D2.4 Project Start Architecture (PSA) – First iteration

Document Identification			
Status	Final	Due Date	30/06/2020
Version	2.3	Submission Date	30/10/2020

Related WP	WP2	Document Reference	D2.4
Related Deliverable(s)	D2.1	Dissemination Level (*)	PU
Lead Participant	MINBZK/ICTU	Lead Author	Harold Metselaar (MINBZK/ICTU)
Contributors	Alexander Bielowski (MinBZK/ICTU), Alberto Crespo (ATOS), Mavi Cristache (MINBZK/ICTU), Syed Iftikhar Hussain Shah (IHU), Ivar Vennekens (RVO), Malin Norlander (BOLAGSVERKET), Carl-Markus Piswanger (BRZ), Christoph Zehetner (BRZ),	Reviewers	Gérard Soisson (CTIE) Sven Rostgaard Rasmussen (DIGST)

	Thashmee Karunaratne (DSV), Muhamed Turkanović (UM), Martina Šestak (UM), Tanja Pavleska (JSI), Ana Rosa Guzmán Carbonell (SGAD), Miro Lozej (MPA), Philipp Shevtchenko (BOSA), Ignacio Gonzalez (ATOS), Tomaž Klobučar (JSI), José Antonio Eusamio (MPTFP-SGAD), Blaž Podgorelec (UM), Patrick Öberg (Skatteverket)		

Keywords:
Project Start Architecture, PSA, Once-Only Technical System, Interaction Patterns, ABB, SBB, Building Blocks

List of Contributors	
Name	Partner
Alberto Crespo Garcia	ATOS
Alexander Bielowski	MINBZK/ICTU
Ana Rosa Guzmán Carbonell	MPTFP-SGAD
Blaž Podgorelec	UM
Carl-Markus Piswanger	BRZ
Christoph Zehetner	BRZ
Harold Metselaar	MINBZK/ICTU
Ignacio Gonzalez Fernandez	ATOS
Ivar Vennekens	RVO
José Antonio Eusamio	MPTFP-SGAD
Malin Norlander	BOLAGSVERKET
Martina Šestak	UM

List of Contributors	
Name	Partner
Mavi Cristache	MINBZK/ICTU
Miro Lozej	MPA
Muhamed Turkanović	UM
Patrick Öberg	SU/SKV
Philipp Shevtchenko	BOSA
Syed Iftikhar Hussain Shah	IHU
Tanja Pavleska	JSI
Thashmee Karunaratne	SU
Tomaž Klobučar	JSI

Document History			
Version	Date	Change editors	Changes
0.01	07/04/2020	Harold Metselaar (MinBZK/ICTU)	Initial version of document
0.02	14-4-2020	Harold Metselaar (MinBZK/ICTU)	Added mediation interaction pattern
0.03	17/04/2020	Alexander Bielowski (MinBZK/ICTU)	Process identification and variation
0.04	24/04/2020	Alexander Bielowski (MinBZK/ICTU)	
0.05	29/04/2020	Alexander Bielowski (MinBZK/ICTU)	Update of the 4.2 Addition of 2.3
0.06	11/06/2020	Alexander Bielowski (MinBZK/ICTU)	Aligned TOC with planning, Extension of 2.3 Update of 4.2
0.1	14/06/2020	Alexander Bielowski (MinBZK/ICTU)	Some cleaning of document Section descriptions as guidance
0.11	17/06/2020	Harold Metselaar (MinBZK/ICTU) Alexander Bielowski (MinBZK/ICTU)	Added process realization and application collaboration diagrams and tables Started List of Abbreviations
0.12	19/06/2020	Harold Metselaar (MinBZK/ICTU)	Editorial Released as v0.2
0.3	26/6/2020	Ivar Vennekens (RVO),	Incorporated inputs DBA pilot

Document History			
Version	Date	Change editors	Changes
		Malin Norlander (BVE)	
0.3	26/6/2020	Syed Iftikhar Hussain Shah (IHU)	Incorporated inputs semantic SBBs
0.3	26/6/2020	Ivar Vennekens (RVO)	Incorporated inputs SBBs
0.31	1/7/2020-2/7/2020	Alexander Bielowski (MinBZK/ICTU)	Added User-supported Intermediation pattern Further edits on Interdisciplinary questions
0.32	3/7/2020	Harold Metselaar (MinBZK/ICTU)	Editorial
0.32	3/7/2020	Carl-Markus Piswanger (BRZ), Christoph Zehetner (BRZ)	Incorporated inputs SBBs TOOP
0.32	3/7/2020	Muhamed Turkanović (IHU), Martina Šestak (IHU)	Incorporated inputs SBBs blockchain/VC
0.33	3/7/2020	Syed Iftikhar Hussain Shah (IHU), Ana Rosa Guzmán Carbonell (SGAD), Miro Lozej (MPA), Thashmee Karunaratne (SU)	Incorporated summary of semantic solution (section 3.4)
0.4	3/7/2020	Mavi Cristache (MINBZK/ICTU)	Version for internal release
0.41	3/7/2020-5/7/2020	Alexander Bielowski (MinBZK/ICTU)	Addition of business process collaboration views for the user-supported intermediation and verifiable credential pattern Edits on interdisciplinary questions Some transitional texts and descriptions in 4.2
0.42	09/07/2020	Harold Metselaar (MinBZK/ICTU)	Incorporated BB assessments
0.42	09/07/2020	Malin Norlander (BOLAGSVERKET),	Incorporated initial architecture log DBA
0.42	09/07/2020	Muhamed Turkanović (UM)	Updated business process collaboration views for the verifiable credential pattern
0.43	10/07/2020	Tanja Pavleska (JSI)	Added first draft introduction BB assessment

Document History			
Version	Date	Change editors	Changes
0.43	10/07/2020	Harold Metselaar (MinBZK/ICTU)	Added first version of process realization and application collaboration diagrams and tables for User Supported Intermediation
0.5	13/7/2020	Mavi Cristache (MINBZK/ICTU)	Version for internal release
0.51	17/07/2020	Philipp Shevtchenko (BOSA)	Incorporated assessed SBBs
0.52	17/07/2020	Syed Iftikhar Hussain Shah (IHU) Ana Rosa Guzmán Carbonell (SGAD), Miro Lozej (TBD), Thashmee Karunaratne (DSV)	Revised summary semantic solution, section 3.4
0.53	17/07/2020	Harold Metselaar (MinBZK/ICTU)	Improved section 4.2.3, added tables data objects Improved section 4.3.3, completed AS descriptions Editorial
0.54	17/07/2020	Ignacio Gonzalez Fernandez (ATOS)	Incorporated assessed SBBs.
0.6	17/07/2020	Mavi Cristache (MINBZK/ICTU)	Version for internal release
0.61	20/07/2020	Tomaž Klobučar (JSI)	Incorporated inputs SA pilot
0.62	20/07/2020	Harold Metselaar (MinBZK/ICTU)	Editorial
0.63	24/07/2020	Blaž Podgorelec (UM), Muhamed Turkanović (UM), Alexander Bielowski (ICTU)	Updated sections 0 and 4.6.2, Verifiable Credential interaction pattern
0.64	24/07/2020	José Antonio Eusamio (MPTFP-SGAD)	First version section 5, Business Risk Register
0.65	24/07/2020	Harold Metselaar (MinBZK/ICTU)	Populated sections 4.6.3 and 4.6.4 with ArchiMate drawings and placeholders for tables Editorial
0.7	24/07/2020	Mavi Cristache (MINBZK/ICTU)	Version for internal release

Document History			
Version	Date	Change editors	Changes
0.71	28/07/2020 – 29/07/2020	Harold Metselaar (MinBZK/ICTU)	Section 1.1 Sections 4.2.3 and 4.3.3, updated ArchiMate diagrams intermediation pattern and USI pattern, AS and Application component descriptions
0.72	29/07/2020 – 31/07/2020	Alexander Bielowski (MinBZK/ICTU)	Updated sections 4.3.1, 4.3.2, 4.2.1 and 4.2.2 Updated section 2.3 Interdisciplinary Questions
0.73	30/07/2020	Harold Metselaar (MinBZK/ICTU)	Updated section 4.2.4 and 4.2.4: added texts for application collaboration diagrams
0.74	30/07/2020	Ivar Vennekens (RVO)	Updated section 7 (revision) Added SBBs for Intermediation pattern
0.75	31/07/2020	Blaž Podgorelec (UM), Muhamed Turkanović (UM)	Updated section 4.6 VC pattern
0.76	31/07/2020	Tanja Pavleska (JSI)	Revised sections of chapter
0.77	31/07/2020	José Antonio Eusamio (MPTFP-SGAD)	Updated chapter 5
0.78	31/07/2020	Harold Metselaar (MinBZK/ICTU)	Editorial
0.8	31/07/2020	Mavi Cristache (MINBZK/ICTU)	Editorial Version for internal release
0.81	03/08/2020	Alexander Bielowski (MinBZK/ICTU)	Updated section 2.3 Interdisciplinary Questions
0.82	03/08/2020	Tanja Pavleska (JSI), Harold Metselaar (MinBZK/ICTU)	Update sections 9.1-9.4
0.83	04/08/2020	Alexander Bielowski (MinBZK/ICTU), Harold Metselaar (MinBZK/ICTU), Mavi Cristache (MINBZK/ICTU)	Section 2.1 First draft executive summary Updates eProcedure application collaboration Section 3.1 Section 10 Incorporated feedback (IHU, RVO, BRZ), section 9.3 Editorial
0.84	04/08/2020	Ignacio Gonzalez Fernandez (ATOS)	First draft section 3.3 Trust Model
0.85	05/08/2020	Harold Metselaar (MinBZK/ICTU),	Incorporated feedback (MPTFP-SGAD), section 9.3

Document History			
Version	Date	Change editors	Changes
		Alexander Bielowski (MinBZK/ICTU)	Executive Summary
0.86	06/08/2020	Blaž Podgorelec (UM)	Update section 4.6 Verifiable Credentials
0.87	06/08/2020	Harold Metselaar (MinBZK/ICTU), Alexander Bielowski (MinBZK/ICTU)	Walkthrough document Finalizing Update section 4.6 Verifiable Credentials Section 2.2 Relation to the Once-Only Technical System Editorial
0.88	07/08/2020	Harold Metselaar (MinBZK/ICTU), Tanja Pavleska (JSI), José Antonio Eusamio (MPTFP-SGAD), Ignacio Gonzalez Fernandez (ATOS)	Finalized section 9 Updated section 5 Business Risk Register Finalized section 3.3 Editorial
0.9	07/08/2020	Harold Metselaar (MinBZK/ICTU)	Version for internal review
0.91	24/8/2020-25/08-2020	Harold Metselaar (MinBZK/ICTU), Alexander Bielowski (MinBZK/ICTU)	Merged feedback Processing feedback Accepted minor changes Closed some comments Editorial
0.92	25/08/2020	Ivar Vennekens (RVO)	Updated chapter 7
0.93	26/08/2020	Harold Metselaar (MinBZK/ICTU), Alexander Bielowski (MinBZK/ICTU)	Updated section 1.1 Updated section 2.3 Interdisciplinary Questions Updated section 4 Reference Interaction Patterns
0.94	27/08/2020	Ignacio Gonzalez Fernandez (ATOS)	Updated section 3.3 Trust Model
0.95	27/08/2020	Martina Šestak UM), Blaž Podgorelec (UM)	Completed descriptions of chapter 4.6 Verifiable Credentials

