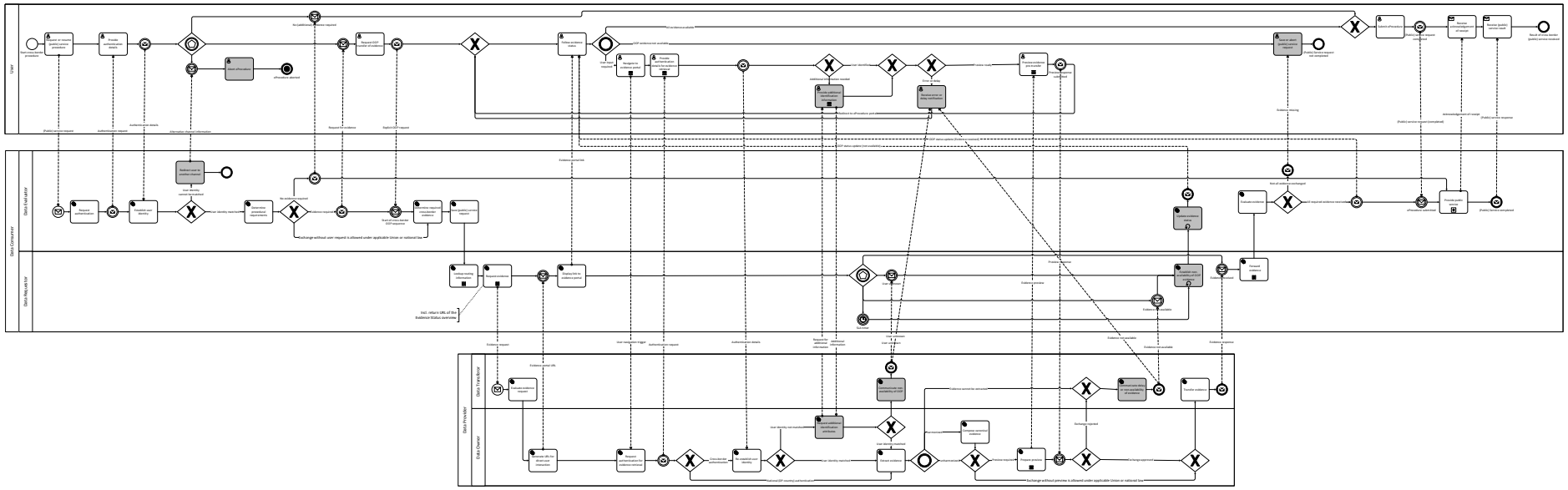


Figure 5 Business Process Collaboration View of the User-supported Intermediation Pattern

See also Annex 2 for larger size

In Table 7 the business activities of all three processes are listed roughly in chronological order from left to right. The first column names the activities shown in Figure 5 above. The second column provides the abbreviation of the responsible role. For a definition of these roles, please refer to the DE4A Deliverable D2.1 Architecture Framework [2]. The third column contains the task type as shown in Figure 5 above (please refer to the BPMN 2.0 standard specification[20]). Please consider that the task type 'User' means that it is a Human/Computer interaction task, not that it is in the responsibility of the User (U) as defined in the Architecture Framework or in Article 3(1) of the SDGR. The fourth column describes the business activity in concise language.

© 870635 DE4A Project Partners

Table 7 Business Activities of the User-supported Intermediation Pattern

Activity / UC	Role	Type	Description
Request or resume (public) service procedure	U	User	Identical with the Intermediation Pattern: The User navigates to the eProcedure in the DC country and requests a (public) service. This means they fill in the required information and start the eProcedure. It is specific to the MS and the eProcedure how much information is provided by the User (i.e. which fields to be filled out) in this activity (i.e. prior to authentication) or when submitting the eProcedure later in the process. Email should be included as means to contact the User or provide updates. If the User is returning to a previously started procedure, the eProcedure will return to original instance after authentication.
Request authentication	DE	Service	Identical with the Intermediation Pattern: The DE requests the User to authenticate themself. This can happen in two ways, either using eIDAS (default) or using the eID of the DC MS, in case that the User has the national eID of the DC country available. The DE provides both options to the User.
Provide authentication details	U	User	Identical with the Intermediation Pattern: The User uses the means available to them to provide the authentication details. This can happen at the User's discretion using the eID of the DC MS or eIDAS. In the second case, the User is forwarded to the authentication service of the identity provider of their means of authentication. If the User is representing another entity (typically a legal person), this relation is also retrieved as part of this authentication.
Establish user identity	DE	Service	Identical with the Intermediation Pattern: The DE establishes the identity of the User in the DC MS environment. In the eIDAS case, this means that the eIDAS uniqueness ID must be linked to the national identification number used to access the MS registries. In the national eID case, this means that the eIDAS attributes (mandatory and optional) must be retrieved for further use in the process. In case of business user, the company identification must be matched. The match of the representing natural person to a population register is not required in all MS.
Redirect user to another channel	DE	Service	Identical with the Intermediation Pattern: Exception handling activity: The User cannot be identified in an automated way by the DC and alternative digital or

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			non-digital channel information (depending on the eProcedure at hand user and potentially dependent on the type of identification error) is collected and provided to the User.
Abort eProcedure	U	User	Identical with the Intermediation Pattern: Exception handling activity: Alternative channel information is displayed to the User and the User exits the e-procedure.
Determine procedural requirements	DE	Service	Identical with the Intermediation Pattern: The DE compares the available information (i.e. in the DC MS registries via the national OOP layer) with the information required by the eProcedure. The result can be a (list of) required evidence, defined in terms of the DC country, which is then displayed to the User as a request to provide the evidence, together with the option for the User to request the evidence via the OOTS. This activity is not trivial and should prevent that we ask a User for evidence that is readily available in the DC MS and might not be available in the OOTS cross-border scope. Example: It would not make any sense for a Dutch DC to ask a German national born in the Netherlands to provide a birth certificate (which he could not get via the OOTS as it is not cross-border). A similar situation would be asking a French national with a Belgian university diploma to provide that diploma in order to be admitted for a PhD in another Belgian university.
Request OOP transfer of evidence	U	User	Identical with the Intermediation Pattern: The User choses to request the evidence to be fetched for them using the OOTS – the explicit OOP request. The User also indicates – in a guided way – which MS, and possibly lower administrative level, issues the required evidence. Alternatively, the User could provide (i.e. upload) the evidence, but that would not involve the OOTS at all, so we are not considering this case in the reference architecture.
Determine required cross-border evidence	DE	Service	Identical with the Intermediation Pattern: The required evidence type (in terms of the DC country) is translated into equivalent evidence types that are issued in a lawful way in the DP country indicated by the User.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
Save (public) service request	DE	Service	The eProcedure and all information provided by the User is automatically saved, in order for the User to be able to resume the procedure at a later time, e.g. after a session time-out during the interaction between the User and the DP.
Lookup routing information	DR	Service	The DR retrieves the technical routing information (e.g. eDelivery rooting identifier or URL of the webservice provider), based on the evidence type (in terms of DP country) and the issuing competent authority (or geographic scope of authority).
Request evidence	DR	Service	The DR encrypts, signs, and sends the evidence request to the identified technical data service interface of (potentially several) DP. The evidence request must include the return URL of the Evidence Overview in the eProcedure portal, enabling the DP to direct the User back to the DC eProcedure. It should also include user information that enables the DP to identify for which User or represented company the evidence must be issued.
Evaluate evidence request	DT	Service	The DT receives and decrypts the request and checks whether the request meets formal requirements and can be accepted. Because of the direct interaction between User and DP the authority check is not needed, i.e. to check whether the requesting competent authority can reasonably and rightfully request that specific type of evidence.
Generate URL for direct user interaction	DO	Service	The DP generates a URL as landing place for the User that is specific for the required evidence type.[3]
Display link to evidence portal	DR	Service	The link to the specific landing page, received from the DP, is displayed as clickable element (link or button) in the Evidence Status overview.
Navigate to evidence portal	U	User	The User clicks on a link to the evidence portal of the respective DP that is displayed in eProcedure portal of the DC.
Request authentication for evidence retrieval	DO	Service	The DO requests the User for to authenticate themself. This can happen in two ways, either using eIDAS (default) or using the eID of the DP MS, in case that the User has the national eID of the DP country available. The case of using the national eID scheme would consequently be quite common.

[3] WP5 addressed a number of points to avoid issues with the USI pattern [30]

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			The DP provides both options to the User.
Request additional identification attributes	DO	Service	If the User identity cannot be matched, the DO displays to User a UI requesting additional identification attributes to improve the probability of finding a match.
Provide authentication details for evidence retrieval	U	User	The User uses the means available to them to provide the authentication details. This can happen at the User's discretion using the eID of the DP MS or eIDAS. In the second case, the User is forwarded to the authentication service of the identity provider of their means of authentication.
Re-establish user identity	DO	Service	The DO matches the information about the User (i.e. eIDAS attributes) with DP country records to identify the User in their systems. This amounts to matching the eIDAS attributes to a national identification number. (If the national eID is used, this task is skipped). Data Owner activity, because in a distributed scenario, the Data Transferor might not have a legal basis to do so.
Provide additional identification information	U	User	Exception handling activity: Interactive form- or chat-based Q&A for additional identification information (beyond eIDAS attributes). The requested information clearly depends on the available information at the Data Provider.
Communicate non-availability of OOP	DT	Service	Identical with the Intermediation Pattern: Exception handling activity: The DT informs the DR that the User cannot be identified unequivocally and the OOTS cannot be used to transfer the evidence.
Extract evidence	DO	Service	Identical with the Intermediation Pattern: The DO extracts the requested evidence from their registry and forwards it to the DT.
Communicate non-availability or delay of evidence	DT	Service	Identical with the Intermediation Pattern: Exception handling activity: The DT informs the DR that the requested evidence cannot be provided or cannot be provided within the agreed SLA.
Prepare preview	DO	Service	The DO prepares a preview for the User and displays it in the UI of the evidence portal. In addition, the name of the DE to which the evidence is to be transferred is displayed, in order to provide full transparency to the User what exchange he is accepting.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
Receive error or delay notification	U	User	Exception handling activity: The DP displays error or delay information to the User. These error messages are listed above in the activity 'Establish non-availability of OOP' In addition, the exception UI informs the User to return to the eProcedure portal of the DC.
Preview evidence pre-transfer	U	User	The User can view the evidence in the UI of the DP and can either approve or decline the transfer of evidence. Additionally, the Preview UI informs the User to return to the eProcedure portal of the DC after accepting the evidence exchange.
Transfer evidence	DT	Service	Identical with the Intermediation Pattern: The DT creates the evidence response message (compliant to agreed message format), encrypts, and signs the message and sends it to the DR.
Establish non-availability of OOP	DR	Service	Exception handling activity: The DR catches the negative (non-evidence) response from the DT and establishes the reason in terms of the DC country system and language: There are potentially several reasons why an OOP transfer of evidence is not available. The DT communicates these reasons to the DR in all cases that the evidence request cannot be fulfilled by sending the digitally available evidence within the agreed SLA as described above. At the moment we expect at least the following reasons for such an exception that should be framed in standard error messages or codes, each one with a corresponding recommendation to the User. 1) User cannot be uniquely identified – fall back to another channel (i.e. IMI) 2) Evidence not found – Check whether the request specified the correct geographical scope of authority and contact the DP directly if that was the case 3) Evidence is not readily available in a digital format now. Expected time for the evidence to be available is x days – return after x days and issue a new evidence request
Update evidence status	DE	Service	Identical with the Intermediation Pattern: The DE updates the status of a requested evidence and provides that update to the User in the evidence overview. Additionally, the update could be sent to the User via e-mail, including a link to the status overview page.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
Follow evidence status	U	User	After the User requested the OOP transfer of evidence, they observe the status of the evidence request on an evidence status overview. It essentially shows the progress or the request for each separate evidence requested. These statuses should include: 1) Evidence requested, expected response in x seconds 2) User input required (click-here {link to evidence portal}) 3) Evidence available 4) SLA overrun – please try again later 5) User identification failed 6) Evidence not available 7) Evidence expected to be available in y days – please return If User input is required, a link to the evidence portal of the DP is included for the User to follow.
Forward evidence	DR	Service	The DR registers the receipt, decrypts the message and in many cases encrypts the message in a MS specific format to hand it on to the DE.
Evaluate evidence	DE	Service	Identical with the Intermediation Pattern: The DE checks whether all requested evidences are available and validates that they conform to the evidence type requested. In the positive scenario that all evidences are available, the DE communicates to the User that the procedure can be submitted. In the negative case that not all evidences are received, the DE communicates this back to the User. The Procedure can then not be completed.
Save or abort (public) service request	U	User	Identical with the Intermediation Pattern: Exception handling activity: The User is informed that not all required evidence could be received, hence that there are still missing evidences preventing the eProcedure to be completed. It depends (only) on the functionality of the specific eProcedure portal what options are provided to the User. We expect that in most cases the User can save the procedure in order to return at a later stage, to repeat the cross-border OOP request or to provide the missing evidence themself.
Submit eProcedure	U	User	Identical with the Intermediation Pattern: The User fills the remaining fields required for the eProcedure. It is specific to the MS and the eProcedure which

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			fields to be filled out in this activity or when requesting the eProcedure at the start of the process. Usually, the User is prompted to verify the provided information in an overview before hitting the Submit button.
Receive acknowledgement of receipt	U	Receive	The User is waiting to receive the acknowledgment that their (public) service request is received in order and that the service will be provided, oftentimes incl. an indication of the expected time needed. The acknowledgment can be is displayed in the eProcedure portal or sent by e-mail or deposited in a government-hosted, secure message box or a combination of the above.
Provide public service	DE	Subprocess	Identical with the Intermediation Pattern: This is a subprocess that is very heterogeneous in composition and timeline, depending on which public service is provided and by which competent authority. Theoretically, the subprocess could be fully automated in some cases, but typically this is a back-office process involving multiple activities of public servants and might take days to several weeks. In many countries the maximum time for this process is defined by law.
Receive (public) service result	U	Receive	Identical with the Intermediation Pattern: Once the public service is completed, the result is provided to the User. This communication is fully dependent on the functionalities of the eProcedure portal (e.g. e-mail and/or government-hosted, secure message box).

Table 8 describes the conversation between User and DC by listing the exchanged messages in chronological order. Table 9 does the same for the conversation between DC and DP and Table 10 for User and DP.

Table 8 User-supported Intermediation - Conversation between User and Data Consumer

From	Message	To	Description
U	(Public) service request	DC	Identical with the Intermediation Pattern: The choice of public service requested and an initial set of information from the User required for the initiation of the request (breadth and type of information can vary between MS and requested service and can be substantial in some cases. Essentially this includes all information that the User provides prior to the point in the procedure where authentication is required).

© 870635 DE4A Project Partners

From	Message	To	Description
			Inclusion of e-mail could facilitate (additional) messages to the User.
DC	Authentication request	U	Identical with the Intermediation Pattern: Link to UI of identity service provider, potentially to several alternative eID services.
U	Authentication details	DC	Identical with the Intermediation Pattern: Identity information of the User (i.e. uniqueness ID + identification data set).
DC	Alternative channel information	U	Identical with the Intermediation Pattern: Contact information (e.g. email, telephone, or address) of an alternative channel to request the public service or to complete authentication/registration.
DC	Request for evidence	U	Identical with the Intermediation Pattern: List of evidences (in terms of the DC country) that are required to complete the eProcedure.
U	Explicit OOP request	DC	Identical with the Intermediation Pattern: Information about the geographic scope of authority for identifying the type of evidence and the data service provider (e.g. which MS ministry, region, municipality).
DC	Evidence portal link	U	Navigable link to the evidence portal that the User can follow in order to support the DP in retrieving and transferring the correct evidence
DC	OOP status update (not available)	U	Error message to the User (see activity description) explaining the reason why the evidence could not be retrieved and recommendation of action. In contrast to the intermediation pattern, the User was already informed by the DP.
DC	Evidence missing	U	Identical with the Intermediation Pattern: Message to the User that not all evidence could be retrieved and that they can resume the eProcedure once all evidence can be provided (either by the User or via the system).
U	(Public) service request (completed)	DC	Identical with the Intermediation Pattern: Complete and final submission of the (public service request), including all required information.
DC	Acknowledgement of receipt	U	Identical with the Intermediation Pattern: Acknowledgement that all required evidence was submitted and the (public) service can be provided to the User.
DC	(Public) service response	U	Identical with the Intermediation Pattern: The result of the (public) service, irrespective of how it is provided (post, email, secure message box, personal appearance.

© 870635 DE4A Project Partners

Table 9 User-supported Intermediation - Conversation between Data Consumer and Data Provider

From	Message	To	Description
DC	Evidence request	DP	Identical with the Intermediation Pattern: Must include User identification (eIDAS attributes, mandatory and possibly optional). Could additionally include the User email for direct communication
DP	Evidence portal URL	DC	Message containing the persistent URL for user-redirection to the evidence portal.
DP	User unknown	DC	Identical with the Intermediation Pattern: Message that the User could not be identified.
DP	Evidence not available	DC	Identical with the Intermediation Pattern: Message that the evidence does not exist or could not be retrieved in time.
DP	Evidence response	DC	Identical with the Intermediation Pattern: The evidence in electronic format.

Table 10 User-supported Intermediation - Conversation between User and Data Provider

From	Message	To	Description
U	User navigation trigger	DP	User followed the link to the evidence portal
DP	Authentication request	U	Link to UI of the identity service provider, potentially to several alternative services
U	Authentication details	DP	Identity information of the User (i.e. uniqueness ID + identification data set)
DP	Request for additional information	U	Depending on the information on record at the DP this request can include different attributes (e.g. matriculation number for universities, national identifiers for ministries, maiden name….)
U	Additional information	DP	The information attribute that the DP requested to perform the extended identify matching
DP	User unknown	U	Message that the User could not be identified
DP	Evidence not available	U	Message that the evidence is not existing or could not be retrieved in time
DP	Evidence preview	U	Rendered preview of the evidence
U	Preview response	DP	Accepting or declining of the evidence exchange

3.2.3. Process Realization

Figure 6 shows how the User process is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by application collaborations which are presented below.

© 870635 DE4A Project Partners

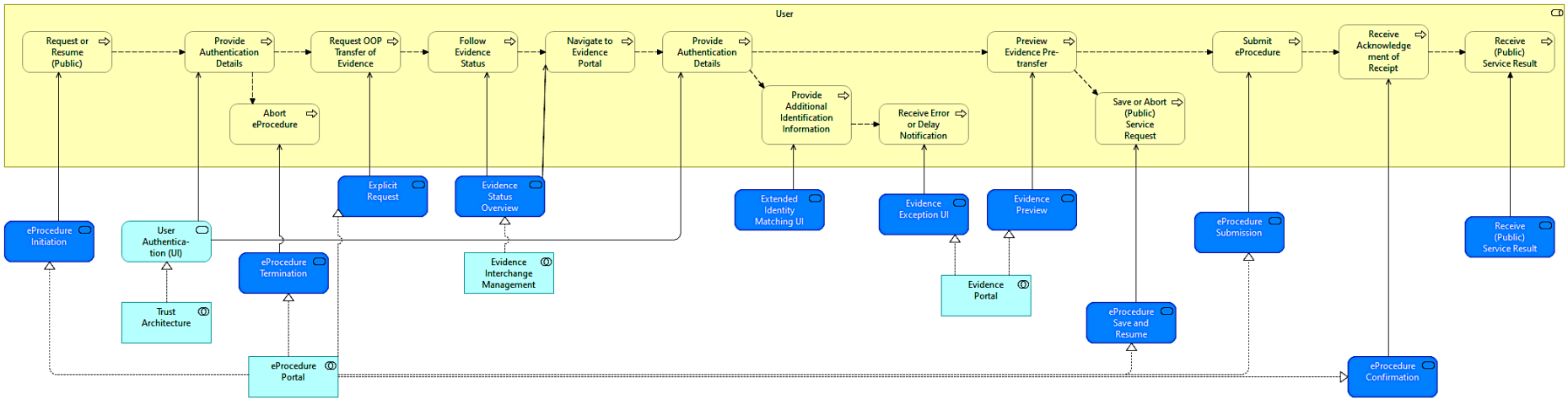


Figure 6 Process Realization of the User Process

The User requests (or resumes) a public service via the eProcedure Portal (see section 4.1 below) and has to authenticate themself with the help of Trust Architecture (see section 4.4 below). The User can choose to abort the eProcedure, or, if the authentication is successful, request a transfer of evidence via the OOP Technical System (eProcedure Portal). The User can follow the Evidence Status with the help of Evidence Interchange Management (see section 4.3 below). Next the User is redirected to DP (Evidence Interchange Management) where they must re-authenticate themself using Trust Architecture, provide additional attributes if needed. Errors or a notification of delay is handled by the Evidence Portal (see section 4.6 below), as well as the preview of the evidence at DP side before it is transferred to the DC. If the User wishes so the eProcedure can be aborted or saved to continue at a later point in time (eProcedure Portal). Finally, submission of the eProcedure is also provided by eProcedure Portal after which the Public service can be offered to the User.

© 870635 DE4A Project Partners

Figure 7 shows how the Data Consumer process is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by application collaborations named below.

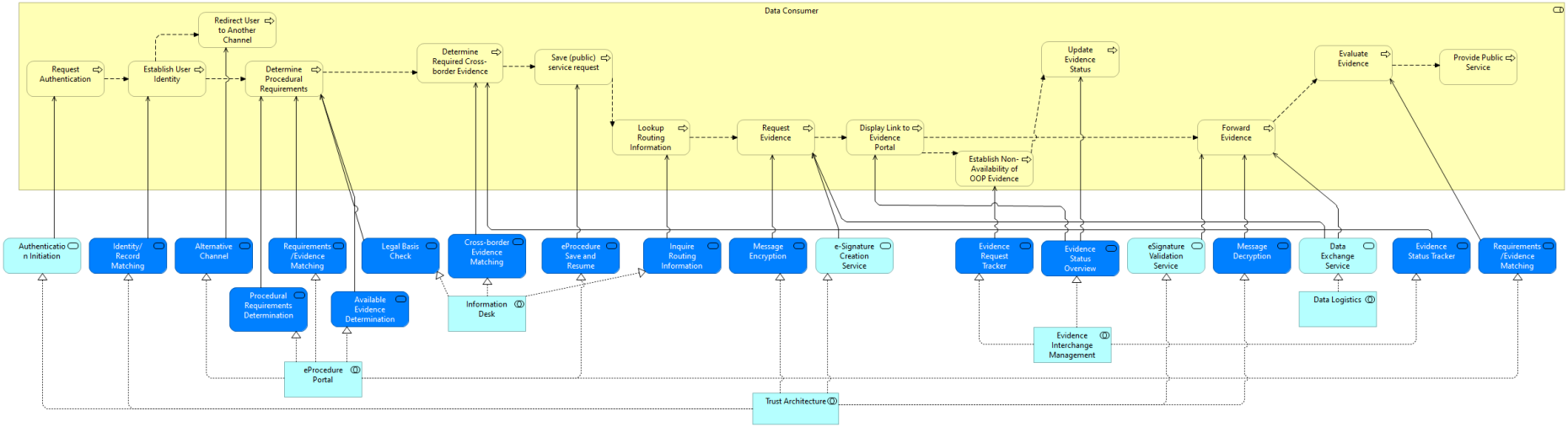


Figure 7 Process Realization of the Data Consumer Process

The DC initiates the authentication of the User in order to establish their identity (Trust Architecture, section 4.4 below). If this fails, the User may be directed to an alternative channel via the eProcedure Portal (see section 4.1 below). If authentication is successful the DC has to determine the procedural requirements, match those requirements with the Evidence needed and determine what Evidence is already available (all through the eProcedure Portal). With the help of the Information Desk (see section 4.2 below) the required cross-border evidence is determined, and the relevant routing information is looked up. Next the Evidence can be requested, the request message is encrypted and digitally signed using the Trust Architecture and exchanged using Data Logistics (see section 4.5 below).

The User is forwarded to the DP (see Figure 8 below). On return of the User there are two possible outcomes: either the OOP evidence is not available, or the evidence was received by the DC (exchanged by Data Logistics). In both cases the evidence status is updated (through Evidence Interchange Management, see section 4.3 below).

Assuming the happy flow the signature of the received message is validated, and the message decrypted (Trust Architecture). Via eProcedure Portal the evidence is evaluated and if all is well the public service can be provided to the User.

© 870635 DE4A Project Partners

Figure 8 shows how the Data Provider process is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by the application collaborations named below.

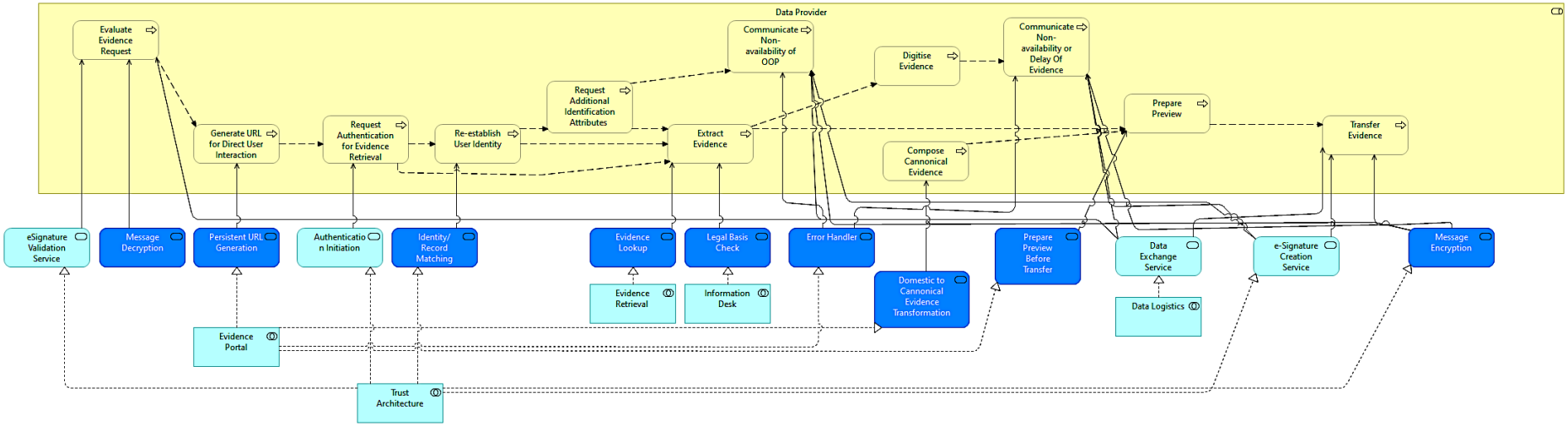


Figure 8 Process Realization of the Data Provider Process

The Evidence request is received via Data Logistics (see section 4.5) and with the help of Trust Architecture (section 4.4) the DP checks the signature of the request message and decrypts it. The DP generates a URL (Evidence Portal, section 4.6) for user redirection (from DC to DP). Once the User arrives at DP, they have to reauthenticate themself using Trust Architecture. If needed additional information is needed in order to establish the User 's identity. If authentication fails, the non-availability of OOP is communicated to the User via the Evidence Portal.

If successful, the evidence is looked up in the registry (Evidence Retrieval, see section 4.7 below) and transformed to canonical format (Evidence Portal). The evidence might need to be digitized which is communicated as non-availability or delay of the evidence (Evidence Portal). The Evidence Portal also takes care of preparing the preview of the evidence. If successful (the User consents to the transfer) the evidence send as an encrypted and signed message (Data Logistics and Trust Architecture respectively).

© 870635 DE4A Project Partners

3.3.Verifiable Credentials Pattern

https://wiki.de4a.eu/index.php/Verifiable_Credentials_Pattern

The Verifiable Credentials Pattern (VC Pattern) is one of the cross-border interaction patterns of the DE4A Reference Architecture. It is a user-managed access pattern in D2.1 terminology [2]. It is used by the "Diploma/Certs/Studies/Professional Recognition" use case (SA UC3, see section 5.1 below).

Data stored in the form of Verifiable Credentials (VC) are data representations in the form of a set of claims about some subject (i.e. User) issued by the issuer (i.e. Data Provider). Verifiable Credentials can be cryptographically verified by any third party i.e. Data Consumer (DC) to whom Verifiable Credentials is presented (usually in the form of a Verifiable Presentation (VP)).

The VC Pattern utilizes blockchain technology features in several ways. First, storing decentralized identifiers (DIDs) and its correlating DID documents, which includes all relevant entity pieces of information about the issuer, including associated cryptographic keys, endpoints, etc. that can be used to authenticate the issuer (i.e. Data Provider (DP), and cryptographically validate VC that was issued by its DID. Second, storing and maintaining a list of verified/trusted issuers, i.e. DPs. Third, keep the list of revoked VCs. Furthermore, all other entities (i.e. DC, and Users) also have DIDs, and related DID documents, that are different than the DC information stored directly on their devices, i.e. Agents (edge or cloud). These DIDs are used for setting direct, i.e. DID communication between entities.

The VCs are issued to a User in a cryptographically secure manner, collected in a user-maintained digital wallet that is part of the edge agent (i.e. mobile phone) in their possession. An Edge agent serves as an instrument with which Preview is done and all secure interchanges are managed (i.e. Initiate DID connection, Accept DID connection, Accept Verifiable Credential, Present Verifiable Credential). Moreover, the managing of DID connections, VC issuing and verifying operated by DPs and DCs is handled through a dedicated cloud agent.

3.3.1. Working Hypotheses and Implementation Principles

The present reference architecture is valid under several working hypotheses and implementation principles, which are working hypotheses that are either validated or decided upon by the DE4A partners.

Table 11 Verifiable Credentials Pattern Working Hypotheses and Implementation Principles

Interdisciplinary Topic	Hypotheses / Principle	Implications and Limitations
Orchestration / Choreography	The orchestration of the evidence exchange is performed by the User, who is supported in identifying the right DP to communicate with.	The VC pattern is a version of a User-managed access pattern as identified in D2.1 Architecture Framework.
Complementary, overlapping, or conflicting	Complementary evidence cases must in principle be supported by the technical system. Deep analysis on	The DE4A pilot case applying this pattern (see section 5.1 below) does not to suffer from this issue and the common VC schema approach

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypotheses / Principle	Implications and Limitations
evidence equivalents	whether they are jointly valid or are contradicting each other is left to the public service provider and not included as functionality in the cross-border OOP sequence.	also means that this issue is usually resolved at the DP-side.
Interrupted vs. Uninterrupted exchange	The VC pattern can support interrupted procedures and deferred responses based on established DID connection and the User Agent as uncoupling point.	The “save and resume” functionality of the eProcedure portal of the DC is required for the VC pattern to function.
Explicit request and transitivity between actors	The VC pattern does not include an explicit request for evidence transfer as it is a User-managed Access pattern.	The User requests the use of verifiable credentials. Requesting the VC from the DP can be considered an implicit User request.
Preview & Approval UI	The User Agent provides the preview between getting the Verifiable Credential (VC) issued by the DP and providing the Verifiable Presentation (VP) to the DC.	We are not considering the exchange without User request and approval (i.e. based on national or Union law) in the VC pattern.
Identity and Record Matching	The assumption can be relaxed in comparison to the Intermediation pattern: The User has direct interaction with both the DC and the DP and can easily assist with additional information.	In case of a User authentication at the DP, using an eID of the DP country, record matching is not needed. If eIDAS is used, then the DP can solicit additional information from the User to perform the match.
Transitivity of user identity	The assumption can be relaxed in comparison to the Intermediation pattern, because the User plays the central role in this pattern.	The User authenticates themself at the DP.
Hand-on of UI between actors	The User navigates from the DC eProcedure portal to the DP evidence portal – this hand-on of the User is facilitated by the DC	The routing information for the VC pattern consists of URLs of the respective evidence portals, not DIDs. The DID connection is established directly between User and DP.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypotheses / Principle	Implications and Limitations
Mandate and Proxy	Identical to Intermediation, however not relevant for the VC Pattern in the scope of DE4A.	Mandates and powers are not in scope for the Studying Abroad Pilot's VC Use Case.
Encryption Gap	The assumption can be relaxed in comparison to the Intermediation pattern.	Encryption is handled by the DID connection between User and DC and between User and DP respectively.
Structured data vs. unstructured data	All evidence using this pattern are represented as structured and machine-readable data in the form of Verifiable Credentials adhering to a common VC schema for any given evidence-type	For each evidence-type in scope of the pilot, a common VC schema must be agreed.
Automated re-use of data	Adherence to a common VC schema makes automated re-use much more likely	This is not to say that the provision of the (public) service can be end-to-end automated. In the diploma recognition use case, for example, the matching of study subjects and requirements will remain an expert task for the foreseeable future.
Data Transferor re-issues the evidence in the form of VC	We assume that the DT can re-issue the evidence in the form of VC again in the name of the Data Owner.	Issuing of the VC is not equivalent to the issuing of the original evidence. For the diploma use case this means, for example, that the VC is an evidence that a diploma is existing, meaning is different from the diploma issued by a university previously.
Issuing VC with diploma claims	We are not issuing new diplomas but VCs, which have those claims that a diploma, already in the registry, has.	This does not preclude that in the future, a university can directly issue a diploma in form of a VC that corresponds to the VC schema adopted by DE4A. This case is compatible with the VC pattern proposed in this document.
Multi-evidence Case	Only the Multiple Data Providers case is relevant for the VC pattern as each evidence is equated to one VC that is issued separately. If Data Providers (Issuers) are not highly integrated on MS-level, then the Users need to re-authenticate on several different platforms and establish DID	The Use Case "Diploma/Certs/Studies/Professional Recognition" (SA UC3) does not involve multiple evidences for its first iteration.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypotheses / Principle	Implications and Limitations
	connection with different SSI Authority agents.	

3.3.2. Business Process Collaboration

Figure 9 models the Verifiable Credential pattern in BPM notation. Using the colouring of the tasks in the BPMN, the different points of interaction of Users is clarified. The yellow colour represents the agent (digital wallet) activity. The green colour represents the activities performed in the DC portal and interaction management, while the blue colour represents the activities performed in the DP portal. In the table of this section all business activities are described.

© 870635 DE4A Project Partners

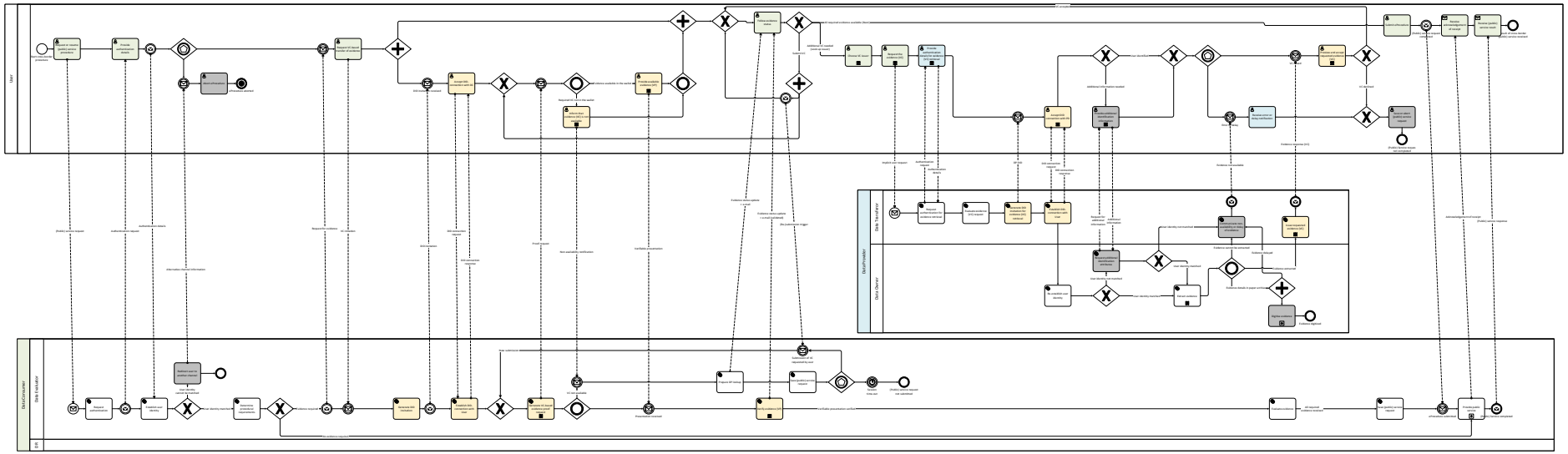


Figure 9 Business Process Collaboration View of the Verifiable Credential Pattern

See also Annex 3 for larger size

© 870635 DE4A Project Partners

The business collaboration diagram can be roughly divided into three sections: The first section shows the dialogue between the User and the DC via the eProcedure portal concerned with setting up the communication (i.e. DID connection) and submitting credentials in form of Verifiable Presentations (VP), leading up to the User task 'Follow evidence status'. This task is central for the management of the evidence exchange. The second section shows the conversation between User and DP and is required if the User has not all VCs available in their wallet and wants to collect additional credentials from one of several DPs. Note that in this pattern, there is no direct conversation between DC and DP. The third section concerns the evaluation of the evidence by the DP, the submission of the (public) service request and includes the subprocess 'Provide (public) service'.