Document History			
Version	Date	Change editors	Changes
0.96	27/08/2020	Alexander Bielowski (MinBZK/ICTU)	Updated sections 2.1 Functional Scope of the DE4A Pilots, 2.2 Relation to the Once-Only Technical System and 10 Conclusion
0.97	28/8/2020	Harold Metselaar (MinBZK/ICTU), Tanja Pavleska (JSI)	Final tweak section 9.3
0.98	28/8/2020	Ana Rosa Guzmán Carbonell (SGAD), Thashmee Karunaratne (DSV)	Update of section 3.4
0.99	28/8/2020	Harold Metselaar (MinBZK/ICTU)	Cleaned up version for QA
1.0	31/08/2020	Julia Wells, Ana Piñuela (ATOS)	Quality check for approval and submission
1.10	07/09/2020	Harold Metselaar (MinBZK/ICTU),	Re-put content for SA and MA Pilots
1.11	11/09/2020	Harold Metselaar (MinBZK/ICTU)	Added section 3.2 generic application services
1.12	14/09/2020	Harold Metselaar (MinBZK/ICTU)	Added section 3.2 generic application components
1.13	15/09/2020	Tomaž Klobučar (JSI)	Update and completion of chapter 6 Studying Abroad Pilot
1.14	15/09/2020	Patrick Öberg (SU/SKV)	Update and completion of chapter 8 Moving Abroad Pilot
1.15	15/09/2020	José Antonio Eusamio (MPTFP-SGAD)	Update chapter 5 Business Risk Register
1.16	16/09/2020	Mavi Cristache (MINBZK/ICTU)	Editorial
1.17	16/09/2020	Tanja Pavleska (JSI)	Update chapter 9 Building Blocks
1.18	16/09/2020	Harold Metselaar (MinBZK/ICTU)	Editorial Updated Executive Summary and sections 1 Introduction and 10 Conclusions
1.19	16/09/2020	Harold Metselaar (MinBZK/ICTU)	Version for internal delta-review
1.20	06/10/2020	Harold Metselaar (MinBZK/ICTU)	Updated section 3.2
1.21	08/10/2020	Harold Metselaar (MinBZK/ICTU)	
1.22	09/10/2020	Tomaž Klobučar (JSI)	Updated chapter 6 Studying Abroad Pilot

Document History			
Version	Date	Change editors	Changes
1.23	09/10/2020	José Antonio Eusamio (MPTFP-SGAD)	Updated chapter 5 Business Risk Register
1.24	09/10/2020	Patrick Öberg (SU/SKV)	Updated chapter 8 Moving Abroad Pilot
1.25	09/10/2020	Harold Metselaar (MinBZK/ICTU)	Cleaned up version for QA
1.26	27/10/2020	Julia Wells (Atos)	QA of updated sections: executive summary, Introduction (1), 3.2, chapters 5,6,8, 9, Conclusions (10)
2.0	28/10/2020	Ana Piñuela Marcos (ATOS)	Approval for resubmission
2.1	14/01/2021-22/01/2021	Alexander Bielowski (MinBZK/ICTU), Harold Metselaar (MinBZK/ICTU)	Incorporating review comments Commission: • Added appendix for BPMN diagrams for improved readability • Update Ch9 in order to explain more clearly that recommended BBs are not mandatory but can be considered.
2.2	8/02/2021-19/02/2021	Alexander Bielowski (MinBZK/ICTU) Thashmee Karunaratne (DSV)	Update of section 3.4.2
2.3	01/03/2021	Alexander Bielowski (MinBZK/ICTU) Mavi Cristache (MINBZK/ICTU)	Final editorial changes and formatting for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Alexander Bielowski (MinBZK/ICTU)	09/10/2020
Quality manager	Julia Wells (ATOS)	27/10/2020
Project Coordinator	Ana Piñuela Marcos (ATOS)	28/10/2020

Table of Contents

Table of Contents 10
List of Tables 13
List of Figures 15
List of Acronyms 17
Executive Summary 18
1 Introduction 20
1.1 Purpose of the document 20
1.2 Structure of the document 21
2 Background 22
2.1 Functional Scope of the DE4A Pilots 22
2.2 Relation to the Once-Only Technical System 23
2.3 Interdisciplinary Questions 25
2.3.1 Orchestration / Choreography 25
2.3.2 Multiple, complementary, overlapping or conflicting evidence equivalents 25
2.3.3 Interrupted vs. Uninterrupted exchange 26
2.3.4 Explicit request and transitivity between actors 26
2.3.5 Preview & Approval UI 26
2.3.6 Identity and Record Matching 26
2.3.7 Transitivity of user identity 27
2.3.8 Hand-on of UI between actors 27
2.3.9 Mandate and Proxy 27
2.3.10 Encryption Gap 27
2.3.11 Structured data vs. unstructured data 28
2.3.12 Automated re-use of data 28
2.3.13 Production system and real-life cases 28
2.3.14 EESSI integration 29
2.3.15 BRIS integration 29
2.3.16 eIDAS and national authentication systems 29
2.3.17 Non-notified eIDs 29
2.3.18 Payment for evidence 30
2.3.19 Trust Management 30
2.3.20 Legal validity or SSI and block chain technology 30
2.3.21 Explicit scope of Article14 30
2.3.22 Matching evidences between Member States 31
3 Generic Architecture Building Blocks 32
3.1 Introduction 32
3.2 Common Application Services and Components 32
3.2.1 Common Application Services 32
3.2.2 Common Components 36

3.3 Trust Model 40
3.3.1 Intermediation and user-supported intermediation patterns 41
3.3.2 Verifiable credentials pattern 42
3.4 Semantic Solution 43
3.4.1 Availability and usability of semantic standards 43
3.4.2 Evidence type translation and approaches 47
4 Reference Interaction Patterns 51
4.1 Scope and Process Identification 51
4.2 Intermediation 52
4.2.1 Working Hypothesis and Implementation Principles 52
4.2.2 Business Process Collaboration 55
4.2.3 Process Realisation 63
4.2.4 Application Collaboration 69
4.3 User-supported Intermediation 81
4.3.1 Working Hypothesis and Implementation Principles 81
4.3.2 Business Process Collaboration 83
4.3.3 Process Realization 91
4.3.4 Application Collaboration 96
4.4 Subscription and Notification 103
4.5 Lookup 103
4.6 Verifiable Credentials 104
4.6.1 Working Hypotheses and Implementation Principles 104
4.6.2 Business Process Collaboration 106
4.6.3 Process Realization 113
4.6.4 Application Collaboration 120
5 Business Risk Register 134
6 Studying Abroad Pilot 137
6.1 Selection of interaction patterns 137
6.1.1 Use case #1: Application to public higher education 137
6.1.2 Use case #2: Applying for study grant 138
6.1.3 Use case #3: Diploma/certs/studies/professional recognition 138
6.2 Implications and exceptions to principles 139
6.3 Candidate Solutions and Building Blocks 140
6.3.1 User-supported intermediation pattern 140
6.3.2 Verifiable credentials pattern 144
7 Doing Business Abroad Pilot 148
7.1 Selection of interaction patterns 148
7.1.1 Use case #1: Starting a business in another member state 148
7.1.2 Use case #2: Doing business in another member state 150
7.2 Implications and exceptions to principles 151
7.3 Candidate Solutions and Building Blocks 154

7.3.1 Intermediation pattern 154
7.3.2 Lookup pattern 158
7.3.3 Subscription and notification pattern 158
8 Moving Abroad Pilot 159
8.1 Architectural Drivers & Requirements 159
8.2 Use Case #1: Request address change 161
8.3 Use case #2: Request an extract or copy of civil state certificate 163
8.4 Use case #3: Request Pension Information – Claim Pension 165
8.5 Interaction Pattern Selection 169
8.5.1 User-Supported-Intermediation Pattern 169
8.6 Implications and exceptions to principles 172
8.7 Candidate Solutions and Building Blocks 173
9 Building Blocks 177
9.1 Introduction 177
9.2 Theoretical background 177
9.2.1 Objectives and scope 177
9.2.2 Available methodologies 177
9.2.3 Methodological considerations 180
9.3 Methodology 180
9.3.1 Conceptual framework 180
9.3.2 Empirical framework 184
9.3.3 Recommendations and Gap Analysis 185
9.4 Summary 191
9.5 TOOP Infrastructure and Functionalities 191
9.5.1 Overview on the TOOP 191
9.5.2 TOOP Solution Architecture 192
9.5.3 Criterion Evidence Type Rule Base (CERB) 193
9.5.4 Data Service Directory (DSD) 193
9.5.5 SMP/SML and BDXL (eDelivery) 194
9.5.6 TOOP Exchange Data Model (EDM) 194
9.5.7 TOOP Connector (TC) 195
9.5.8 TOOP Gateway (AS4) 196
9.5.9 TOOP Testing Tools 196
9.5.10 TOOP pilots 197
9.5.11 Recommendation on TOOP re-use capabilities 197
10 Conclusions 199
References 204
Appendix 207

List of Tables

Table 1: Common Application Services 32
Table 2: Common Application components 36
Table 3: Mapping of requirements to the semantic assets 44
Table 4: High-level comparison of criteria-based and evidence-based approach 48
Table 5: Intermediation pattern working hypotheses and implementation principles 52
Table 6: Business Activities of the Intermediation Pattern 57
Table 7: Intermediation - Conversation between User and Data Consumer 62
Table 8: Intermediation - Conversation between Data Consumer and Data Provider 63
Table 9: Application Services of the Intermediation Pattern 67
Table 10: Application Components of the eProcedure Portal 71
Table 11: Data objects eProcedure Portal 71
Table 12: Application Components of the Information Desk 73
Table 13: Data objects Information Desk 73
Table 14: Application components of Evidence Interchange Management 75
Table 15: Application components of Trust Architecture 76
Table 16: Data objects Trust Architecture 77
Table 17: Application components of Data Logistics 78
Table 18: Application components of Evidence portal 79
Table 19: Data objects Evidence portal 79
Table 20: Application components of Evidence retrieval 80
Table 21: Data objects Evidence Retrieval 81
Table 22: User-supported Intermediation pattern working hypothesis and implementation principles 81
Table 23: Business Activities of the User-Supported Intermediation Pattern 84
Table 24: User-Supported Intermediation - Conversation between User and Data Consumer 89
Table 25: User-Supported Intermediation - Conversation between Data Consumer and Data Provider 90
Table 26: User-Supported Intermediation - Conversation between User and Data Provider 90
Table 27: Application Services of the User Supported Intermediation Pattern 93
Table 28: Application components of the Evidence Portal 98
Table 29: Data objects Evidence portal 99
Table 30: Application components of Evidence Interchange Management 99
Table 31: Application Components Trust Architecture 101
Table 32: Data objects Trust Architecture 101
Table 33: Verifiable Credentials pattern working hypothesis and implementation principles 104
Table 34: Business Activities of the Verifiable Credential Pattern 108
Table 35: Verifiable Credentials Pattern Conversations 112
Table 36: Application Services of the Verifiable Credentials Pattern 116
Table 37: Application components of Authority agent 121
Table 38: Data objects of Authority agent 121
Table 39: Application components of User agent 122
Table 40: Data objects of User agent 123
Table 41: Application components of eProcedure Portal 125
Table 42: Data objects of eProcedure portal 126
Table 43: Application components of Evidence Portal 128
Table 44: Data objects of Evidence portal 128
Table 45: Application components of Evidence Retrieval 129

Table 46: Data objects of Evidence Retrieval 129
Table 47: Application components of Information Desk 131
Table 48: Data objects of Information Desk 131
Table 49: Application components of Trust architecture 133
Table 50: Data objects of Information Desk 133
Table 51: Business Risk Register 135
Table 52: Architecture log SA 139
Table 53: SBBs for User-supported Intermediation Pattern 140
Table 54: SBBs for SA Verifiable Credentials Pattern 144
Table 55: DBA UC1 in context 150
Table 56: DBA UC2 in context 151
Table 57: Architecture log DBA 151
Table 58: SBBs for DBA Intermediation Pattern 155
Table 59: Architecture log Moving Abroad (MA) 173
Table 60 SBBs for the Moving Abroad Pilot Use Cases 1 and 2 173
Table 61 Conceptual BB assessment framework 183
Table 62: BB recommendations 185
Table 63: Process Steps TOOP infrastructure components 192

List of Figures

Figure 1 Intermediation and user-supported intermediation patterns trust architecture 41
Figure 2 Detail of trust persistent storage components 42
Figure 3: Evidence location and distribution 50
Figure 4 Business Process Collaboration view of the Intermediation Pattern 56
Figure 5 Process Realization of the User Process 64
Figure 6 Process Realization of the DC Process 65
Figure 7: Process Realization of the DP Process 66
Figure 8: eProcedure Portal 70
Figure 9: Information Desk 72
Figure 10: Evidence Interchange Management 74
Figure 11: Trust Architecture 76
Figure 12: Data Logistics 78
Figure 13: Evidence portal 79
Figure 14: Evidence Retrieval 80
Figure 15: Business Process Collaboration view of the User-Supported Intermediation Pattern 84
Figure 16: Process Realization of the User process 91
Figure 17: Process Realization of the Data Consumer process 92
Figure 18: Process Realization of the Data Provider Process 93
Figure 19: eProcedure Portal 97
Figure 20: Evidence Portal 98
Figure 21: Evidence Interchange Management 99
Figure 22: Trust Architecture 100
Figure 23: Data Logistics 102
Figure 24: Evidence Retrieval 103
Figure 25: Business Process Collaboration view of the Verifiable Credential Pattern 107
Figure 26: Process Realization of the User Process 114
Figure 27: Process Realization of the Data Consumer Process 115
Figure 28: Process Realization of the Data Provider Process 116
Figure 29: Authority agent 120
Figure 30: User agent 122
Figure 31: eProcedure Portal 124
Figure 32: Evidence Portal 127
Figure 33: Evidence Retrieval 128
Figure 34: Information Desk 130
Figure 35: Trust Architecture 132
Figure 36 DBA UC1 in context 149
Figure 37: DBA UC2 in context 151
Figure 38 -BPM Model, Request address change 163
Figure 39 -– BPM Model, Request an extract or copy of civil state certificate 165
Figure 40 -– BPM Model, Request pension information 167
Figure 41 – BPM Model, Claim pension 169
Figure 42: Taxonomy of Building Blocks 182
Figure 43 (and figure 44) Taxonomy of assessed BBs with their recommendations 189
Figure 44 189
Figure 45. EAAF Maturity levels 190
Figure 48 Overview on CEF eDelivery 192
Figure 49 TOOP EDM 195

Figure 50 TOOP System Overview (2 different implementations) 196
Figure 51 Intermediation pattern 207
Figure 52 User supported intermediation pattern 208
Figure 53 Verifiable Credential Pattern 209

List of Acronyms

Abbreviation / acronym	Description
ABB	Architecture Building Block
ADMS	Asset Description Metadata Schema
AS	Application Service
BB	Building Block
BRIS	Business Register Interconnection System
CCCEV	Core Criteria and Core Evidence Vocabulary
CETRB	Criterion and Evidence Type Rule Base
CRUD	Create Read Update Delete
DBA	Doing Business Abroad – one of the three DE4A pilots
DC	Data Consumer
DE	Data Evaluator
DE4A	Digital Europe for All
DO	Data Owner
DoA	Description of Action
DP	Data Provider
DR	Data Requestor
DSI	Digital Service Infrastructure
DT	Data Transferor
Dx.y	Formal Deliverable x.y
EESSI	Electronic Exchange of Social Security Information
MA	Moving Abroad – one of the three DE4A pilots
MS	European Union Member State(s)
MVP	Minimal Viable Product
OOTS	Once-Only Technical System
PSA	Project Start Architecture
SA	Studying Abroad – one of the three DE4A pilots
SBB	Solution Building Block
SEMPER	Secure Electronic Marketplace for Europe
TBP	To Be Provided
TL	Task Leader
Tn.m	Task n.m
TOOP	The Once Only Principle
U	User
USI	User Supported Intermediation
VC	Verifiable Credential
VP	Verifiable Presentation
WP	Work Package

Executive Summary

The Project Start Architecture (PSA) provides a starting point and guidance to the three DE4A pilots, which 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 to WP3 - Semantic Interoperability Solutions and WP5 – Common Components Design & Development that will develop common components and semantic solutions for them. In parallel to this project, the SDGR [3] creates in Article 14 the basis for the first truly cross-domain Once-only Technical System on European level. The preparations for the implementation of the Once-only Technical System is well under way, led by the CEF Preparatory Action on Once-Only. Consequently, more direct contribution of DE4A to this endeavour is of high interest for internal and external stakeholders with continued alignment efforts geared to this effect. The scoping of the DE4A pilots and the reference interaction patterns in this PSA show some focussed on SDG use-cases and the OOP principle while extending to additional interoperability requirements expressed by the participating Member States (MS) and the investigation of the potential of innovative block-chain technology. This is in line with the DoA (Description of the Action contractual document). The PSA uses a structured architecture definition approach and provides guidance on 22 interdisciplinary questions (section 2.3) concerning the exchange of evidence.

WP2 Architecture Vision and Framework provides a central structure to the overall project, which sets the Pilots in context to each other and to the generic reference interaction patterns. The PSA builds on the insights provided by deliverables D1.1 – Member state eGovernment Baseline, D1.3 Member state Once Only and data strategy Baseline, D1.5 - Baseline EU Building Blocks supporting Once Only and standard data sharing patterns and D3.1 - Initial requirements for semantic assets and is fundamentally based on the requirements expressed in D4.1, D4.5 and D4.9 – Use case definition and requirements of the Studying Abroad (SA), Doing Business Abroad (DBA) and Moving Abroad (MA) pilots respectively. Close cooperation with T2.2 and WP3 additionally yielded preview summaries of deliverable D2.2 – Initial DE4A Trust Management Models and D3.3 Semantic framework Initial version that are included as sections 3.3 and 3.4. As external input, the Once-Only Technical System High Level Architecture and the insights gained during the participation in SDG Coordination group, SDG working group meetings as well as bilateral alignment meetings with the CEF Preparatory Action, TOOP [18], BRIS [19], EESSI [20], ESSIF and EBSI [21] must be mentioned.

The reference architecture description on conceptional/functional level (3 and 4) is brought together with a catalogue and quick scan assessment of candidate Building Blocks (BB) mapped to required Application Services that they are intended to deliver in the context of each pilot. Gaps are identified that need common components and semantic solutions to be developed by WP5 and WP3 respectively. This is extended with the initial architecture logs of the three pilots that provide additional guidance in terms of implications and exceptions to the DE4A Derived Principles [6].

The main results/finds of this PSA are manifold:

1. Interdisciplinary topics: As a result of the structured architecture analysis and from numerous external interactions and sources stated above, 22 main interdisciplinary questions are identified, and preliminary guidance is provided in terms of working hypotheses linked to architectural choices. Different interaction patterns require different hypotheses to be true, which helps to focus the discussion and is expected to contribute also to the consensus building in context of the SDG.
2. Identification of business risks and mitigation: Business risks, both functional and operational that are related to the four interoperability dimensions (legal, organisational, semantic and technical) are collected, for the DE4A project scope.
3. Elicitation of several interaction patterns and their application to the pilot use-cases:

In this version of the PSA three interaction patterns are elaborated: Intermediation, User supported Intermediation (USI) and Verifiable Credentials (VC). An extended version of the PSA (expected to be published early 2020) will contain additionally the Subscription/Notification and the Lookup patterns identified in D2.1 Architecture Framework [6] and especially relevant for DBA.

4. In close cooperation with the Pilots their uses cases are matched to the patterns for best fit to their specific requirements. The current choice hinges on some working hypotheses that are still under discussion, especially pertaining to the Explicit request and transitivity between actors (section 2.3.4). The mapping is hence not yet final:
    a. Doing Business Abroad: Intermediation, Subscription/Notification and Lookup pattern
    b. Studying Abroad [preliminary choice]: User-supported Intermediation (USI) and Verifiable Credential (VC) pattern
    c. Moving Abroad [preliminary choice]: USI pattern
5. The pattern choice per pilot is motivated considering the specific pilot requirements and contrasted with the derived principles set out in D2.1 Architecture Framework thereby populating an initial version of the Architecture logs.
6. An initial selection of Solution Building Blocks completes the start architecture for the Pilots. The BB assessment and the Pilot's choice of SBBs uncovers gaps and will feed into WP3 - Semantic Interoperability Solutions and WP5 - Common Component Design & Development.
7. BB assessment, methodology and framework: The suitability of the BBs identified and catalogued in Task 1.5 are assessed for use within the DE4A project. Different existing methodologies were considered and the Enterprise Architecture Assessment Framework (EAAF) selected. The overall methodology requires a phased approach. In the PSA the first phase takes stock of the entire list of BBs that can have potential use in the project and as part of the piloting. A conceptual and an empirical framework for evaluation is developed in preparation of task T2.4 – Service interoperability solutions toolbox.
   For the conceptual framework we adopt CEFs Digital Services Model (DSM) and its taxonomy for categorizing BBs. This enables the gap analysis of the BBs. The empirical framework is essentially an implementation of the conceptual framework. It allows for qualitative and comparative analysis of the BBs, as well as extraction of concrete recommendations for piloting. The methodology and framework are meant to be generic and can be used by other Large-Scale Pilots and implementation projects in the future.

The structured architecture development approach and the interdisciplinary PSA process yielded robust initial guidance on the 22 main questions identified. The detailed reference interaction patterns are found to be a good fit for the use-cases of our pilots, which were selected from the life events of Annex II of the SDGR [3]. The Intermediation pattern and its extension/variant - the USI pattern - appear to be largely aligned with the legal requirements of Article 14, whereas the VC pattern is geared towards the use of Block-chain technology for evidence exchange and less relevant for the SDGR - context.

Finally, as preliminary conclusion, the available BBs on European level appear to provide a solid basis to build from, e.g. eIDAS and eDelivery incl. SMP/SML/BDXL. Also, the reuse of results from TOOP and SEMPER look promising.

1 Introduction

1.1 Purpose of the document

The main goal of the document is to define the starting point for the three DE4A Pilots (WP4) and provide architectural guidance for the Pilot implementations. 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. It is a living document in so far that the underlying project task will continue to provide guidance alongside the technical work packages and document further insights in an architecture log. D2.5 (M18 – June 2021) will consolidate these insights in an updated, public deliverable as starting point of the second pilot iteration.

This document follows the Architecture Framework proposed in D2.1 [6] and contributes content to this framework to be 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 [2] and ArchiMate [1] 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 processing with a focus on the OOP exchange of evidence and are the central communication views for stakeholder alignment. Process Realisation 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 Application Service classification is aligned with EIRA and is expected to become a major input to the Portfolio Backlog of the technical work packages (e.g. T5.1 Consolidation of Features and Patterns). Each Application Service is realised by an Application Collaboration, which in terms is worked out in an Application Collaboration view, comprised of interacting Application Components and Interfaces. These views are meant as bridge to and as initial context for the specification of the Pilot solutions.

An initial list of existing and emerging Building BBs together with a methodology and assessment framework is presented. DE4A performed a first assessment of the BBs (see chapter 9) as an preliminary input to common component development (cf. WP5) and as basis for the pilot specific mapping of Application Services to Solution Building Blocks in chapters 6, 7 and 8. It is in the nature of the PSA that this mapping is an expression of intent, a starting point for the solution development for the Pilots.

The basis of this mapping is the choice of the best-fit interaction pattern per pilot use case, internally often called “pattern matching”. Even though extended discussion went into this matching, no complete consensus was reached between all participating Member States, hinging on a number of underlying working hypotheses.