In the case that the User needs to collect additional VCs, the processes need to return to the first section for the submission of the VC to the DC. This is modelled using a process pattern called "ad-hoc loop". They are drawn bold to make them stand-out as they are part of the normal flow [ad-hoc loops are more typically used to model corrective exception flows]. It helps the understanding to recall the BPMN collaboration diagrams [2] models the participant processes (here User, DC, and DP) as essentially independent sequence flows that communicate via message flows (dashed lines).

Looking first at the User process and following the bold ad-hoc loops that return the User to submitting the VC to the DC after they received a new VC from a DP, you can see that the User first returns to the activity 'Follow evidence status' in the DC portal. Here they select to submit the required VC. This throws a message to the DC to trigger the (re-)submission and then waits for the receipt of new 'Proof request'. A parallel gateway is used in this return flow to depict the fact that the User returns to the evidence status overview in the DC portal while in parallel interacting with their (mobile) wallet. Upon receiving the 'Proof request' the User follows the normal "forward" flow submitting the VP.

In the DC process, we see that the fact that a required VC is not available moved the DC on a process path 'Prepare DP lookup' and wait for the receipt of the above mentioned '(re-)submission trigger' from the User (or alternatively for a session time out, which would require a re-authentication of the User to resume the Procedure). Upon receiving the trigger, the DC process follows via the bold return flow to 'Generate VC-based evidence proof request' from where they follow again the "forward" path to receiving the Verifiable Presentation and on to validating it.

Table 12 Business Activities of the Verifiable Credentials Pattern

Activity / UC	Role	Type	Description
Request or resume (public) service procedure	U	User	Identical with the Intermediation Pattern: The User navigates to the eProcedure in the DC country and requests a (public) service. This means they fill in the required information and start the eProcedure. It is specific to the MS and the eProcedure how much information is provided by the User (i.e. which fields to be filled out) in this activity (i.e. prior to authentication) or when submitting the eProcedure later in the process. Email should be included as means to contact the User or provide updates. If the User is returning to a previously started procedure, the eProcedure will return to original instance after authentication.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
Request authentication	DE	Service	Identical with the Intermediation Pattern: The DE requests the User to authenticate themself. This can happen in two ways, either using eIDAS (default) or using the eID of the DC MS, in case that the User has the national eID of the DC country available. The DE provides both options to the User.
Provide authentication details	U	User	Identical with the Intermediation Pattern: The User uses the means available to them to provide the authentication details. This can happen at the User's discretion using the eID of the DC MS or eIDAS. In the second case, the User is forwarded to the authentication service of the identity provider of their means of authentication. If the User is representing another entity (typically a legal person), this relation is also retrieved as part of this authentication.
Establish user identity	DE	Service	Identical with the Intermediation Pattern: The DE establishes the identity of the User in the DC MS environment. In the eIDAS case, this means that the eIDAS uniqueness ID must be linked to the national identification number used to access the MS registries. In case of a business User, the company identification must be matched. The match of the representing natural person to a population register is not required in all MS.
Redirect user to another channel	DE	Service	Identical with the Intermediation Pattern: Exception handling activity: The User cannot be identified in an automated way by the DC and alternative digital or non-digital channel information (depending on the eProcedure at hand User and potentially dependent on the type of identification error) is collected and provided to the User.
Abort eProcedure	U	User	Identical with the Intermediation Pattern: Exception handling activity: Alternative channel information is displayed to the User and the User exits the e-procedure.
Determine procedural requirements	DE	Service	Identical with the Intermediation Pattern: The DE compares the available information (i.e. in the DC MS registries via the national OOP layer) with the information required by the eProcedure. The result can be a (list of) required evidence, defined in terms of the DC country, which is then displayed to the User as a request to provide the evidence, together with

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			the option for the User to request the evidence via the OOTS. This activity is not trivial and should prevent that we ask a User for evidence that is readily available in the DC MS and might not be available in the OOTS cross-border scope. Example: It would not make any sense for a Dutch DC to ask a German national born in the Netherlands to provide a birth certificate (which he could not get via the OOTS as it is not cross-border). A similar situation would be asking a French national with a Belgian university diploma to provide that diploma in order to be admitted for a PhD in another Belgian university.
Request VC-based transfer of evidence	U	User	The User chooses to request the transfer of evidence in the form of Verifiable Credentials (VC). This action starts the process of the preparation for a DID Connection between the User and DE.
Generate DID invitation	DE	Service	The DE generates an invitation for a DID connection with a User. The invitation is presented to the User in the form of a QR code. The invitation holds data about the DID document of the DE, stored on a distributed ledger. The DID document also holds the DE endpoint, which is used for DID communication with User Agent.
Accept DID connection with DC	U	User	The User responds with accepting or rejecting an invitation for a DID connection generated by DE by scanning a QR code presented on the eProcedure portal. Note that this step is vulnerable for a "shoulder attack", meaning that a different mobile agent could be used than the one of the User authenticated in the previous step via eIDAS. The pilot could attempt to use encrypted VCs, however, we hope that this vulnerability will be closed by the new European identity wallet.
Establish DID connection with User	DE	Service	Both parties (agents) create a DID connection in case none-existed before, otherwise the DID connection is just initialized. The DE informs User about the success of the connection establishment.
Generate VC-based evidence proof request	DE	Service	Based on the procedural requirements, the DE generates an evidence request for the User.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
Provide available evidence (VP)	U	User	The User is informed about available evidence (VCs) that matches the procedural requirements and has the option to select which proofs in the form of Verifiable Presentation (VP) he will share with DE. After the VC's are chosen, a VP of those is provided to the DE.
Inform that evidence (VC) is not available	U	User	The User is informed about available evidence (VCs) that matches the procedural requirements and has the option to select which proofs in the form of Verifiable Presentation (VP) he will share with DE. If the User does not have any required evidence or does not select any of the matched ones to share with DE, the DE is informed that VC is not available.
Prepare DP lookup	DE	Service	The DE retrieves the technical routing information (e.g. routing identifier or URL of the evidence portal provider), based on the evidence type (in terms of DP country) and the issuing competent authority (or geographic scope of authority).
Save (public) service request	DE	Service	The DE saves public service request and determines the time window in which the User can provide required evidence in the form of VP.
Follow evidence status	U	User	After the User chooses to provide the evidence required in the form of a VC and establishes a DID connection with the DE, the eProcedure portal shows them an evidence status overview. It essentially shows the progress of the request for each separate requested evidence (VC). These statuses should include: 1) Required 2) Provided In the case the evidences are required, the User has the option to provide the evidence or look up the VC issuer.
Choose VC issuer	U	User	The User chooses a DP that is capable to provide evidence in the form of VC's that are needed for User to submit eProcedure.
Request the evidence (VC)	U	User	The User informs a DP that they request the evidence in the form of VCs by way of following the link displayed in the Procedure portal. Note that the URL will need to include a parameter specifying the VC schema requested. This action starts the process of the preparation for a DID Connection and VC issuing process between User and DT.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
Request authentication for evidence (VC) retrieval	DT	Service	The DO requests the User to authenticate themself. This can happen in two ways, either using eIDAS (default) or using the eID of the DP MS, in case that the User has the national eID of the DP country available. The case of using the national eID scheme would consequently be quite common. The DP provides both options to the User.
Provide authentication details for evidence (VC) retrieval	U	User	The User uses the means available to them to provide the authentication details. This can happen to the User's discretion using the eID of the DP MS or eIDAS. In the second case, the User is forwarded to the authentication service of the identity provider of their means of authentication.
Evaluate evidence (VC) request	DT	Service	The DT receives the request and checks whether the request meets formal requirements and can be accepted. It should e.g. be checked whether the requesting User can reasonably and rightfully request that specific type of evidence.
Generate DID invitation for evidence (VC) retrieval	DT	Service	The DT generates an invitation for a DID connection with a User. The invitation is represented to the User in the form of a QR code. The invitation holds data about the DID document of the DT, stored on a distributed ledger. The DID document also holds the DT endpoint, which is used for DID communication with User Agent.
Accept DID connection with DP	DT	Service	The User responds with accepting or rejecting an invitation for a DID connection generated by DE by scanning a QR code presented on the DT portal. Note that this step is vulnerable for a "shoulder attack", meaning that a different mobile agent could be used than the one of the User, authenticated in the previous step via eIDAS. The pilot could attempt to use encrypted VCs, however, we hope that this vulnerability would be closed by the new European identity wallet.
Establish DID connection with User	DT	Service	Both parties (agents) create a DID connection in case none existed before, otherwise the DID connections is just initialized. The DT informs User about the success of the connection establishment.
Re-establish user identity	DO	Service	Identical with the User-supported Intermediation pattern: The DO matches the information about the User (i.e. eIDAS mandatory and optional attributes) with DP

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			country records to identify the User in their systems. This amounts to matching the eIDAS attributes to a national identification number. (If the national eID is used, this task is skipped). Data Owner activity, because in a distributed scenario, the Data Transferor might not have a legal basis to do so.
Request additional identification attributes	DO	Service	Identical with the User-supported Intermediation pattern: If the User identity cannot be easily matched, the DO displays to User a UI requesting additional identification attributes to improve the match.
Provide additional identification information	U	User	Identical with the User-supported Intermediation pattern: Exception handling activity: Interactive form- or chat-based Q&A for additional identification information (beyond eIDAS attributes). The requested information clearly depends on the available information at the Data Provider.
Extract evidence	DO	Service	Identical with the Intermediation Pattern: The DO extracts the requested evidence from their registry and forwards it to the DT.
Digitize evidence	DO	Subprocess	The DO digitizes required evidence if evidence details are in the paper archive.
Communicate non-available or delay of evidence	DT	Service	Exception handling activity: The DT informs the User that they cannot be identified unequivocally and the OOTS cannot be used to transfer the evidence or that the requested evidence cannot be provided or cannot be provided within the agreed SLA.
Receive error or delay notification	U	User	Identical with the User-supported Intermediation pattern: Exception handling activity: The DP displays error or delay information to the User. These error messages are listed above in the activity 'Establish non-availability of OOP' In addition, the exception UI informs the User to return to the eProcedure portal of the DC.
Save or abort (public) service request	U	User	Identical with the Intermediation Pattern: Exception handling activity: The User is informed that not all required evidence could be received, hence that there are still missing evidences preventing the eProcedure to be completed. It depends (only) on the

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			functionality of the specific eProcedure portal what options are provided to the User. We expect that in most cases the User can save the procedure in order to return at a later stage, to repeat the cross-border OOP request or to provide the missing evidence themself.
Issue requested evidence (VC)	DT	Service	The DT issues evidence in the form of VC to a User.
Preview and accept requested evidence (VC)	U	User	The User receives requested evidence in the form of VC from the DT, review it, and decide to accept or reject the storage of this evidence to their digital wallet.
Verify evidence (VP)	DE	Service	The DE receives evidence in the form of VP. In this activity, the following pieces of information inside the VP are verified: • evidence issuer (DP) is checked (is evidence issuer competent in issuing such evidence?) • evidence issuer (DP) digital signature is validated (is provided evidence issued from stated evidence issuer) • User verification (is the authenticated User subject of provided evidence?), • the validity in time of evidence is checked (is provided evidence valid at the time of presentation, i.e., revoked, etc.).
Evaluate evidence (VC)	DE	Service	Identical with the Intermediation Pattern: The DE checks whether all requested evidences are available and validates that they conform to the evidence type requested. Validity of the evidence with respect to a registered schema is checked against a Trusted Schema Registry in the blockchain infrastructure. In the positive scenario that all evidences are available, the DE communicates to the User that the procedure can be submitted. In the negative case that not all evidences are received, the DE communicates this back to the User. The Procedure can then not be completed.
Submit eProcedure	U	User	Identical with the Intermediation Pattern: The User fills the remaining fields required for the eProcedure. It is specific to the MS and the eProcedure which fields to be filled out in this activity or when requesting the eProcedure at the start of the process.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			Usually, the User is prompted to verify the provided information in an overview before hitting the Submit button.
Provide public service	DE	Subprocess	Identical with the Intermediation Pattern: This is a subprocess that is very heterogeneous in composition and timeline, depending on which public service is provided and by which competent authority. Theoretically, the subprocess could be fully automated in some cases, but typically this is a back-office process involving multiple activities of public servants and might take days to several weeks. In many countries the maximum time for this process is defined by law.
Receive acknowledgment of receipt	U	Receive	Identical with the User-supported Intermediation pattern: The User is waiting to receive the acknowledgment that their (public) service request is received in order and that the service will be provided, oftentimes incl. an indication of the expected time needed. The acknowledgment can be is displayed in the eProcedure portal or sent by e-mail or deposited in a government-hosted, secure message box or a combination of the above.
Receive (public) service result	U	Receive	Identical with the Intermediation Pattern: Once the public service is completed, the result is provided to the User. This communication is fully dependent on the functionalities of the eProcedure portal (e.g. e-mail and/or government-hosted, secure message box).

Table 13 Verifiable Credentials Pattern Conversations

From	Message	To	Description
U	(Public) service request	DC	Identical with the Intermediation Pattern: The choice of public service requested and an initial set of information from the User required for the initiation of the request (breadth and type of information can vary between MS and requested service and can be substantial in some cases. Essentially this includes all information that the User provides prior to the point in the procedure where authentication is required). Inclusion of e-mail could facilitate (additional) messages to the User.

© 870635 DE4A Project Partners

From	Message	To	Description
DC/DP	Authentication request	U	Link to UI or identity service provider, potentially to several alternative eID services.
U	Authentication details	DC/DP	Identical with the Intermediation Pattern: Identity information of the User (i.e. uniqueness ID + identification data set).
DC	Alternative channel information	U	Identical with the Intermediation Pattern: Contact information (e.g. email, telephone, or address) of an alternative channel to request the public service or to complete authentication/registration.
DC	Request for evidence	U	Identical with the Intermediation Pattern: List of evidences (in terms of the DC country) that are required to complete the eProcedure.
U	Evidence (VC) initiation	DC/DP	A User request to the eProcedure portal to start an evidence exchange in the form of VC using DID communication
DC/DP	DID invitation	U	The authority (DC/DP) prepares a QR code, which is sent to the User to be scanned. The QR code presents a DID invitation, which includes all required information for the establishment of DID communication between User's agent and authority (DC/DP) agent. The invitation can also be sent in other forms, e.g., HTTP, NFC, Bluetooth.
U	DID connection request	DC/DP	By scanning the QR code, the User's agent decodes the QR code into a human-readable form, which is shown on the agent's UI (information about the authority's agent with which the DID connection will be established). After the review, the User decides to accept the DID invitation. The information about the User agent is sent to the authority (DC/DP).
DC/DP	DID connection response	U	The information about the success of the DID communication establishment.
DC	Evidence (VC) Proof request	U	The information, which evidences in the form of VC's are required for public service.
U	Evidence (VC) non-availability notification	DC	The information that some of the required VC's are not currently available in the digital wallet that is part of the User agent.
U	Evidence (VC) Verifiable presentation	DC	Evidence (VC) in the form of a Verifiable Presentation.
DC	Evidence status update with DP	U	The information, which holds the status of required evidence and the information, also includes a list of DPs,

© 870635 DE4A Project Partners

From	Message	To	Description
	lookup (VC not provided)		which can provide required evidence (VC) in case some evidence is missing.
DC	Evidence status update + email (VC provided)	U	The information, which holds the status of the required evidence. Furthermore, it also includes a list of DPs, which can provide required evidence (VC) in case some evidence is missing.
U	Evidence (Re)submission trigger	DC	The information that triggers new evidence (VC) proof request.
U	Implicit user request	DP	The choice for a DP to provide the evidence (issuance of VC) and an initial set of information about requested evidence (VC), such subject and evidence type.
DP	Request for additional information	U	Identical with the User-supported Intermediation pattern: Depending on the information on record at the DP this request can include different attributes (e.g. matriculation number for universities, national identifiers for ministries, maiden name….)
U	Additional information	DP	Identical with the User-supported Intermediation pattern: The information attribute that the DP requested to perform the extended identify matching.
DP	Evidence not available	U	The information that evidence cannot be provided.
DP	Evidence response (VC)	U	Requested evidence in the form of verifiable credentials.
U	(Public) service response completed	DC	The information about the submission of the eProcedure.
DC	Acknowledgment of receipt	U	The information that submission of the eProcedure has been received.
DC	(Public) service response	U	The result of public service

3.3.3. Process Realization

Figure 10 below shows how application services serve the User process (cf. figure 9, Business Process Collaboration View of the Verifiable Credential Pattern). The application services are realized by application collaborations, which are presented in chapter 4.

© 870635 DE4A Project Partners

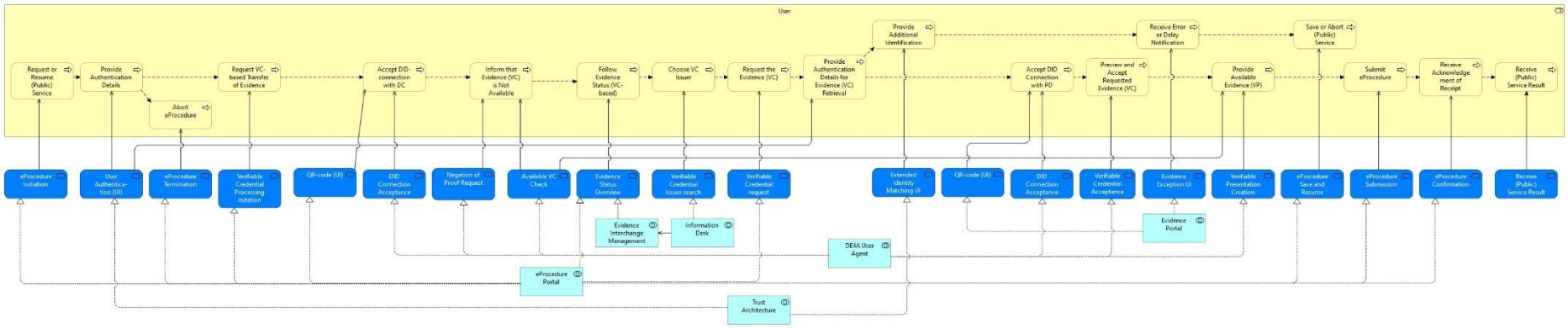


Figure 10 Process Realization of the User Process

Through the eProcedure Portal (section 4.1 below), the User requests or resumes a public service, and via the Trust Architecture (section 4.4 below) provides their authentication details. At this point, the User can decide to abort the eProcedure or choose the form of evidence needed for (public) service. User Agent (section 4.9 below), amongst other things, supports the User requesting to provide evidence in the form of a VC, which are (if already acquired) stored in their edge agent (i.e. mobile phone). Next, the QR code as the method of initiation of the DID connection establishment is presented to the User. By scanning the QR code by the User Agent information about the Data Consumer agent (cloud) are presented to the User who now has the choice to accept (or reject) the establishment of DID connection.

After the connection is established, the User Agent checks if proper evidence is already present. Alternatively, the User has a choice to inform the DC that evidence in the form of VC is not available. Moreover, the User can follow the status of the evidence (Evidence Interchange Management, section 4.3 below) to check which evidence has already been provided to the DC. In case that the User does not hold the required evidence, the User can perform a search for the Data Provider who can contribute relevant evidence (in the form of a VC) through the Information Desk (section 4.2 below).

After the DP is found, the User can request the re-issuance of the evidence in the form of a VC. For this action, via Trust Architecture, the User needs to provide authentication details to (possibly, with additional identification data) to the DP. In case of any exception, a notification about the error or delay is provided, and the (public) service request can be saved or aborted. After the authentication, the Evidence Portal (section 4.6 below) shows the User QR code, which includes all information about the DID connection establishment with the DP. Now, the User's DE4A User Agent can accept DID connection with DP.

In case of a successful DID connection establishment between the User and DP, the requested re-issued evidence in the VC form is delivered. The User can preview the evidence and choose to accept the requested evidence. As a result of acceptance, the evidence is stored in a digital wallet in the User Agent. Now

© 870635 DE4A Project Partners

the User can provide available evidence in the form of Verifiable Presentation to the DC, and when all required pieces of evidence are successfully presented to the DC, submit the eProcedure. After this, the User receives an acknowledgment of receipt and finally receive (public) service result.

Figure 11 shows how the DC process (cf. Figure 9 Business Process Collaboration View of the Verifiable Credential Pattern) is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by application collaborations which are named below and described in chapter 4.

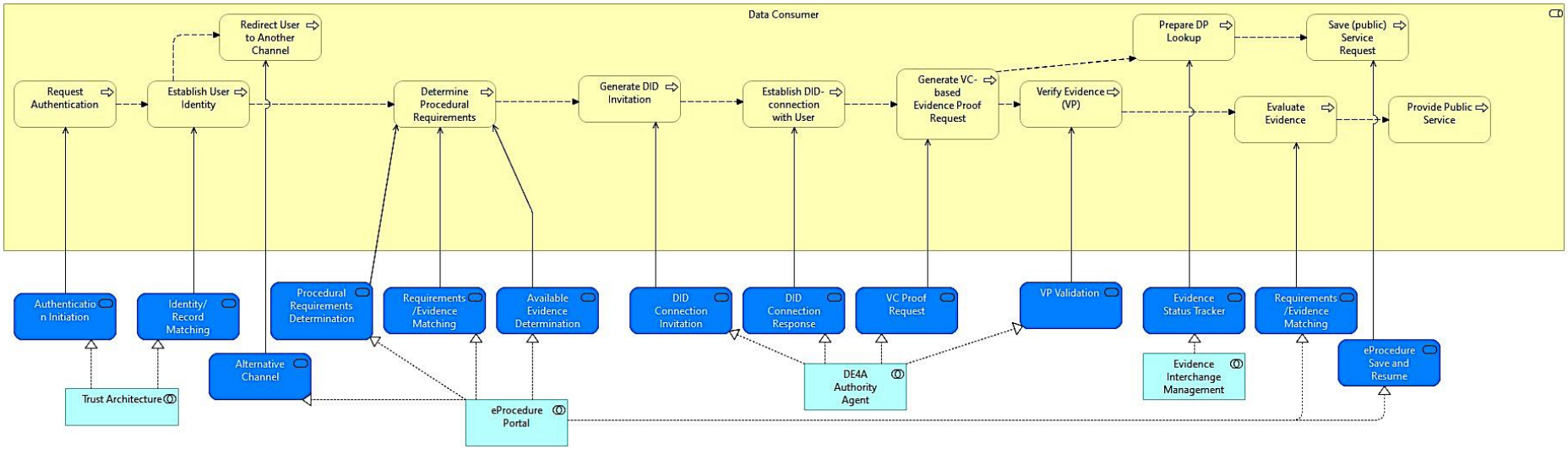


Figure 11 Process Realization of the Data Consumer Process

The Data Consumer, through the Trust Architecture (section 4.4 below), authenticates the User and establishes their identity. Next, through the eProcedure Portal (section 4.1 below), the determination of procedural requirements is performed, and later, through the portal cloud agent (i.e., DE4A authority agent), the DID connection with User is established, including the generation of DID invitation and DID connection response. Subsequently, the evidence (VC) proof request is generated, and after the proof is provided (in the form of Verifiable Presentation) by the User, this proof is cryptographically validated and evaluated from the business requirements standpoint of view. When all required pieces of evidence are provided and successfully validated and evaluated, the public service is provided to the User.

If the User does not hold all the necessary pieces of evidence, a DP lookup where the missing evidence can be acquired is prepared (Evidence Interchange Management, section 4.3 below).

© 870635 DE4A Project Partners

Figure 12 shows how the DP process (cf. Figure 9 Business Process Collaboration View of the Verifiable Credential Pattern) is served by application services. The application services are realized by the application collaborations named below.

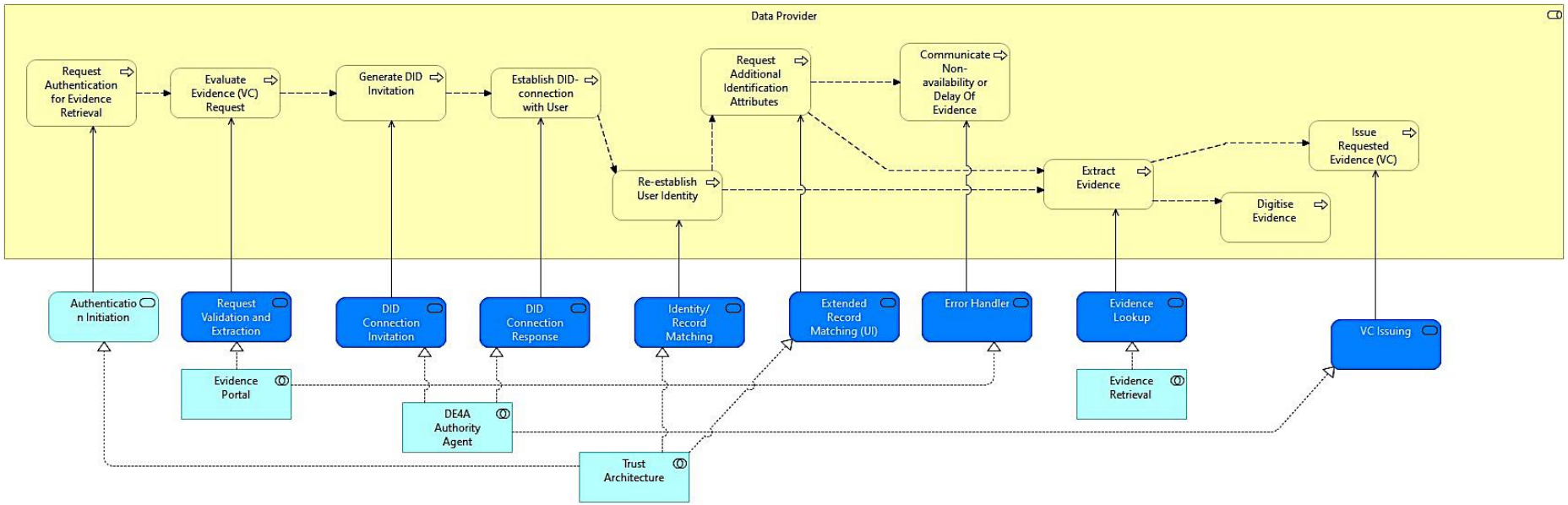


Figure 12 Process Realization of the Data Provider Process

The Data Provider authenticates the User through the Trust Architecture (section 4.4 below), and if needed, requests additional identification attributes and re-establish the User's identity. An evaluation of the User's request for (re)issuing of evidence in the form of VC is performed. Later, through the Portal cloud agent (i.e. Authority Agent, section 4.8 below), the DID connection with the User is established, including the generation of a DID invitation and DID connection response.

The requested evidence is extracted through Evidence Retrieval (if necessary, also digitized) and (re)issued to the User in the form of VC (through Authority Agent). In case of an error or delay within the process mentioned above, the User is informed through the Evidence Portal.

© 870635 DE4A Project Partners

3.4.Subscription and Notification Pattern

https://wiki.de4a.eu/index.php/Subscription_and_Notification_Pattern

The Subscription and Notification Pattern is used by the Doing Business Abroad Pilot in Use Case "Doing Business in Another Member State" (DBA UC2, see section 5.2 below).

After receiving evidence from a Data Owner (DO), it can be essential for a Data Evaluator (DE) to be informed on changes regarding the subject of this evidence to be able to take appropriate action. The goal of this interaction pattern is to allow the DE to subscribe to a service of the DO that provides automatic and regular notifications. The cross-border message exchange for the subscriptions and notifications are put in the responsibility of the Data Requestor (DR) and the Data Transferor (DT) respectively to allow an easier distribution of responsibility on national level, i.e. to intermediary platforms and national gateway providers.

3.4.1. Functional Variants of the Subscription and Notification Pattern

There are two distinct purposes, or business requirements for Subscription and Notification, both of which are relevant for the DE4A Doing Business Abroad Pilot: Evidence update notification and Event notification.

Table 14 Business Requirements for Subscription and Notification

Business requirement	Goal	Description
Evidence Update Notification	To keep previously shared evidence data that is stored at the DE up to date	Data may change in the base register. In case the DE wants an exact copy of the evidence data on record, they need to be notified in case the data has changed in the base registry.
Business or Life Event Notification	To assess the impact of changes to the subject (e.g. company) on the public services provided by the DE.	Some public services oblige the subject (i.e. company or citizen) to continue in a specific situation or state to remain entitled to the benefits of the public service provided. An agricultural company may, for example, receive a subsidy for its permanent pasture. As a prerequisite, the company must preserve the pasture for five consecutive years. The DE needs to be notified of the company ending its operations and hence not meeting the five-year requirement. “Ending its operation” is an example of a business event. Other examples are going bankrupt, a merger, etc. Some Business or Life Event Notifications could be linked Evidence Update Notifications so both business requirements can be linked in some scenarios.

Essentially there are two ways to approach the dual requirements for Subscription and Notification, either specific solutions for each requirement or hybrid approaches that can serve both.

© 870635 DE4A Project Partners

Looking at specific solutions means that two specialized systems would need to be developed and implemented:

1. Specific Evidence Update Solution: The subscription would be linked directly to the previously exchanged evidence, hence the subscription would need to register the evidence type, the subject ID, and the subscriber ID. For any data change in the evidence type data set at the DO, the DT would need to push a completely new evidence to the DE, irrespective of that specific change being relevant for the public service provided to the User by the DC. Apart from this being not optimal from a data minimization principle perspective, it cannot cover changes of the subject that are not represented in the evidence type data set, giving rise to the need of a second subscription system for events. In addition, the subscription system would be impacted by changes in the canonical evidence type definitions over time. This approach might, however, be easier to integrate in the legal framework of the SDGR (see Legal Considerations below).
2. Pure Event Notification: The subscription is not directly related to a previously exchanged evidence, but the subscription could be registered for an agreed set of events relating to a given subject. The subscription system would consequently be based on a list of events, rather than a list of evidence types. Quite obviously, this requires an agreement on a set of DE4A events, or canonical cross-border events.

Technical approach and business requirements do not relate one to one, giving rise to several hybrid approaches, where one solution is used to cater for both requirements:

1. Extended Evidence Type: The Specific Evidence Update can be used to derive relevant Events at the DC, if the evidence type definition is scoped, or extended, so that all relevant events are represented by data changes in the evidence type data set. This would require the DC to run an event identification routine (either immediately or periodically) after receiving updates in order to react accordingly. The extension of evidence type definitions beyond what is actually required by the eProcedure is, again, not optimal from a data minimization principle perspective. This hybrid solution cannot resolve events that are dealt with by procedural means at the DP-side, rather than by data mutations.
2. Extended Notification Message: The pure Event Notification could be extended to carry an updated evidence as part of the Notification message, essentially piggybacking the evidence onto an event notification. This approach would need to extend the event-centric subscription system to maintain with underlying evidence type, or potentially multiple evidence types, are relevant for each event type, so that evidence can be retrieved and packed as extension of the Notification Message. Which evidence is required for which event can additionally differ by public service provided and hence per subscriber. This solution would consequently end up being rather complex and again not optimal from a data minimization principle perspective. [A BPMN Process Analysis of this approach is available on request]
3. Event Notification + Lookup: The pure Event Notification is used as described above, while it is made sure that the agreed event set of canonical DE4A events is complete in the sense that it covers also relevant update needs. For example a company that moved headquarters means that the address (part of the Company Registration evidence) changed as an effect. It is then left at the discretion of the DC, whether a particular event requires an update of the evidence on record. It could be that, i.e. the postal address of a company is not relevant for the continuation of the public service provisioning, in which case a flag that the address on record is not up to date, or a change to "unknown" would be sufficient as event response. This is fully in line with the data minimization principle perspective. If the DC considers that an update of one evidence or potentially several evidences is required as part of the event response, then the DC would use the Lookup Pattern (see section 3.5 below) to request new copies of

© 870635 DE4A Project Partners

evidences if and when required. The effort needed to make this approach work for evidence updates mostly concerns the Notification process: The DP might need to add "weak" events to their platform to cover changes that are not considered relevant enough to be in their event list yet, e.g. change of e-mail address. The DC will need to define or extend a decision table that relate event type to public service and returned the correct action to be taken, i.e. request a new evidence via the Lookup Pattern.

The reference Architecture for the DE4A projects focusses on the third option, the combination of Event Notification and Lookup Pattern to cover both business requirements with one hybrid solution, rather than setting up two specific solutions next to each other. During the elaboration of the Solution Architecture, it will be further assessed how this combination of both patterns impacts on the respective actors that need to deploy them. The combination of Event Notification and Lookup Pattern appears to be the most flexible approach and is expected to have the following advantages:

- Data minimization: Evidences are only requested if they are actually needed for the public service provided by the DC
- Low complexity of message definitions: The required message definitions for the notifications and updates between DP and DC remains low in complexity: A simple event notification (consisting of event type, identifiers and timestamp) and evidence response analogous to the event response message of the Intermediation Pattern (section 3.1 above) and User-supported Intermediation Pattern (section 3.2 above).
- Multiplicity: Case that single events require multiple evidences to be updated, or several events require the update of the same evidence can be covered quite easily without requiring complex message definitions.
- Flexibility in legal basis and authorizations: As the Event Notification does only contain identifiers and not the underlying (personal) data (which requires the eIDAS revision to create a European Unique Identifier for natural persons), the legal basis and corresponding authorizations might differ between Notification and Lookup, adding flexibility to the overall solution.
- Independence from a previously shared evidence: The solution approach is not directly linked to a previously shared evidence, which means that a subscription and subsequent lookup can also be applied in cases where the original procedure (leading to the public service being provided) was completed without any automated evidence exchange, i.e. evidence was provided by the User electronically or in person, provided that there is a legal basis (see 3.4.3 below).
- Extension of scope: New events can be added flexibly without immediate impact on existing subscriptions and without maintaining different versions of an (canonical) evidence definition.

3.4.2. Working Hypotheses and Implementation Principles

Table 15 Subscription and Notification Pattern Working Hypotheses and Implementation Principles

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Orchestration / Choreography	Subscription: The DC controls the overall flow for the subscription. This means that the process on DP side is a child process of the process on the DC side.	If issues on the DC-side (subscriber) prevented receiving notifications, a resubmission would need to be requested explicitly. The DP requires

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
	Notification: The Notification is conceived as a "fire and forget" conversation, meaning that the processes are not really orchestrated. The DP process triggers (if successful) the DC process.	functionality for such (manual) resubmission of notifications. There could be complexities in order to address mana ging these situations, i.e. DP's would need to detect missing ACKs.
Interrupted vs. Uninterrupted exchange	Both the Subscription and the Notification are considered to be uninterrupted, not sending any deferred responses.	For the subscription, this means that the DC must assume that the subscription was not successful if not receiving a confirmation message. For the DP, this means that their subscription system must be robust against receiving the same subscription twice.
Encryption Gap	OOP does not require true E2E encryption. The exchange between DR and DT must be encrypted and signed, as well as the transfers (if applicable on national level) between DR and DE on DC side and DT and DO on DP side (i.e. using the national OOP layer), but the encryption gap within the systems of the DR and DT is acceptable.	This might not hold for cases where the gateway would be outsourced to a private sector subcontractor, which is not foreseen for the DE4A pilots.
Automated re-use of data	Subscription and Notification are structured and adhere to known semantics and format that allow fully automated processing after receipt.	To facilitate automated re-use of data requires establishing canonical event definitions.
Production system and real-life cases	If the events relate to a legal person, not a natural person, subscription and notification can be run in production environments (see: Legal Considerations below)	The DC still needs a legitimate reason to subscribe to events of a subject (i.e. company)
Payment for evidence	In the context of the pilots, we assume that no payments are required.	This can restrict transition of pilot solutions to production in cases that competent authorities require payment for issuing evidence.
BRIS integration	A technical re-use or bridge to BRIS is not possible because of differences in scope and accessibility by competent authorities other than business registers.	The pilot system for the Doing Business Abroad Pilot need to be set-up separate from BRIS.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Matching evidences between Member States	The Event Subscription and Notification is based on a set of harmonized events definitions.	The participants need a semantic agreement in a set of standardized life/business events.