Furthermore, per pilot a response (“Comply or explain”) to the architecture principles from [6] is given. This can be considered a first version of the Architecture Log and is a means to uncover and document barriers to interoperability. In addition to the future lesson learned 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

Chapter 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 required. Chapter 3 and 4 constitute the DE4A reference architecture with special attention to semantics (3.4) and (technical) trust management (3.3). Chapter 5 contains the Business Risk Register. Chapters 6,7 and 8 apply the reference architecture and principles to the Pilots' specific context and relate it to candidate Building Block (BB). A quick scan assessment of these BB is provided as chapter 9. Please see below an overview of the contents of each of the 10 chapter:

Chapter 1	–	Introduction to the Project Start Architecture
Chapter 2	–	Background, relation to the Once-Only Technical System, Functional Scope of the DE4A Pilots, relation to the Once-Only Technical System, Interdisciplinary Questions
Chapter 3	–	Generic Architecture Building Blocks, Common Application Services and Components, Trust Model, Semantic Solution
Chapter 4	–	This section contains the Reference Interaction Patterns used in the pilots. Per pattern the following topics are addressed: Working Hypothesis and Implementation Principles, Business Process Collaboration view, Process Realization view, and the Application Collaboration view.
Chapter 5	–	This section contains the Business Risk Register. It defines the main identified business risks of OOP, including probability, impact and mitigation options.
Chapter 5	–	Studying Abroad Pilot: choice of interaction pattern, initial Architecture Log and mapping to candidate Building Blocks (BB)
Chapter 6	–	Doing Business Abroad Pilot: choice of interaction pattern, initial Architecture Log and mapping to candidate BB
Chapter 5	–	Moving Abroad Pilot: choice of interaction pattern, initial Architecture Log and mapping to candidate BB
Chapter 9	–	This chapter deals with the within DE4A identified possible candidates for reuse in the shape of Building Blocks. This section explains the approach followed (methodology, taxonomy of BBs and framework used) and summarizes the results of the quick scan assessment of the candidates.
Chapter 10	–	Conclusions

2 Background

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 evidence exchange 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 EIF Building Blocks and extending OOP to fully online procedures in the context of Life Events in the SDGR, with citizens' and businesses 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 - 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 [6], and put them to the test of reality in real-life use cases already selected by the DE4A Member States. The pilots represent a secure, privacy-preserving and trustworthy realisation 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, organisational, semantic and technical-, with an analysis of governance models (together with WP6 'Sustainable Impact and new governance models'), thus enabling as well a deeper and better understanding of the roles and responsibilities 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 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, D4.5, D4.9 "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,

business persons 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, business persons 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 realisation.
- Support strategic EC & MS priorities (SDGR esp. Art.14, Tallinn Declaration, eGov Action Plan, DSM).

In order to realize each and 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, therefore designing and evaluating multiple service patterns is at the core of DE4A. Also, DE4A pilots projects 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 Article 14 entering into force on December 12th 2023) than the Once-Only Technical System (OOTS) for which the aforementioned Article forms constitutes its legal basis. This broader scope is especially valuable if considering that December 12th 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* [5].

Although this H2020 Action is not a formal part of the process of further specifying the SDG-Regulation [3], 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
- 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)
- 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/approve"

[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.

- Uncover detailed challenges, such as identity and record matching or cross-border transitivity of user identity 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 exploring of different aspects of the underlying trust model 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 [5] 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 realise OOP Technical System.*

DE4A takes the reality as its starting ground - the needs and the capacities of the Member States [5] 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 Implementing Act of 12th June 2021 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)[3].

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.

Legal and organisational 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 realise the OOP Technical System* [5] – 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* [5], while exploring *the transformative impact of new technologies such as blockchain* [16], 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.

2.3 Interdisciplinary Questions

This section introduces a number of interdisciplinary challenges 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 could be 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 4, using the DE4A architecture metamodel, and through the specification of implications and exceptions to the DE4A Principles specific to each of the three pilots in chapters 6, 7 and 8. The DE4A metamodel and DE4A Principles are part of the project deliverable D2.1 DE4A Architecture Framework [6].

Working hypotheses for the relevant topics are formulated in the sections of the different interaction patterns in chapter 4 (e.g.: 4.2 for the Intermediation Pattern.) and the in chapters 6, 7 and 8 for pilot specific considerations.

2.3.1 Orchestration / Choreography

The automated cross border exchange of evidence requires many actors and systems to collaborate in an orderly manner. 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 PD and several organisations in-between facilitating the exchange. In addition, we expect that a purely uninterrupted scenario might be too restrictive to cover the breadth of real-life scenarios.

2.3.2 Multiple, 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. 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.

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 have a mechanism to migrate the requested evidence on demand. Including this possibility would increase the volume of evidence that can be exchanged in the pilots.

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. At the moment it is not entirely clear 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. DE4A Legal Compliance Work Package has produced a White Paper on ‘Explicit Request’.

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 DP. We should consider the need for a user interface for the once-only technical system that is separate from the eProcedures form itself. DE4A Legal Compliance Work Package has produced a White Paper on ‘Preview of Evidence Exchanged’. Consensus on this point between Member States is not yet final and the PSA includes reference interaction pattern for all three cases: preview at the DC, the DP or the U.

2.3.6 Identity and Record Matching

This is the already reasonably well understood 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 eIDAS mandatory and in some cases the optional attributes. 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 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 Minimal Viable Product (MVP)) 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 above in 2.3.3.

2.3.7 Transitivity of user identity

This problem arises in the Intermediation Pattern, because the user first authenticates himself 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 can differ between Member States and can change over time).

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 same exceptions flow problematic as above applies (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.

2.3.8 Hand-on of UI 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 person. This is a complexing factor in the identification and OOP exchange of evidence that we cannot ignore. 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]), given among others the aging population of the Union. 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. 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 organisations that are separate entities or authorities from the Data Owners (DO) and Data Evaluators (DE). This is fully in line with the 4-corner model. 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. 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

In how far only structured or also unstructured data is to be supported by OOTS. 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 mid-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 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.

Unfortunately, this discussion is often combined 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. irreversible), it becomes apparent that enabling automated reuse of data is a major challenge across different MS.

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 standardisation and standardisation 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 are fully productive and 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) could also be investigated to alleviate this limitation and to substantiate a consensus on the interpretation of Article 14 (11).

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, ie. - Request Pension Information & Claim Pension, - both in regard to relevant authorities and to exchanged information. We will need to know early in the MS pilot whether some EESSI capabilities are to be reused. This reuse can reach 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 harmonised data models and definitions.

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 participating business registers, however, the possibility of DE4A to create legal and technical changes on the existing BRIS system is very limited. We will need to understand early in the business pilot whether some BRIS capabilities are to be reused or not in order to move the pilot along. Form and intensity can vary as stated above in section 2.3.14

2.3.16 eIDAS and national authentication systems

The question of user authentication in OOP centres around the user 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; Demark, Netherlands and Slovenia support only eIDAS IN.

2.3.17 Non-notified eIDs

Until now the pilots can only move to production with Member States that notified their eID only. 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 eID's might solve this issue to a certain extent. Further research is needed though. Austria, Slovenia, Romania and have not notified yet their identification scheme.

2.3.18 Payment for evidence

Some competent authorities charge fees for retrieving or issuing evidence. Pricing models usually cater for national data consumers, not for cross-border users. This could limit piloting real data in the production environment. 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 U and DP.

2.3.19 Trust Management

Consistent framework needed that provide trust services across the complete OOTS. Having several PKI 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.

Irrespective of the technical representation of trust relationships, there might also be an organisational 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)

2.3.20 Legal validity or SSI and block chain technology

There are several legal concerns around the applicability of Self-Sovereign Identity and Block-chain technology, such as the storage of personal data in on distributed ledgers or he validity of a decentral identifier. This led Spain to all but ban blockchain from application in eGovernment. By RDL 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). Presently these questions are not clear and 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.

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, with 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.

Fourth, the Once-Only Technical System High Level Architecture is in a 0.3 draft version and allows extensions. Starting with one pattern in 2020 might be a sensible choice, given the challenging timeline until 2023, but it should not be the only choice by design.

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]. 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 harmonised evidence types and corresponding schemas and definitions exist and domains without such prior harmonisation, which pose a much larger challenge. The approach for matching required evidences (DC side) and available evidences (DP side) could consequently also differ between harmonised and non-harmonised sectors. DE4A is currently working on designing different data models, services and components in the context of the Semantic Framework of WP3.

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 on-going efforts (e.g. EAR project, ENIC-NARIC Network) will be considered in the Studying Abroad Pilot.

3 Generic Architecture Building Blocks

3.1 Introduction

This chapter deals with generic aspects of the architecture, specifically with the Architecture Building Blocks (ABBs) that are encountered in the context of DE4A.

In section 3.2 the common application services and components that realise them are presented.

Section 3.3 contains the preliminary results from T2.2 Trust Management Models.

In section 3.4 some preliminary results from the Semantic Work Package (WP3) are presented. Availability and usability of standards is looked at and a mapping of the Pilot's semantic requirements to semantic assets is given. Two main evidence type translation and approaches are given: Criterion and Evidence Type Rule Base and Canonical Evidences.

3.2 Common Application Services and Components

This section lists the common application services and components. Common is understood as generic, i.e. used in more than one place.

3.2.1 Common Application Services

The table below (Table 1: Common Application Services) provides an overview of the common services encountered in DE4A. It considers all services as defined for all three patterns in chapter 4. A service is classified as "common" when it is used in two or more places and is referenced from in the tables listing the Application Services per pattern in chapter 4.

Table 1: Common Application Services

Application Service	Description	Application Component
1. 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.	Data Exchange Component
2. Evidence status overview	The DC updates the evidence status. This is supported by this service.	• Evidence interchange front-end • Online procedure portal back-end • Online procedure portal front-end
3. 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	Trust Service Provisioning Component

Application Service	Description	Application Component
	or logically associated with other data in electronic form and which is used by the signatory to sign.	
4. 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)."	eProcedure rules engine
5. 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 the user in some MS local registry. This service deals with the record matching (automatic and/or manually).	Record matching
6. Authentication initiation	The DC asks the user to authenticate him/herself. This service initiates the authentication process.	Identity Management Component
7. 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.	Evidence query
8. eProcedure save and resume	"Saving the (public) service request to continue at a later point in time is handled by this service. This is an important service making the user's life easier. An eProcedure application form usually requires the user to provide several inputs, wait for evidence transfers and/or upload documents themselves. The save and resume function allows them to complete the form over several days (up to some limit), saving changes e.g. an SLA timeout on the exchange of evidence, and editing the form again as needed before submitting the final application. Beside this voluntarily choice there is also the case that things go wrong: a timeout on the exchange of evidence, a system that is down, network errors etc. The save and resume functionality also supports to recover from some error situations preventing that the user must start all over again.	• Procedure management • Session Management

Application Service	Description	Application Component
9. Message encryption	Both DC and DP encrypt messages to allow for secure cross-border exchanges of data. This service handles encryption of data (symmetrical, asymmetrical or a combination).	Data encryption/decryption
10. Error handler	This application service is used for handling error situations with respect to: • non-availability of OOP • non-availability or delay of evidence	Evidence portal back-end
11. User Authentication (UI)	User Interface for entering credentials, e.g. user/password, to be used for authentication purposes.	Identity Management Component
12. 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.	Authorization controller
13. Evidence status tracker	The DC keeps track of evidence requested versus evidence received. This service bundles the UI and logic to support this.	Evidence interchange back-end
14. Message decryption	Both DC and DP decrypt messages to allow for secure cross-border exchanges of data. This service handles decryption of data (symmetrical, asymmetrical or a combination).	Data encryption/decryption
15. e-Signature Verification and Validation Service	Both DC and DP verify/validate eSignatures supported by this service. 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.	Trust Service Provisioning Component
16. eProcedure termination	An eProcedure can be aborted. This service terminates the requested eProcedure (public) service.	Online procedure portal front-end
17. 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.	Online procedure portal front-end
18. 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.	Evidence interchange front-end