3.4.3. Legal Considerations

From a legal perspective, the central challenge is the need for a legal basis that allows impacted authorities to exchange Evidence Updates and/or Event Notifications. This is certainly critical for personal data (since the GDPR requires a legal basis), but even in the case of pure business data that contains no personal data, authorities will need to be able to demonstrate that they have a legal basis allowing them to send Evidence Updates and/or Event Notifications abroad.

The SDGR is in principle not an answer to this issue, since it focuses on user-driven exchanges (based on a user request, and with a preview option). While a user request could have been scoped in a way that allows a user to define a time period for exchanges ('I request authority A to send evidence X to authority B, including any updates, for a period of Y years'), this is not the implementation path that has been chosen in the Implementing Act. Moreover, such a request would not enable a preview as the SDGR requires. Thus, referring to the SDGR is not a sufficiently encompassing option.

This does not imply that subscriptions or event notifications are impossible, but rather than an alternative legal basis must be found. A few options are available, which will be discussed briefly below. For the avoidance of doubt: these options should only be applied in relation to business data; subscriptions/event notifications relating to individual persons (citizens) do not have a clear legal basis under data protection law, and due to the public sector context, reliance on consent or legitimate interest of the public administrations is not legally feasible.

For business data subscriptions and event notifications, the following options would be available:

- there should be no legal challenge in principle if the relevant information is already made publicly accessible by the relevant authority. If the information can be freely accessed and lawfully used by the public, proactively communicating it to specific authorities (in the form of evidence or a notification) should not be problematic either. While typically some terms and conditions would apply even to publicly accessible databases (e.g. to forbid commercial exploitation), it would be possible to conclude comparable agreements in the context of DE4A as well.
- exchanges should similarly be possible for information that is not publicly available, but that can only be accessed and used by parties if they conclude a suitable agreement with the relevant business register. In some Member States, business register data is made available to commercial entities on the basis of (usually) paid contracts, e.g. allowing them to integrate that data into business intelligence services. Companies can subscribe to such services to check e.g. credit rating or bankruptcy status of their customers. In countries that support this model, it should be legally feasible to conclude similar agreements to support DE4A pilot exchanges, hopefully on a free of charge basis, if this is acceptable to the data source.

These scenarios are likely more relevant for Updates of evidences than for pure Event Notifications, since formal evidences (extracts, certificates, attestations etc) are normally not included in these models.

Specifically, for Evidence Subscriptions, the principal legal solution would be to establish a legal basis for the subscription outside of the SDGR. This could be viable under national laws, in combination with

© 870635 DE4A Project Partners

the request of a representative of the affected legal entity. A pure appeal to national law (without any request for a subscription service from the User) likely will not work; this is only possible if there is already a specific legal basis for direct evidence exchanges between the authorities, and that does not seem to be the case. The BRIS Directive is the closest approximation but does not provide a basis for evidence subscriptions. Therefore, the request is important, as a way to strengthen the legal mandate of the evidence provider, allowing them to build on any existing right of the company representative to obtain evidences in relation to their company.

3.4.4. Business Process of the Event Subscription and Notification Pattern

The subscription and notification pattern realizes the goal to inform the Data Evaluator of relevant changes in the subject (i.e. company or citizen). This is done in two steps:

1. In the subscription step the DE expresses the need to be informed on changes regarding a certain subject and this need is registered as a subscription.
2. In the notification step the DO monitors the subject and if a change occurs, all subscribers will be informed on this change.

These two steps are independently triggered processes and are hence represented below in two separate BPMN Business Process Collaboration views. Please note that the Subscription is triggered by the DC (i.e. DC is the upper participant in the Subscription BPMN diagram), while the Notification is triggered by the DP (i.e. the DP is the upper participant in the Notification BPMN diagram).

Some high-level starting points for the process design of this pattern are:

- Harmonized DE4A events: a list of harmonized, canonical events needs to be agreed upon, so DE knows how to interpret events notified by DO. For the DE4A-pilots, i.e. the Use Case "Doing Business in Another Member State" (DBA UC2), it is an option to start with a short list of harmonized business evens.
- Subscription registration: the subscription consists at least of the subject identifier and the subscriber identification (i.e. DE ID).
- Business- or Life event-based notification: the event-based approach informs the DC, i.e. the subscriber, of every business of life event of the subject (i.e. company or citizen) subscribed to. Examples of such events: address changed, new owner, bankruptcy, employed/unemployed, death.
- Notification message: the notification consists at least of the subject (i.e. company) identifier, the harmonized event type of the event that took place and the timestamp of the event.
- Data Evaluator post-processing: the DE needs to interpret the event and decide on the actions needed: e.g., request updated data, discard notification, start a specific procedure.

3.4.4.1. Event Subscription

Figure 13 shows the Business Process Collaboration of DC and DP that starts with the need for a subscription being identified (i.e. in a public service procedure) and leads to the DE logging the confirmation that their subscription was successful.

© 870635 DE4A Project Partners

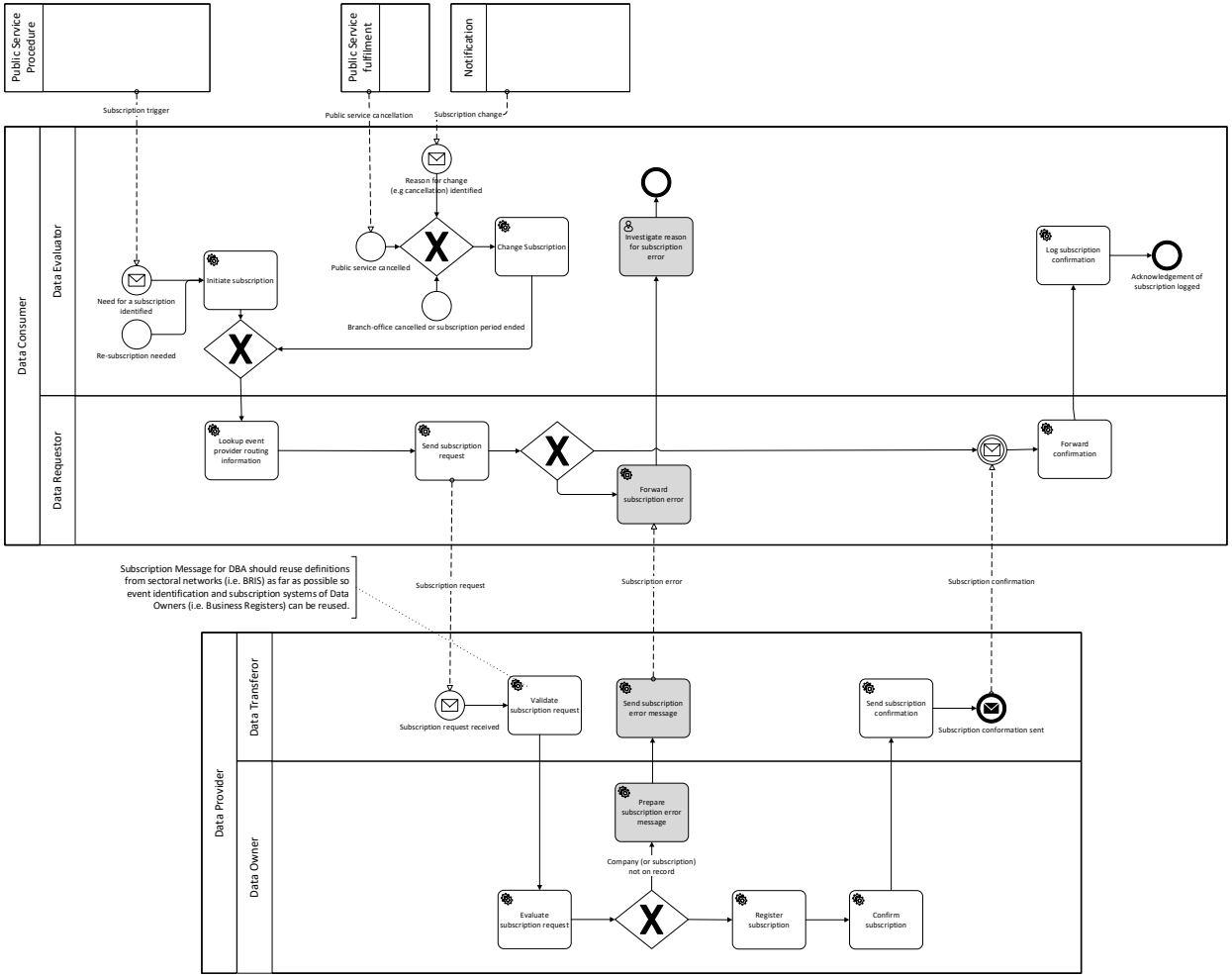


Figure 13 Event Subscription Business Process Collaboration View

See also Annex 4 for larger size

© 870635 DE4A Project Partners

The DE initiates the subscription and lets the DR identify the correct DO and sending the subscription request. Please note that a change of an already existing subscription follows the same process; changing the subscription end-date would, for example, be used for the cancellation or prolongation of a subscription. The option of a perpetual subscription with explicit cancellation was also discussed and discarded. The DP process registers the subscription and returns a confirmation or an error (in case the subject could not be found in the registry). The Table below provides a description of each of the activities in the process.

Table 16 Business Activities of the Event Subscription Pattern

Activity / UC	Role	Activity Type[4]	Description
Trigger: Need for a subscription identified	Public Service Procedure	Process	A procedure of a public service provider (e.g.: subsidy) leads to the registration of a subject (e.g. company). After this registration, events can occur to the subject that could have impact on the service delivery to this subject. In order to be informed on these events, the public service provider can subscribe to the life-events or business-events of the subject. The subscription process can also be triggered for technical reasons: for instance, to resend failed subscription requests. E.g.: In the pilot Doing Business Abroad the subject is the represented company itself or a new branch of the represented company (the parent-company of the branch) and Data Evaluators subscribe to be notified on the business events of the represented company.
Trigger: Change subscription	eProcedure / Public service / Notification	Process	Potential triggers to change a subscription are: • Public service: public service delivery can lead to the need to cancel the subscription (the public service has ended, e.g. a multi-year subsidy procedure, the country can decide to cancel the branch-office registration). • eProcedure: the User can also withdraw from service and thereby initiating cancellation of the subscription. • Notification: after receiving a notification the assessment can be that the subscription is no longer needed (exception flow). • Technical reasons: for instance, an error at the DO-side could lead to the need to resend the request to cancel a subscription.

[4] Activity Type and Task Type in accordance with BPMN 2.0

© 870635 DE4A Project Partners

Activity / UC	Role	Activity Type[4]	Description
Initiate subscription	DE	Service	To initiate subscription data is collected and the subscription need is formulated: • subject identifier • Data Owner identifier • subscriber identifier • event catalogue • action 'subscribe' • subscription start and end date The subscription need is forwarded to the Data Requestor.
Change subscription	DE	Service	To change a subscription data is collected and the changed subscription need is formulated: • subject identifier • Data Owner identifier • subscriber identifier • event catalogue • action 'cancel subscription' • new subscription end date The cancellation of a subscription is thus a change of the end date to the current date. The changed subscription need is forwarded to the Data Requestor.
Lookup event provider routing information	DR	Service	The DR uses the Data Owner identifier to look up routing information of the competent authority that facilitates subscription service. It is possible that at the DP-side the service provider of the subscription is different from the service provider of the evidence.
Send subscription request	DR	Service	The request to subscribe is send to the participant facilitating the subscription service using the previously retrieved routing information. The subscription request contains: the participant id of the subscriber, the subject identifier, the event catalogue, the period of subscription and the requested action (subscribe / cancel subscription).
Validate subscription request	DT	Service	The request is validated on a technical level and checked on DE authorization. If the request is valid, it is forwarded to the Data Owner.
Evaluate subscription request	DO	Service	The subscription request is evaluated to check if the request can be completed: Subscription functional checks: does subject exist, is event

© 870635 DE4A Project Partners

Activity / UC	Role	Activity Type[4]	Description
			catalogue supported, is the subscription changing an existing subscription (i.e. update) If the request does not pass the functional checks, the request is rejected and an error message will be sent.
Exception: Prepare subscription error message	DO	Service	Collect the content of the error message and send it to the Data Transferor. The subscription error message contains: participant id of subscriber, subject identifier, requested action, reference to the request message, and the error code.
Exception: Send subscription error message	DT	Service	The error message is forwarded to the Data Requestor from whom the request was received.
Exception: Forward subscription error	DR	Service	The subscription error message received from DT is forwarded to the DE.
Exception: Investigate reason for subscription error	DE	User	The received error message is analysed and appropriate actions are taken. This exception flow is not further detailed in this design.
Register subscription	DO	Service	The Data Owner creates or changes the subscription according to the subscription request.
Confirm subscription	DO	Service	The confirmation of the subscription is created and sent to the Data Transferor. The confirmation message contains subscription result (success), timestamp of subscription, subscription request reference, subscription id.
Send subscription confirmation	DT	Service	The subscription confirmation is sent to the Data Requestor from whom the request was received. The subscription confirmation message is added to the log.
Forward confirmation	DR	Service	The confirmation of the subscription (received from the DT) is forwarded to the Data Evaluator.
Log subscription information	DE	Service	The confirmation is logged to complete the audit trail. Note: register in a way that it is easily readable (optional: include subscription id).

© 870635 DE4A Project Partners

Design decisions

- **Explicit request and preview**

  The nature of the subscription and notification pattern leads to a different use of the explicit request and preview as stated in the SDG Regulation:

  - Notification is performed without a user involvement, making real-time explicit request and preview impossible.
  - Fraud prevention is an important driver for notifications, making explicit request and preview less opportune.
  - The public nature of company data relaxes the need of explicit request and preview.

  Implementing an explicit request for future notifications introduces the burden of creating and maintaining an explicit request administration or even management of consent, with for instance options to revoke a previously given consent - these are arguably more relevant for citizen use cases.

  Design decision: for the Business event notification explicit request and preview as defined in the SDG Regulation is not applicable.

- **Positioning of subscription registration**

  For the location of the subscription registration various options can be considered:

  - At the data providing MS: The subscription is registered at the data providing Member State. The DE sends messages to the DO via DR and DT to manage the subscription (subscribe, change subscription).
  - Split between data provider and data consuming MS: It is a possibility to split the register; the DO then only registers which MS subscribe to a certain company, and the DC MS registers which DE subscribe to the company. The process flow would be: (1) a central component at the DT registers which DEs subscribe to which subjects of which Data Owners; (2) the DT registers as a MS for this company; (3) the DO registers which MS subscribes to which company and sends notifications to the DT (4) the DT distributes the notification to all DE.
  - At a central component: The DE4A architecture implements the four-corner model, a central subscription register would conflict with this principle. Moreover, a subscription is a direct relation between a DO and a DE regarding a subject, there will be no added value to place such a subscription in an external, central component.

  Design decision: The registration of subscriptions is placed within the data providing Member State. DP MS is free to choose in which environment this is (DT, DO or another environment). The assumption for the design of the S&N pattern is that the subscription registration is fully placed in the environment of the DO.

- **Subscription period**

  Both perpetual subscriptions and the use of a subscription period with start and end date were considered. A perpetual subscription would require an explicit cancellation from the DE if the subscription is not needed anymore. This option was discarded, mainly because of the risk of an increasing number of "ghost subscriptions" that send automated notifications that are then automatically filtered out as irrelevant upon receiving.

© 870635 DE4A Project Partners

Design decision: a subscription period with mandatory start and end dates is included in the subscription.

- **Evidence exchange and subscription request**

  The main flow of the DBA pilot is that the intermediation pattern triggers the Subscription and Notification pattern. Part of the Intermediation pattern is the exchange of evidence: DE requests a specific evidence type from a specific company from the DO. In the happy flow the DE subscribes to receive notifications regarding this company. This trigger can be implemented in different ways:

  - As a part of the request for evidence. The evidence exchange request then consists at least of: company identifier, requested evidence type, DE identifier, subscribe y/n.
  - In a separate subscription request message: after a user consent to the preview and a successful completion of the registration process a separate subscription message is sent.

  Design decision: the subscription request is not combined with the evidence exchange request but is sent after successful registration of the company/branch.

  Design decision: not all business events are related to an evidence, subscriptions must therefore be made to business events to cover all notifications to be sent.

3.4.4.2. Event Notification

Figure 14 shows the Business Process Collaboration view of the Event Notification process that starts by analysing domestic event definitions from a Registry (considered external to this process) and concludes with the DE logging the appropriate action to be taken as result of the notification. Please note that the process starts with the DP, hence the upper pool in the diagram is the DP.

© 870635 DE4A Project Partners

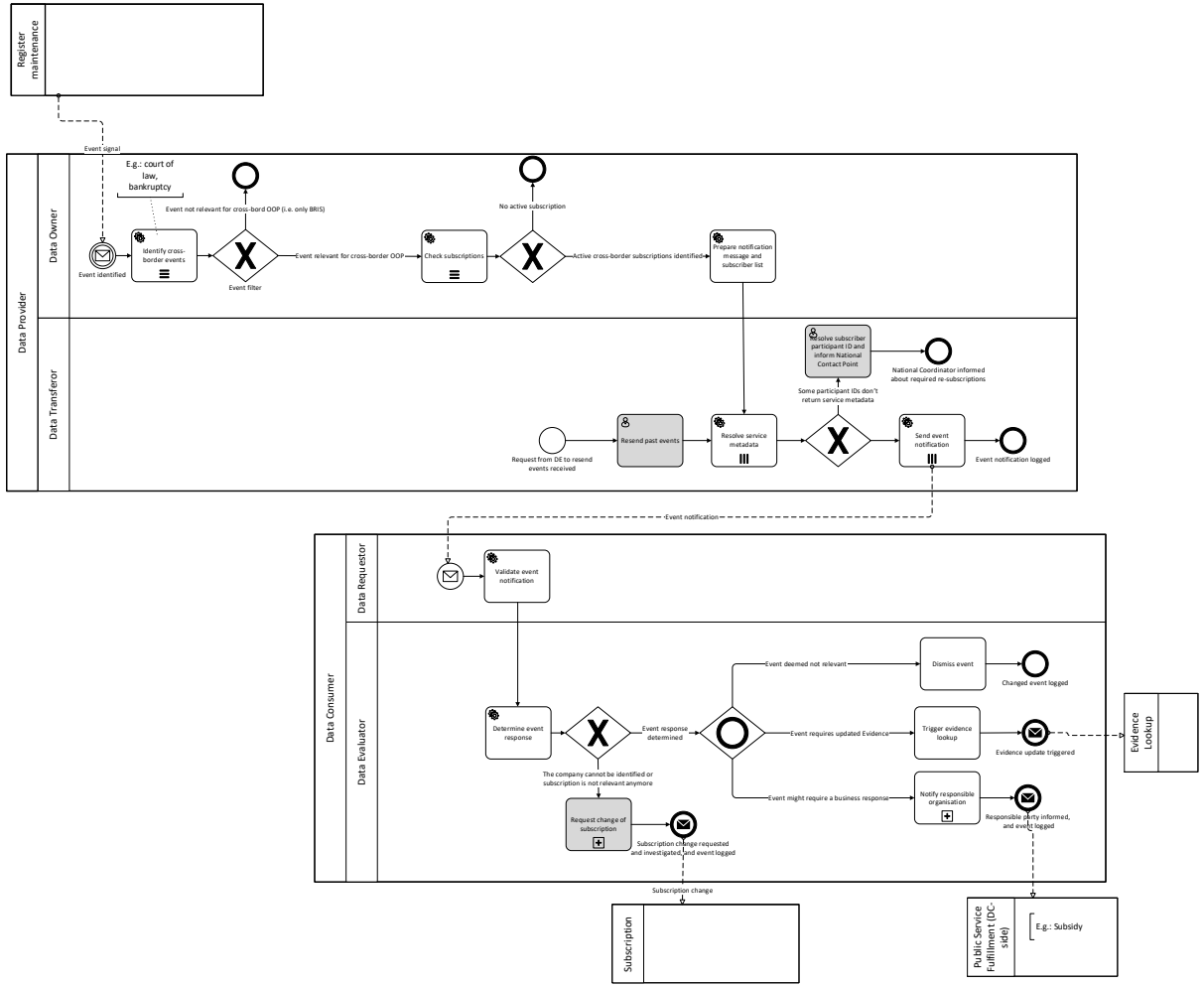


Figure 14 Business Process Collaboration View of the Notification Process

See also Annex 5 for larger size

© 870635 DE4A Project Partners

As can be seen in Figure 14, the Notification is not expecting any business-level confirmation. The DP filters events from the registry that are relevant for cross-border notifications and the DT sends them to the DC. The set of harmonized events allows for an automated processing of the notification and the identification of the correct action. These actions are not only dependent on the type of event (identified by the DP), but also the type of public service provided by the DC. A simple response would be to lookup a changed evidence (see Lookup Pattern in section 3.5 below). More complex cases will require a business response and expert analysis. The reference process informs the responsible organization or department to come into action.

Table 17 Business Activities of the Event Notification Pattern

Activity / UC	Role	Type	Description
Identify event	DO	Service	The Data Owner evaluates all events identified in the register and identifies events that are potentially relevant for cross-border notifications. Note that the DO must have a mapping of its own business events to the list of DE4A business events.
Check subscriptions	DO	Service	The subscription register is queried for subscribers to the subject (e.g. company) related to the event: • No active subscriptions: end of process • Active subscriptions for the DE4A event catalogue found: continue notification process
Prepare notification message and subscriber list	DO	Service	Make a list of the subscribers to notify in terms of cross-border participant identifiers and create the payload of the notification, mainly the DE4A event name and subject identifier and the timestamp the event took place.
Exception trigger: Request from DE to resend event notifications	DE	User	Exception flow for missed notifications (failed or non-failed): if a DE misses notifications a resend of notifications can be requested.
Exception: Resend past events	DT	User	The resending of previously sent notifications requires a manual action at the DT, based on logs. Note: when the number of manual interventions increases scalability might become an issue, i.e. thousands of messages exchanged via the DT. A (partially) automated solution would then be recommended. This is not further elaborated in the PSA.
Resolve service metadata	DT	Service	Single notifications messages (one for each subscriber) are created from the list of subscribers and the notification payload. The routing information for each notification message is looked up. The messages contain: subject identifier, secondary subject identifier (in case the identifier changed),

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			subscriber identification, event identification, event timestamp, subscription reference (optional).
Exception: Resolve subscriber participant ID and inform National Contact Point	DT	User	If address / DE participant ID is not found in the metadata, manual action is needed: contact DE / MS of participant to analyse the exception and take appropriate measures.
Send event notification	DT	Service	The event notification is sent to the Data Requestor, a technical acknowledgement that the notification has been received by the DR is received. The audit log is updated with both the event notification and the acknowledgement.
Validate event notification	DR	Service	The Data Requestor performs a technical validation of the event notification and forwards it to the Data Evaluator. A technical exception flow is out of scope of this process description.
Determine event response	DE	Service	The notified event is analysed, and the appropriate response is determined. Depending on the event, different courses of action are possible: • Event is not relevant • Event requires a new (i.e. updated) evidence • Business response required • Exception: The notification does not match the record or the record is not active, hence the subscription needs to be changed (i.e. cancelled) The determination result is logged as a part of the audit trail: • Subject identifier • Notified event • Request ID • Determined response • Timestamp of determination
Request change of subscription	DE	Subprocess	When the company cannot be identified, or the registered company or branch is no longer active, a change (i.e. cancellation) of the subscription is requested. Afterwards this will be analysed to find the cause of this apparently wrong subscription and to take appropriate measures. This subprocess includes user tasks and is not end-to-end automated.
Dismiss event	DE	Service	The notified event does not have impact on the procedures of the Data Evaluator and is dismissed. No further actions need to be taken.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
Trigger evidence lookup	DE	Service	The Lookup Pattern is triggered to request a new, current, copy of the relevant evidence. The Doing Business Abroad Pilot will e.g.: request the Company Registration Evidence.
Identify business response and notify responsible party	DE	Subprocess	The responsible organizational unit is identified and informed in order to take appropriate action. It depends on the specific process if this action can be performed automated or manually.

Design decisions

- **Response on event notification**

  Functional responses from Data Evaluator to Data Owner after receiving an event notification, for example to inform that appropriate actions have been taken, are out of scope of the Subscription and Notification pattern.

- **Notifications from Subscriber**

  Notifications from Data Evaluator to Data Owner, for example to inform Data Owner on changes in the branch registration, are out of scope of the Subscription and Notification pattern.

3.4.5. Process Realization

As with the Business Process Collaboration Views above, the Subscription & Notification pattern has two sets of Process Realization Views that provide the details on functional Application Services required to realize the business process.

- Two Views concerning Event Subscription, starting with the view for the DC, as it is the DC that starts a Subscription
- Two Views concerning Event Notification, starting with the view of the DP, as it is the DP that starts a Notification

This pattern does not provide any User Process Realization views as the User is not directly involved in the exchange. As can be seen in the Business Process above, Subscription is triggered by a public service process that requires updates for as long as the public service is provided, and the Notification is triggered by Events identified in the Base Registry.

Please see to the respective sections per Application Collaborations in the Reference Application Architecture for detailed descriptions of each Application Service.

3.4.5.1. Event Subscription

Figure 15 shows the Process Realization of the Subscription process at the Data Consumer, triggered by the need for a subscription, i.e. for public service provided over an extended period of time, and resulting (if successful) in receiving and logging the subscription.

© 870635 DE4A Project Partners

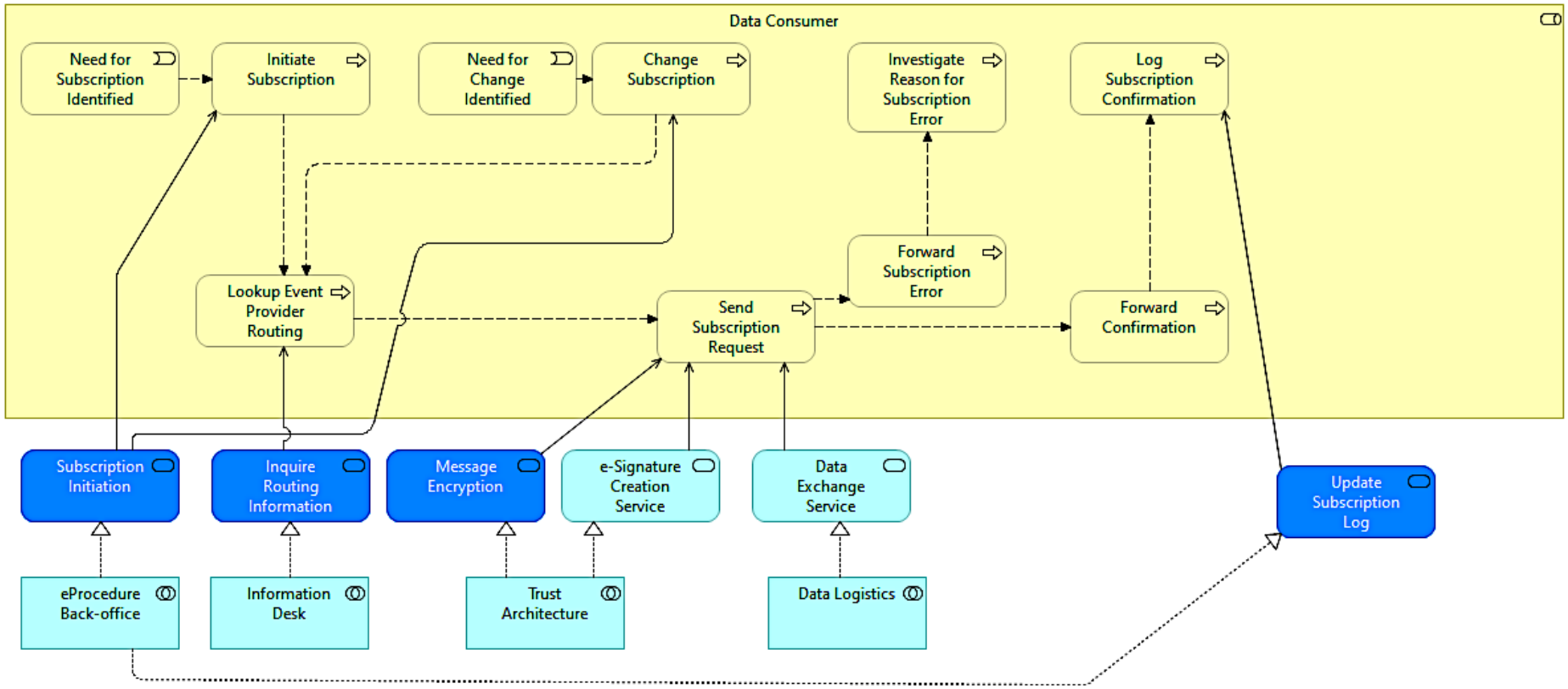


Figure 15 Subscription Process Realization of the Data Consumer

The Process Realization view above shows that both Initiation and Change subscription is provided by essentially the same service from the eProcedure Back-office (section 4.11 below). Changes, i.e. changes of the subscription end-date are handled in the process essentially identical as new subscriptions and are used to effect prolongations (new, later end-date) and cancellation (new end-data set to current date) of subscriptions. This provides maximum freedom to Cross-border Subscriptions (section 4.10 below) systems of the DP to handle cancellations and prolongation in the context of their own application

© 870635 DE4A Project Partners

architecture. For update cases a reference to the original subscription could be included as optional attribute in the request message. Service from the Information Desk (4.2), the Trust Architecture (4.4) and Data Logistics (4.5) are used to address and send the subscription request to the right DP. Even if the DP identity might already be known, at least the technical routing information is looked up, given the highly distributed nature of cross-border systems.

The right half of the Process realization shows reaction to receiving either a subscription error or confirmation. Investigating the reasons for a subscription error is a subprocess that usually includes manual work, as reasons can reach from simple ID mismatches to fraud.

Application Collaborations used in this Process Realization diagram:

- eProcedure Back-office (4.11)
- Information Desk (4.2)
- Trust Architecture (4.4)
- Data Logistics (4.5)

© 870635 DE4A Project Partners

Figure 16 shows the Process Realization of the Subscription process at the Data Provider, triggered by receiving a subscription request from the DC and resulting, if successful, by sending a confirmation that the subscription was registered in the Cross-border Subscriptions system.

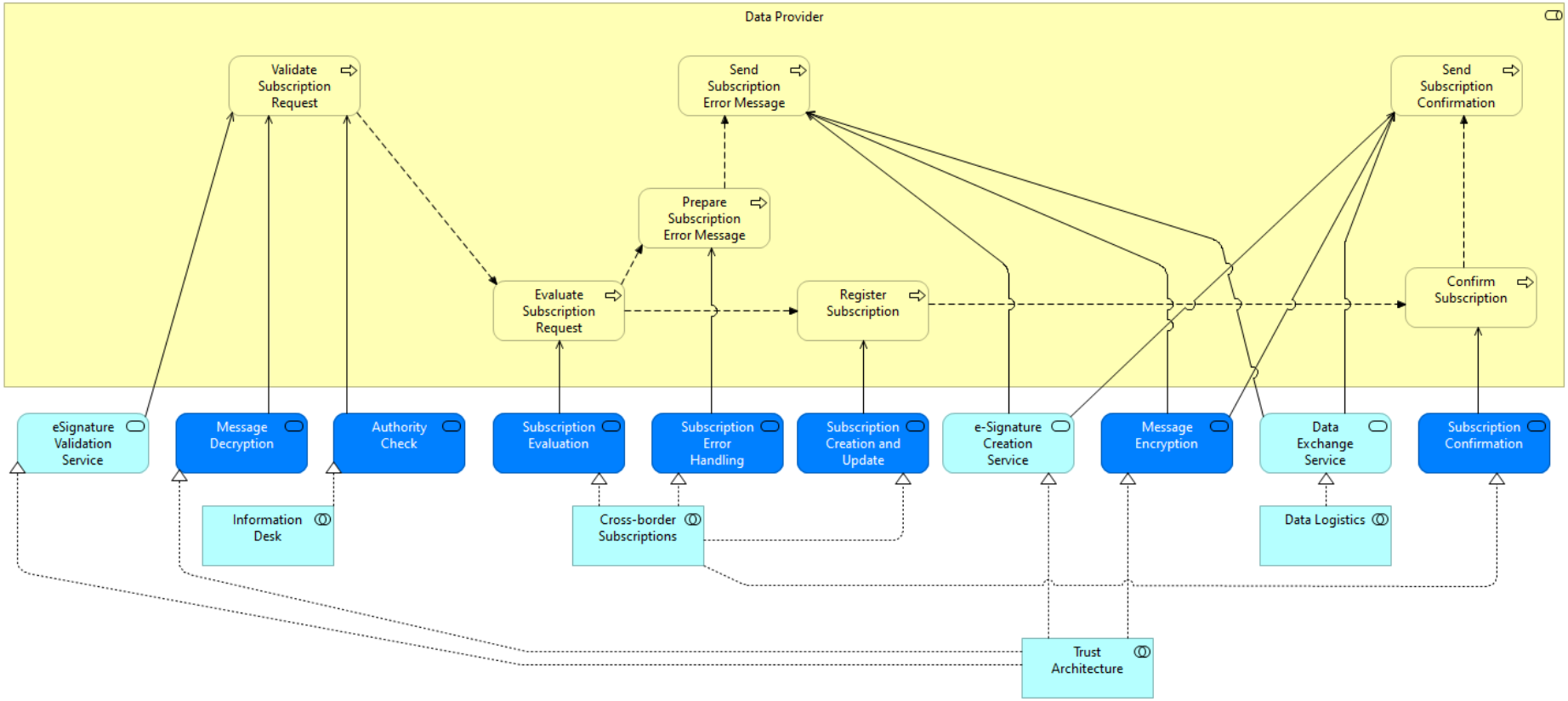


Figure 16 Subscription Process Realization of the Data Provider

The Process Realization view above shows that the process requires, apart from a simple technical validation, some sort of authorization at the start, the Authority Check, realized by the Information Desk (section 4.2 below). This is considered more relevant for Subscriptions than for the Intermediation Pattern, let alone the User-supported Intermediation Pattern, because the User is not directly involved here. The main part of the process is supported by a Cross-

© 870635 DE4A Project Partners

border Subscriptions system (see section 4.10 below). This application collaboration realizes all Application services required to evaluate, register, and confirm the subscription. Please note that the Subscription Creation and Update Service must identify whether a subscription request relates to an already existing subscription, i.e. is an update. This should happen at least as fall-back option, based on the subject ID and subscriber ID and overlapping subscription times, rather than a mandatory subscription ID, which could remain optional. In addition, Trust Architecture and Data Logistics are involved to guarantee secure and reliable message exchange.

Application Collaborations used in this Process Realization diagram:

- Cross-border Subscriptions (4.10)
- Information Desk (4.2)
- Trust Architecture (4.4)
- Data Logistics (4.5)

3.4.5.2. Event Notification

Figure 17 shows the Process Realization of the Notification process at the Data Provider, triggered by changes in the base registry and resulting, if successful, in sending a Notification to the DC.