Application Service	Description	Application Component
19. 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.	Online procedure portal front-end
20. eProcedure confirmation	The acknowledgment that all required evidence is received by the DC is confirmed to the U by this service.	Online procedure portal front-end
21. 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.	eProcedure rules engine
22. Alternative channel	If the user identity cannot be established the user is redirected to an alternative channel. This service supports the handling of this.	• Online procedure portal back-end • Online procedure portal front-end
23. Available evidence determination	The DC looks what required evidence is already available for the user on national level (doesn't have to be requested). This service includes querying national base registers for available evidence.	• eProcedure rules engine • Online procedure portal back-end
24. Extended identity matching UI	The U is presented with a UI in order to provide additional information in order to do the identity matching. This service handles this.	TBD
25. DID connection acceptance	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.).	SSI edge agent front-end
26. DID connection invitation	The service generates and provides a data (DID document) with which the different stakeholders (e.g., users) can start the process of DID connection establishment.	SSI cloud agent back-end
27. 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.	Evidence interchange back-end
28. Inquire routing information	The DC looks up where to send the request for evidence to. This service acts as an API to lookup the routing information.	Data service lookup
29. QR code (UI)	A service that provides a QR code to be displayed on the UI for the user to be scanned.	• Evidence portal front-end

Application Service	Description	Application Component
		• Online procedure portal front-end
30. Available VC check	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 their delivery to DC. The service also resolves the situation where the user does not hold the required evidence (VC) in his wallet (current agent) and starts the procedure of the lookup of DP, which may provide the user with required evidence (VC).	SSI edge agent back-end
31. Cross-border evidence matching	The DC must match required evidence cross-border. This service bundles UI and logic to support this process.	Evidence type translator
32. DID connection response	The service validates and provides a response to the incoming DID connection invitation. As a result of this action, information on the DID connection establishment is provided.	SSI cloud agent back-end
33. Evidence exception UI	Through this service the U is informed about errors or delays with respect to the requested evidence and the U is told to return to the eProcedure portal of the DC.	• Evidence interchange front-end • Evidence portal front-end
34. Explicit request	The user must make an explicit request for OOP transfer of evidence. This service handles the request.	Online procedure portal front-end

3.2.2 Common Components

Underneath table (Table 2: Common Application components) gives an overview of all common application components encountered in DE4A. It considers all components defined for all three patterns in chapter 4. An application component is classified as “common” when it is used in two or more places. They are referenced from the tables listing the Application Services per pattern in chapter 4. The application services which are served by the component are also included in the table.

Table 2: Common Application components

Application Component	Description	Application Service
a. TBD	This component offers the functionality needed to do identity matching in case normal record matching (see q below) is not successful.	Extended identity matching UI

	Through this component the U is presented with a UI in order to provide additional information in order to do the identity matching.	
b. Authorization controller	Application component to establish which evidence types can be exchanged between competent authorities and whether this is allowed under allowed under applicable Union or national law without user request and preview.	• Authority check • Legal basis check
c. Data encryption/decryption	Application component providing encryption and decryption functionality (symmetrical, asymmetrical or a combination thereof).	• Message encryption • Message decryption
d. Data Exchange Component	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.	Data Exchange Service
e. 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.	• Inquire routing information • Verifiable Credential Issuer search
f. eProcedure rules engine	Application component taking care of matching procedural requirements with evidence and establishing available and missing evidence.	• Requirements/evidence matching • Procedural requirements determination • Available evidence determination
g. Evidence interchange back-end	Application component managing the tracking of evidence requests and supporting the removal of evidences.	• Evidence status tracker • Evidence request tracker
h. Evidence interchange front-end	Application component bundling UI and logic to handle the status overview and preview and approval of requested evidences.	• Evidence status overview • Evidence Preview • Evidence exception UI
i. 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).	• Evidence validation and extraction • Data Exchange Service • Persistent URL generation • Error handler

	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.	
j. 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.	• QR code (UI) • Evidence exception UI
k. 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.	Evidence lookup
l. Evidence type translator	Application component taking care of translating one type of evidence in MS of DC to other (potentially multiple), equivalent, type of evidence in MS of DP by using a mapping of evidences.	Cross-border evidence matching
m. Identity Management Component	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;	• Authentication initiation • User Authentication (UI)
n. Online procedure portal back-end	Application component managing the entire interaction between the user and the Online Procedure Portal, including e.g. UI framework, specific forms integration with the Online Procedure Portal Backend.	• Evidence status overview • Alternative channels • Available evidence determination

o. Online procedure portal front-end	Application component managing the entire interaction between the user and the Online Procedure Portal, including e.g. UI framework, specific forms integration with the Online Procedure Portal Backend. In case of VC also handles the establishment of DID connections between DP and users.	• Evidence status overview • eProcedure termination • eProcedure Initiation • eProcedure submission • eProcedure confirmation • Alternative channels • QR code (UI) • Explicit request
p. Procedure management	Application component handling the session management for the user.	eProcedure save and resume
q. Record matching	Application component that provides identity matching based on attributes. Provided attributes are matched against attributes in some local registry.	Identity/record matching
r. Session Management	Application component handling the session management 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 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 he/she left off.	eProcedure save and resume
s. SSI cloud agent back-end	Application component managing the DID connections and handling the VC/VP related events.	• DID connection invitation • DID connection response
t. SSI edge agent back-end	Application component managing the DID connections and handling the VC/VP related events.	Available VC check
u. SSI edge agent front-end	Component building UI and logic to handle DID connections and the VC/VP related events.	DID connection acceptance
v. Trust Service Provisioning Component	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	• e-Signature Creation Service • e-Signature Verification and Validation Service

	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.	

3.3 Trust Model

The trust model developed in T2.2 (being developed at the time of writing this document), covers a general scope from a high-level perspective, so the particularities of each single situation can be covered in a smooth way. This trust model is based on the eIDAS regulation and eDelivery Building Block trust approach, also covering the trust management guidelines followed in the implementation of the CEF Building Blocks and its alignment with the three interaction patterns described in this Project Start Architecture (intermediation pattern, user-supported intermediation pattern and verifiable credentials pattern).

The trust models used in the implementation of the CEF Building Blocks can be depicted into:

- **Dedicated domain PKI**
  In this trust models, the digital certificates are associated to a single trust anchor, so it serves to a single domain (dedicated anchor). Because of having one dedicated Certification Authority, the workload of definition and managing security policies which are tailored and specific to the domain.
  In this approach, the trust is limited to the domain covered by the scope of the Certification Authority used to generate digital certificates.
- **Shared domain PKI**
  This trust models relies on the concept of the trust anchor serving multiple domains (shared anchor). The digital certificates keep associated to a single trust, in the form of a Certification Authority. In this approach, a local trust store is desirable in order to check that the certificate is issued in the appropriate domain.
- **Mutual exchange**
  The main characteristic of this trust model is the management of certificates from different trust anchors. This implies a secure protocol aimed to a trustworthy distribution of the certificates. This can be managed by thirds parties as a secure portal acting as intermediaries among organisations.
- **Domain trusted lists**
  This approach, described in the eIDAS regulation, is based on the issuing Certification Authorities available on a domain trusted list. The trust in this case is obtained as the digital certificates are issued under a Certification Authority in the domain trusted list. Furthermore, the domain trusted lists can belong to different business domains that rely on a single domain policy.

This set of very representative trust models are the high-level implementation approaches of the trust architecture of the interaction patterns detailed in the following subsections. For example, the intermediation pattern implementation can address the “domain trusted lists” trust model by implementing from the technical point of view the trusted lists mechanisms for issuing the certificates. In other cases, attending to the particularities and special circumstances of the domains and

environments in which the solution will be implemented/deployed, other different trust models will be needed to address.

These approaches are used for the exchange of messages in a secure and trusted manner according to a set of security tools, further details of each one of this trust models will be delivered in the D2.2 Trust models.

Looking at the three different interaction patterns that are detailed in this deliverable at the time of releasing this chapter (intermediation pattern, user-supported intermediation pattern and verifiable credentials pattern), we can propose a set of guidelines in each one of the business activities that can be grouped into a trust model.

3.3.1 Intermediation and user-supported intermediation patterns

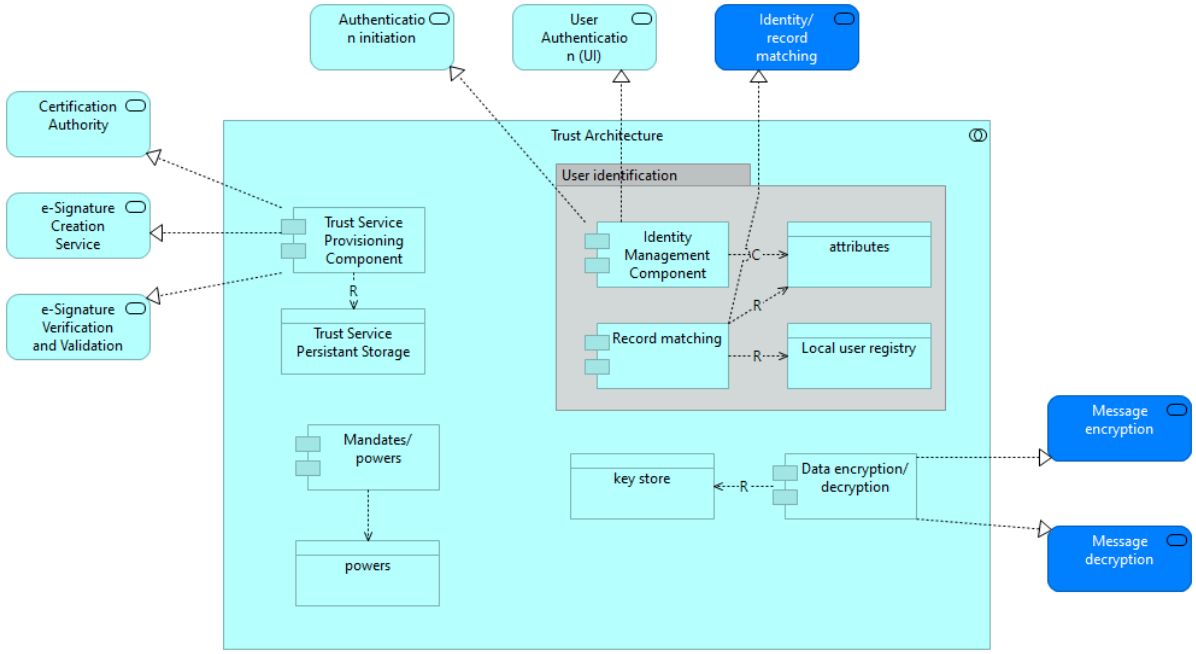


Figure 1 Intermediation and user-supported intermediation patterns trust architecture

After and assessment and evaluation of the different components described in the proposed trust architecture, we have identified the need of a storing mechanism which stores in a persistent way the tools managed by the Trust Service Provisioning Component.

This new conceptual component (data object according to ArchiMate terminology, a self-contained piece of information) would be the Trust Service Persistent Storage, in which the storage of certificates, e-signatures, e-timestamps and e-seals (tools and elements used by the Trust Service Provisioning Component) is managed when is needed. Depending on the characteristics of the use case, which is going to be implemented and deployed, this component will be enabled or not.