© 870635 DE4A Project Partners

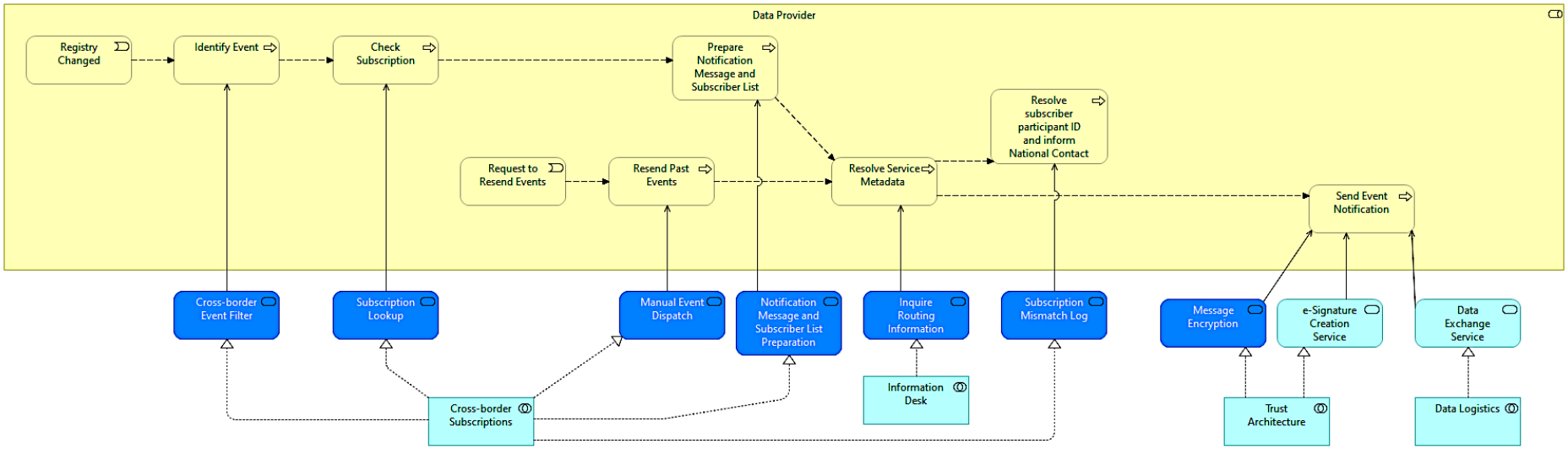


Figure 17 Notification Process Realization of the Data Provider

The Process Realization view above shows that the event stream from the base registry is first filtered to identify Cross-border events, i.e. events that are mapped to DE4A canonical event definitions. These events are then used to lookup active subscriptions, which are then collected into a subscriber list per event, coupled to the Notification Message (i.e. event type and subject ID). All of these steps are realized by the Cross-border Subscriptions Application Collaboration (see section 4.10 below). The Information Desk (section 4.2) is again used to look up at least the technical part of the routing. This gives rise to an exception flow if for a subscriber, registered in Cross-border Subscriptions, no service metadata (i.e. consumer) can be found in the Information Desk. Resolving such a situation is a subprocess, involving manual work and often resulting in corrective action required at the subscriber-side (e.g.: reorganization in the DC country did not update subscriptions, service metadata not maintained). Finally, Trust Architecture and Data Logistics providing for secure messaging.

It is important to note that the DP Process ends with sending the actual Notification message. Even though the transport protocol should ensure that this Notification was received by the gateway of the DC, this still means that it is functionally a "fire and forget" exchange; the DP is not informed whether the Notification was successfully processed by the DC. This gives rise to a second starting point of the process for exception handling: The DT might be asked by a

© 870635 DE4A Project Partners

DC, who experiences problems receiving or processing notifications to have all notifications (both successful and unsuccessful) of a given time period to be resent from the logs.

Application Collaborations used in this Process Realization diagram:

- Cross-border Subscriptions (4.10)
- Information Desk (4.2)
- Trust Architecture (4.4)
- Data Logistics (4.5)

© 870635 DE4A Project Partners

Figure 18 shows the Process Realization of the Notification process at the Data Consumer, triggered by receiving an Event Notification message and resulting in the correct event response being triggered and logged.

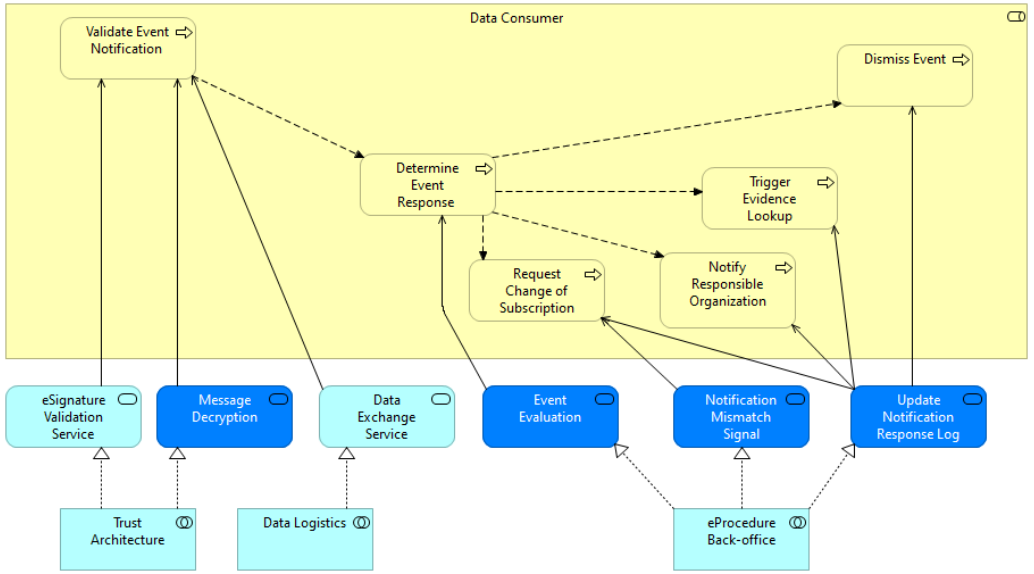


Figure 18 Notification Process Realization of the Data Consumer

The Process Realization view above shows that Trust Architecture and Data Logistics play again their role in secure message exchange, while the eProcedure Back-office plays the central role in determining the event response and in triggering the associated actions.

- For the hybrid approach described above, a lookup of an evidence (i.e. company registration) could be triggered.
- Changing or cancelling the subscription
- Notifying the responsible organization to take actions (e.g. termination of public service, suspicion of fraud)
- No immediate reaction is required

Application Collaborations used in this Process Realization diagram:

- Trust Architecture (4.4)
- Data Logistics (4.5)
- eProcedure Back-office (4.11)

© 870635 DE4A Project Partners

3.5.Lookup Pattern

https://wiki.de4a.eu/index.php/Lookup_Pattern

The pattern is used by the Doing Business Abroad Pilot in Use Case "Doing Business in Another Member State" (DBA UC2).

3.5.1. Functional Variants of the Lookup Pattern

The basic logic of the Lookup pattern is a simple Request-Response interaction between DC and DP without any user involvement. This is only applicable in cases where the exchange has a legal basis and can be executed without explicit request or consent from the User. Its main characteristic is online and near real-time (NRT) use of information. This should be understood as a synchronous/uninterrupted exchange of information. The pattern must be "light weight". DC and DP usually know each other up front and the communication relationship is set up to cover a number of repetitive interactions over time.

We identified two functional variations: the Evidence Lookup and the Attribute Lookup. The first one is a case where the Lookup pattern could be used in conjunction with the Subscription & Notification pattern.

Evidence Lookup

This variant is for looking up a complete Evidence. Once it is established that a lookup of the evidence is needed, e.g. via a notification from the DP to DC (see for instance the Subscription and Notification Pattern in section 3.4 above), the evidence can be retrieved in its entirety. This flavour of the Lookup Pattern can also be used for integration in public service (back-office) processes for cases where a legal basis for data sharing exists (e.g. bilateral agreement or publicly available data).

Table 18 Message Exchange of the Evidence Lookup

Request	Response
Evidence type ID	The evidence in its entirety

Attribute Lookup (i.e., using API)

This variant is for getting updates for specific attribute(s) as well as addressing the need for an API approach. Reusing existing APIs that already exist in MSs and providing a light-weight alternative for eDelivery.

Table 19 Message Exchange of the Attribute Lookup

Request	Response
(array of) attribute(s) [canonical of domestic]	A partial evidence, i.e., a number of attributes (key/value pairs or a data structure)

Alternative Solution Approaches

- Evidence Lookup

© 870635 DE4A Project Partners

It makes sense to reuse what has already been implemented, i.e., the Intermediation Pattern. This way we are leveraging the AS4-infrastructure and message definitions which are already put in place. Because the Lookup Pattern does not imply user intervention the Intermediation pattern can be simplified i.e., no explicit request and no preview and less multiplicity concerns.

This alternative is the proposed solution approach for DBA second iteration.

- Attribute Lookup

  This flavour of the Lookup Pattern addresses the need for a 'lightweight' alternative for eDelivery as well as the need for reusing existing APIs in MSs.

  One such example in context of our Doing Business Abroad Pilot: The Netherlands is calling an API in Belgium to retrieve some simple piece of information. Redeveloping existing solutions in order to make use of the eDelivery infrastructure cannot be justified.

The Commission also recognizes the need for a simple, complementary alternative. An interesting development is the piloting of an API approach in ISA^2 [18]. This project investigates new patterns of data access by request and data sharing. The initiative will facilitate design choices on the legal, organizational, semantic, and technical level necessary for setting up APIs. It includes the piloting of such an approach through a combination of the CEF eDelivery building block and a REST-based profile (a.k.a. "the APIs approach"). This looks like a promising initiative and an interesting development for the future. At this point in time however, there is no mature BB for DE4A to be used. This is one of the reasons why we recommend the Evidence Lookup as solution direction for the DBA Pilot.

3.5.2. Working Hypotheses and Implementation Principles

Table 20 Lookup Pattern Working Hypotheses and Implementation Principles

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Orchestration / Choreography	The DC is orchestrating the overall flow. This means that the process on DP side is a child process of the process on the DC side.	The DC controls the status of the DP evidence retrieval process. The DC can retain overall control by reacting to responses of the DP (evidence or error) and monitoring that a response is received in a reasonable amount of time (i.e. SLA)
Complementary, overlapping, or conflicting evidence equivalents	Cases of ambiguous evidences must in principle be supported by the technical system. These cases are expected to be rare for lookup, because it is always related to a single Evidence request, single Evidence Type and single DP in contrast to the Intermediation Pattern that by definition needs to be able to handle multiple Evidence requests to multiple DPs in potentially different countries relevant for a single eProcedure.	The DE4A pilot cases appear not to suffer from this issue and the canonical evidence approach also means that this issue is usually resolved at the DP-side.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Interrupted vs. Uninterrupted exchange	The whole lookup is handled in an uninterrupted manner. This means that any exception during the lookup leads to its termination, potentially to be repeated later as a new attempt.	
Identity and Record Matching	From experience on MS-level we see that a reasonably good match can result from the use of the (mandatory) eIDAS attributes. The working hypothesis is that this insight can be generalized to all pilot MSs and that the subject of the lookup can be identified with a similar set data set. This data set can be delivered by the DC as part of the Evidence Request.	The DC must be in possession of the identification data set when requesting the evidence. If the subject is a natural person, then the DC must have a legal basis to transmit the identification data set as it is personal data. The problem is not relevant for DBA: there the subject is a company and the European Unique Identifier for companies (EUID) can be used which is available to the DC.
Encryption Gap	Identical to Intermediation: OOP does not require true E2E encryption. The exchange between DR and DT must be encrypted and signed, as well as the transfers (if applicable on national level) between DR and DE on DC side and DT and DO on DP side (i.e. using the national OOP layer), but the encryption gap within the systems of the DR and DT is acceptable.	This might not hold for cases where the gateway would be outsourced to a private sector subcontractor, which is not foreseen for the DE4A pilots.
Structured data vs. unstructured data	Identical to Intermediation: Evidence is handled as structured data. This is not contradicting the addition of an unstructured or scanned document/certificate as part of the structured data transfer (hybrid approach) for reasons of legal validity as identified as barrier in D1.7: L4: National requirements for original and /or certified copies of evidence.	
Automated re-use of data	Identical to Intermediation: Evidence and its use in public service procedures has legal consequences. We assume that automated re-use without harmonization of evidence data definitions is not	To facilitate automated re-use of data requires establishing canonical evidence definitions. For DBA, this is the case.

© 870635 DE4A Project Partners

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
	applicable for the OOP transfer of evidence between MS.	
Production system and real-life cases	The lookup pattern is not covered by the SDGR or only as so far as the exchange is allowed under national or Union law. This means that it requires a separate legal basis (see also legal considerations below).	For DBA, company registration data is already publicly available which serves a legal basis for the lookup.
Payment for evidence	In the context of the pilots, we assume that no payments are required.	This can restrict transition of pilot solutions to production in cases that competent authorities require payment for issuing evidence. As this is often the case for business registers and could impact the exploitation of the DBA results.
BRIS integration	A technical re-use or bridge to BRIS is not possible because of differences in scope and accessibility by competent authorities other than business registers. The semantic definitions of BRIS can be largely reused.	The pilot system for the DBA need to be set-up separate from BRIS.
Matching evidences between Member States	The final system should support both non-harmonized and harmonized evidence types and the architecture is taking account of both bases. In the pilot context, focus will be put on establishing deep semantic interoperability through the definition of canonical evidences	Heterogeneous, national evidence types do not need to be matched in run-time in the pilots. For all evidence types in DE4A, a canonical form is defined and agreed between the pilot partners. Each partner needs to implement a transformation from national to canonical evidence.
Multi-evidence Cases	The system should support all four multi-evidence cases, which means that an array of evidence types and evidences could be included in a single OOP request/response.	The second iteration should expand the MVP restriction to a single request to single evidence cases, which requires an update of the Exchange Information Model. It is likely that piloting would focus on simpler cases to show the inclusion of multiple evidences in a single evidence response.

© 870635 DE4A Project Partners

3.5.3. Legal Considerations

In terms of legal challenges, the lookup pattern faces the complexity that it is not directly supported by the SDGR. The objective of the lookup pattern is not to transfer evidence in accordance with the SDGR, since evidence transfers under the SDGR are driven (in principle) by an explicit user request. The lookup pattern instead by definition aims to transfer information directly at an authority's request, without any necessary involvement of a User in the specific exchange.

However, this is not necessarily a fundamental problem. If the lookup pattern focuses on information that is publicly available (e.g. in a publicly accessible database or using an open web service or API), then it would be perfectly feasible for an authority to query that database using the lookup pattern. This would be lawful even outside of the context of the SDGR, assuming that the data holder has the legal authority to indeed make the relevant information publicly accessible, and that the Data Evaluator has the legal authority to request such information without user request (i.e. if there is no legal requirement on them to rely exclusively on information provided by the User). If those two prerequisites are satisfied, the lookup pattern can be piloted in DE4A, without any reliance on the SDGR.

It is worth cautioning for an additional complexity when using the lookup pattern for personal data. The challenge is not the legal basis for personal data processing, which both the data holder and Data Evaluator should be able to find in their respective legal mandates under national law. Instead, the challenge is transparency: the Data Evaluator will be using the obtained data under its own legal responsibility, acting as a data controller. This implies that it is legally bound to provide transparency information to the data subject. This will generally only be feasible if there has been direct communication between the Data Evaluator and the data subject, so that this information can be provided (basically that the lookups will happen, and what the information will be used for). If such direct contact is not legally possible, then lookups of personal data are legally inadvisable.

3.5.4. Business Process of the Evidence Lookup

Figure 19 shows the BPMN Business Process Collaboration view of the Evidence Subscription Process, which is either triggered because a Notification was interpreted to require an evidence update, or it is triggered by a Public Service procedure that requires an evidence that can be fetched based in bilateral agreement or national or Union law. Please note that this pattern is **not** triggered by the User. The Evidence Lookup could therefore also be used in a traditional procedure based on a transaction with the User.

© 870635 DE4A Project Partners

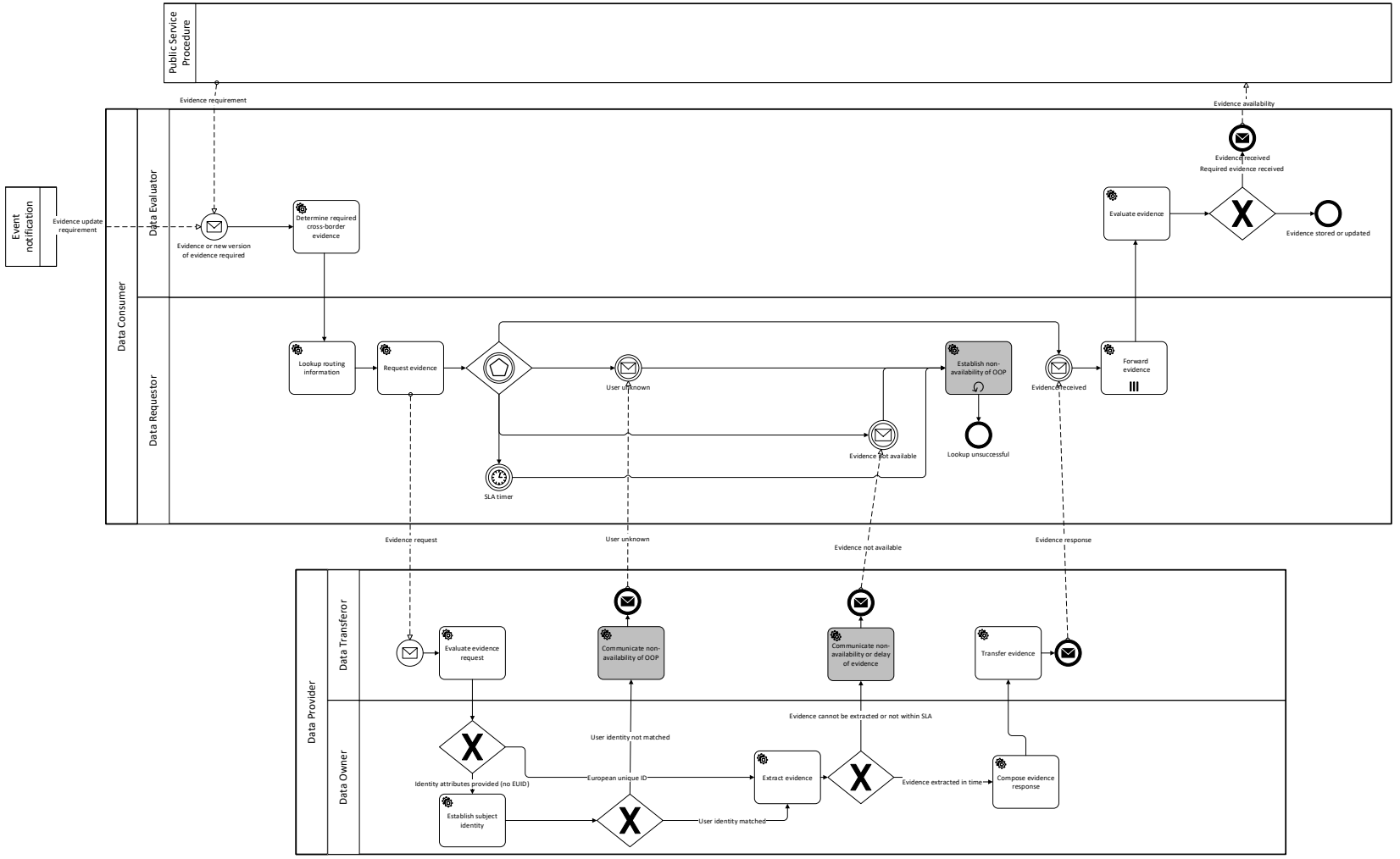


Figure 19 Evidence Lookup Business Process Collaboration

See also Annex 6 for larger size

© 870635 DE4A Project Partners

As can be seen in the Business Process Collaboration view above, the process of looking up an evidence for the first time or looking up a new version of the evidence is essentially identical. These variants have, however, different legal implications and might consequently differ in the authorization aspect of the Evaluate Evidence Request activity. The process is also very similar to the Intermediation Pattern, even though not all activities listed below are equally relevant for all use cases. The Establish Subject Identity activity, for example, is not relevant for all business use-cases that can base identification on a European unique identifier. The DC looks up the correct DP, which might be simplified for pilot purposes, and sends an Evidence request to the DP. The DP checks the request, extracts the evidence, and returns the Evidence response that is then saved by the DC.

Table 21 Business Activities of the Lookup pattern

Activity / UC	Role	Type	Description
Determine required cross-border evidence	DE	Service	This step makes sure that the DE always requests the recent version of the Evidence type (cf. canonical evidences); in the evidence update case, for example, the evidence type definitions might have changed since the last lookup. In cases where the evidence type is not harmonized, the required evidence type (in terms of the DC country) is translated into equivalent evidence types that are issued in a lawful way in the DP country indicated by the User (not in pilot scope).
Lookup routing information	DR	Service	The DR retrieves the technical routing information (e.g. eDelivery routing identifier), based on the evidence type (in terms of DP country) and the issuing competent authority (or geographic scope of authority). Note that the Evidence Lookup is used in DE4A in combination with the Subscription and Notification Pattern, so as long as the subscription and lookup service is provided by the same DC, the participant ID of the DP can be assumed to be known and be included in the Evidence update requirement.
Request evidence	DR	Service	The DR encrypts, signs, and sends the evidence request to the DT. The evidence request must include subject (i.e. company) information that enables the DP to identify for which subject the evidence must be issued. Companies already have a European unique identifier available (EUID), which is sufficient identification information.
Evaluate evidence request	DT	Service	The DT receives and decrypts the request and checks whether the request meets formal requirements and can be accepted. It should be checked whether the requesting competent authority can reasonably and rightfully request that specific type of evidence (The authority check is not piloted in DE4A)
Establish subject identity	DO	Service	This activity is only relevant in absence of a European Unique Identifier. The DO matches identification information about the subject (i.e. equivalent to eIDAS mandatory and optional attributes) with the DP country's records to identify the subject in their systems. This amounts to matching the eIDAS

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			attributes to a national identification number. This is a Data Owner activity, because in a distributed scenario the Data Transferor might not have a legal basis to do so.
Communicate non-availability of OOP[5]	DT	Service	This exception handling activity is only relevant in absence of a European Unique Identifier: The DT informs the DR that the subject cannot be identified unequivocally, and the system cannot be used to transfer the evidence.
Extract evidence	DO	Service	The DO extracts the requested evidence from their registry and forwards it to the DT.
Communicate non-availability of evidence	DT	Service	Exception handling activity: The DT informs the DR that the requested evidence cannot be provided or cannot be provided within the agreed SLA.
Establish non-availability of OOP	DR	Service	Exception handling activity: The DR catches the negative (non-evidence) response from the DT and establishes the reason in terms of the DC country system and language: There are potentially several reasons why an OOP transfer of evidence is not available. The DT communicates these reasons to the DR in all cases that the evidence request cannot be fulfilled (i.e. by sending the digitally available evidence within the agreed SLA as described above). At the moment we expect at least the following reasons for such an exception that should be framed in standard error messages or codes, each one with a corresponding recommendation. • Subject cannot be uniquely identified – fall-back to another channel (i.e. IMI) • Evidence not found – Check whether the request specified the correct geographical scope of authority and contact the DP directly if that was the case • Evidence transfer blocked for legal or authorization reasons – Contact the DP directly • Evidence is not readily available in a digital format now. Expected time for the evidence to be available is x days – return after x days and issue a new evidence request
Compose evidence response	DO	Service	The DO prepares the extracted evidence to be sent as an evidence response. Depending on the level of harmonization of the evidence type this task can differ in complexity. If a canonical evidence definition is agreed, as is the case in DBA,

[5] Like in other patterns there are two occurrences of this activity, one for DT (only related to identification of subject) and one for DR (see further in the table). OOP should be read as OOP Transfer, though formally speaking it is probably better to call it OOPTS.

© 870635 DE4A Project Partners

Activity / UC	Role	Type	Description
			then this task includes the translation of the national definitions into the canonical evidence.
Transfer evidence	DT	Service	The DT creates the evidence response message (compliant to agreed message format), encrypts, and signs the message and sends it to the DR.
Forward evidence	DR	Service	The DR registers the receipt, decrypts the message and in many cases encrypts the message in a MS specific format to hand it on to the DE.
Evaluate evidence	DE	Service	The DE validates that the evidence conforms to the evidence type requested and stored or updates the evidence. If it is a new evidence that was requested as part of a public service procedure, the availability of the evidence is signalled to the active procedure.

© 870635 DE4A Project Partners

3.5.5. Process Realization of the Evidence Lookup

Figure 20 shows how application services serve the Data Consumer process. The application services are realized by application collaborations.

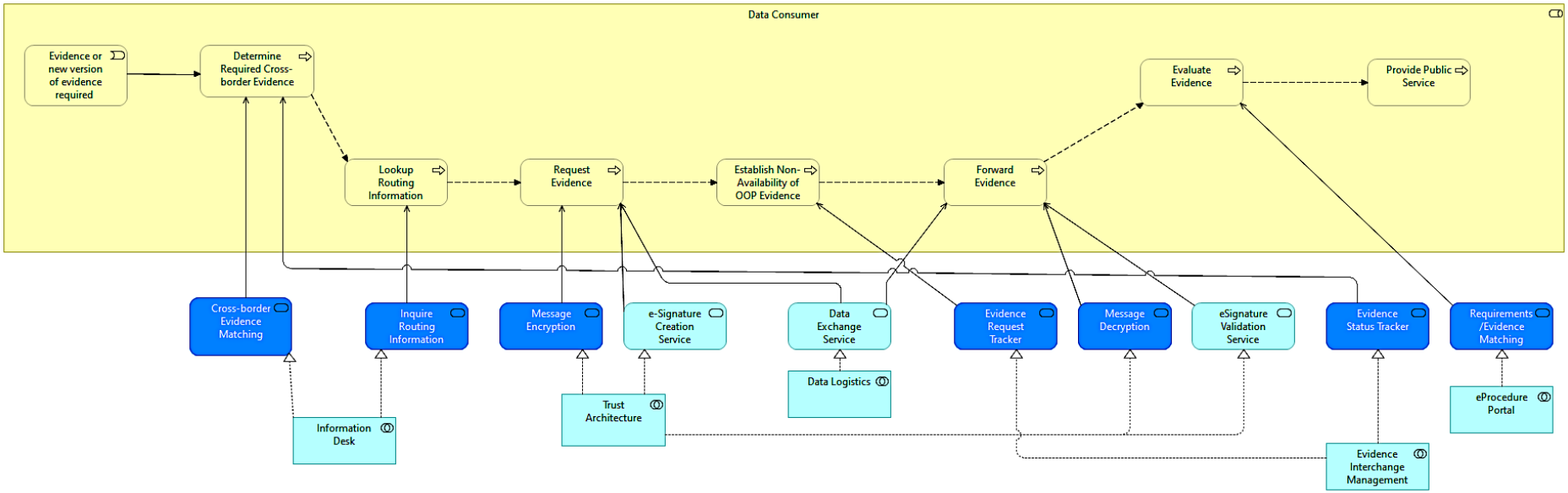


Figure 20 Process Realization of the Data Consumer

The process starts by an external business trigger identifying the need for an evidence or update thereof. With the help of the Information Desk (see section 4.2 below) the required cross-border evidence is determined, and the relevant routing information is looked up.

Next, the Evidence can be requested, the request message is encrypted and digitally signed using the Trust Architecture[6] (section 4.4). The evidence is exchanged using Data Logistics (section 4.5) and can be tracked using Evidence Interchange Management (section 4.3). The signature of the Evidence response message is validated, and the message decrypted (Trust Architecture). Next the evidence can be evaluated by the DC (eProcedure Portal, section 4.1) and if all is well the public service can be (or continued to be) provided.

[6] This functionality is at eDelivery level.

© 870635 DE4A Project Partners

Figure 21 shows how application services serve the Data Provider process. The application services are realized by application collaborations.

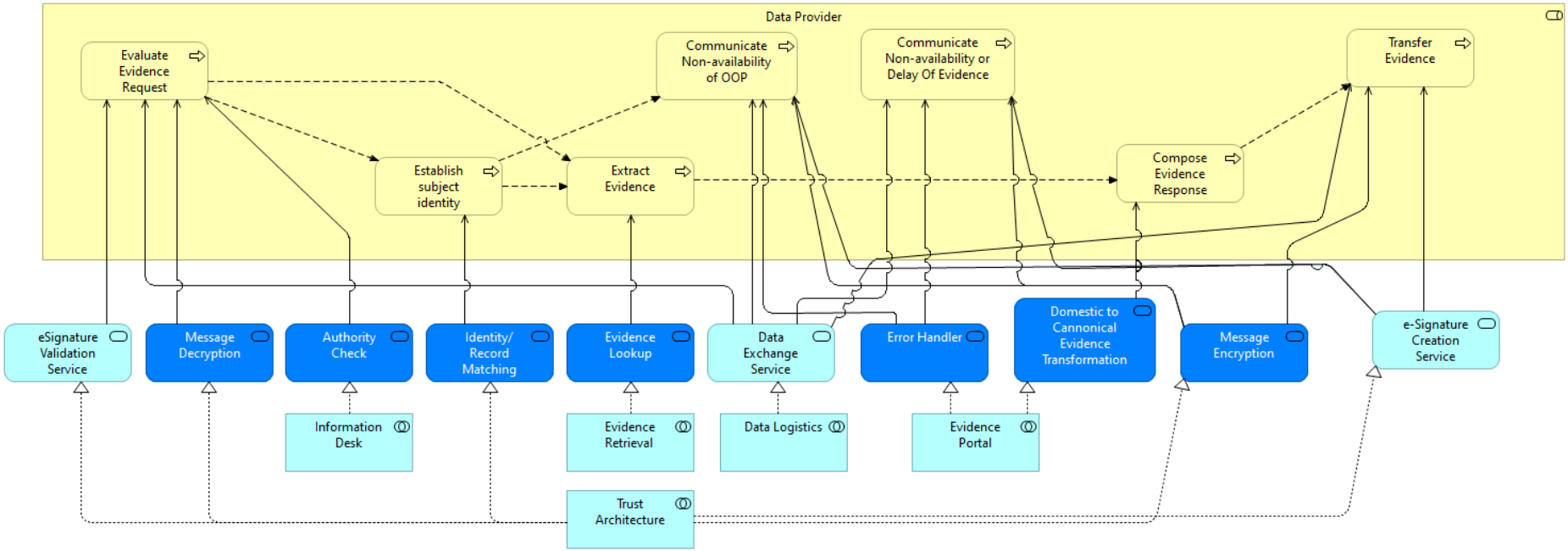


Figure 21 Process Realization of the Data Provider

The Evidence request is received via Data Logistics (section 4.5) and with the help of Trust Architecture[7] (section 4.4) the DP checks the signature of the request and decrypts it. An Authority check may be performed using the Information Desk (section 4.2) establishing that the DC is allowed to request the evidence type, which is most likely not in scope of the pilot with a limited number of participants. Next the subject identity is established using Trust Architecture. If successful, the evidence is extracted by Evidence Retrieval (section 4.7) and transformed to canonical form (Evidence Portal, section 4.6). Various exceptions like non-availability of OOP or the delay or non-availability of evidence are handled by Evidence Portal and Data Logistics. If all is well, the Evidence response is composed and prepared for transfer (Evidence Portal), encrypted and digitally signed using Trust Architecture and ultimately exchanged using Data Logistics.

[7] This functionality is at eDelivery level.

© 870635 DE4A Project Partners

3.5.6. Future Extension: Attribute Lookup Using API

As elaborated above, an interesting development is a pilot project of ISA[2]. We think this development holds great promise for future cross border data exchange in specific contexts. [18]

Source	European Commission
Action Owner	CONNECT (DIGIT, JRC).
Objectives & scope	Develop relevant legal, organizational, and technical artefacts trialled through a combination of the CEF eDelivery building block with blockchain-based transactions' log and a REST-based profile (a.k.a. APIs approach), that support new patterns of data access by request and data sharing. The initiative will facilitate design choices on the legal, organizational, semantic, and technical level necessary for setting up APIs.

The REST-based profile is relevant for the DE4A Attribute Lookup pattern; however, the scope of the API project is (much) wider. The envisaged implementation is an extension of the eDelivery BB. In the next section, we summarize some of the results of that Pilot project, e.g. the business case, the envisaged Light Context and the requirements which were fed into the activity as well as the legal basis for this data exchange approach. We conclude with an analysis from a DE4A point of view, which could act as a checklist of decisions to be made when implementing an API approach for cross-border eGovernment interoperability.

Business Case

The need for a complementary alternative to eDelivery was identified. The data exchange would operate in a so-called "light context". A BB with a profile to cater for the REST API architectural style primarily addressing different architectures and communication patterns than those already supported by the eDelivery AS4 profile.

Light Context

The term "light context" refers to a set of constraints and circumstances applying to organizations or environments that do not run (in) an enterprise IT data centre (non-limitative):

- Organizational constraints
- Hardware and IT infrastructure constraints
- "Low throughput" scenarios
- Limitations introduced by sandbox environments

Requirements

Several requirements were drawn up for the envisaged specification:

- Simple or automatic installation of the software
- Minimal or zero configuration that assumes no advanced knowledge of the used technology
- Minimal operation and maintenance
- Ease of use with immediate start and no complicated enrolment
- Reduced requirements on the hardware resource

© 870635 DE4A Project Partners

- Reduced access privileges on the host

Legal Basis

Legal basis: the activity is carried out under the ISA² action on Innovative Public Services, legal artefacts are also envisaged.

See also Legal Consideration above.

Analysis - Checklist of Required Decisions for Applying API-Approach

The analysis of the proposed API-approach for the ISA² pilot yields the following list of aspects to be considered when implementing an API approach:

The number of corners to be supported, 2 or more

The specification/profile could consider a variable number of corners, starting with as few as two and extending the model to support an arbitrary number greater than four (interoperability with other existing protocols and message/data exchange networks).

1. 2-corner – traditional client-server call (proposed for DE4A as simplifying assumption)
2. 3-corner – a reduced version of the 4-corner where corners C1 and C2 are collapsed into a single corner, C1+2, or corners C2 and C3 are collapsed into a single corner, C2+3 (examples include a conference call app or sending an email directly via SMTP)
3. Four corners or more, in particular in the sense of not introducing accidental barriers to interoperability between the REST API profile and other existing protocols and message/data exchange networks is concerned (CEF eDelivery AS4, SDG, X-Road, GAIA-X). The profile should strive to minimize the need for a conformant API to be adapted for use in different such networks.

Communication patterns

Various communication patterns can be considered, e.g.:

1. Synchronous business response (the sending corner (C1) sends a business message to the receiving corner (C2) via an http request and expects a business response. The http response it receives from C2 contains a business message and completes the exchange) (proposed as a simplifying assumption for DE4A).
2. Asynchronous business response (the sending corner (C1) sends a business message to the receiving corner (C2) via an http request and expects a business response. The http response it receives from C2 contains no business message, but only an acknowledgment of receipt. The business response will be obtained later, e.g., through a pull or web socket).
3. No business response (the sending corner (C1) sends a business message to the receiving corner (C2) via an http request and does not expect a business response. The http response it receives from C2 contains only an acknowledgment of receipt and completes the exchange).
4. reliable delivery (in a 3-corner model, by enabling retry calls from C2 to C3)
5. broadcast (in a 3-corner model, by forwarding the call to a list of recipients)
6. asynchronous send buffer / streaming (send buffer instead of full message)
7. correlated calls to transmit multi-part messages

© 870635 DE4A Project Partners

How to manage identity

Direct management of certificates is impractical in a "light context", alternative authorization approaches relying on protocols designed for the web/mobile application world are required instead. There are a number of candidates to be considered. Currently, it is not clear what standard(s) should be supported:

1. OAuth 2.0 / OpenID Connect
2. JSON Web Token
3. SAML
4. Web authentication
5. FIDO 2
6. potentially others (e.g., EU Login)

Transport protocols

An obvious candidate is HTTP/JSON, which would also be our recommendation for DE4A, however, there are alternatives, e.g. XML.

Integrity & confidentiality

Here we have a clear recommendation for TLS[27].

The message signing option would have to be investigated.

(Q)ERDS = Qualified Electronic Registered Delivery Service

This would not be required for DE4A but implies some interesting use cases.

As can be concluded from the above analysis the API approach is definitely more complex than the initially envisaged lookup pattern from D2.1 (a simple synchronous request/reply to obtain a few attributes). However, it holds promise in the sense that we could leverage existing APIs in the MSs to facilitate cross-border data exchange instead of costly redevelopments to make it fit the eDelivery/AS4 solution.

© 870635 DE4A Project Partners

4. Reference Application Architecture

At the highest level of the Application Architecture, we have the Application Collaborations. They are aggregations of Application components, Data objects and Interfaces. The Application Collaboration views show how different functional application components interact via interfaces to provide the services identified in the Business Process realization Views. In addition, data objects are represented that are accessed by the Application Components. The access relations are specialized using the CRUD classification.

A total of 11 Application Collaborations have been elaborated, together specifying all 5 Interaction Patterns:

1. eProcedure Portal
2. Information Desk
3. Evidence Interchange Management
4. Trust Architecture
5. Data Logistics
6. Evidence Portal
7. Evidence Retrieval
8. Authority Agent
9. User Agent
10. Cross-border Subscriptions
11. eProcedure Back-office

Some Application Collaborations are pattern-specific while most are shared between multiple patterns. Each Application Collaboration is depicted by one or more diagrams showing the differences per pattern if needed.

Each Application Collaboration section contains a table with all relevant Application Components with an indication to which pattern they are applicable. Each Application Component has its own section listing all Applications Services it realizes again with an indication to which pattern the Application Service is applicable.

We would like to stress that the Application Architecture is one multi-pattern architecture and not an architecture per pattern. The collection of Application Collaborations should be seen as one solution for all.

4.1.eProcedure Portal

https://wiki.de4a.eu/index.php/EProcedure_Portal

The eProcedure portal application collaboration aggregates multiple co-operating application components. It resides at the DC and bundles important 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. The User can initiate the eProcedure and later also choose to terminate it if they so wish. 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 might offer functionality for save and resume. This to avoid that the User must start all over in case of exceptions (e.g., a piece of evidence not available or when it takes longer than

© 870635 DE4A Project Partners

expected). The portal supports the DC in requirements/evidence matching and the determination of already available evidence so that it is clear what is still to be requested to DPs.

For VC the portal front-end component provides the User with several features, such as initiate or terminate the procedure, accept request for VC from the DC, scan QR code, view evidence status, submit and confirm eProcedure and similar. To enable this level of procedure flow control to the User, there must be a collaboration with the Procedure Management subcomponents. On the other side, the eProcedure back-end component communicates with the Edge Agent (Wallet) through an interface regarding establishing the DID connection through the QR code and it captures all necessary events in the system log files.

The back-end also communicates with the Information Desk to retrieve information about available DPs for issuing the missing VC to the User. The Rules engine component is responsible for evaluating the current evidence status for the User; namely, retrieving the information about evidence that the User currently has available (through evidence matching) and identifying missing evidence according to procedure requirements obtained from querying the eProcedure.

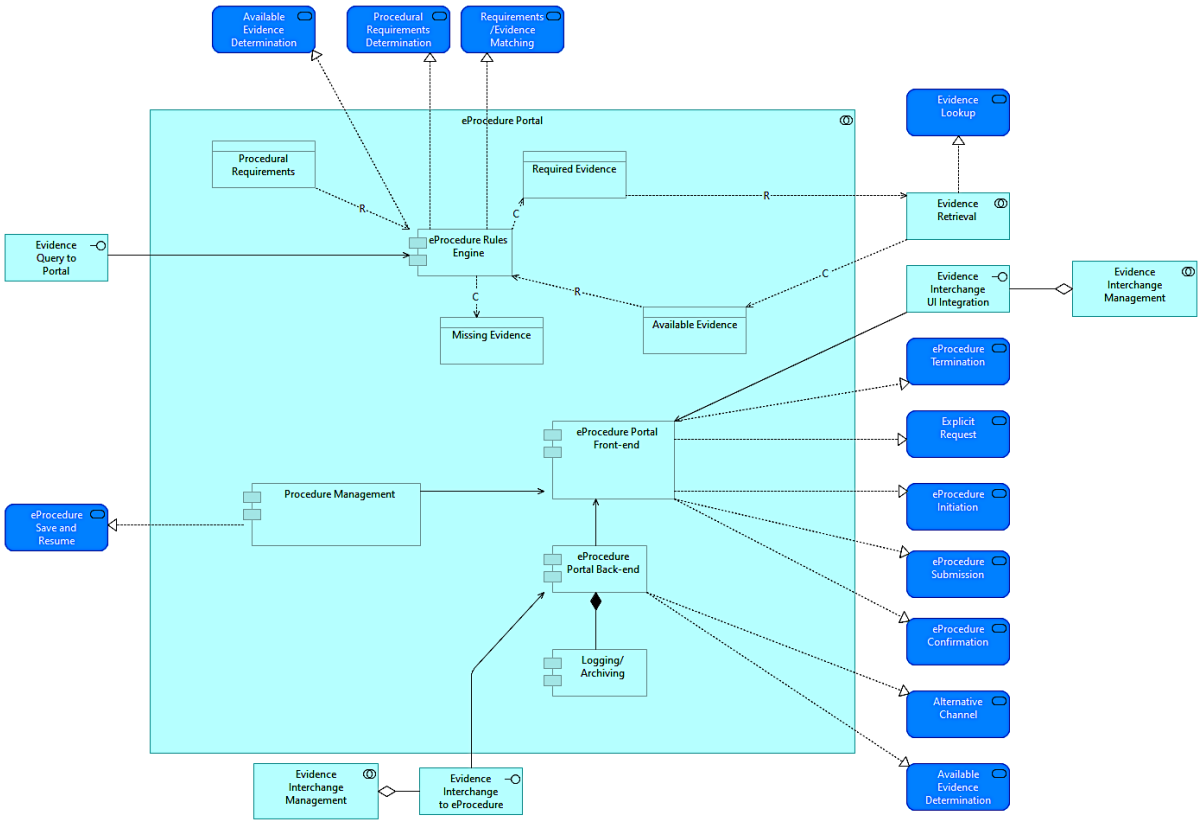


Figure 22 Graphic Representation of the eProcedure Portal Application Collaboration in the IM Pattern

© 870635 DE4A Project Partners

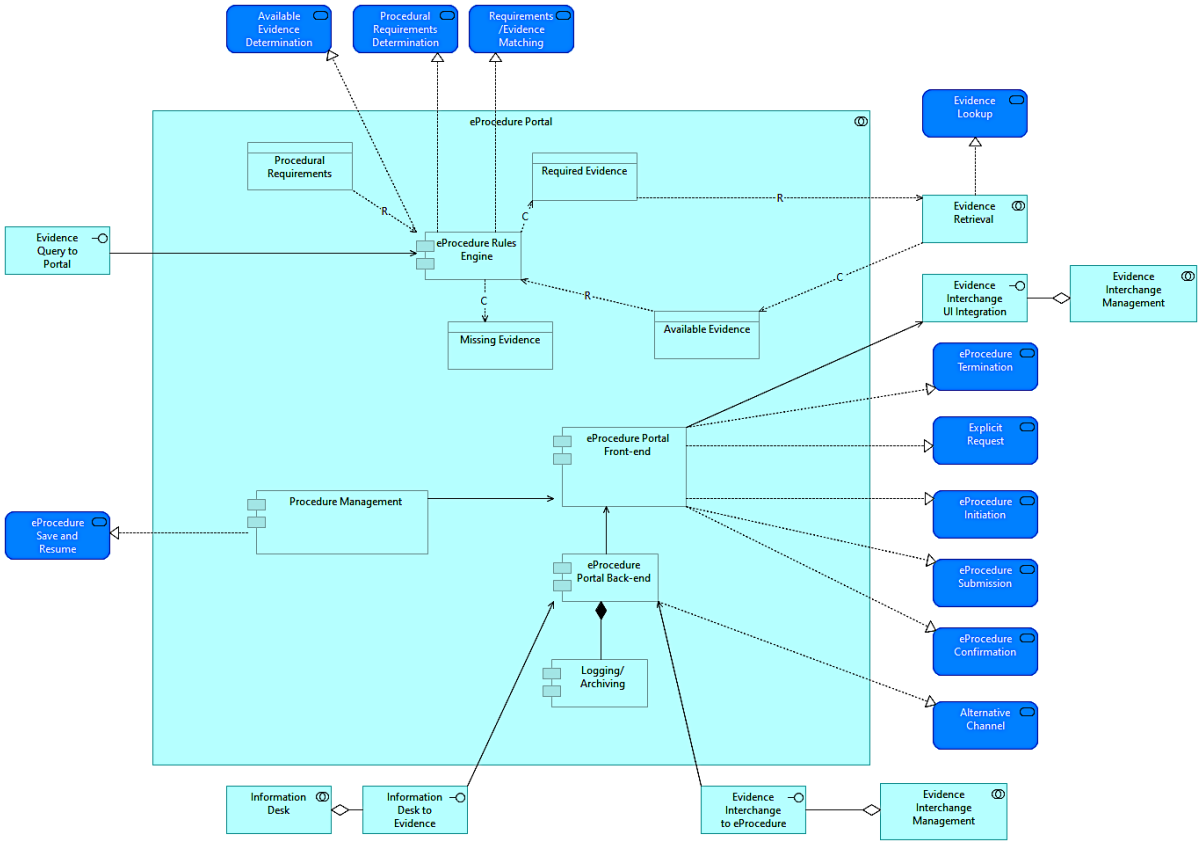


Figure 23 Graphic Representation of the eProcedure Portal Application Collaboration in the USI Pattern

© 870635 DE4A Project Partners

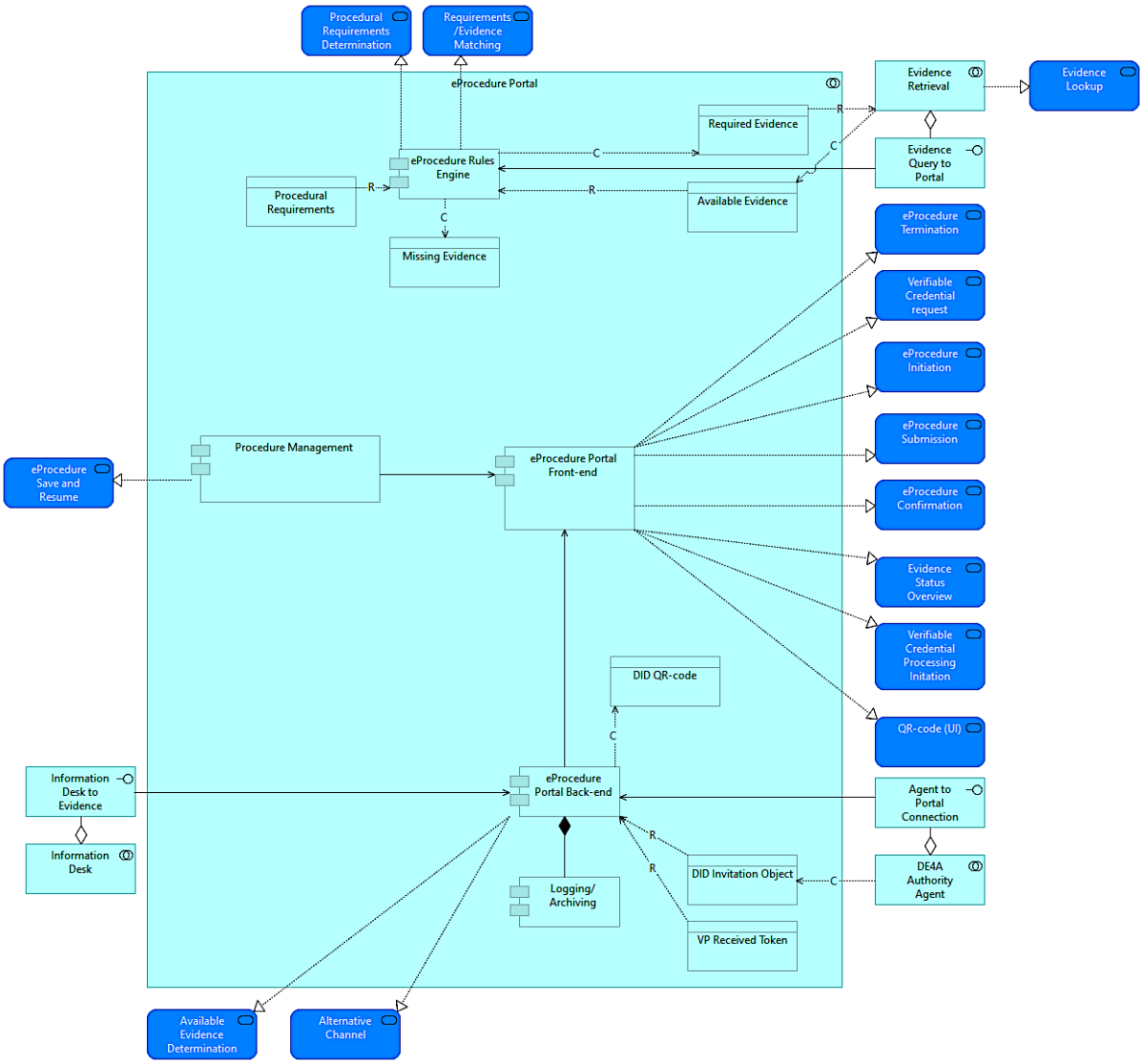


Figure 24 Graphic Representation of the eProcedure Portal Application Collaboration in the VC Pattern

© 870635 DE4A Project Partners

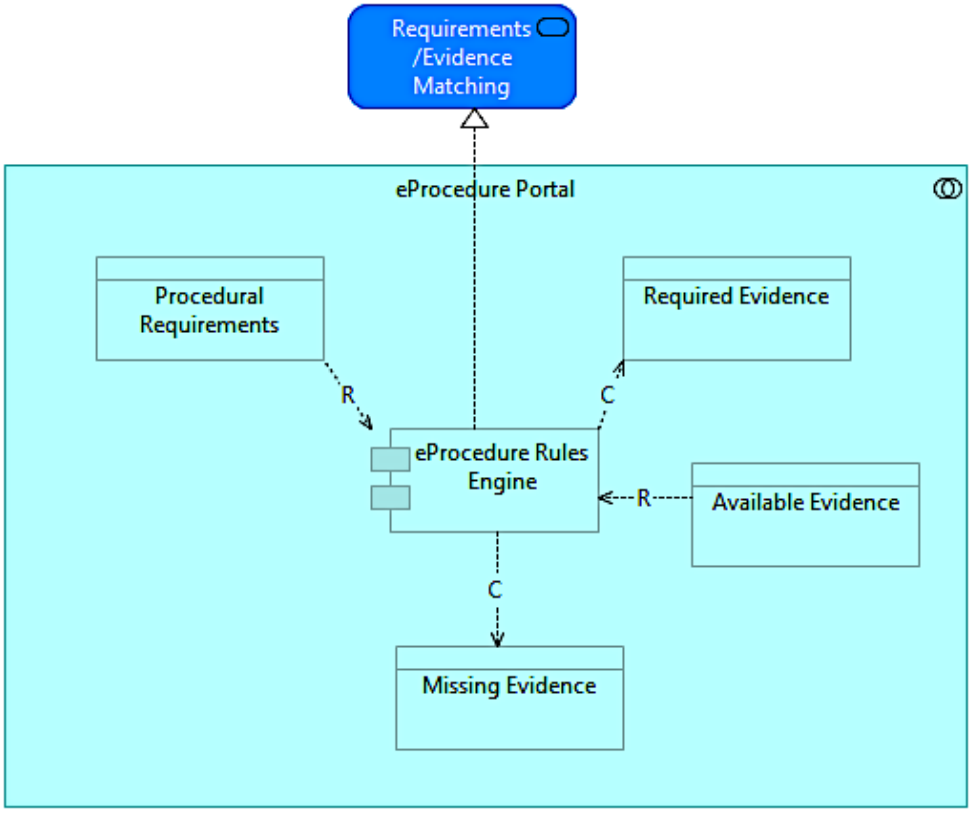


Figure 25 Graphic Representation of the eProcedure Portal Application Collaboration in the Lookup Pattern

Table 22 Application Components of the eProcedure Portal

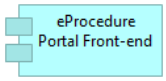
Application Component	Description	Pattern(s)
eProcedure Portal Front-end	Application component managing the entire interaction between the User and the eProcedure Portal, including e.g. UI framework, specific forms integration with the eProcedure Portal Backend. In case of VC also handles the establishment of DID connections between DP and Users.	IM, USI, VC
eProcedure Portal Back-end	Application component consisting of all functionality needed to implement the back-end of an eProcedure Portal and it integrates with all necessary DC systems. For VC it is also where the Authority Agent is deployed.	IM, USI, VC
Procedure Management	Application component managing the procedure, possibly spanning multiple sessions, for the User. Completing a request for a public service might take longer than one session, e.g. waiting for evidence to be exchanged between DP and DC. Furthermore, exception flows must be considered as errors may occur in the flow. Saving the (public) service request to	IM, USI, VC

© 870635 DE4A Project Partners

	continue at a later point in time is therefore important functionality making the User's life easier. The component takes care of persisting the session so it can be resumed at a later point in time avoiding that the User has to start all over again but instead can take it from where they left off.	
eProcedure Rules Engine	Application component taking care of matching procedural requirements with evidence and establishing available and missing evidence.	IM, USI, VC, LKP
Logging/Archiving	Application component managing logging and archiving of data. Also, to support the audit trail.	IM, USI, VC

The following tables present the application services per application component of the eProcedure Portal.

Table 23 Application Services Realized by the eProcedure Portal Front-end

	Description	Pattern
eProcedure Initiation	The User can start a specific eProcedure to receive a public service and provide an initial set of information. The service bundles UI and handling of the data provided by the User.	IM, USI, VC
Explicit Request	The User must make an explicit request for OOP transfer of evidence. This service handles the request.	IM, USI
eProcedure Termination	An eProcedure can be aborted. This service terminates the requested eProcedure (public) service.	IM, USI, VC
eProcedure Submission	After all evidence is available and the requirements of the procedure have been fulfilled, the User can submit the request. This service bundles UI and handling of request submission.	IM, USI, VC
eProcedure Confirmation	The acknowledgment that all required evidence is received by the DC is confirmed to the User by this service.	IM, USI, VC
Verifiable Credential Request	The service that generates a request for the issuance of evidence in the form of VC on the DP side. It includes the information of the required VC schema.	VC
Verifiable Credential Processing Initiation	The User chooses to request the transfer of evidence in the form of Verifiable Credentials (VC). This service prepares and provides the DC's DID data, which will be later used for the preparation of a DID Connection between the User and DC.	VC
Evidence Status Overview	The DC updates the evidence status. This is supported by this service.	VC
QR-code (UI)	A service that provides a QR code to be displayed on the UI for the User to be scanned.	VC

© 870635 DE4A Project Partners

Table 24 Application Services Realized by the eProcedure Portal Back-end

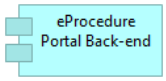
	Description	Pattern
Available Evidence Determination	The DC looks what required evidence is already available for the User on national level (does not have to be requested). This service includes querying national base registers for available evidence.	IM, VC
Alternative Channel	If the User identity cannot be established the User is redirected to an alternative channel. This service supports the handling of this.	IM, USI, VC

Table 25 Application Services Realized by the Procedure Management

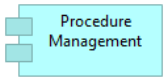
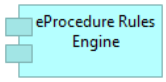
	Description	Pattern
eProcedure Save and Resume	Handling the session management for the User.	IM, USI, VC

Table 26 Application Services Realized by the eProcedure Rules Engine

	Description	Pattern
Procedural Requirements Determination	The DC determines the applicable requirements for a procedure. This service supports this requirements determination and bundles UI and logic to do so.	IM, USI, VC
Requirements /Evidence Matching	The DC matches the requirements with available evidence. This service bundles UI and logic to match the requirements with available evidence in order to establish if there is a delta (missing evidence). The first use of this service takes place after establishing the procedural requirements (i.e., evidence already available in the DC MS), the second use is after evidence collection to establish completeness (i.e. then also including exchanged evidence).	IM, USI, VC, LKP
Available Evidence Determination	Generic. The DC looks what required evidence is already available for the User on national level (does not have to be requested to DPs across borders). This service includes querying national base registers for available evidence.	IM, USI

© 870635 DE4A Project Partners

Table 27 Application Services Realized by the Logging/Archiving

	Description	Pattern
All application services		IM, USI, VC

© 870635 DE4A Project Partners

4.2.Information Desk

https://wiki.de4a.eu/index.php/Information_Desk

The Information Desk application collaboration combines multiple co-operating application components, see [6] D3.5 Semantic Toolkit-Initial Version. It is a logic component that offers information to help DC and DP to perform the OOP exchanges. For IM and USI, it offers information to the DC for helping the User to locate the proper competent authority to provide the required cross-border evidence and for finding the routing information to do the request. The DP consults the information desk [5] to establish that the DC is authorized/allowed to request some evidence type. Besides, the Information Desk can help Users and civil servants to understand cross-border evidence. For VC, the Information Desk serves as a supporting mechanism for the User, which can help them find the relevant VC issuer (i.e. possible DP) in case they are missing any evidence for the procedure.

The information desk [8]functionality is achieved through the collaboration of several application components. The Data service lookup component provides an interface to the eProcedure, where the User can retrieve the list of competent authorities (i.e. DPs) within a given geographic area for the evidence the DC is missing. The list is obtained by reading the entries from the Service registry, which communicates with the Authorization controller to register any changes in the Competent authorities list and the Authority to evidence matrix.

Note The grey coloured elements in the diagrams are out of scope of DE4A.

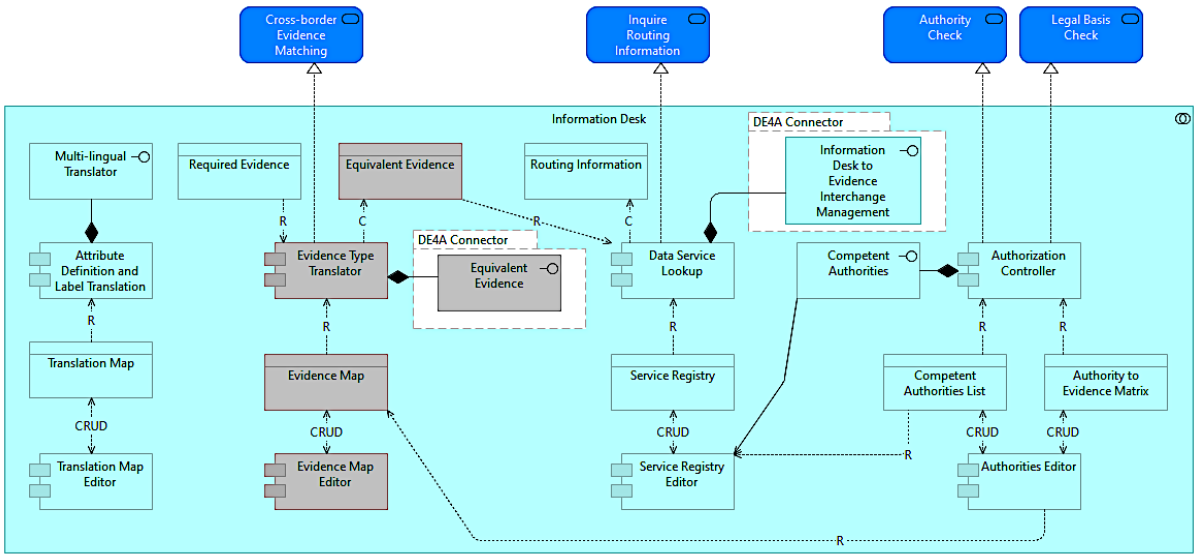


Figure 26 Graphic Representation of the Information Desk Application Collaboration in the IM and USI patterns

[8] https://wiki.de4a.eu/index.php/Information_Desk contains a table explaining the mapping between the terminology used in the reference architecture, by WP3 solution SDG OOTS and in the HLA.

© 870635 DE4A Project Partners

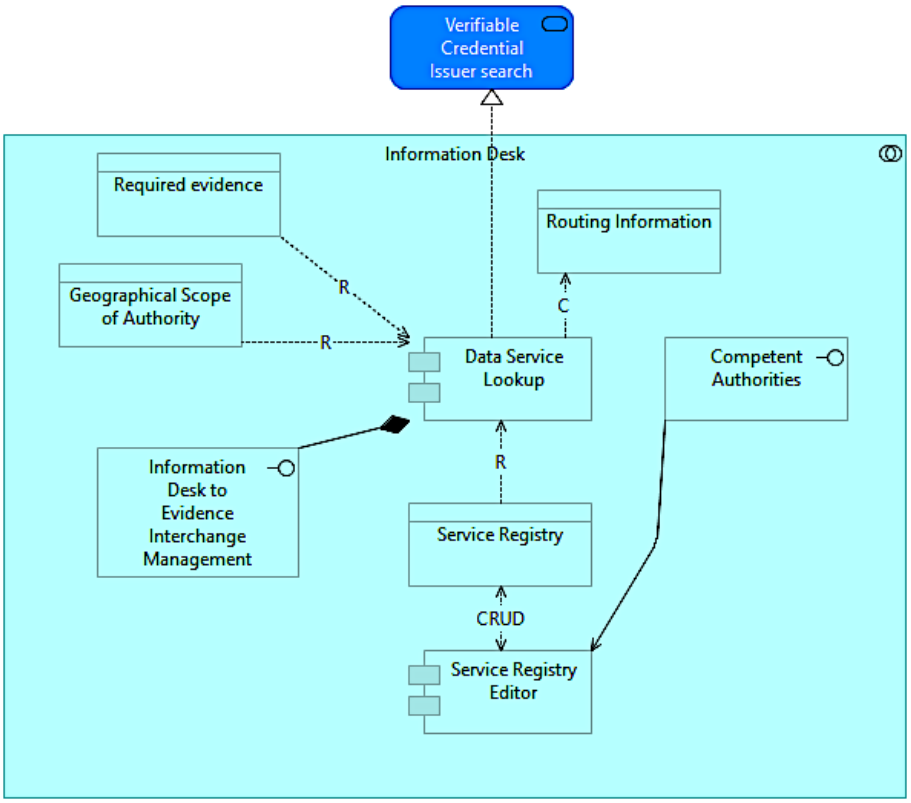


Figure 27 Graphic Representation of the Information Desk Application Collaboration in the VC Pattern

© 870635 DE4A Project Partners

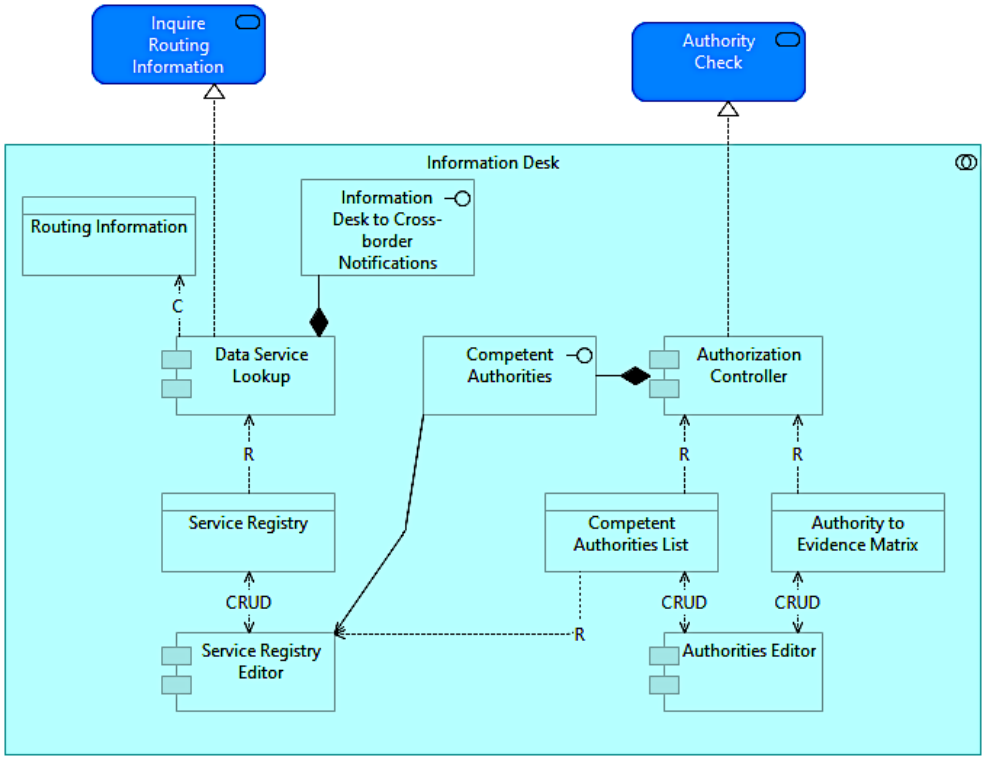


Figure 28 Graphic Representation of the Information Desk Application Collaboration in the S&N Pattern

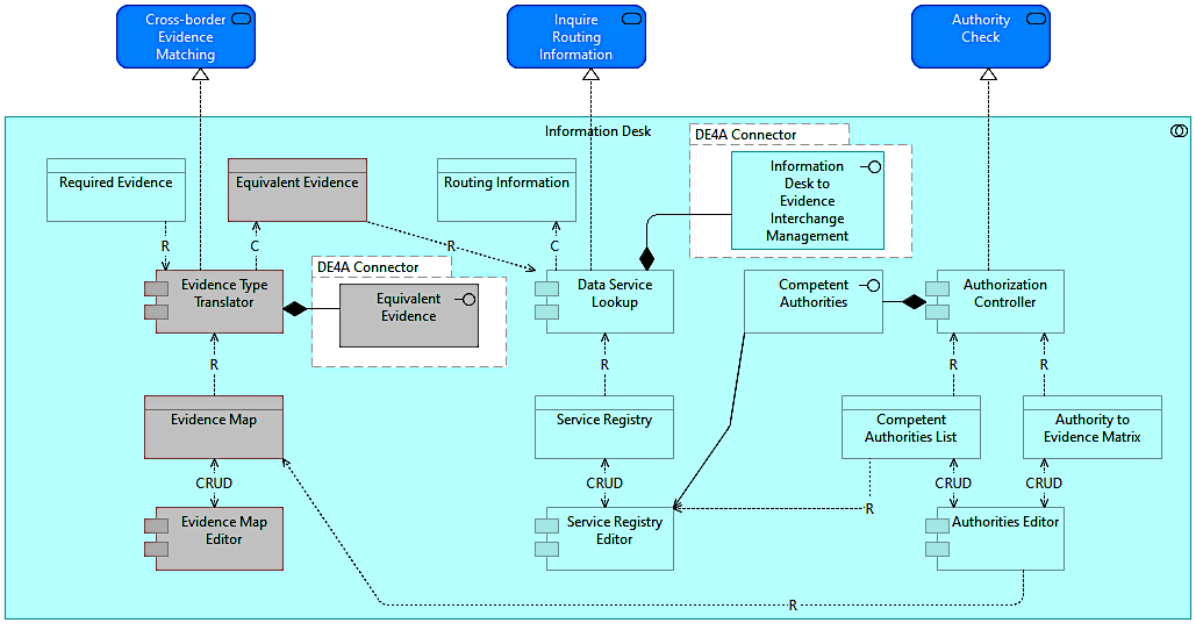


Figure 29 Graphic Representation of the Information Desk Application Collaboration in the Lookup Pattern

© 870635 DE4A Project Partners

Table 28 Application Components of the Information Desk

Application Component	Description	Pattern(s)
Data Service Lookup	Application component for looking up the data service(s) that can be used to request an evidence. In case of VC it returns the URL of the evidence portal.	IM, USI, VC, S&N, LKP
Service Registry Editor	Application component maintaining the service registry.	IM, USI, VC, S&N, LKP
Authorization Controller	Application component to establish which data service, e.g. evidence types can be requested and whether this is allowed under allowed under applicable Union or national law without User request and preview. This applies also to the subscription service.	IM, USI, S&N, LKP
Authorities Editor	Application component maintaining the list of competent authorities and the relationships between those authorities and evidences.	IM, USI, S&N, LKP
Evidence Type Translator	Application component for translating one type of evidence from its domestic form to the corresponding canonical form. Since canonical evidence types are the ground for the DE4A semantic interoperability of cross-border evidence, and semantic and syntactic aspects of domestic evidence types can vary significantly, the evidence type translator should be implemented by each evidence consumer and provider according to their specificities.	IM, USI, LKP
Evidence Map Editor	Application component for helping evidence consumers and providers to map their domestic evidence to the corresponding canonical evidence by semantically and syntactically describing each canonical evidence type for a common understanding.	IM, USI, LKP
Information Desk to Evidence Interchange Management	Interface to Data Service Lookup exposed to Evidence Interchange Management.	IM, USI, VC, LKP
Information Desk to Cross-border Notifications	Interface to Cross-border Notifications providing the routing information for the notifications	S&N
Equivalent Evidence	Interface to Evidence Type Translator for identifying equivalent evidence. Note Won't be piloted in DE4A	IM, USI, LKP

© 870635 DE4A Project Partners

Application Component	Description	Pattern(s)
Competent Authorities	Interface exposing the Authorization Controller for establishing that a Competent Authority is allowed to request a certain Evidence Type.	IM, USI, LKP
Attribute Definition and Label Translation	Application component taking care of the translation of attribute definitions and labels. This would allow to provide canonical evidences as in agreed and accepted translations, i.e. during the preview. This service could also be integrated in public service back-office systems to support the work of public servants (beyond DE4A pilot scope). This service, based on agreed semantic equivalence, is meant to resolve the legal barrier 'L4: Requirements for translation of data/evidences' identified in D1.7	IM, USI
Multi-lingual Translator	Interface to the Attribute Definition and Label Translation for looking up multi-lingual translations of attribute definitions and labels.	IM, USI
Translation Map Editor	Application component maintaining the mapping used for translations.	IM, USI

© 870635 DE4A Project Partners

The following tables present the application services per application component of the Information Desk.

Table 29 Application Services Realized by the Data Service Lookup

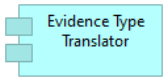
	Description	Pattern
Inquire Routing Information	The DC looks up where to send the request (e.g. for evidence). This service acts as an API to lookup the routing information. Depending on the chosen solution, this service can be performed in several steps: Identification of the addressed DP competent authority (i.e. a unique identifier), identification of the specific data service provided by that competent authority and lookup of the technical address of that data service. Solution components can realize instances of the Inquire Routing Information service that include all or any of these steps. Especially the first step, identifying the right competent authority, is meant to resolve the barrier 'O9: Different systems for distribution of regulatory responsibility in MSs can complicate finding right authority' identified in D1.7.	IM, USI, S&N, LKP
Verifiable Credential Issuer search	The service, based on the information from the information desk, performs a list of all possible issuers of evidence (VC) that may be later used by the User to satisfy procedural requirements. The list consists of the name of the institution, MS, region, and a link for its related evidence portal.	VC

Table 30 Application Services Realized by the Authorization Controller

	Description	Pattern
Authority Check	The DP establishes that the DC can request the evidence or subscription. This service handles the lookup of authorization. At the moment we consider the possibility for this check to be specific to the evidence type, i.e. is authority A allowed to request evidence type X, or event set.	IM, S&N, LKP
Legal basis check	The DC establishes for both the request and the preview whether this is allowed under applicable Union or national law in which case no User request or approval is needed.	IM, USI

© 870635 DE4A Project Partners

Table 31 Application Services of the Evidence Type Translator

	Description	Pattern
Cross-border Evidence Matching	The DC must match required evidence cross-border to equivalent evidences from another MS. This service bundles UI and logic to support this process. This service is meant to resolve the barrier 'S1: Diverse and non-harmonized types of criteria and evidences in different Member States can make it difficult to find and request relevant evidences' identified in D1.7. In the DE4A pilots, semantic interoperability is managed by the definition of canonical evidences, which means that this service is not in the pilot scope	IM, USI, LKP

© 870635 DE4A Project Partners

4.3.Evidence Interchange Management

https://wiki.de4a.eu/index.php/Evidence_Interchange_Management

The Evidence Interchange Management application collaboration aggregates two high-level application components providing all functionality to manage the interchange of evidence. The back-end component supports keeping track of the requests and status of evidence(s). It also supports the erasure of evidence at DC side (only applicable to Intermediation) if the User elects to do so. The front-end component provides an evidence status overview for the User as well as the important preview functionality with which the User can preview the evidence. In case of the Intermediation pattern the DC prepares the preview and the User can preview it using some UI. Evidence Interchange Management application collaboration interfaces with Data logistics in order to exchange the evidence.