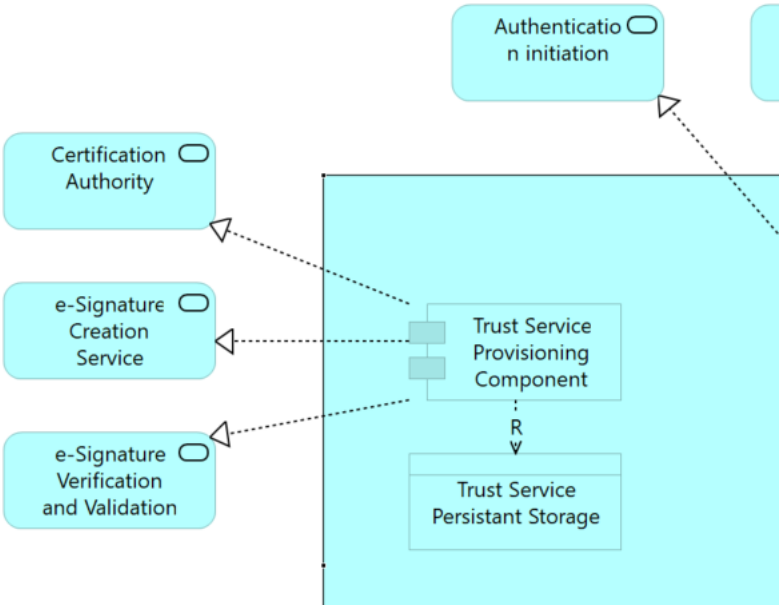
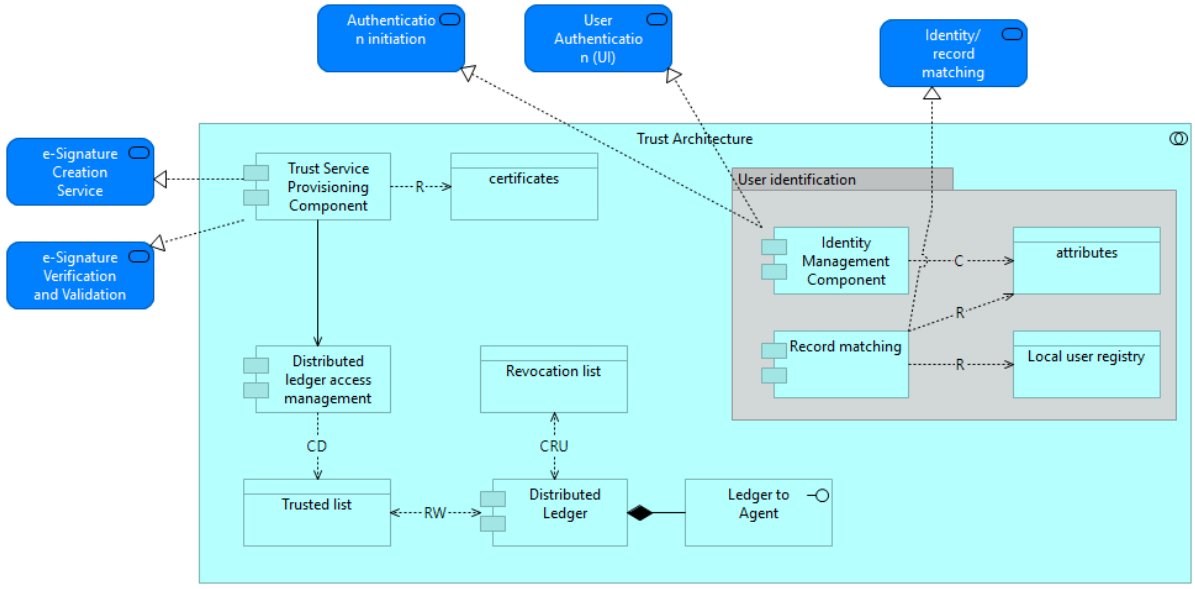


Figure 2 Detail of trust persistent storage components

Furthermore, a logical representation of the Certification Authority has been added outside the scope of the Trust Architecture. This approach relies on the needs of specific implementation which will use external certification services.

3.3.2 Verifiable credentials pattern



The verifiable credentials interaction pattern is based on the "Domain trusted lists" approach from CEF Building Blocks trust models. This approach manages a trusted list with all the available domain names in the policy set up by the administrator, and the certificates issued by these domains will be automatically trusted by the rest of the logical components. The policy designed is complemented with other component, the "Revocation List", which stores the serial numbers of the revoked certificates

and are not valid (so, not trusted). When a Certification Authority issues a certificate, it has an expiration date, after that, it must be renewed, otherwise it'll be included in this "Revocation List".

One of the most interesting characteristics of the trust architecture of the Verifiable Credentials interaction pattern is that it relies on a distributed ledger to manage the transparency, auditability, security and accountability of the certificates managed by cryptographical means. This decentralized approach also covers other threats with its consensus mechanisms and avoids the single point of failure that can cause other derivate problems to the trust architecture.

3.4 Semantic Solution

3.4.1 Availability and usability of semantic standards

In this section, the ISA2 vocabularies including Core Criteria and Core Evidence Vocabulary (CCCEV), Data Catalogues - Application Profile (DCAT-AP), and TOOP Exchange data model (TOOP EDM), that is based on these standards, are described as essential standards to consider in the PSA scope. The SDG metadata model specification is also considered. Descriptions are based on the following concepts:

- **Public service:** General information about the public service, such as description, modification date, thematic area, language, requirements, competent authority, input (evidence), output, contact information (based on SDG model and TOOP).
- **Event**: An event that is related to public service. It includes business and life events (based on SDG model and TOOP).
- **Public service dataset**: This contains the descriptions of metadata of where the dataset is being described (based on the SDG model and TOOP).
- **Criterion**: A Criterion can be expressed as a set of requirements where every requirement must be valid. It is used as the basis for making a judgment or decision, like a requirement set in a public tender or a condition that must be fulfilled for a public service to be executed.
- **Evidence**: It is defined as any resource that can document or support a criterion response. It contains information that proves that a criterion requirement exists or is true. Evidence is used to determine that a specific criterion is met (based on CCCEV, SDG model, and TOOP).
- **Agent**: Agent class is any resource that acts or has the power to act. This includes people, organizations and groups (based on SDG model and TOOP).
- **Public organisation**: Defines the concept of a Public Organisation and associated properties and relationships (based on the SDG model and TOOP).
- **Business (Legal Entity)**: Represents a business that is legally registered. A Legal Entity is able to trade, is legally liable for its actions, accounts, tax affairs, etc. (based on the SDG model and TOOP).
- **Person**: Represents a natural person. One subcategory is the EU citizen (based on the SDG model and TOOP).
- **Registered Organisation:** Extension of the Register Organization Vocabulary (ROV) [21]. The Registered Organization Vocabulary is a profile of the Organization Ontology for describing organizations that have gained legal entity status through a formal registration process, typically in a national or regional register.
- **Catalogue:** A catalogue or repository hosts the Datasets being described.

The possibility of using the abovementioned semantic assets is investigated against the requirements identified by the outcomes of DE4A deliverables D4.1, D4.5 and D4.9 use cases. The result is summarised in Table 1.

Table 3: Mapping of requirements to the semantic assets

	Semantic Requirement	DE4A Pilots Deliverables	Semantic Asset	Synthesis description
1	Semantic interoperability between (each type of) evidences on the basis of agreed principles, formats and standards for both "Studying Abroad" and "Moving Abroad" use cases.	D4.1, D4.5, D4.9	TOOP CETRB (CEF HLA)	CETRB is an application profile of CCCEV that supports the mapping of specific procedural requirements (criterion, information and constraint) to each MS. In the case of the information requirement class, CETRB associates the Evidence Type class that uses known domain-specific ontologies to describe common data structures to satisfy each information requirement. However, there is no solution for non-structured data evidences or identification of evidence types to be agreed on considering the SDG scope.
2	A semantic mechanism to validate powers across borders is a pre-condition to successful piloting.	D4.5	TOOP model	They are covered by "hasLegalRepresentative" property in the RegisteredOrganisation class. This mechanism is not in place yet and is semantically challenging as it does not include an identifier. The semantic model of SEMPER, along with necessary modifications could be considered, such as to handle the cross-border exchange of required evidence for approval of mandate between DC and DP.
3	Company / Organization identifier: a number of strings that uniquely represents an entity across DE4A MS.	D4.5	Core Business Vocabulary, BRIS Legal Entity Data model	CBV includes the unique property “legalIdentifier” of the class “Identifier” which is provided by an authority within a given jurisdiction. This property has a narrow relationship with the LEF property “companyRegistrationNumber”. Legal Identifier is therefore a fundamental relationship between a legal entity and the authority with which it is registered. The details of the registration are provided as properties of the Identifier class. The Core vocabulary sets no restriction on the type of legal identifier. CBV also considers the optional and multiple attribute “identifier” that are given by authorities in different

	Semantic Requirement	DE4A Pilots Deliverables	Semantic Asset	Synthesis description
				domains, such social security, taxation, etc. The H2020 project euBusinessGraph has produced the deliverable 2.1 which includes a system of identifiers, ontologies and vocabularies in the business domain.
4	Standard format needed for companies' (postal, visiting) address subcomponents	D4.5	Core Location Vocabulary, BRIS Legal Entity Data model	CLV is used by the Core Business Vocabulary for the property "registeredAddress". This property has a narrow relationship with the BRIS LED property "companyRegisteredAddress"
5	DC needs to find the related DPs for the request at hand to identify the needed company data through a catalogue	D4.5	TOOP Data Services Directory	This requirement is covered by the TOOP Data Services Directory, which uses a profile of BRegDCAT-AP v1. However, BRegDCAT-AP v1 is still evolving. The version 1.04 is the last one published on 22/06/2020.
6	The request must be semantically transformed into the concepts understood by the data provider (non-functional)	D4.5	TOOP CETRB	The CERTB allows to map procedural requirements from different MS through the top-level criterion and information requirements, and associated evidence types. However, the transformation between domestic evidences and evidence types is not covered by TOOP. This is a task for the DP.
7	DC has to be notified of updates in company data. Therefore, the data model should be able to handle and identify changes in company data.	D4.5	Core Business Vocabulary, BRIS Legal Entity Data model	The Core business vocabulary property "company status" is meant to provide information on the status of the company with legal implications, such as 'insolvent', 'bankrupt' and 'in receivership'. This property has a narrow relationship with the BRIS LED property "companyStatus". However, the status of this requirement seems to be an alert on the modification of any relevant data of the company, such as the "cbv:companyData".
8	Business event: Taxonomy of business events based on use cases like "Starting a	D4.5	SDG model, xEBR Taxonomy	The SDG model includes a Business Event class; however, it currently has limited properties and the class instances have not been defined.

	Semantic Requirement	DE4A Pilots Deliverables	Semantic Asset	Synthesis description
	business in another Member State" and adoption of suitable scenario.			The xEBR Taxonomy is accessible only for registered members. ISA2 launched an action to define European taxonomy for public services, but this is only in its early stages. A proposed list can be found at: https://ipsoeu.github.io/cos-taxonomy/.
9	Life event vocabulary: A concise identification and description of life events is needed for D4.9. There is currently no suitable vocabulary to cover this subject. It should as a minimum cover birth, marriage, relocation/address change and death.	D4.9	SDG model "Life Event class."	The SDG model includes a Life Event class; however, it currently has limited properties and the class instances have not been defined. ISA2 launched and action to define a European taxonomy for public services, but this is only in its early stages. A proposed list can be found at: https://ipsoeu.github.io/cos-taxonomy/.
10	Taxonomy (and/or vocabulary?) for jurisdictions	D4.9	SDG model, TOOP	There is a class for jurisdiction in the ISA2 semantic Core Vocabularies. For public authorities, jurisdictions correspond to NUTS and LAU code lists provided by Eurostat.
11	Vocabulary and taxonomy for pension	D4.9	Not Covered	Domain experts should be consulted in this regard. The "Social Protection" division of the Classification of the functions of government (COFOG) could be a reference to explore, which is used by Eurostat for the pension expenditure and beneficiary statistics by type of pension.

In summary, for automatic exchange of evidences across borders there are domains that lack mapping. For example, as the recent study on Data Mapping for the cross-border application of the Once-Only Technical System reports [11], very few evidence types are harmonized at EU level. The eInvoicing in the eProcument domain is one such harmonised domain. The university diploma supplement is harmonised by the nature, level, content and results of the studies, as a consequence of the Bologna process on higher education. The Deloitte report also highlights the diversity of same type evidences within Member States, because of multiple issuing authorities in the same country. These evidences are not harmonised and can therefore vary in both content and format. Such situations could be challenging to tackle.