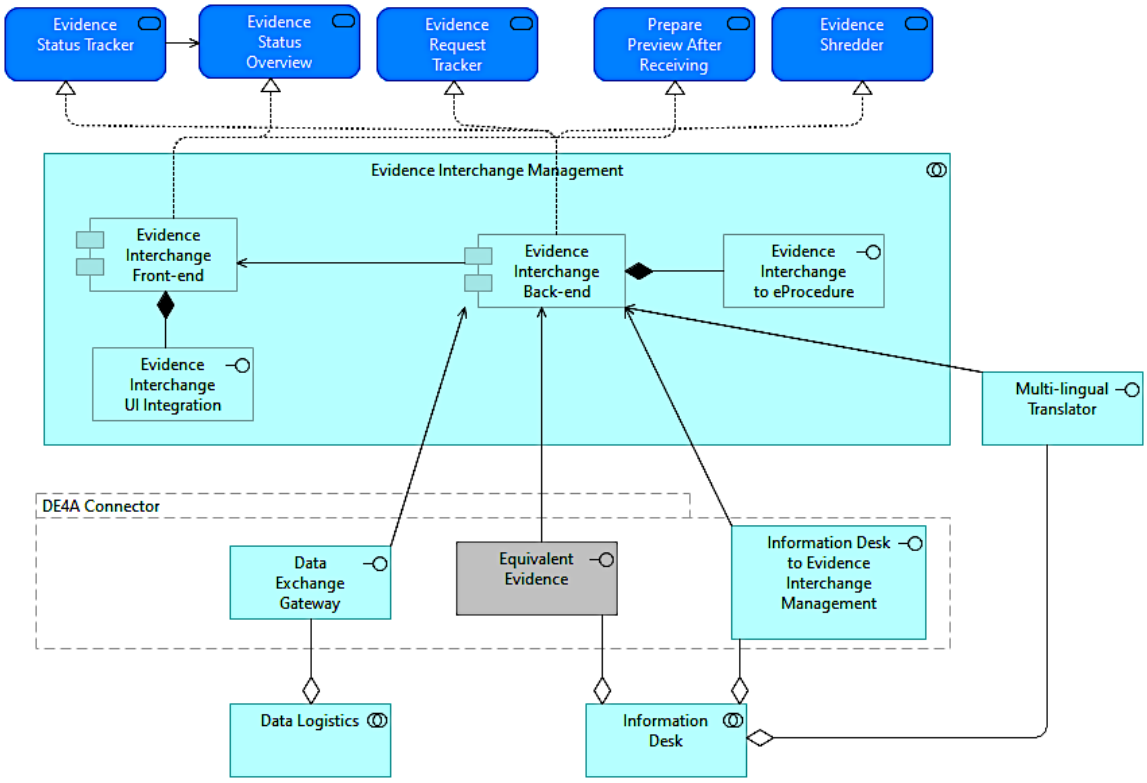


Figure 30 Graphic Representation of the Evidence Interchange Management Application Collaboration in the IM Pattern

© 870635 DE4A Project Partners

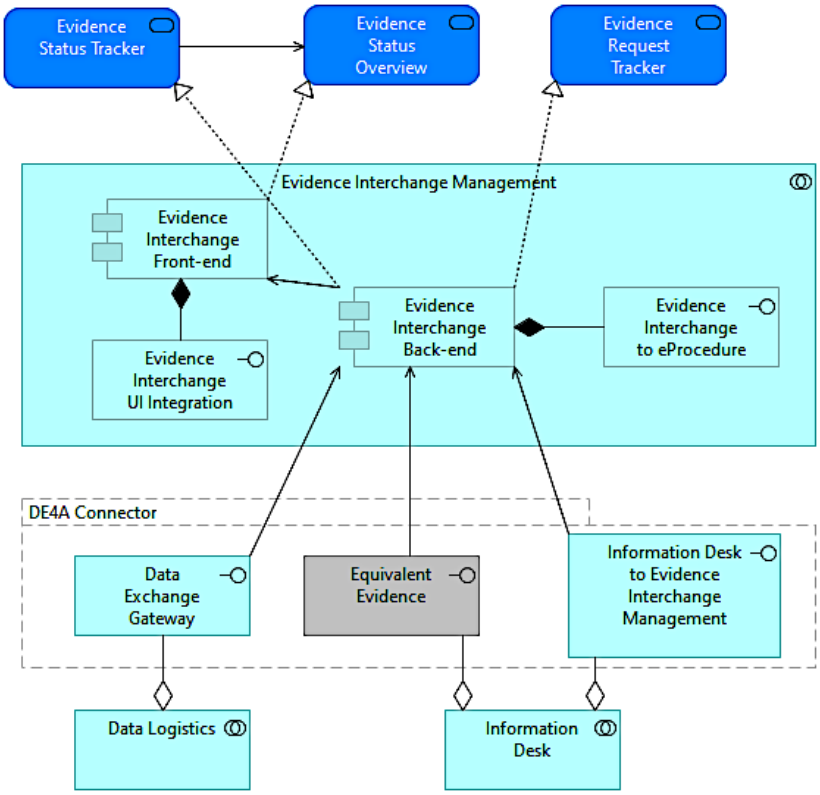


Figure 31 Graphic Representation of the Evidence Interchange Management Application Collaboration in the USI Pattern

© 870635 DE4A Project Partners

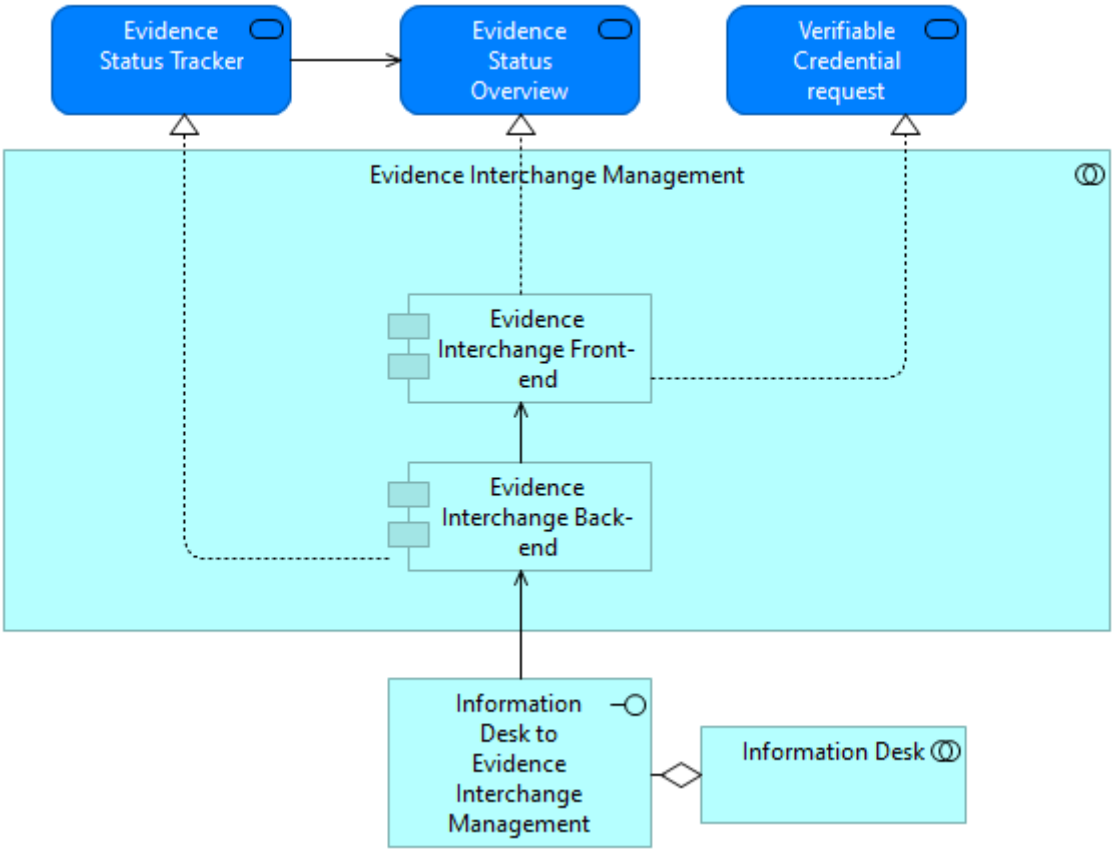


Figure 32 Graphic Representation of the Evidence Interchange Management Application Collaboration in the VC Pattern

© 870635 DE4A Project Partners

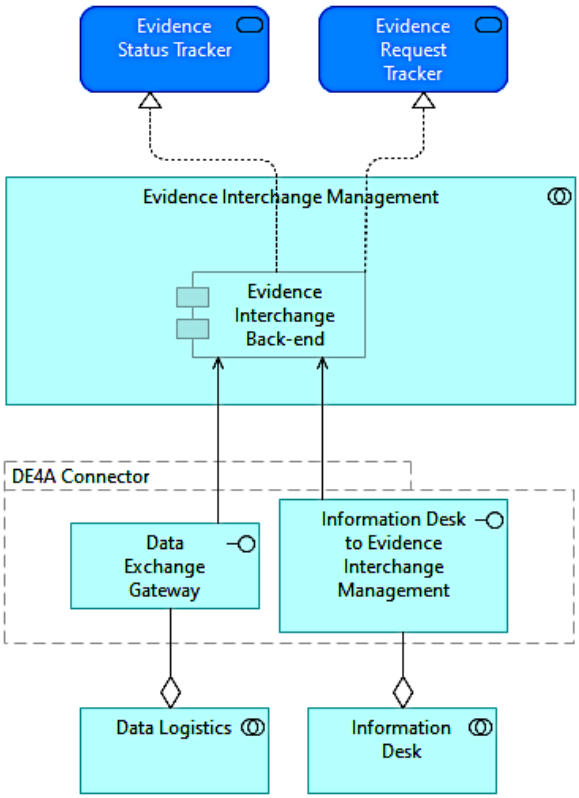


Figure 33 Graphic Representation of the Evidence Interchange Management Application Collaboration in the Lookup Pattern

Table 32 Application Components of the Evidence Interchange Management

Application Component	Description	Pattern(s)
Evidence Interchange Front-end	Application component bundling UI and logic to handle the status overview and preview and approval of requested evidences.	IM, USI, VC
Evidence Interchange Back-end	Application component managing the tracking of evidence requests and supporting the removal of evidences. This can be especially important for the multiple evidence cases.	IM, USI, VC, LKP
Evidence Interchange UI Integration	The Evidence Interchange Front-end Component exposes an interface in order for other components to integrate it in their UI.	IM, USI
Evidence Interchange to eProcedure	The Evidence Interchange Back-end Component exposes an interface in order for the eProcedure portal to make use of it.	IM, USI

© 870635 DE4A Project Partners

The following tables present the application services per application component of the Evidence Interchange Management.

Table 33 Application Services of the Evidence Interchange Front-end

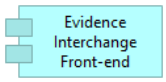
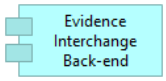
	Description	Pattern
Evidence Status Overview	The DC updates the evidence status, which is supported by this service.	IM, USI, VC
Prepare Preview After Receiving	The User must be able to preview and approve the evidence. This service bundles UI and approval handling before the DC can use the evidence.	IM
Verifiable Credential Request	The service that generates a request for the issuance of evidence in the form of VC on the DP side. It includes the information of the required VC schema.	VC

Table 34 Application Services of the Evidence Interchange Back-end

	Description	Pattern
Evidence status tracker	The DC keeps track of evidence requested versus evidence received. This service bundles the logic to support this.	IM, USI, VC, LKP
Evidence request tracker	The DC establishes the technical availability of evidence. Was some piece of evidence received, did a timeout occur (SLA) or was an error code returned by the DP? This service keeps track of requested evidence.	IM, USI, LKP
Evidence Shredder	For various reasons (request by User or established time limit for the data) evidence must be deleted. This service bundles UI and logic to support this.	IM

© 870635 DE4A Project Partners

4.4.Trust Architecture

https://wiki.de4a.eu/index.php/Trust_Architecture

The Trust Architecture application collaboration aggregates multiple co-operating application components realizing all needed services to implement the DE4A trust models. The identity management application component is used to initiate the authentication process and it implements functionality so the User can authenticate themself. Both DC and DP use the component to perform the identity matching based on attributes. The Trust Service provisioning component is also used by both DC and DP to provide functionality to handle the digital signing of messages and security at the level of transport layer (TLS). The data encryption/decryption component is again used by both DC and DP to support the encryption and decryption of messages. The Trust Architecture also provides functionality so that natural persons can represent other natural and legal persons.

For VC the situation is different. The interaction between the User identification components remains the same. The difference lies in how signing and verification is done. For VC this is performed by the Authority Agents at the DE and DO respectively and they are not signed with an eSignature or eSeal but with the corresponding key associated to the DID of the VC issuing authority.

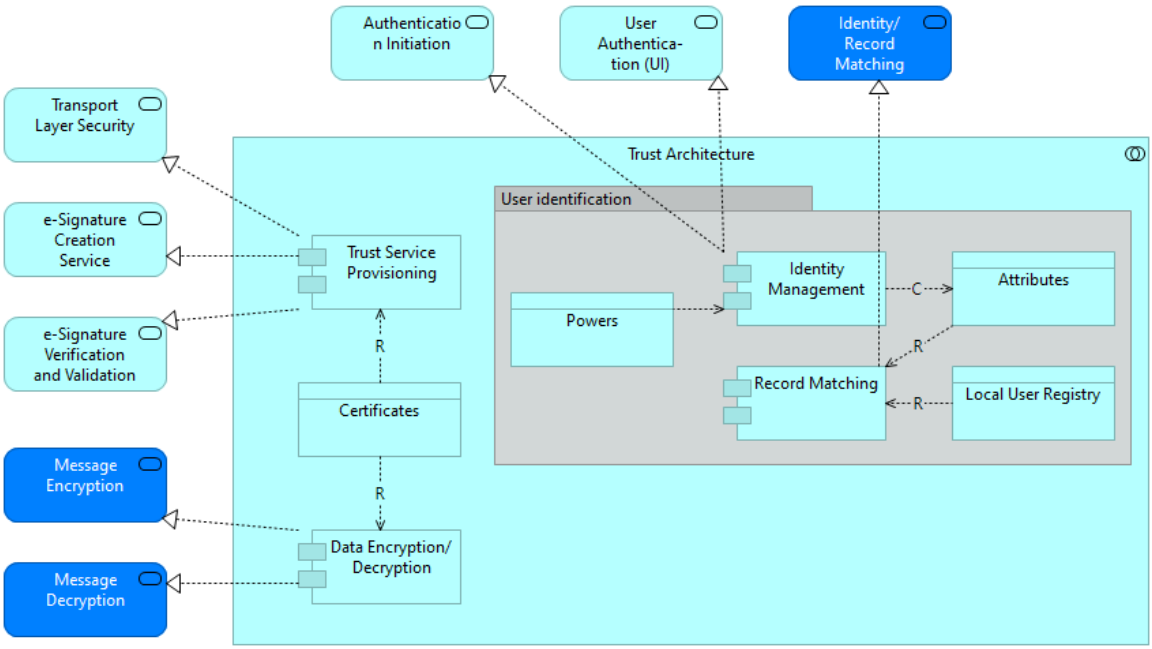


Figure 34 Graphic Representation of the Trust Architecture Application Collaboration in the IM Pattern

© 870635 DE4A Project Partners

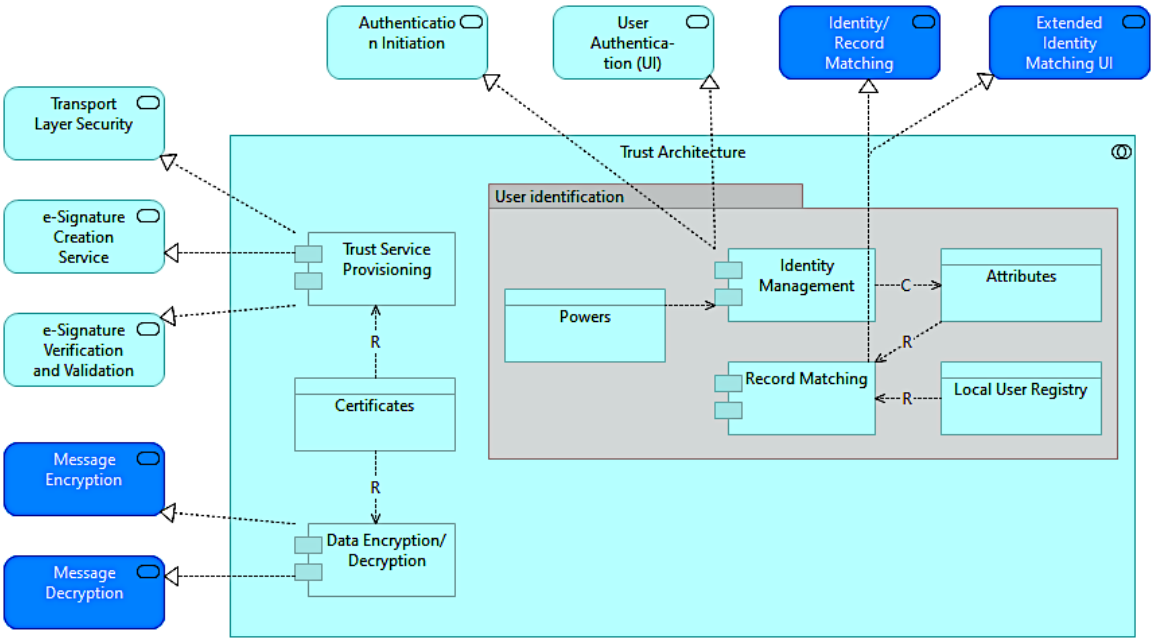


Figure 35 Graphic Representation of the Trust Architecture Application Collaboration in the USI Pattern

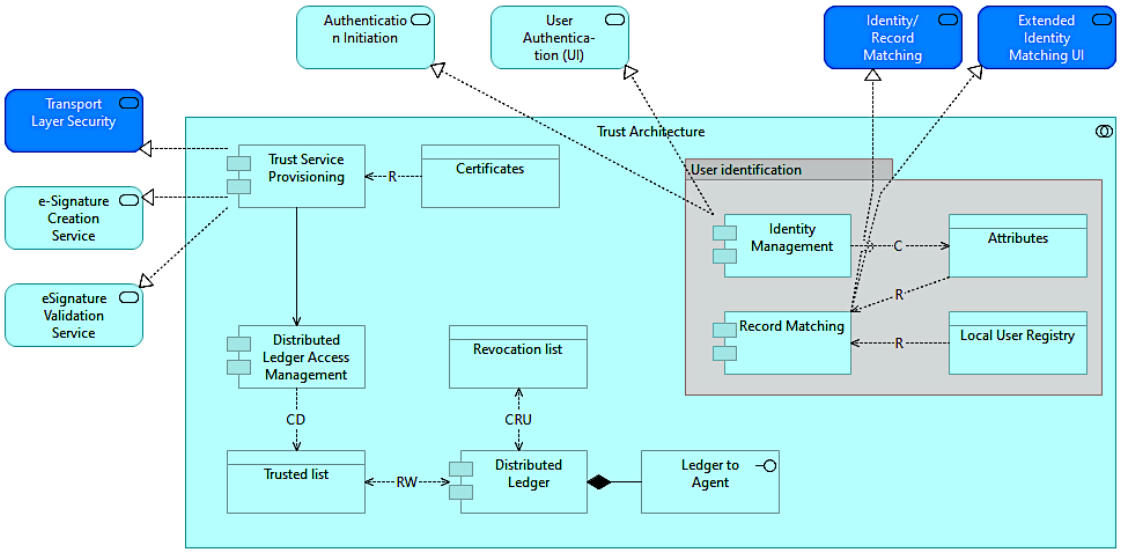


Figure 36 Graphic Representation of the Trust Architecture Application Collaboration in the VC Pattern[9]

[9] In the VC pattern the signing related functions are implemented with the Authority Agent (at Solution Architecture level).

© 870635 DE4A Project Partners

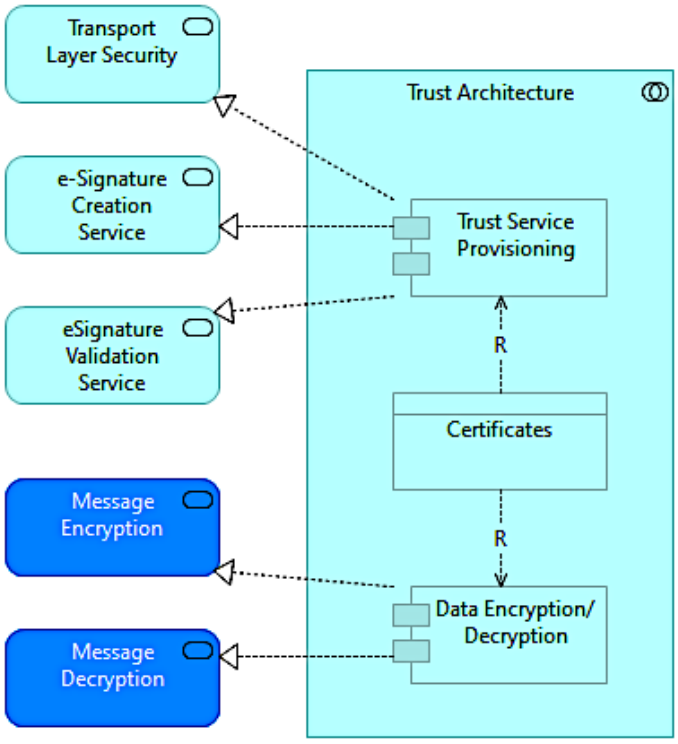


Figure 37 Graphic Representation of the Trust Architecture Application Collaboration in the S&N and Lookup patterns

© 870635 DE4A Project Partners

Table 35 Application Components of the Trust Architecture

Application Component	Description	Pattern(s)
Trust Service Provisioning	Implements the functionalities encapsulating the trust services functionalities. A 'trust service' means an electronic service which consists of these functionalities: i) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or ii) the creation, verification, and validation of certificates for website authentication; or iii) the preservation of electronic signatures, seals or certificates related to those services. Not all trust services are needed in the context of DE4A.	IM, USI, VC, S&N, LKP
Identity Management	Implements the functionality of User authentication. 'Electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. 'Authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.	IM, USI, VC,
Record Matching	Application component that provides identity matching based on attributes. Provided attributes are matched against attributes in some local registry.	IM, USI, VC
Data Encryption/Decryption	Application component providing encryption and decryption functionality (symmetrical, asymmetrical or a combination thereof).	IM, USI, S&N, LKP
Distributed Ledger[10]	Application component that handles connections and operations related to the distributed ledger.	VC
Distributed Ledger Access Management[11]	Application component that manages the access management related to Write/Read access into distributed ledger storage.	VC
Ledger to Agent	Interface that will connect to the Distributed Ledger (i.e., EBSI) in order to use e.g., the DID registry, Trusted Issuer Registry (TIR), Revocation list, etc.	VC

[10] The Authority Agent has a subcomponent managing the EBSI APIs (at Solution Architecture level)
[11] Such access authorization is managed by EBSI directly

© 870635 DE4A Project Partners

The following tables present the application services per application component of the Trust Architecture.

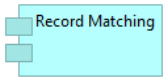
Table 36 Application Services Realized by the Trust Service Provisioning

	Description	Pattern
e-Signature Creation Service	Shares the functionality of signing data in electronic form, e.g. by using PKI based certificates. In EIRA sense it means signed by a natural person, no legal person, and an 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.	IM, USI, VC, S&N, LKP
e-Signature Verification and Validation Service	Both DC and DP verify/validate eSignatures supported by this service. It makes use of trust lists, like LoTL/gTSL/others. Shares the functionality of the verification of documents that are signed electronically. An 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. 'validation' means the process of verifying and confirming that an electronic signature is valid.	IM, USI, VC, S&N, LKP
Transport Layer Security	Application service which provides communications security over a computer network	IM, USI, VC, S&N, LKP

Table 37 Application Services Realized by the Identity Management

	Description	Pattern
Authentication initiation	The DC asks the User to authenticate themself. This service initiates the authentication process.	IM, USI, VC
User Authentication (UI)	User Interface for entering credentials, e.g. user/password, to be used for authentication purposes.	IM, USI, VC

Table 38 Application Services Realized by the Record Matching

	Description	Pattern
Identity/Record Matching	Some identity matching is foreseen on both DC and DP side based on eIDAS attributes (mandatory and possibly optional attributes) as well as (maybe) additional attributes to establish the identity of	IM, USI, VC

© 870635 DE4A Project Partners

	Description	Pattern
	the User in some MS local registry. This service deals with the record matching (automatic and/or manually).	
Extended Identity Matching UI	The User is presented with a UI in order to provide additional information in order to do the identity matching. This service handles this.	USI, VC

Table 39 Application Services Realized by the Data Encryption / Decryption

	Description	Pattern
Message Encryption	Both DR and DT AS4 Gateways encrypt messages to allow for secure cross-border exchanges of data. This service handles encryption of data (symmetrical, asymmetrical or a combination).	IM, USI, S&N, LKP
Message decryption	Both DR and DT decrypt messages to allow for secure cross-border exchanges of data. This service handles decryption of data (symmetrical, asymmetrical or a combination).	IM, USI, S&N, LKP

© 870635 DE4A Project Partners

4.5.Data Logistics

https://wiki.de4a.eu/index.php/Data_Logistics

The Data Logistics application collaboration consists of one high-level component realizing 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.

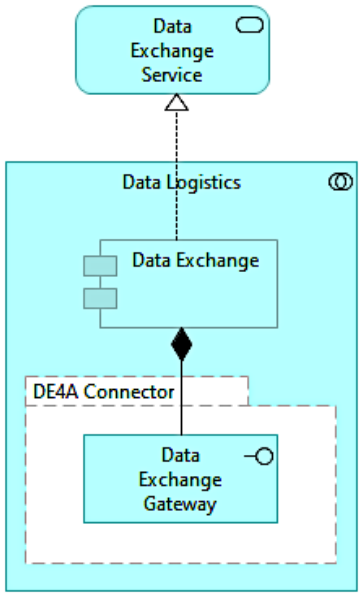


Figure 38 Graphic Representation of the Data Logistics Application Collaboration in the IM, USI, S&N and Lookup patterns

Table 40 Application Components of the Data Logistics

Application Component	Description	Pattern(s)
Data Exchange	Shares the functionality that enables the secure exchange of messages, records, forms, and other kinds of data between different ICT systems. This includes data routing, except endpoint discovery.	IM, USI, S&N, LKP
Data Exchange Gateway	The Data Exchange Component exposes an interface in order for other components to make use of it.	IM, USI, S&N, LKP

© 870635 DE4A Project Partners

The following table presents the application services per application component of the Data Logistics.

Table 41 Application Services Realized by the Data Exchange

Data Exchange	Description	Pattern
Data Exchange Service	Shares the functionality that enables the secure exchange of messages, records, forms, and other kinds of data between different ICT systems. This includes data routing, except endpoint discovery.	IM, USI, S&N, LKP

4.6.Evidence Portal

https://wiki.de4a.eu/index.php/Evidence_Portal

The Evidence portal application collaboration constitutes back-end and front-end functionality and interfaces with Evidence retrieval and Data logistics. The front-end supports am Evidence Exception UI to inform the User about errors or delays, functionality to preview the evidence and a UI for handling the QR-code. The backend takes care of the error handling, the transformation of domestic to canonical evidence, the generation of a persistent URL for user redirection, preparing the preview and Request validation and extraction.

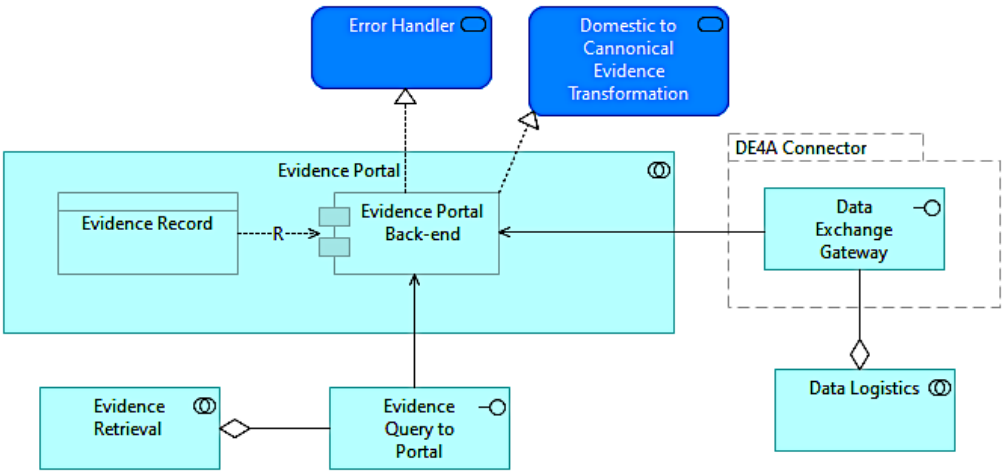


Figure 39 Graphic Representation of the Evidence Portal Application Collaboration in the IM and Lookup patterns

© 870635 DE4A Project Partners

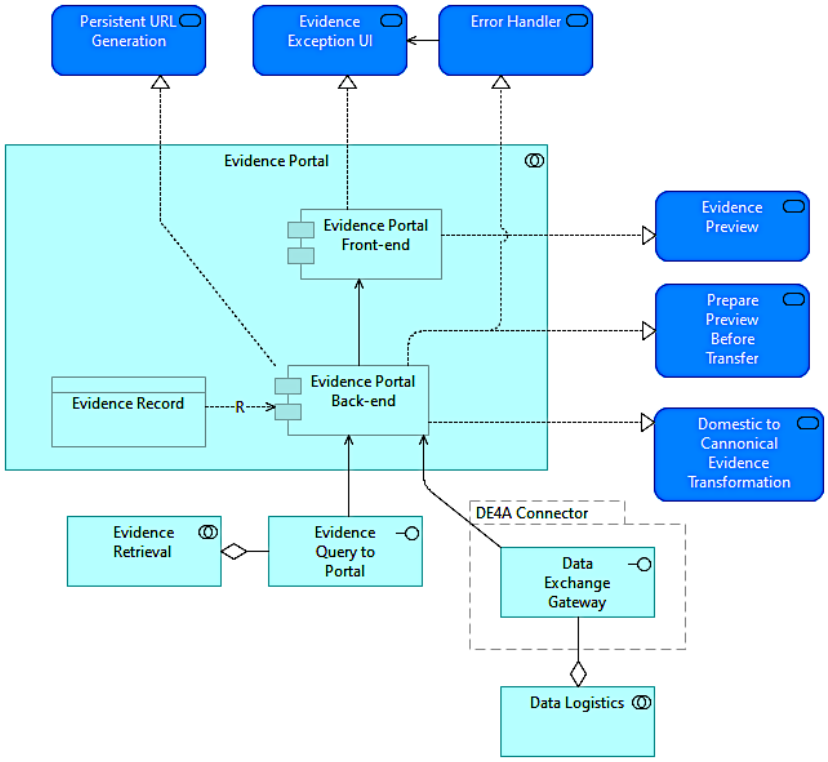


Figure 40 Graphic Representation of the Evidence Portal Application Collaboration in the USI Pattern

© 870635 DE4A Project Partners

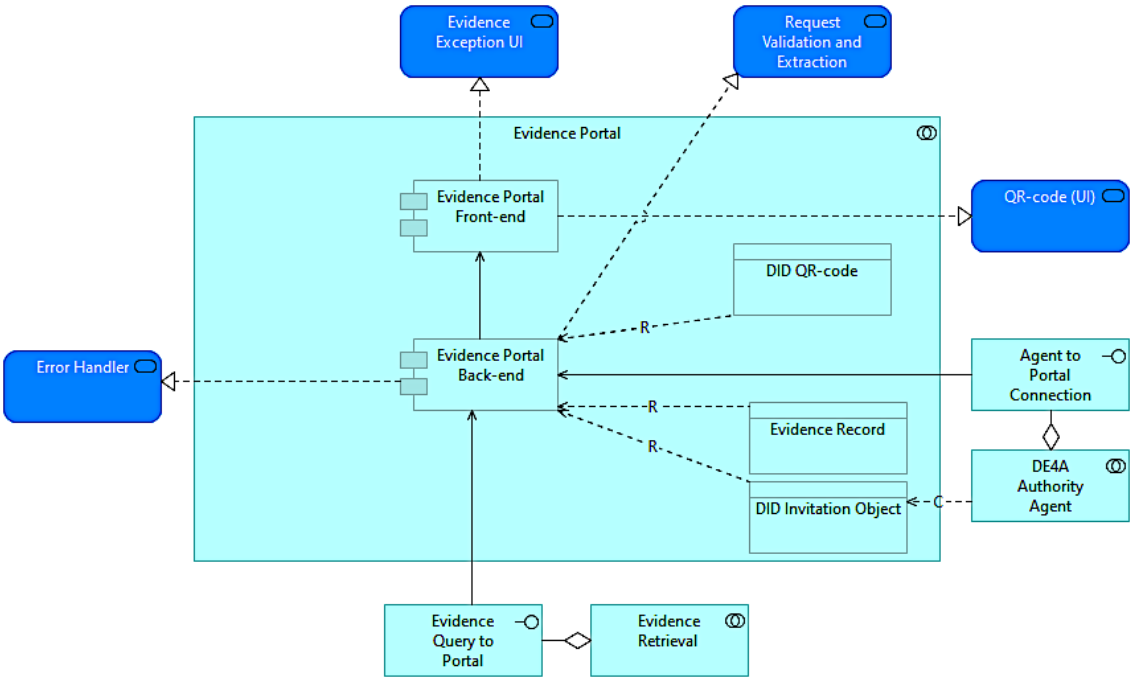


Figure 41 Graphic Representation of the Evidence Portal Application Collaboration in the VC Pattern

Table 42 Application Components of the Evidence Portal

Application Component	Description	Pattern(s)
Evidence Portal Front-end	This application component implements UI functionality to handle exceptions connected to evidences as well as the preview of evidences. For VC this also includes the enabler of DID connection establishment with the User.	IM, USI, VC
Evidence Portal Back-end	Shares the functionality that enables the secure exchange of messages, records, forms, and other kinds of data between different ICT systems. This includes the DID connection handling and evidence related events (VC). Generation of persistent URL, which will be communicated to the DC enabling the User to return to “the right place” at a later point in time (USI). Error handling connected to evidences and rendering the evidence so it can be previewed by the User. The back-end also takes care of the transformation of domestic to canonical evidence.	IM, USI, VC, LKP

© 870635 DE4A Project Partners

The following tables present the application services per application component of the Evidence Portal.

Table 43 Application Services Realized by the Evidence Portal Front-end

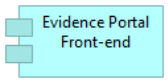
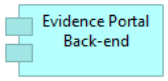
	Description	Pattern
Evidence Exception UI	Through this service the User is informed about errors or delays with respect to the requested evidence and the User is told to return to the eProcedure portal of the DC.	USI, VC
Evidence Preview	The User must be able to preview and approve the evidence. This service bundles UI and approval handling before the DC can use the evidence.	USI
QR-code (UI)	A service that provides a QR code to be displayed on the UI for the User to be scanned.	VC

Table 44 Application Services Realized by the Evidence Portal Back-end

	Description	Pattern
Domestic to Canonical Evidence Transformation	This application service is used for transformation of evidences. It takes as input a domestic evidence and transforms it to canonical form. Domestic evidence types can vary significantly, the transformation should consequently be implemented by each evidence consumer and provider according to their specificities.	IM, USI, LKP
Error Handler	This application service is used for handling error situations with respect to: • non-availability of OOP • non-availability or delay of evidence	IM, USI, VC, LKP
Prepare Preview Before Transfer	This application service prepares the preview so it can be previewed at DP side (before the evidence is transferred to DC).	USI
Persistent URL Generation	A persistent URL is generated for the purpose of navigation. Based on this URL the DC can forward/redirect the User to the portal of the DP for the required evidence.	USI
Request Validation and Extraction	Service to extract from the request of the User whether it confirms to a schema that can be provided by the DB and whether the subject of the request is corresponding to the requesting User.	VC

© 870635 DE4A Project Partners

4.7.Evidence Retrieval

https://wiki.de4a.eu/index.php/Evidence_Retrieval

The Evidence retrieval application collaboration aggregates multiple components to implement the looking up of evidence from an evidence registry by both DP and DC (from eProcedure portal). The evidence editor is MS specific and supports the lifecycle of evidences. It offers an interface so a portal can retrieve an evidence.

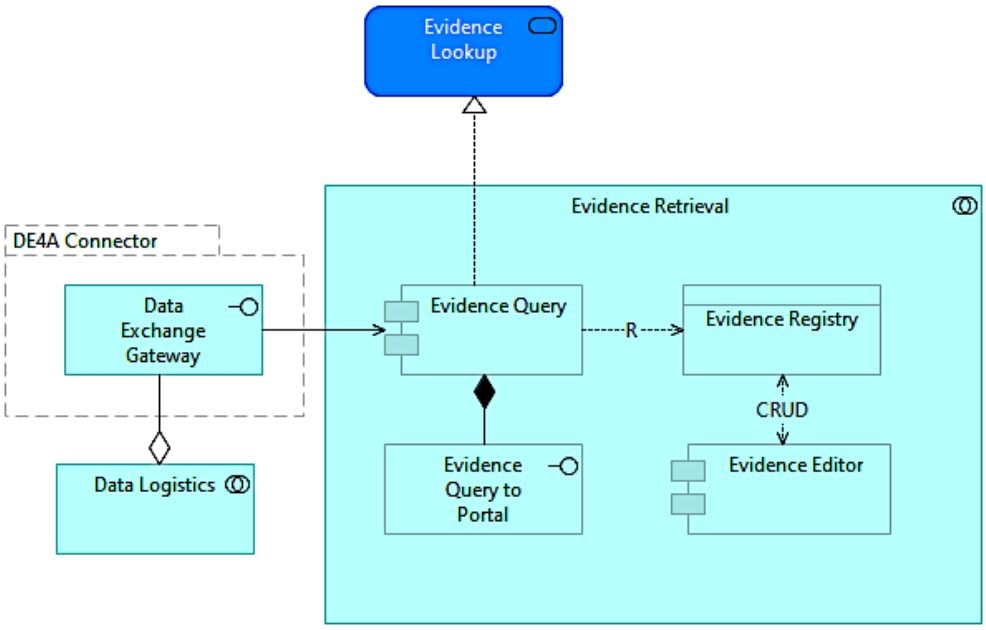


Figure 42 Graphic Representation of the Evidence Retrieval Application Collaboration in the IM, USI and Lookup patterns

© 870635 DE4A Project Partners

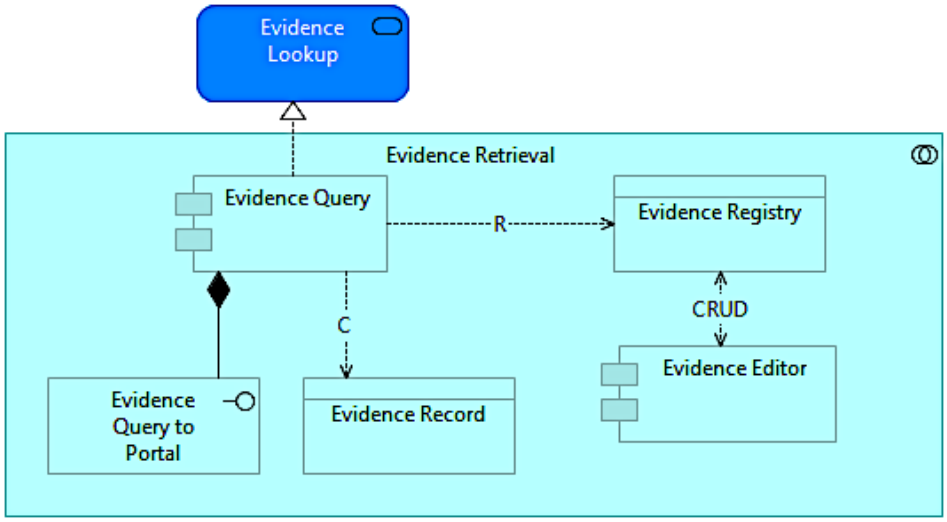


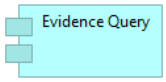
Figure 43 Graphic Representation of the Evidence Retrieval Application Collaboration in the VC Pattern

Table 45 Application Components of the Evidence Retrieval

Application Component	Description	Pattern(s)
Evidence Query	Application component providing functionality to query an evidence registry for retrieving evidence and providing an interface to expose this functionality to the outside.	IM, USI, VC, LKP
Evidence Editor	Application component to manage creation/insertion, modification and deletion of evidences in an evidence registry.	IM, USI, VC, LKP
Evidence Query to DC Portal	The Evidence Query Application Component exposes an interface in order to make use of it.	IM, USI, VC, LKP

The following table presents the application services per application component of the Evidence Retrieval.

Table 46 Application Services Realized by the Evidence Query

	Description	Pattern
Evidence Lookup	The DP has to extract the evidence from some registry. This service bundles the functionality to look up and retrieve the evidence from a DP or central MS registry	IM, USI, VC, LKP

© 870635 DE4A Project Partners

4.8.Authority Agent

https://wiki.de4a.eu/index.php/Authority_Agent

The Authority agent is responsible for managing the connections between User and authorities (i.e. DP, DC) and activities related to Verifiable Credentials/Presentations (i.e. proof requests, validation, issuing). To do so, it includes collaboration between several application components. The Verifiable Credential Generator reads the original evidence record on the DP side to generate and digitally sign the VC. This component is used by the SSI cloud agent, which is also responsible for managing the DID invitations to the User and providing interfaces for the communication between the Agent (cloud or edge) and the Evidence portal or the Ledger necessary to issue or verify VC/VP.

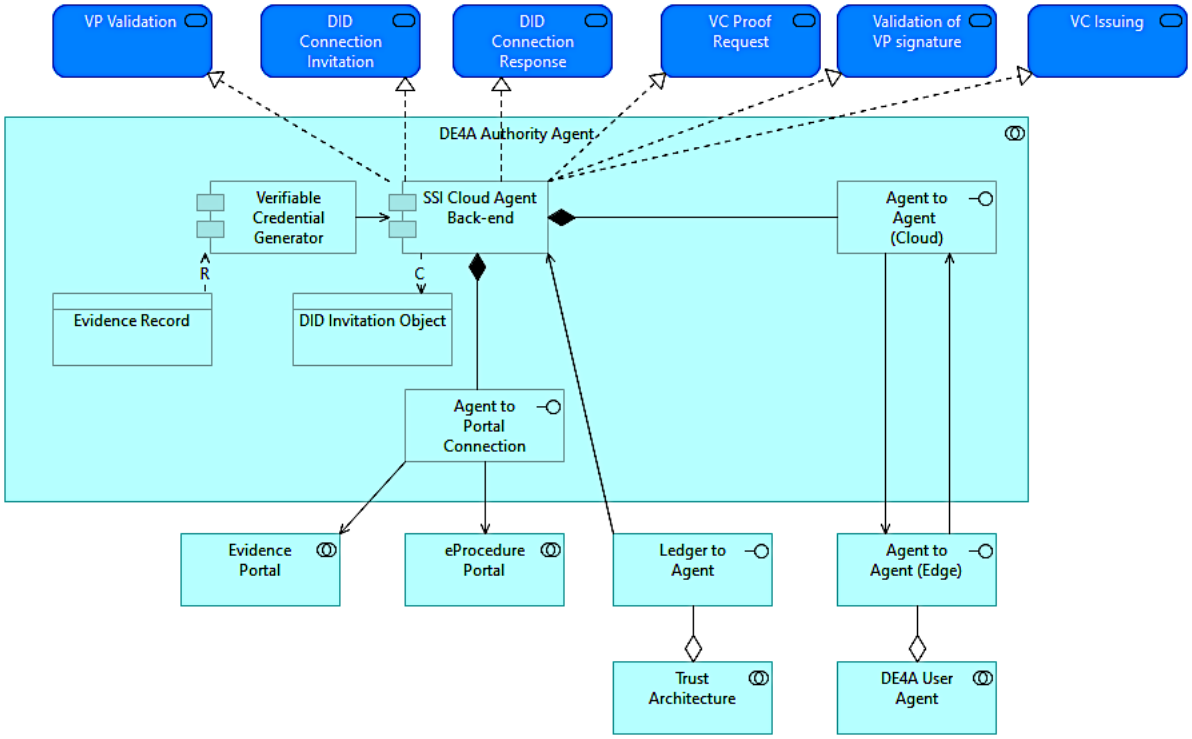


Figure 44 Graphic Representation of the Authority Agent Application Collaboration in the VC Pattern

Table 47 Application Components of the Authority Agent

Application Component	Description	Pattern(s)
Verifiable Credential Generator	Application component managing the generation, i.e., issuance of VC by the DP as issuer to the User as the holder of the newly generated (i.e., re-issued) evidence (VC). The component also includes the processes of evidence record retrieval, its translation into the form of VC, and the digital signing by the issuer of the evidence.	VC

© 870635 DE4A Project Partners

Application Component	Description	Pattern(s)
SSI Cloud Agent Back-end	Application component managing the DID connections and handling the VC/VP related events.	VC
Agent to Portal Connection	This interface provides two main functions to Evidence Portals and the eProcedure portal: 1. The creation of a DID connection requires a DID Invitation Object from the Agent to be displayed as a QR Code in the Portals (both Evidence and eProcedure) 2. For the Evidence Portal, this interface is able to receive an Evidence Record that is then transformed into a VC by the Verifiable Credential Generator of the Authority Agent. 3. For the eProcedure Portal, e.g. for VP Validation.	VC
Agent to Agent (Cloud)	Interface between Agents that provides the functionalities of a DID connection, e.g.: exchange of DID documents, Verifiable Credentials and Verifiable Presentations	VC

The following table presents the application services per application component of the Authority Agent.

Table 48 Application Services Realized by the SSI Cloud Agent Back-end

Description	Pattern(s)
DID Connection Invitation	Generic. The service generates and provides a JSON invitation (DID document) with which the different stakeholders (e.g., Users) can start the process of DID connection establishment.	VC
DID Connection Response	Generic. The service validates and checks the User's response to the generated DID connection invitation. As a result of this action, information on the DID connection establishment is provided.	VC
VP Validation	The service performs an initial screening and validation of the VP submitted by the User with regard to its schema structure, eIDAS identity matching and the validity of the digital signature. The result of this action is the information on the validity of the VP submitted for the procedure.	VC
VP Request	The service, dependant on procedural requirements, generates a request for evidence in the form of verifiable presentations (VPs). It requires evidences to be aligned with a specific VP format.	VC
VC Issuing	The service provides functionalities related to (re)issuing of requested evidence in the form of a VC. The VC is issued through an established DID connection and accepted VC.	VC

© 870635 DE4A Project Partners

4.9.User Agent

https://wiki.de4a.eu/index.php/User_Agent

The User Agent includes the collaboration between the SSI edge agent front-end and back-end components on the User side in order to manage incoming DID invitations, checking VCs issued to the User (acceptance or negation) or create VPs. It also provides an interface to communicate with the cloud Authority Agent. The User can manage his received VCs inside his Digital Wallet (i.e. store them, select VCs (VPs) which are to be sent to DC, etc.) by communicating with the Authority Agent.

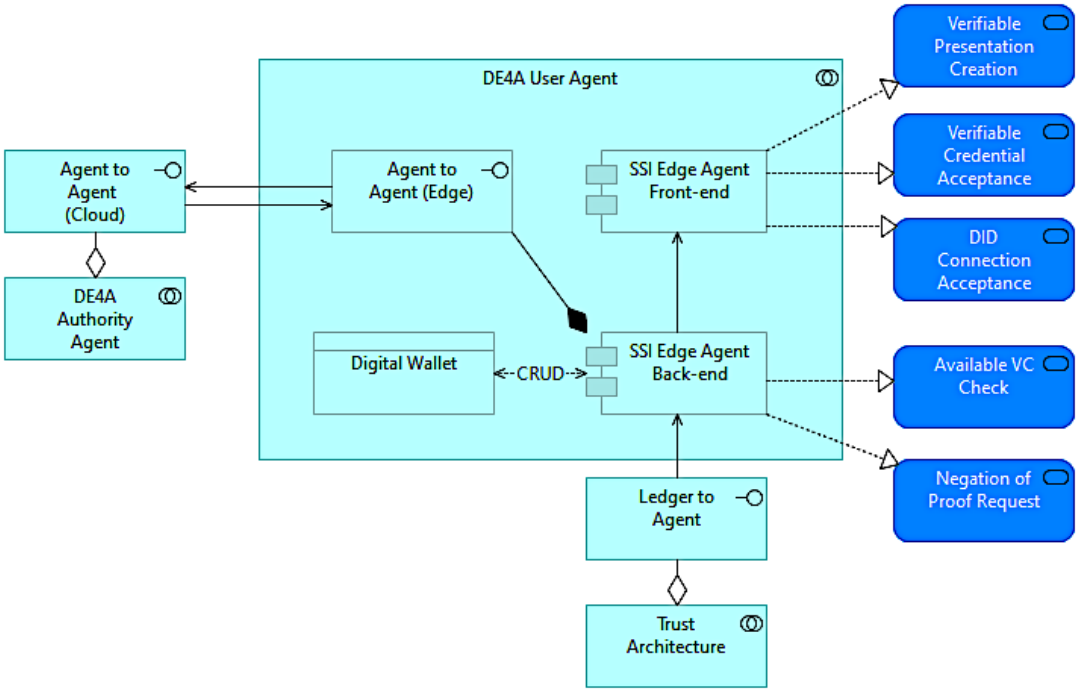


Figure 45 Graphic Representation of the User Agent Application Collaboration in the VC Pattern

Table 49 Application Components of the User Agent

Application Component	Description	Pattern(s)
SSI Edge Agent Front-end	Component building UI and logic to handle DID connections and the VC/VP related events.	VC
SSI Edge Agent Back-end	Application component managing the DID connections and handling the VC/VP related events.	VC
Agent to Agent (Edge)	Interface between Agents that provides the functionalities of a DID connection, e.g.: exchange of DID documents, Verifiable Credentials and Verifiable Presentations. This is a symmetric interface to the interface to the 'Agent to Agent (Cloud)'	VC

© 870635 DE4A Project Partners

The following tables present the application services per application component of the Authority Agent.

Table 50 Application Services Realized by the SSI Edge Agent Front-end

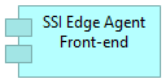
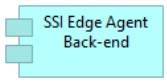
	Description	Pattern
DID Connection Acceptance	Generic. A service that resolves DC DID to the DID document. The DC document holds the endpoint of the DC agent and establish a DID connection. The service forwards the information about the User related DID document, which includes relevant information about his agent (e.g., DID, cryptographic data, endpoint, etc.).	VC
Verifiable Presentation Creation	The service supports the creation of Verifiable Presentation (VP) from the evidences (VC) selected by the User.	VC
Verifiable Credential Acceptance	This service offers Users the ability of a preview and acceptance of evidence (VC), which was issued from DP to them. Furthermore, the service manages the storing of provided evidence in a User-managed digital wallet, which is part of his agent.	VC

Table 51 Application Services Realized by the SSI Edge Agent Back-end

	Description	Pattern
Available VC Check	Generic. Based on procedural evidence (VC) requirements, this service matches the evidence (VC) stored in user digital wallet (agent) that may satisfy procedural requirements. With this service, the User has the option to preview each matched evidence (VC) and the option to decide about its delivery to DC. The service also resolves the situation where the User does not hold the required evidence (VC) in their digital wallet (current agent) and starts the procedure of the lookup of DP, which may provide the User with required evidence (VC).	VC
Negation of Proof Request	A service that resolves the situation where the User decides not to provide the evidence (VC). This service also initiates the procedure of the lookup of DP, which can likely provide the User with other evidence (VC) that may be used to satisfy procedural requirements.	VC

© 870635 DE4A Project Partners

4.10. Cross-border Subscriptions

https://wiki.de4a.eu/index.php/Cross-border_Subscriptions

The Cross-border Subscriptions application collaboration consists of various co-operating application components implementing multiple application services used by both Notification Process Realization (DP) and Subscription Process Realization (DP). It implements:

- the full life cycle of subscriptions (CRUD) in a MS and offers functionality to validate and confirm subscriptions as well as error handling;
- the event handling, i.e., filtering local (national) events for relevant cross-border events and creating the notifications messages and preparing the list of subscribers for particular cross-border events that need to be dispatched;
- the notifications of events, it provides a UI (front-end) in order to inspect log files and manually dispatch events if needed. A back-end serves this front-end and connects with the event handling.

It uses interfaces to communicate with the Base Registry of companies in the MS.

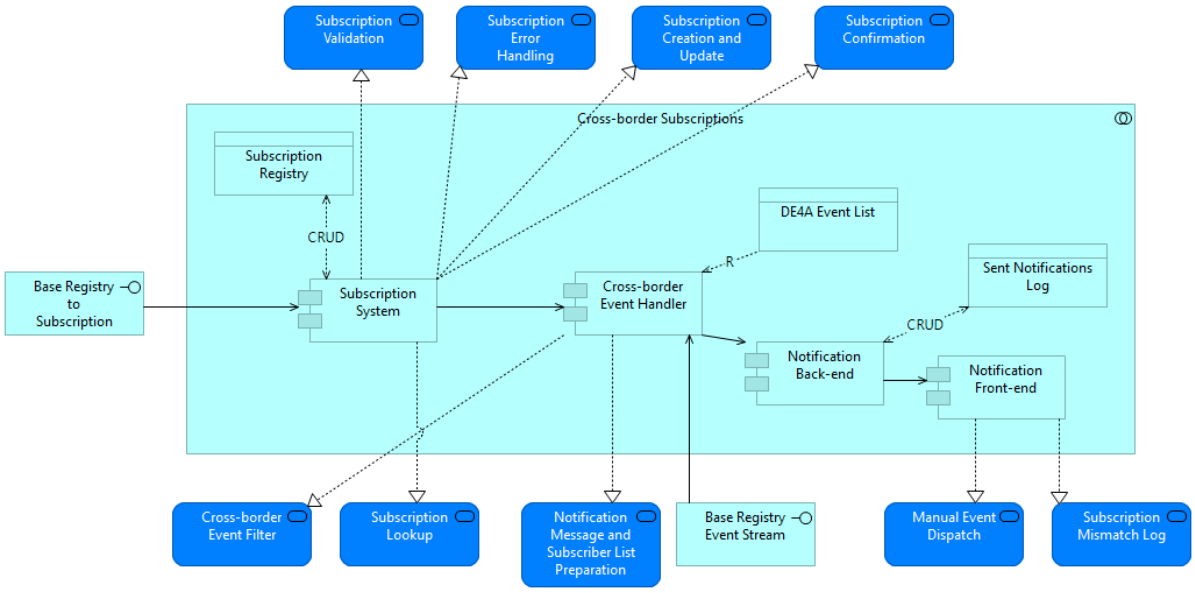


Figure 46 Graphic Representation of the Cross-border Subscriptions Application Collaboration in the S&N Pattern

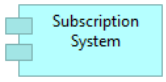
© 870635 DE4A Project Partners

Table 52 Application Components of Cross-border Subscription

Application Component	Description	Pattern(s)
Subscription System	Application component managing the entire life cycle of subscriptions, i.e., creation and maintaining subscriptions. It also offers functionality for validating subscriptions (does subject exist?, is the event supported?, is the subscription changing an existing subscription?), confirmation of a subscription and error handling. The component makes use of an interface to access the base registry.	S&N
Cross-border Event Handler	Application component handling the cross-border events. It filters all domestic events for relevant cross-border events and takes care of preparing a notification message and compiling a subscribers list to which the notification must be send. The component makes use of an interface to access the base registry.	S&N
Notification Back-end	Application component serving the front-end and connecting with event handling.	S&N
Notification Front-end	Application component providing the UI for civil servants to dispatch events and consult logging information for trouble shooting.	S&N

The following tables present the application services per application component of the Authority Agent.

Table 53 Application Services Realized by the Subscription System

	Description	Pattern
Subscription Evaluation	This service evaluates a subscription request to check if the request can be completed. If it fails the validation, the request is rejected and an error message will be sent.	S&N
Subscription Error Handling	In case some error occurs in the evaluation of a subscription request this service will handle it. The content of the error message is collected and sent to the Data Transferor.	S&N
Subscription Creation and Update	A service to record a subscription in the registry of the DO as well as update the subscription when needed. This service needs to be able to identify updates based on subject ID, subscriber ID and subscription time	S&N
Subscription Confirmation	After a subscription was successfully registered the requesting company needs to be notified. This service takes care of this.	S&N

© 870635 DE4A Project Partners

Table 54 Application Services Realized by the Cross-border Event Handler

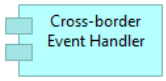
	Description	Pattern
Cross-border Event Filter	This service takes care of filtering all domestic business events for relevant cross-border events. Note that the DO must have a mapping of their own business events to the list of DE4A business events.	S&N
Notification Message and Subscriber List Preparation	A service for compiling the list of subscribers to be notified and preparation of the payload of notification message.	S&N

Table 55 Application Services Realized by the Notification Front-end

	Description	Pattern
Manual Event Dispatch	A service for resending a previously sent notification. It requires a manual action at the DT based on logs.	S&N
Subscription Mismatch Log	If the participant ID cannot be resolved, manual intervention is needed. The DE needs to be informed and appropriate measures taken. This service handles this.	S&N

© 870635 DE4A Project Partners

4.11. eProcedure Back-office

https://wiki.de4a.eu/index.php/EProcedure_Back-office

The eProcedure Back-office application collaboration consists of two high-level components realizing the functionality needed as part of Subscription. It encompasses:

- (backend) collecting relevant data for a subscription request, determining an appropriate response to request, and updating logs;
- (front-end) a UI for User tasks to analyse wrong subscriptions.

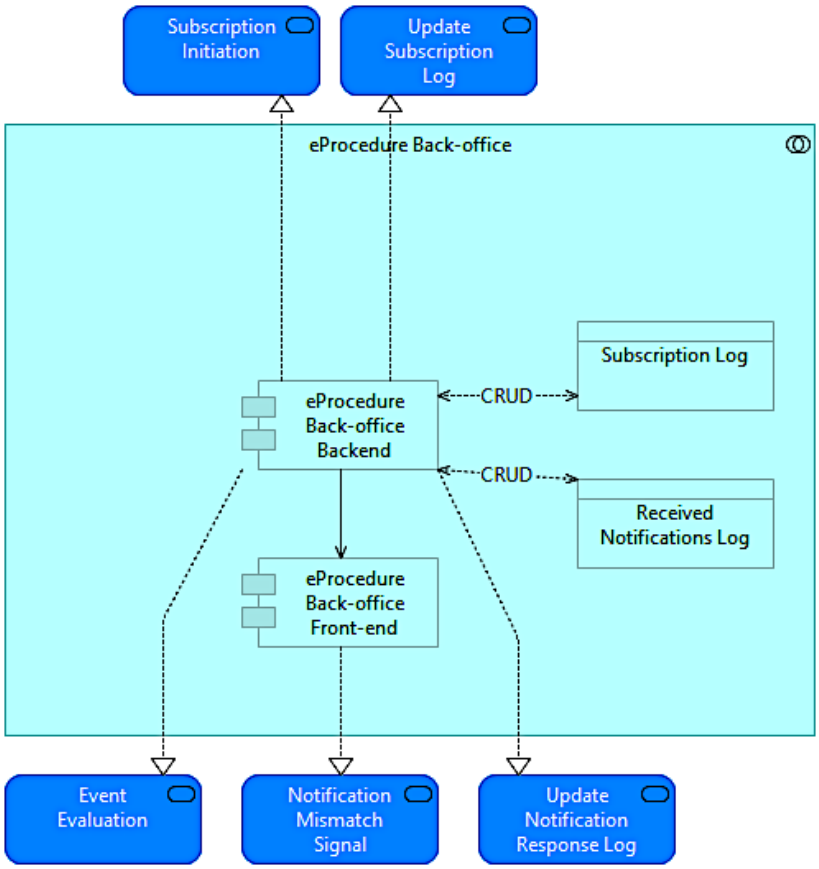


Figure 47 Graphic Representation of the eProcedure Back-office Application Collaboration in the S&N Pattern

Table 56 Application Components of eProcedure Back-office

Application Component	Description	Pattern(s)
eProcedure Back-office Backend	This component implements backend functionality like collecting relevant data for a subscription request, determining an appropriate response to request, and updating logs.	S&N
eProcedure Back-office Front-end	This component provides a UI for User tasks to analyse wrong subscriptions.	S&N

© 870635 DE4A Project Partners

The following tables present the application services per application component of the eProcedure Back-office.

Table 57 Application Services Realized by the eProcedure Back-office Backend

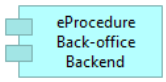
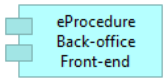
	Description	Pattern
Subscription Initiation	This service takes care of collecting relevant data in preparation of subscription request.	S&N
Update Subscription Log	The subscription is recorded in the subscription log upon receiving the confirmation. The subscription log serves as an overview for the DC of all their subscriptions at different DPs.	S&N
Event Evaluation	A service for determining the appropriate event response. Depending on the event, different courses of action are possible: • Event is not relevant (can be dismissed) • Event requires a new (i.e., updated) evidence • A business response required • Some exception occurs	S&N
Update Notification Response Log	This service logs the responses derived from received event notification.	S&N

Table 58 Application Services Realized by the eProcedure Back-office Front-end

	Description	Pattern
Notification Mismatch Signal	When the company cannot be identified, or the registered company or branch is no longer active a User action must be triggered to a change (i.e., cancellation) the subscription. Afterwards they will need to analyse the mismatch to find the cause of this apparently wrong subscription and to take appropriate measures.	S&N

© 870635 DE4A Project Partners

5. DE4A Pilots

https://wiki.de4a.eu/index.php/Pilots

DE4A includes three cross-border and cross-domain Pilots - Studying Abroad, Doing Business Abroad, and Moving Abroad -, comprising different functional use cases focused on different high-impact and viable administrative procedures, and aimed to realize tangible benefits in fully operational environments to real Users (citizens, students, business persons and public servants). The Pilots are delivered by separate, agile, multi-disciplinary, inter-Member State teams of experts. The focus of these teams is on iterative system integration and configuration, hence on making existing building blocks and solutions work together in real life cases.

5.1.Studying Abroad

https://wiki.de4a.eu/index.php/SA

The Studying Abroad pilot of the "Digital Europe for All" (DE4A) project aims at demonstrating in practice the benefits for different European Higher Education Area stakeholders of realizing across borders the principles of once only and digital-by-default. The pilot will also validate novel technologies and concepts, such as verifiable credentials, self-sovereign identities, and distributed ledgers.

By the combination of three use cases it will demonstrate the optimal process/procedure for students from the three participating Member States (Portugal, Slovenia, and Spain) for registration to higher education and eventually applying for a student grant as well as for studies recognition.

The pilot will run in two iterations, the first from October 2021 to the end of January 2022, and the second from May 2022 to the end of October 2022.

The three use cases are defined in D4.1 [7]:

1. Use case 1: Application to Higher Education

The first use case focuses on the procedure of applying for admission to public higher education institutions. This procedure corresponds to the "Submitting an initial application for admission to public tertiary education institution" procedure from Annex II of the SDGR [17]. Portugal, Slovenia, and Spain are involved in this use case.

2. Use case 2: Applying for Study Grant

The second use case focuses on the procedure of applying for a study grant abroad. This procedure corresponds to the "Applying for a tertiary education study financing, such as study grants and loans from a public body or institution" procedure from Annex II of the SDGR. Slovenia and Spain are involved in this use case.

3. Use case 3: Diploma recognition

The third case focuses on diploma recognition in order to facilitate the use of such information by government and other sectors. This procedure corresponds to the "Requesting academic recognition of diplomas, certificates or other proof of studies or courses" procedure from Annex II of the SDGR [17]. Portugal, Slovenia, and Spain are involved in this use case.

The use cases implement two interaction patterns:

1. USI (User-supported intermediation) – This pattern is implemented in UC#1 and UC#2. The main reason for selecting this pattern were legal requirements of the participating Member States

© 870635 DE4A Project Partners

(Slovenia and Portugal). The national data protection legislation requires Users' approval of evidence transfer before the evidence crosses the border. The User's interaction with DP also facilitates record matching, as the User can provide the DP with any additional required information, if needed.

2. VC (Verifiable credentials) – UC#3 implements this pattern.

Figure 48 below shows the mapping of interaction patterns to use cases.

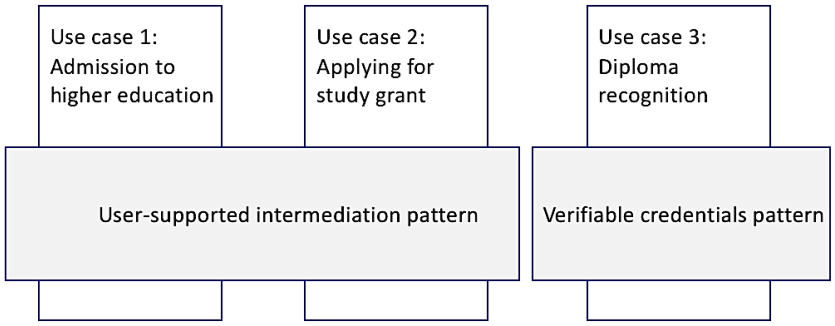


Figure 48 Mapping of SA Use Cases to Interaction Patterns

The business requirements have been included in D4.1[7] and the pilot design for implementing the USI and VC patterns is specified in D4.2 [17]. The solution building blocks for use of the USI pattern (in the SA pilot) and their interfaces have been described in the solution architecture, which is also available in D4.2.

5.2.Doing Business Abroad

https://wiki.de4a.eu/index.php/DBA

D4.5 [9] defines two use cases[12]:

1. Use case 1: Starting a business in another Member State

   At the core of this use case is the fulfilment of procedural obligations to do business in another Member State, especially the initial registration of a company at an eProcedure portal (AT, NL, and RO pilot scenarios), opening a branch and the assessment of tax duties in the destination Member State (in the Swedish pilot scenario). In this use case, a company representative authenticates to the eProcedure portal, registers the company at the portal and applies for a service[13].

2. Use case 2: Doing business in another Member State

   This use case focusses at assessing the consequence for active eServices in case of a business event, e.g. company goes bankrupt, company stops its activities, company merges, etc. The Data Consumer may subscribe to notifications on selected business events. In case such an event occurs, the Data Provider notifies the Data Consumer. The Data Consumer needs to assess the relevance of the notification. It can then for example request the updated data from the Data Provider or decide it does not need any additional data. Furthermore, the Data Consumer may intervene in an active eService (e.g. stop periodical grants or impose a tax

[12] The description of the use cases has been refined after delivery of D4.5.
[13] Sub use case 1a: the enrolment of a foreign company in a customer database of a service provider in another Member State. Sub use case 1b: the enrolment of (a branch of a) foreign company in the business register of another Member State.

© 870635 DE4A Project Partners

obligation). The Data Consumer may also use the notifications as input to a general fraud prevention and protection procedure. All pilot MS participate (AT, NL, SE, RO).

The use cases implement three interaction patterns:

1. The intermediation pattern: for fetching company data at the request of the User from the business register directly.
2. The subscription and notification pattern: for allowing data consumers to subscribe to updates on company data and to receive notifications of changes in company data[14].
3. The lookup pattern: for providing a lightweight alternative to the intermediation pattern for fetching (possibly updated) company data from business registers with direct service calls. This pattern focusses on high frequency, highly standardized data requests to data sources which the Data Consumer is familiar to.

Figure 49 below shows the mapping of the use cases to the interaction patterns.

The first use case – in D4.5[9] – ends with a subscription to receive notifications of business events of the company involved. From a logical process point of view, this is strongly intertwined with the company registration: subscribing to notifications follows directly after registration of the company at the eProcedure portal before the process ends. Hence it is an integrated part of the first use case. From an interaction pattern perspective, the subscription to notifications does not belong to the intermediation pattern but to the subscription & notification pattern. The first part of the subscription and notification pattern deals with managing subscriptions, the second part with sending notifications once a business event took place. So, the first use case spans two interaction patterns.

Something similar goes for the second use case. This use case starts with receiving the notification from the Data Provider. After assessing the notification, the Data Consumer may decide to request updated data from the business register via the lookup pattern. So, use case 2 involves the subscription & notification pattern as well as the lookup pattern.

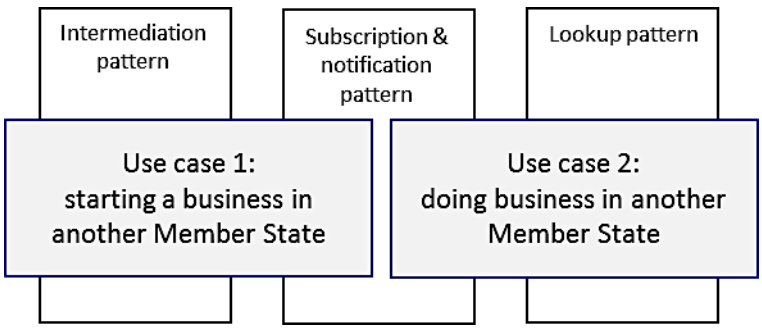


Figure 49 Mapping of DBA Use Cases to Interaction Patterns

[14] Depending on the perspective, you should read "allowing the company representative to subscribe to automatically sending company data updates to the Data Consumer".

© 870635 DE4A Project Partners

Use case 1 could be implemented with the Lookup pattern as well to retrieve the evidence (instead of the Intermediation pattern). This is no project priority and therefore has not been depicted in the diagram above.

The business requirements have been included in D4.5 and the pilot design for implementing the intermediation pattern is specified in D4.6[10]. The solution building blocks to use for the intermediation pattern (in the DBA pilot) and their interfaces have been described in the solution architecture.

For the other two patterns (subscription & notification and Lookup) the DBA solution architecture will be specified following the finalization of the PSA. The pilot will run in two iterations, the first from October 2021 to the end of January 2022, and the second from May 2022 to the end of October 2022.

5.3.Moving Abroad

https://wiki.de4a.eu/index.php/MA

The Moving Abroad pilot of the DE4A project, implements eProcedures for moving and living abroad (MA) in Luxembourg, Portugal, Romania, Slovenia, Spain, and Sweden. It improves currently available cross-border procedures by implementing the Once Only Principle (OOP).

Piloting solutions to these highly complex processes are an important step in breaking down barriers in the European single market. In the end, people should be able to move to another Member State as easily as they do nationally. The MA pilot highly values experience from piloting real eProcedures.

The MA pilot addresses some of the most important (research) questions for successfully implementing the SDGR and SDGR-related processes. Besides validating the OOP technical System for evidence exchange in real use cases it goes beyond the minimum service to support people being more mobile. Furthermore, the MA pilot pilots several SDGR-specific and related functions, like explicit request and preview, canonical evidence, and record matching.

First iteration of the MA pilot focuses on the use cases of Change in population registry, Change of address and Request of Birth, Marriage and Death certificates. The first iteration takes an optimistic approach, with the procedures requiring one evidence from a single authentic source. Furthermore, the domestic evidence is readily available and can be transformed into canonical format and transferred via the technical system immediately.

The second iteration will explore scenarios that are more complex with multiple evidence requests, and procedure interruptions. In the second iteration, we will pilot the Pension use case and may include the Intermediation (IM) pattern. We expect more changes to the second iteration of the MA pilot after the first iteration when we have gained more knowledge and experience.

The MA pilot will run in two iterations, the first from October 2021 to the end of January 2022, and the second from May 2022 to the end of October 2022.

© 870635 DE4A Project Partners

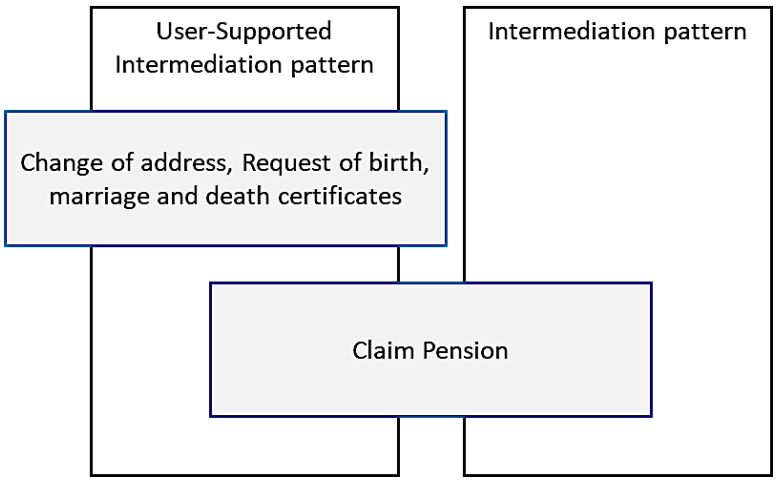


Figure 50 Mapping of MA Use Cases to Interaction Patterns

© 870635 DE4A Project Partners

6. Conclusions

The Project Start Architecture defines a starting point for the 2nd iteration of the three DE4A pilot projects and for WP3 - Semantic Interoperability Solutions and WP5 – Common Components Design & Development, providing guidance on the 25 interdisciplinary questions listed in 2.3. The Reference Interaction Patterns (chapters 3 and 4) provide a top-down analysis of cross-border evidence exchange in the context of (public) service procedures and provided a rich context for the formulation of working hypotheses. These hypotheses were formed in discussion with different stakeholders and experts of the DE4A Member States. Continued internal and external validation is required nevertheless, especially in relation to initiatives like the SDGR[17] Once-Only Technical System, EBSI[24], and recently the eIDAS[25] revision re. European Digital Identity[26]. As stated in the introduction subsequent updates and new insight will be performed on the DE4A Wiki.