3.4.2 Evidence type translation and approaches

Evidences are legal means to prove that procedural requirements are met. Evidences provide the required information to this end. However, in a cross-border and automatic exchange scenario, because of the lack of evidence harmonization at European level, the issuing Member States (MS) might provide the required information fully, partially, or with significant differences. There could also be situations where a MS cannot provide the required information at all. Furthermore, the required information could be provided by the same kind or by a different kind of evidence than is issued in the MS of the procedure. A study, commissioned by the Commission [11], showed that a mismatch between evidence types is a common challenge.

On a single occasion there could be several evidences issued in the same MS to provide the requested information. This is expected to be rare, as usually there is only one source that can lawfully issue evidences regarding specific information. In cases where several equivalent evidences or sources of evidences exist in one MS (e.g.: diploma from a University or confirmation of academic title from a national registry), we reasonably can assume that the issuing MS can make a choice as to which evidence is preferred and hence provided for cross-borders exchange.

SDGR article 14 required to offer evidences through the technical system that are lawfully issued in an electronic format that allows automated exchange. Such evidences can be issued as a document (i.e. an electronic file) or as data (i.e. a set of attributes, potentially including "yes/no" verifications of facts). Consequently, there is a range of possibilities for cross-border and automatic exchange if the evidence is lawfully issued as:

1) a data structure according to
    a. an agreed schema
    b. an agreed schema with only requested attributes
    c. a domestic schema that can form a basis for transformation to the domestic schema of the requesting country
2) a document
    a. in an official language of the issuer
    b. in a multilingual standard form
    c. with an attached data structure according to a certain agreed schema

In addition, these types of evidence provision should ideally be directly useable for the data consumer. For instance, a document in the issuer's official language would be actionable if the consumer shares that same language.

Processing or understanding domestic schemas from another country is only possible if they can be matched to the national domestic schemas of the receiving country, hence the schemas that are used by the procedure at data consumer side. Matching domestic schemas in pairs is a difficult solution to create and maintain. As there are 27 Member States, this would amount to 351 mappings, or more likely ad-hoc mapping by public servants on a case-by-case basis.

The strategy adoped for the pilots would be to map each domestic schema to a common, agreed schema. The technical system may have to support many or all of the mentioned possibilities in order to allow the exchange of evidences in full respect of lawfully issued evidences as required by the SDGR, whereas in the pilot context we can focus on the approach that provides the highest degree of semantic interoperability. The same information meta-data is required to be registered for such a purpose and could be handled by a component that would act as an information desk, especially to

ease the matching between domestic evidences and cross-border evidences. There are two approaches to implement it, criteria-based or evidence-based, which can work together to fulfill the needs of data consumers that work with procedural requirements and those that work with evidences.

Table 4: High-level comparison of criteria-based and evidence-based approach

	Most suitable..	Main challenges/opportunities
Criteria-based	…in sectors with harmonisation on procedural requirements	Large number of criteria/requirements to be agreed and maintained Evidence type matching without evidence harmonization possible
Canonical evidence-based	…in sectors with harmonisation on evidence types or multilingual forms	Fewer instances of relatively large canonical evidences definitions to be agreed on Facilitates deep semantic interoperability

3.4.2.1 Criteria-based approach: Evidence Broker

CETRB is a component used by TOOP and later renamed Evidence Broker, based on the Core Criteria and Evidence Vocabulary of ISA2 and the eCertis tool used by public procurement authorities. The CETRB information model is based on procedural requirements, which can be seen as criteria to be met and satisfied directly by yes/no evidences such as 'is an adult' or as information requirements to be satisfied by evidences in the form of a document or data.

For finding evidences in MS "A" to satisfy procedural requirements in MS "B", the CETRB component relies on agreed top level requirements, criteria or information, which are the connection between MS "A" and MS "B" through the link between their domestic requirements and the top level ones.

Regarding semantic interoperability, the CERTB component focusses on evidences as data [i.e. 1) in the section above] through the element 'evidence type'; there is no explicit coverage for the case of evidences are documents [i.e. 2) in above section]. An 'evidence type' is a set of attributes that represent the information to satisfy certain top-level information requirements and are provided by evidences as data issued by MS. These attributes are defined in aggreed ontologies.

There are two prerequesites for this approach: First, agreements on top level criteria and information requirements must be achieved in domains other than eProcurement, were such agreements at European level are not yet existing. Second, procedural requirements must be centrally registered and associating to top level requirements for each procedure in every MS, as well as the domestic evidences types that can satisfy such procedural requirement in that MS and the association between information requirements and evidence types. Especially if requirements have a higher rate of change than the lawfully issued evidences themselves, this could amount to additional adimistrative effort.

This approach is suited to the needs of fully digitalized procedures (such as the ones forming the focus of SDG and DE4A) because the CETRB allows their automatic processing if evidences as documents are not allowed. This approach is also easily workable in domains with a significant level of harmonization on procedural requirements, such as public procurement where a similar model of information is already in place with selection and exclusion criteria.

Deep semantical interoperability can be achieved if the top level requirements and the corresponding evidence are very fine grained: If single (or a very limited number of attributes) are required to satisfy a requiement, or “yes/no” evidences that are semantically interoperable by default, then automatic processing of the reveived information could be achieved. The criterium-based approach could, however, have its merits where equivalence between very inhomogeneous, potentially complex evidence types needs to be established [ie. 1) c. above], potentially extending to (unstructured) documents.

3.4.2.2 Evidence-based approach: Canonical Evidences

Canonical evidences are defined as structured data models that include a common set of attributes associated with the evidence type that can be provided by the corresponding lawfully issued evidences. Such a definition includes a set of common attributes for every canonical evidence (such as the issuing competent authority and country, the issuing date and time, and the period of validity of the evidence), a set of common attributes for any lawfully issued evidence associated to the canonical evidence and a set of attributes with any specific, additional attribute provided by the associated domestic evidences. This last set of attributes is a super-set that mitigates the lack of a full harmonization. It also resolves the practical problems resulting from the restriction to a minimum, common agreed dataset, cf. restrictions experiences with the eIDAS minimum dataset. With this superset of attributes, there is no limitation to pairwise reuse of evidences between two MSs that share more attributes than the ones included in the sets of common attributes.

Canonical verification evidences (“yes/no” answers) should include only common attributes to all canonical evidence and the corresponding “yes/no” attribute. Besides, canonical verification evidences can be linked to canonical consultation evidences –with several data attributes– if the corresponding assertion is defined, i.e. “is an adult” = “today - birthdate >= 18”.

Canonical attributes are centrally defined and, therefore, are uniquely identified. Lawfully issued evidences from MS are associated to canonical evidences along with the specific canonical attributes they provide. As a result, the canonical approach resolves both the matching of evidence types between memberstates and, allows the semantic interoperability required for automatic reuse of data. For the common set of canonical attributes, only 27 mappings (domestic model to canonical model) are required for this deep semantic interoperability. The creation of the 28th model, i.e. the canonical model, might not easily achieved in sectors with no or little prior harmonization; And it is not mandated by Article 14 of the SDGR[3].

On the other hand, because evidences are proofs with legal value to make decisions within the processing of administrative procedures, evidences need to use an official language of the MS of the procedure. However, since automatic translations still lacks legal value, the proposal is for domain experts to produce text labels for any canonical attribute in every official EU language. With these multilingual labels, it could be possible to provide understandable information with legal value to civil servants that have to process cross-border evidences, as well as to users when previewing the evidence data. Canonical attributes can be represented both by agnostic vocabularies from ISA2 SEMIC initiatives and by domain-specific ontologies that are already being used by cross-border evidence issuers and consumers.

The pilots expect to use this approach that allows the exchanges of lawfully issued evidences as data represented by the canonical attributes, or lawfully issued evidences as document with a canonical data structure of the canonical attributes attached to. But exchanges can also use evidences as documents without such an attachment if the text labels used in the document are the ones registered for the associated canonical evidence and they have been translated to the language of the consuming authority.

This approach focuses on agreements on canonical evidences that are instantiated in the lawfully issued evidences mentioned in the SDGR article 14. The canonical evidence approach is inspired by the work done by the Regulation (EU) 2016/1191 [42], which produced eleven multi-lingual standard forms in the field of public documents. It represents an accepted solution for the cases where such prior harmonization exists. Because it 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 hramonization across several memberstates.

3.4.2.3 Bridging the two approaches

Canonical evidences as evidence types can be connected to top level information requirements (canonical consultation evidences) or as criterion requirements (canonical verification requirements). If there is a link between top level requirements and canonical evidences, data consumers (i.e. public service providers) can locate cross-border domestic evidences through these links, irrespective of procedural requirement or an evidence approach.

In summary, the function “evidence locator” is for locating from MS “A”, the cross-border evidence issued in MS “B” from an input provided by their procedure service, either as a domestic or a /top-level requirement, or a domestic or a /canonical evidence (cf. Figure 3). The output would be the required evidence itself, or a list of competent authorities issuing the evidence in MS “B” which one of them can be selected by the consumer. The output could also be that MS “B” does not issue such an evidence. Once the crossborder evidence is located, a second function should provide information on the available distribution(s) of such evidence to the consumer. The consumer to can then decide whether one particular distribution is better suited to their needs or not. In this context, distributions represent the range of possibilities for the lawfully issuing of the evidence in MS “B”.

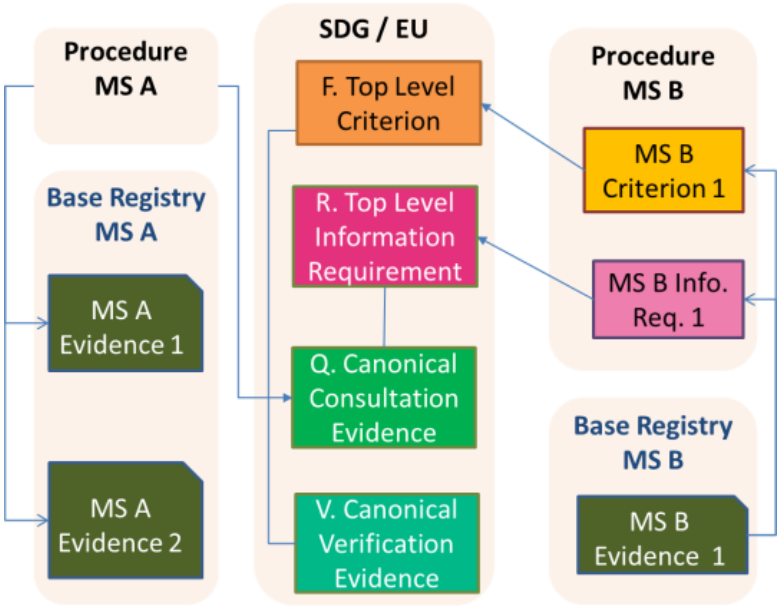


Figure 3: Evidence location and distribution

4 Reference Interaction Patterns

Reference Interaction Patterns are described at the conceptual/functional level of abstraction and agnostic of the specific (public) service provided or evidence exchanged and of the specific solution building blocks employed. They are meant to provide guidance to different use cases in DE4A pilots and beyond.

For each pattern, the section will include a Business Process Collaboration Viewpoint and a Process Realization viewpoint and Application Collaboration viewpoint at the conceptual/functional level of abstraction. In addition, elements specific to the pattern are described here - common elements are described in chapter 3 above.

4.1 Scope and Process Identification

A crucial yet often neglected step in process analysis and design is the identification and delimitation of the process at hand, including the analysis of potential process variations. This exercise considers the process as 'black-box' and defines the scope both in terms of the extension of the process (where does it start and where does it end) and the breadth of variation included in the design (i.e. which cases are covered, and which cases are deliberately left out of scope).