The section below picks up each of the interdisciplinary questions raised in 2.3 and summarized the direction taken in this Project Start Architecture:

1. For the **Orchestration / Choreography** of the overall exchange of evidence, we are trying to avoid the need for a central orchestrating component or the need to agree on correlations that are consistent or even persistent across multiple platforms in different MS. This means that the orchestration is left to the DC in the Intermediation, User-supported Intermediation (USI) and Evidence Lookup patterns and to the User themself in the Verifiable Credential pattern. In the first three cases, this means that we attempt to correlate the request of the DC and the response of the DP in context of the DC. The same is also true for the subscription process of the Subscription& Notification pattern.
2. **Complementary, Overlapping or Conflicting Evidence Equivalents** are complex cases that are considered essentially by all reference interaction patterns included the PSA. The specific cases of the pilots, using canonical evidence types and a limited number of participants, will most likely not suffer from such inconsistencies.
3. **Interrupted vs. Uninterrupted Exchange** is a topic that is under continued discussion with internal and external stakeholders. We recognized MS requirements for interrupted procedures and attempt to “simulate” such procedures without the need to persist process instances across multiple platforms and Member States. A “Save and Resume” functionality is considered a good practice for the eProcedure portals and the Intermediation and USI pattern leave this functionality fully in scope of these portals. This means that an instance of the OOP sequence (User request to DP response) needs to be performed in its entirety and in an uninterrupted way (even though the interaction between User and DP of the USI pattern allows to manage this in a more flexible way). If an evidence cannot be retrieved (within an agreed SLA time), e.g. because the evidence must first be digitized, then the complete OOP sequence must be repeated, starting with a new OOP request. Subscription and Notification as well as Evidence Lookup are considered to be uninterrupted.
4. **Explicit Request and Transitivity Between Actors** is a controversial issue and one of the main reasons for supporting both the Intermediation and the USI pattern. The Intermediation pattern follows the interpretation that SDGR[17] Article 14 forms a legal basis for the exchange of evidence based on an explicit User request that was issued to the DC - essentially the DP is expected to trust an assertion of the DC that the User request was collected. The USI pattern conforms to national legal requirements by including the direct interaction between User and DP. Subscription & Notification and Lookup do not include User interaction and consequently no explicit request. They are not covered by the SDGR.
5. **Preview & Approval UI** is integrated differently in three patterns: The Intermediation pattern assumes that the preview can be prepared by the DC after the evidence was technically

© 870635 DE4A Project Partners

transferred, prior to its inclusion in the eProcedure instance. As the USI pattern already includes a direct interaction between the User and the DP, also the preview functionality is moved to the DP. This allows to relax above stated assumption and caters to privacy concerns of some MSs and legal experts for the citizen domain. In the VC pattern, the acceptance of the transfer by the User is provided by affirmative action when the User submits the Verifiable Presentation (VP) from his wallet to the DC. Subscription & Notification and Lookup do not include User interaction and consequently no preview. They are not covered by the SDGR.

6. **Identity and Record Matching** must be performed twice in the overall process, on DC- side to identify the User in context of the Procedure (some eProcedures will not require this) and once on the DP-side in order to allow the extraction of the correct evidence. In the Intermediation pattern, the identity matching at the DP must be performed solely based on information included in the evidence request of the DC, which means essentially based on available eIDAS attributes or the EUID in case of companies. A perfect match is not always possible, but MS experience shows that a reasonably high percentage of Users can be matched in this way for use in a pilot context. The USI and VC pattern include a direct interaction between User and DP, hence can request additional information to improve the matching. In the Doing Business Abroad pilot context, record matching for Subscription & Notification and Lookup is not needed because of the EUID can be used.
   DE4A will keep vigilant of eIDAS review process inasmuch it can make progress into possible solutions for the record matching problem.
7. **Transitivity of User Identity** is closely related to the identity matching mentioned above as the identity must be established separately by DC and DP. The working assumption is here that the explicit User request (Article 14 (7) SDGR [3]) allows the transfer of personal data (i.e. eIDAS attributes) from DC to DP.
8. A **Hand-over of User Interface Between** Actors is not required in all interaction patterns. The User interacts only with the DC in the Intermediation pattern. The direct interaction with multiple UIs in the USI-pattern (DC and potentially several DPs) and the VC pattern (adding the Wallet as an additional UI) means that the likelihood of the procedure being interrupted (i.e. time outs) could increase for these patterns, making a 'Save and resume' functionality of the eProcedure portal the more important.
9. **Mandate and Proxy** to be included in the user identification is required for the Doing Business Abroad pilot but is considered out of scope for the other two pilots. The expectation is that we can adopt the results of SEMPER in this regard, i.e. extending the eIDAS authentication with mandates and powers.
10. The **Encryption Gap** between the eDelivery gateway and the national systems (e.g. national OOP layer) is a result of applying message-level security between the eDelivery gateways only. The working hypothesis is that this gap is acceptable.
11. The **Structured Data vs. Unstructured Data** discussion is prone to misunderstandings. We consider structured data sets as starting point, meaning that data is structured according to a known data model or schema. Such structured data sets can include an unstructured document or scanned certificate as additional reference. We do not envision one all-encompassing, cross-domain data model, but advocate the reuse of prior, sectoral harmonization efforts to the maximum extent possible.
12. **Automated Re-use of Data**, meaning fully automated parsing of data contained in exchanged evidence in the back-end systems of the receiving competent authority, is the highest level of aspiration for exchange of evidence. Even on national level, i.e. based on a single legal and administrative framework, this is not trivial and by no means always possible, let alone in a European cross-border context covering 27 national legal and administrative frameworks.

© 870635 DE4A Project Partners

The working assumption is that automated reuse is only possible in sectors that harmonized their definitions through legal or voluntary mutual agreements. The reuse of data extracted from exchanged evidence remains in the responsibility and management of the receiving MS and authority.

13. The aspiration of DE4A is to run pilots as much as possible in **Production System and Real-life Cases** in (partially) acceptance environments are considered a good level of achievement if full production go-live is not possible because of legal, organizational or technological barriers. The wish to create immediate business value by fully running on production systems is one reason behind the addition of the USI-pattern to the refence architecture, in order to accommodate present legal limitations of some MS.
14. DE4A decided against **EESSI Integration** because it would mean duplication of an existing EESSI use case. The pensions request procedure won't be implemented, instead we will pilot the pensions info request but with widened scope to include social benefits as well.
15. **BRIS Integration** was investigated and full or partial reuse of the BRIS system proved unpracticable because of incompatible scope (in term of covered cases) and access (in terms of participants). Reuse and extension of the **semantic** harmonization of the company data domain accomplished by BRIS is intended to the maximum extent possible. This is one good example of a domain specific harmonization that adds value to the cross-border exchange of evidence, increasing the likelihood of automated reuse of data.
16. Both **eIDAS and National Authentication Systems** should be supported for the user authentication at the DC-side and (in case of the USI and VC pattern) at the DP-side of the exchange. The underlying reason is exclusive reliance on eIDAS authentication could exclude own nationals (i.e. returning expats) and EU citizen living and working in another MS than their country of origin and often hold eIDs of their host country (population-wise, this user-group amounts to a 28th MS). These are the user groups that might profit most of the existence of a Once-Only Technical System on European level.
    As indicated in section 2.3.16 a new proposal revising the eIDAS regulation is likely to extend the scope of eIDAS and will impact the OOTS currently being defined.
17. We could not yet reach a conclusion concerning the use of **Non-notified eIDs** during the PSA process. This needs further investigation in the context of the individual pilots. Presently, several participating MS do not have notified eIDs and corresponding eIDAS functionality available. This means that we would need to devise some work-around (e.g. using national authentication systems) or limit the pilot population to cases that do not require that functionality. Allowing the use of non-notified eIDs in eIDAS enables more possibilities of doing real life pilots. For this reason it has been proposed to use pre-production eIDAS nodes as they can accept non-notified eIDs.
18. In some national frameworks, **Payment for Evidence** is commonplace, also and especially between authorities, i.e. as a means for creating budget transparency. For the DE4A pilots we consider the payment for evidence to be out of scope. We continue to monitor this discussion in the SDG working groups.
19. We attempt to set up the **Trust Management** relying largely on eIDAS and eDelivery and message-level security for the Intermediation and USI pattern. The aim is to keep the Trust Architecture simple and based on mature technology and to work around the pitfall of overloading the evidence exchange with certificate management that, in a European-wide implementation, would need to cover many thousands of endpoints. The Intermediation, Lookup and the Subscription & Notification pattern additionally include the possibility of an authority check: a control that the requesting authority has a valid reason to request a specific evidence type. The pilots will assume a true circle of trust across all participating,

© 870635 DE4A Project Partners

competent authorities, such that an authority check could be obsolete: this is in line with the current proposal for the SDGR OOTS.

20. **Legal Basis for SSI and Block Chain Technology**: The diploma recognition use case, adopting the VC pattern. We will pilot with real students however it is considered a PoC as we use EBSI pre-production infrastructure. So, while it is true there are legal considerations with respect to the usage of mentioned technologies, it is not considered a problem for DE4A. Furthermore, the new proposal for revising eIDAS Regulation might provide a solid legal basis in the future.
21. The close relation between DE4A and the efforts of implementing the OOTS in context of the SDGR [17] fuels the discussion in how far the pilot solutions of DE4A fall in the **Explicit Scope of Article14**. The Intermediation pattern is meant to be closely aligned with SDGR and the current state of discussion around the Once-Only Technical System High Level Architecture. A final consensus on whether the USI pattern is compliant with Article 14 and OOP has yet to be reached. The VC pattern falls outside of the application or Article 14 and is much more geared towards initiatives like EBSI than the SDG implementation. Subscription & Notification and Lookup are not covered by the SDGR.
22. Another ongoing discussion concerns **Matching Evidences between Member States,** establishing an equivalence between what one MS requests for an eProcedure and what another MS can provide as evidence. Presently, there are two, complementary approaches underrepresented in the PSA: Matching of (non-harmonized) evidence types (i.e. Criterium-based (cf. CCCEV)) and the use of canonical evidences. Because the canonical evidence approach resolves both evidence matching and facilitates deep semantic interoperability, this approach will be investigated further in the pilots. This will help to uncover real-life challenges related to the harmonization across several Member States.
23. There are several sources for **Multi-evidence Cases**, exhibiting differing levels of complexity. The second iteration should expand the MVP restriction to include multi-evidence cases, which requires an update of the Exchange Information Model. It is likely that piloting would focus on simpler cases to show the inclusion of multiple evidence in a single evidence response. Cases involving multiple subjects would create a specific record matching challenge for citizen cases, which is expected to be beyond the DE4A pilot scope. Some multi-evidence cases raise (very) high challenges on existing eGovernment architectures in the MS. This point must be considered and coordinated very carefully.
24. **Stateless DE4A Connector**
    With respect to cross-border exchange of evidence in the context of the OOP Technical System there are complex cases where state needs to be maintained in between sessions. Examples include multiple DPs, multi-evidence, delay in digitizing evidence, extensive input from the user required etc. It will not be feasible or is impracticable to perform this in one user session (cf. 3 above). Irrespective of whether a business process is stateful or stateless, in our view the state should not be maintained in the connector. Instead, this is on the DC for doing so if needed (cf. 1 above).
25. European eGovernment Interoperability means dealing with **Highly Distributed, Cross-border System**. The administrative complexity, heterogeneity of national eGovernment architectures and different approaches to as well as maturity of national OOP solutions means that architecture decisions are taken in a way that assumptions about the working of national systems is kept to a minimum and the complexities as much as possible resolved within the responsibility of a single organization or Member State. This is for example apparent in the way Orchestration/Choreography (see 1 above) or Interrupted exchange (see 3 above) is approached.

© 870635 DE4A Project Partners

Using an iterative approach, starting with the Intermediation pattern (3.1), and employing working hypotheses for each interdisciplinary question to contrast the interaction pattern with pilot and MS specific requirements, we can conclude that the requirements are too heterogeneous to be covered by a single one-size-fits-all solution. A multi-pattern architecture is indeed needed for European eGovernment interoperability. What became very apparent during that exercise is that the nature of the user/subject, i.e., the difference between company and citizen/student use-cases, is highly significant and exerts influence on most of the interdisciplinary questions.

By consolidating the application architecture in a single chapter 4, the PSA second iteration attempts to show more clearly that the application services supporting the different patterns exhibit considerable overlap and should be integrated into a unified application layer. This holds even for the VC pattern that introduces a new paradigm, based on decentral identifies and distributes ledger technology.

The involvement of architects from the pilot teams in the process of compiling this document was instrumental in the alignment of the two work packages and will remain so through the 2nd pilot iteration. The PSA team will continue operation in order to provide ongoing guidance to the pilots and support the elaboration of the Solution Architecture. Any updates to this PSA will be recorded in the DE4A Wiki.

The reference architecture (chapters 3 and 4) and especially the identified Application Services, Application Components and Interfaces are the basis for creating the backlogs for WP3 Semantic Interoperability Solutions and WP5 Common Component Design & Development. Additionally, the architecture content will be further updated in the DE4A Wiki as basis of D2.6 Services Interoperability Solutions Toolbox.

Within WP2, the reference architecture will be further consolidated into a Multi-pattern target architecture beyond SDG 2023 timeline (cf. timeline t=3 of the D2.1 Architecture Framework[2]) that will result in D2.7 - Optimal Interoperability Architecture for cross-border procedures and evidence exchange in light of the Single Digital Gateway Regulation.

Next steps to follow up the PSA in context of the project roadmap are:

- Support of planning of Pilot iteration 2 and solution definition.
- Walkthroughs of the new reference interaction patterns Subscription & Notification and Lookup to maximize the value of the architecture analysis for the overall project.
- Align the required Application Components and Application Interfaces of the chosen interaction pattern with the backlogs of WP3, WP4 and WP5.
- Use models of the reference architecture and derived models as context for feature refinement sessions in the technical work packages WP3, 4 and 5.
- The reference Architecture will be further refined and forms the basis for D2.7 Interoperability Architecture for Cross-border procedures and evidence exchange in light of the Single Digital Gateway Regulation

© 870635 DE4A Project Partners

References

[1] DE4A Deliverable D1.7 Legal, technical, cultural, and managerial barriers

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

[3] DE4A Deliverable D2.2 Initial DE4A Trust Management Models and Blockchain Support Framework, can be consulted via https://www.de4a.eu/project-deliverables

[4] DE4A Deliverable D2.4 Project Start Architecture (PSA), First iteration, can be consulted via https://www.de4a.eu/project-deliverables

[5] DE4A Deliverable D3.3 Semantic Framework - Initial version, can be consulted via https://www.de4a.eu/project-deliverables

[6] DE4A Deliverable D3.5 Semantic Toolkit-Initial Version (currently under review)

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

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

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

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

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

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

[13] DE4A Deliverable D5.1 First inventory of features for products/components - confidential deliverable

[14] DE4A Deliverable D5.3 Initial technical design of interfaces and common specifications - confidential deliverable

[15] DE4A Deliverable D5.5 First release of DE4A Common Components (currently under review)

[16] DE4A Deliverable D7.1 Overview of legal and ethical requirements - confidential deliverable

[17] 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.

© 870635 DE4A Project Partners

[18] ISA2 Action 'Innovative Public Services': Piloting a REST API extension of CEF eDelivery, 30/10/2020 v1.1

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

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

[21] DE4A Description of the Action, Ref. Ares(2019)6449821 - 18/10/2019 (Consortium document, not publicly available)

[22] DT-GOVERNANCE-05-2018-2019-2020: New forms of delivering public goods and inclusive public services; Horizon 2020 Work Programme 2018-2020 - 13. Europe in a changing world – Inclusive, innovative and reflective societies, (European Commission Decision C(2018)4708 of 24 July 2018)

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

[24] European Blockchain Services Infrastructure (EBSI) EBSI (europa.eu)

[25] 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)

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

[27] Policy for Transport Security 1.0.0 2021-04-08 (Consortium document, not publicly available)

[28] CEF eDelivery Access Point Component Offering Description, 26/09/2018

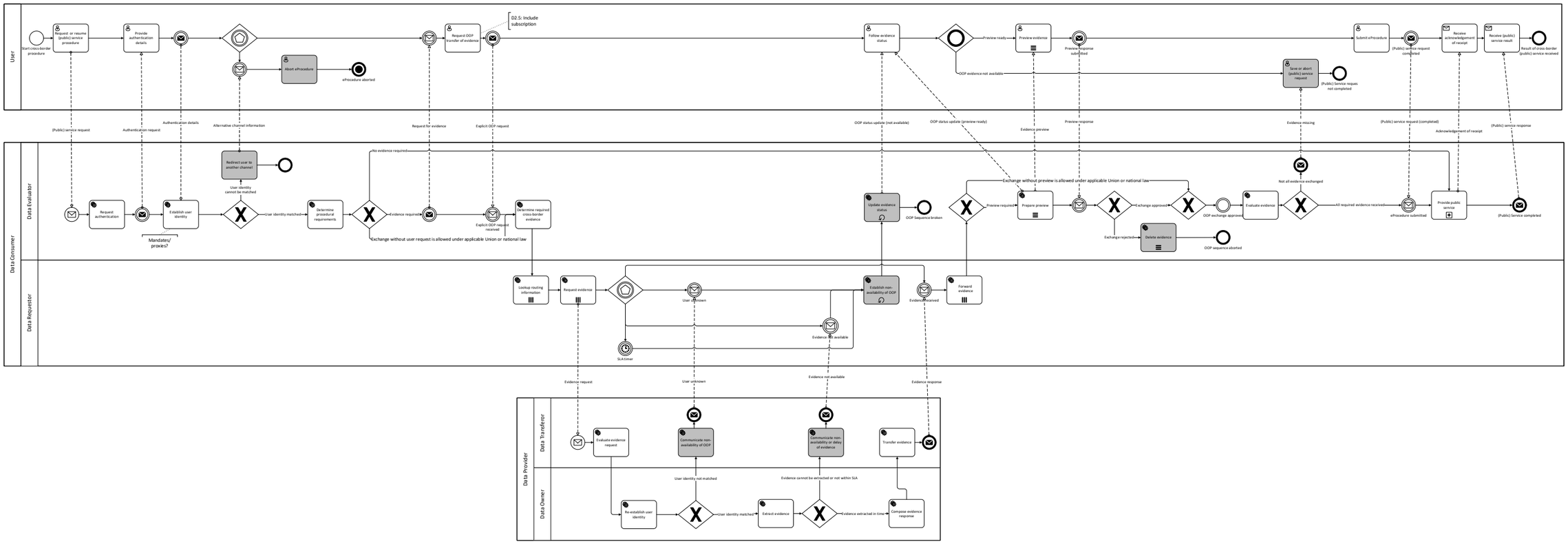
[29] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

[30] Details and common behaviour on the user redirection of the USI pattern v1.1, 2021-05-30

© 870635 DE4A Project Partners

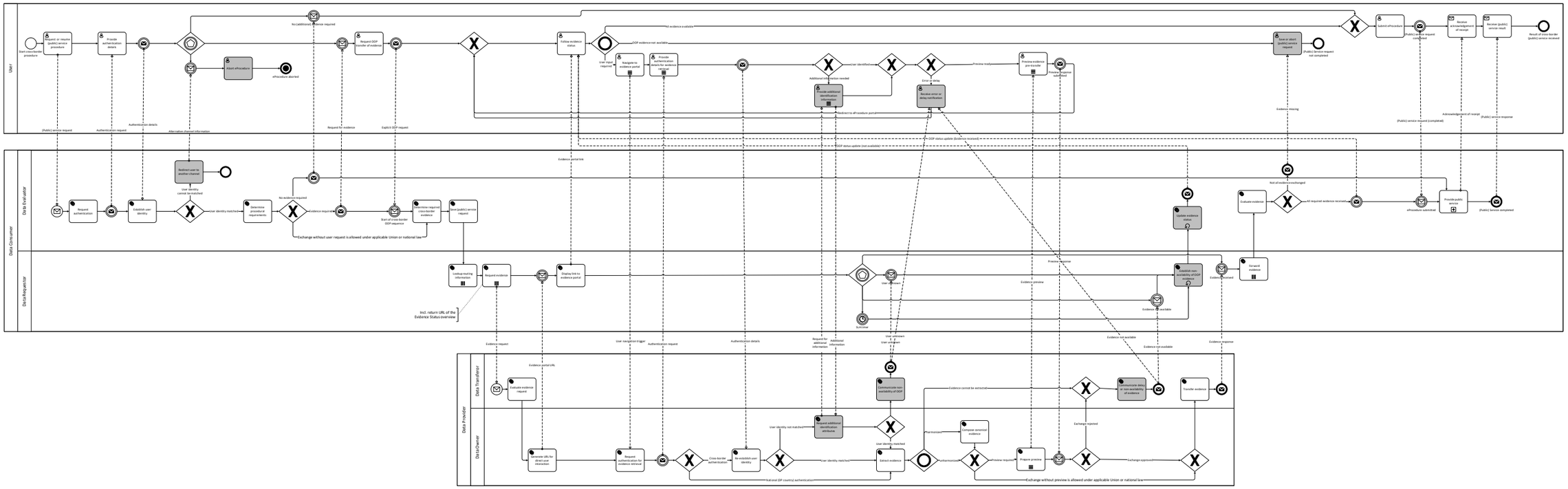
Annexes

Annex 1 Business Process Collaboration View of the Intermediation Pattern



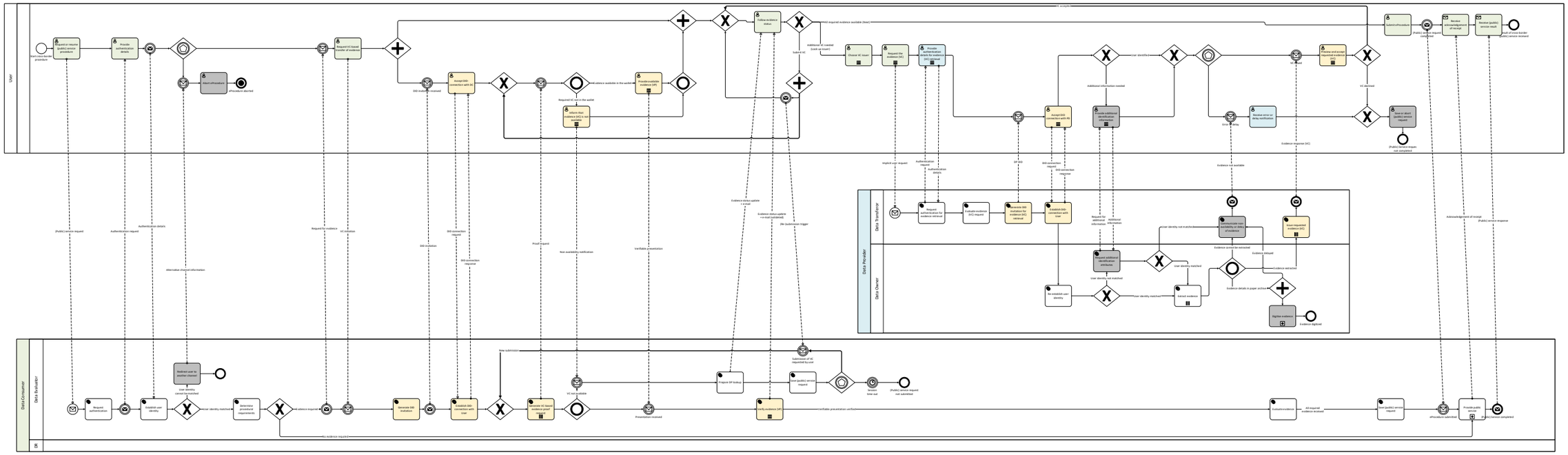
© 870635 DE4A Project Partners

Annex 2 Business Process Collaboration View of the User-Supported Intermediation Pattern

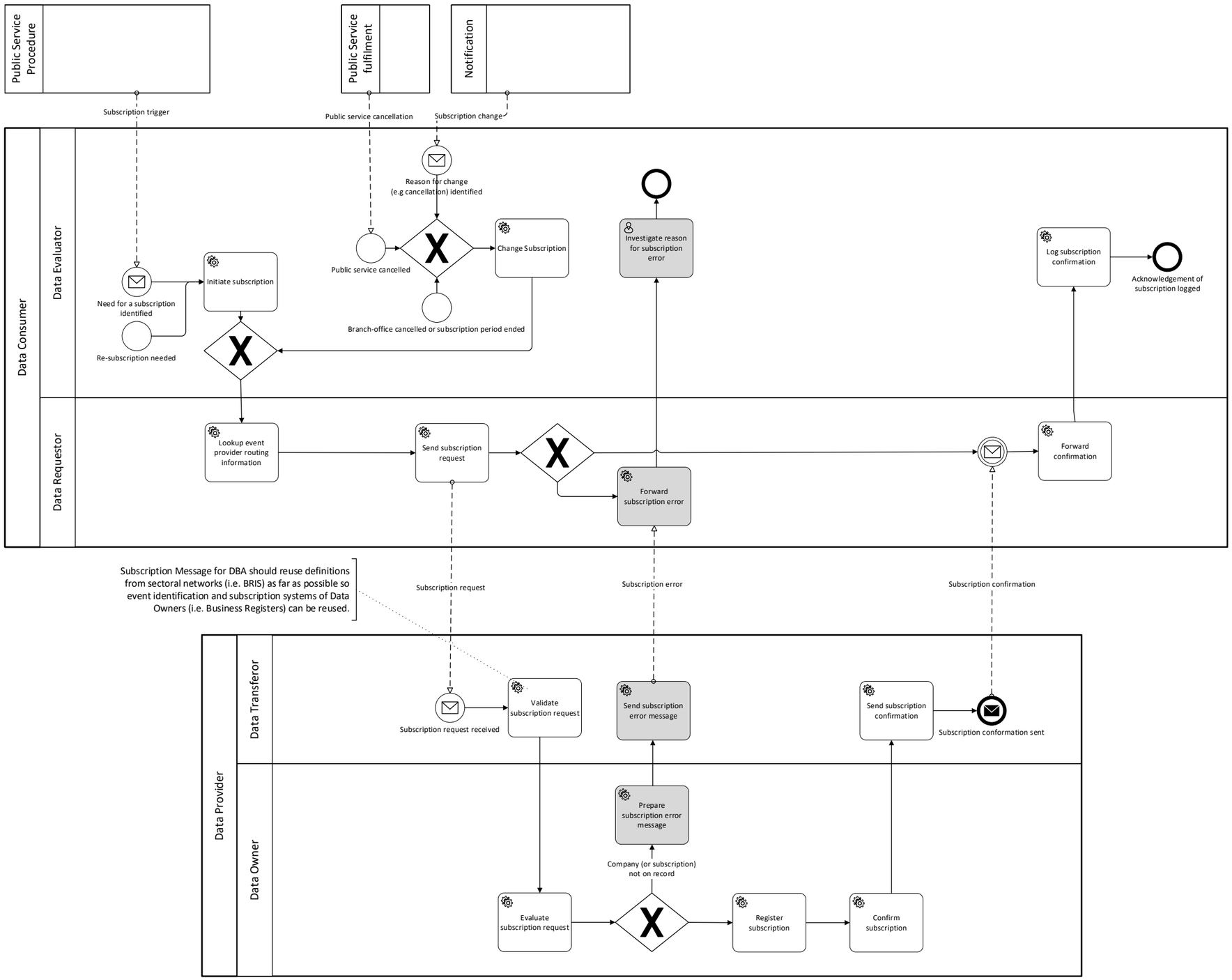


© 870635 DE4A Project Partners

Annex 3 Business Process Collaboration View of the Verifiable Credential Pattern

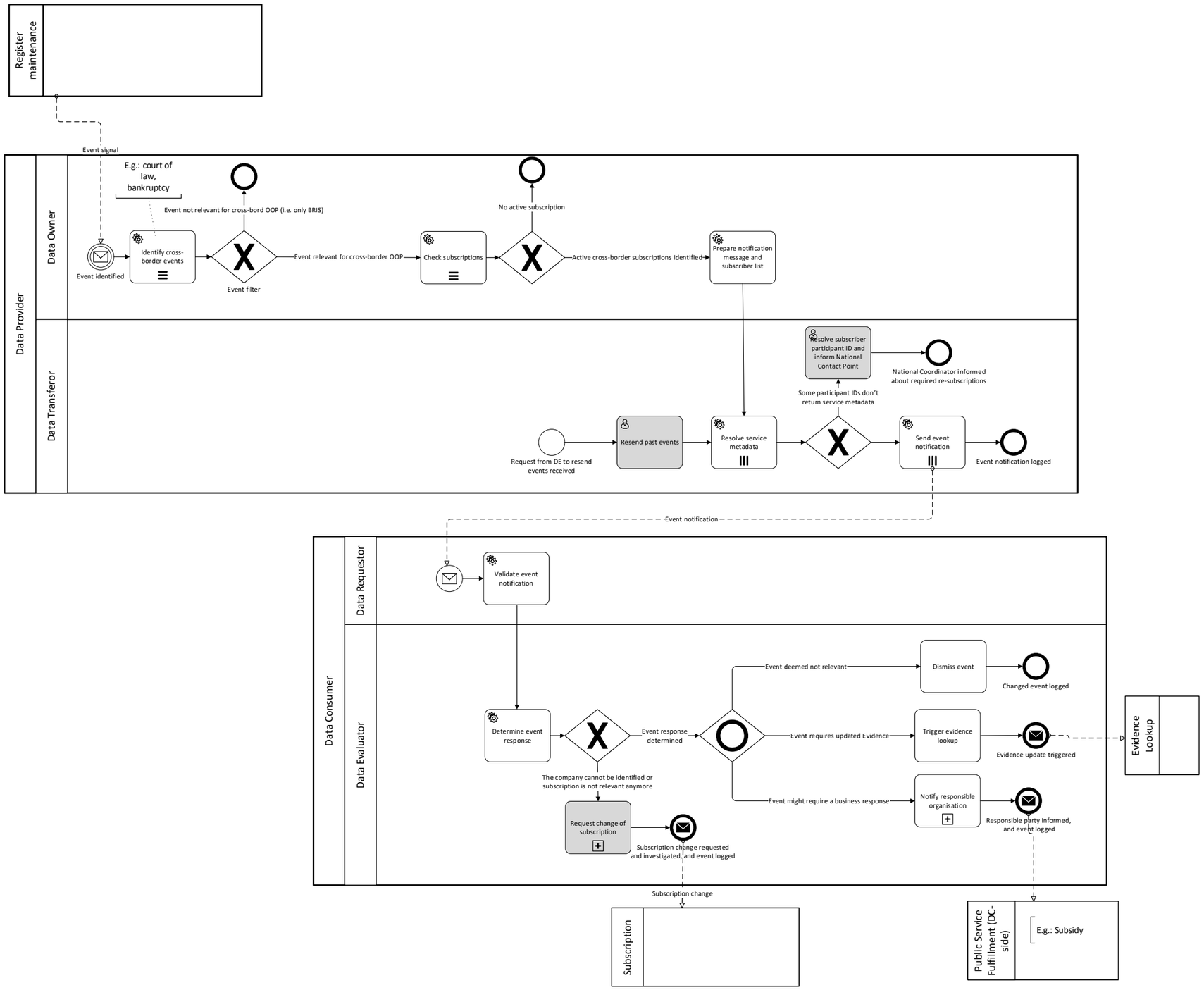


Annex 4 Event Subscription Business Process Collaboration View

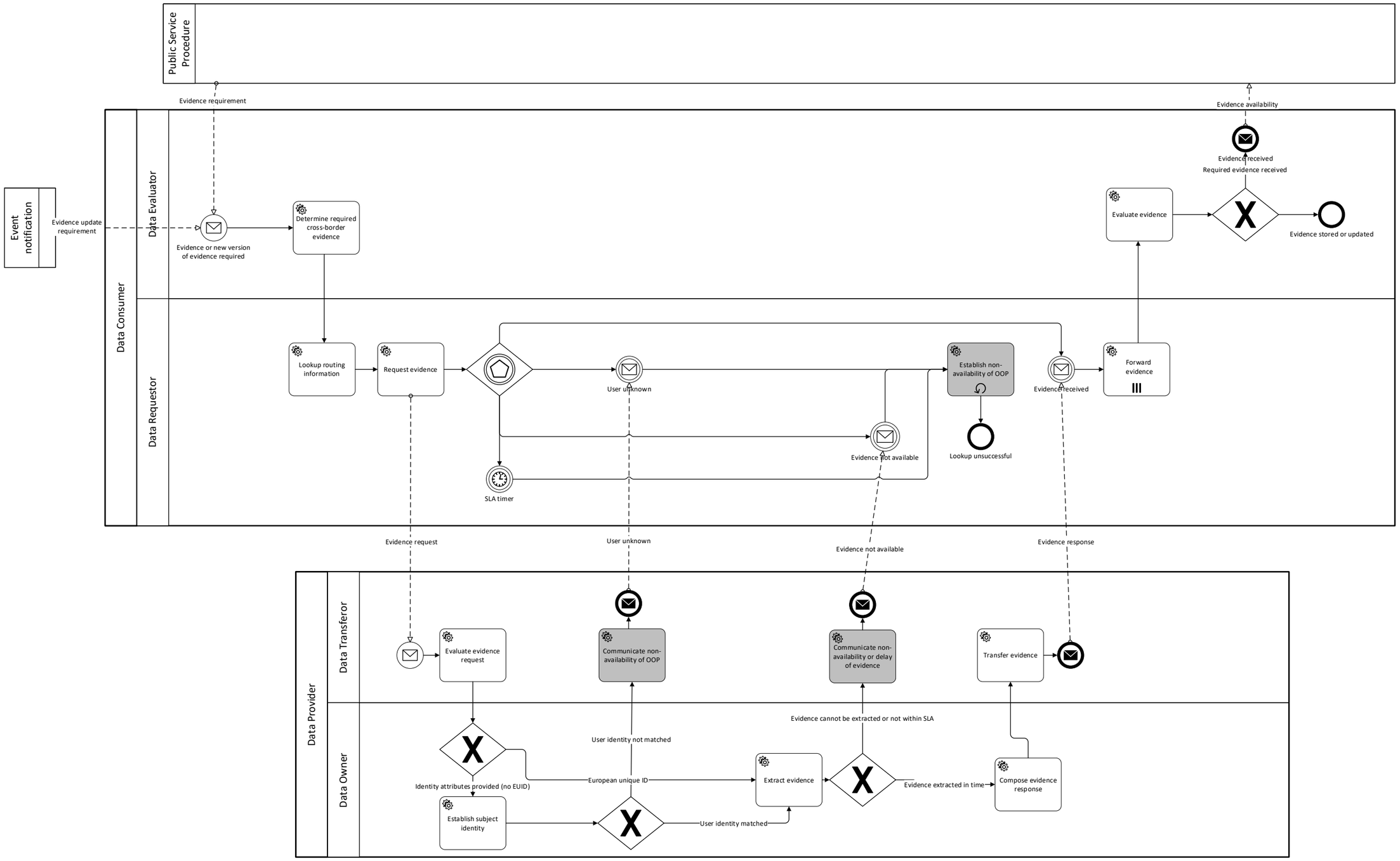


© 870635 DE4A Project Partners

Annex 5 Business Process Collaboration View of the Notification Process



Annex 6 Evidence Lookup Business Process Collaboration



© 870635 DE4A Project Partners