As result of the process identification for this start architecture we chose he value-adding (public) service end to end:

- The starting point (the trigger) is at the User, the **need for a specific public service** in context of a life even. Please consider that the process starts well before the explicit user request for an OOP transfer of evidence but that it does not include the preceding orientation and information gathering process (that the user might go through in the Your Europe gateway).
- The end of the process (the desired outcome) is that the **result of the public service is received** by the user. Please consider that the process extends well beyond receiving the OOP evidence to include providing the actual public service to the user, but it excludes the (potentially) ensuing process of appeal if the user does not agree to the decisions taken by the competent authority.

Each process can have multiple variations. It is crucial for a good process design to define which variations are relevant for the model at hand, hence need to be covered, and which variations are outside of scope. We analysed a total of 8 sources of variations for this process, the most important findings being that the reference process should cover:

- both natural and legal person as users
- include both eIDAS and domestic means of authentication
- focus on structure data and hybrid evidence
- consider complex cases where eID, origin or user and source of evidence (DP) are different MS
- consider complex, multi-country and multi-evidence cases
- Exclude purely domestic use and upload of evidence provided directly by the user even if they might be supported by the eProcedure portal as these variations are not in focus of pilots (i.e. cross-border procedures incl. OOP exchange of evidence)

4.2 Intermediation

4.2.1 Working Hypothesis and Implementation Principles

The Intermediation reference interaction pattern described in this chapter is valid under the working hypotheses listed in Table 5. These working hypotheses are based on preliminary analysis and many have still to be fully validated or decided upon by the members of DE4A.

Table 5: 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.
Multiple, complementary, overlapping or conflicting evidence equivalents	Multi-evidence cases 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.	It is to be investigated whether the pilot cases and MS combinations of the pilots entail multi-evidence cases at all. If that is not the case, the MVP could be restricted to a single request to single evidence case.
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 evidence. This means that any exception during the OOP exchange leads to the termination of this OOP attempt, potentially to be repeated in a later 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	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 evidence that resides still in paper archives. We might 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 [..].

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
	persistent process instances across a multitude of highly independent systems.	
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 that still needs to be validated from a legal point of view and the limitation that the pilot solution cannot transition to full production use 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, access to the evidence data prior to user authorisation, i.e. for example by using administrator rights on the underlying ICT infrastructure.	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. The DC has in any case to implement a solution guaranteeing that “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 generalised 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 matching based on eIDAS attributes is never 100% 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 has to be defined, for example,

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
		to manage the situations where this automatic matching doesn't 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 U 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 basis for the case that the identification does include personal data of other data subjects than the requestor (change of address for families).	We need the MS participating in the pilots adopting the intermediation pattern to sustain this interpretation.
Hand-on of UI between actors	The DC handles all user interaction of the eProcedure, including the OOP transfer of evidence, thus foreclosing 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.	The possibility to use results from SEMPER is being investigated. It will be sought to minimise the real risk that solutions based on this pattern cannot go production live within the timelines of DE4A, as it would require an adjustment of the eIDAS Regulation. Reuse would require establishing formal relationships between the two parallel pilot projects SEMPER and DE4A.

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Encryption Gap	OOP in the public sector does not require true E2E encryption. The exchange between DR and DP 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.	
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 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.
Payment for evidence	In the context of the pilots we assume (at least for the first pilot iteration) that no payments are required.	

4.2.2 Business Process Collaboration

Figure 4 models the 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 6 the activities of all participants are listed roughly in chronological order across all three processes. The conversations between the participants are described in Table 7 and Table 8, listing the messages between the U and DC (Table 7) and between DC and DP (Table 8) respectively.

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 a SLA timer.

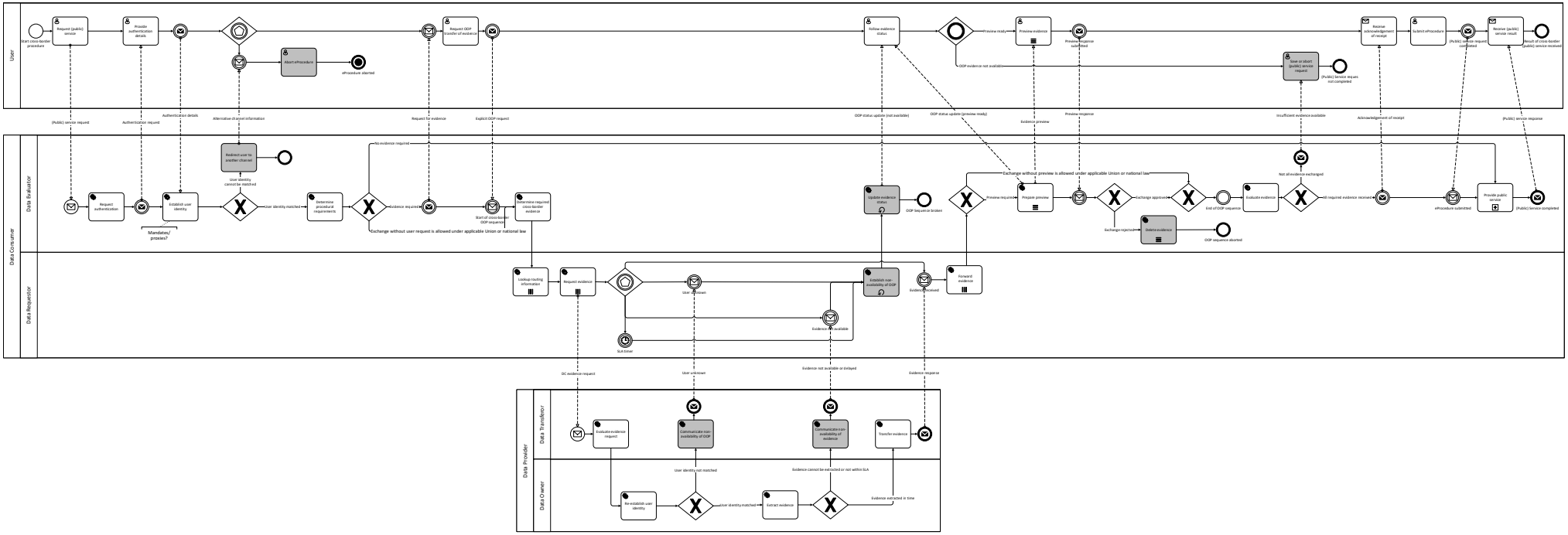


Figure 4 Business Process Collaboration view of the Intermediation Pattern

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.

In Table 6 the business activities of all three processes are listed roughly in chronological order. The first column designates the activities shown in Figure 4 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 [6]. The third column contains the task type (please refer to the BPMN 2.0 standard specification [2]) as shown in in Figure 4 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 [6] or Article 3(1) of the SDGR [3]. The fourth column describes the business activity in concise language.

Table 6: 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 U to authenticate themselves. This can happen in two ways, either using eIDAS (default) or using the eID of the DC MS, in case that the U has the national eID of the DC country available (see cases 3) and 4) in Table 4 above). The DE provides both options to the U.
Provide authentication details	U	User	The U 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 U 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.

Activity / UC	Role	Type	Description
Redirect user to another channel	DE	Service	Exception handling activity: The U 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 U.
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.
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.
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).

Activity / UC	Role	Type	Description
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.
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 form 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 to the user. User cannot be uniquely identified – fallback to another channel (i.e. IMI)

Activity / UC	Role	Type	Description
			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 e-mail, 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 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.
Transfer evidence	DT	Service	The DT encrypts and signs the evidence 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.

Activity / UC	Role	Type	Description
Prepare preview	DE	Service	The DE prepares a preview for the U 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 U 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 back to the U. The Procedure can then not be completed.
Save or abort (public) service request	U	User	Exception handling activity: The U 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 U. 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 themselves.
Receive acknowledgement of receipt	U	Receive	The U is waiting to receive the acknowledgment that all required evidence is received by the DC. The acknowledgment is displayed in the eProcedure portal (optionally a copy sent by e-mail or deposited in a government-hosted, secure message box).
Submit eProcedure	U	User	The U 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 U is prompted to verify the provided information in an overview before hitting the Submit button.
Provide public service	DE	Sub-process	This is a subprocess that is very heterogenous 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

Activity / UC	Role	Type	Description
			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 U. This communication is fully dependent on the functionalities of the eProcedure portal (e.g. e-mail and/or government-hosted, secure message box).

Table 7 describes the conversation between U and DC by listing the exchanged messages in chronological order. Table 8 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 U and DP, in contrast to the User-supported Intermediation pattern (chapter 4.3) and the Verifiable Credentials pattern (chapter 4.6).

Table 7: 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 or 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

From	Message	To	Description
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)
DC	Acknowledgement of receipt	U	Acknowledgement that all required evidence was submitted and the (public) service can be provided to the user
U	(Public) service request (completed)	DC	Complete and final submission of the (public service request), including all required information
DC	(Public) service response	U	The result of the (public) service, irrespective of how it is provided (post, email, secure message box, personal appearance.

Table 8: 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

4.2.3 Process Realisation

The process realization viewpoint is adapted from the Service Realization Viewpoint mentioned in the ArchiMate 3.1 specification as was described in [6]. 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.

The following diagram shows how the User process (cf. Figure 4) is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by application collaborations which are presented in section 4.2.4 below. In Table 9 the application services are described.

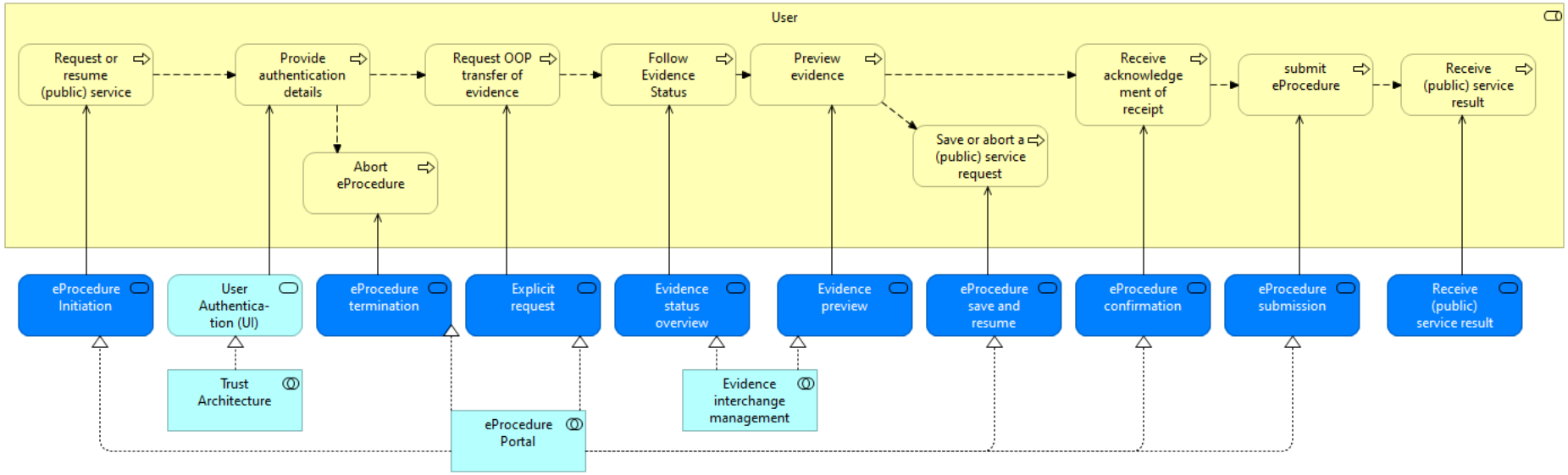


Figure 5 Process Realization of the User Process

The diagram hereunder shows how the Data Consumer process (cf. Figure 4) is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by application collaborations which are presented in section 4.2.4 below. In Table 9 the application services are described.

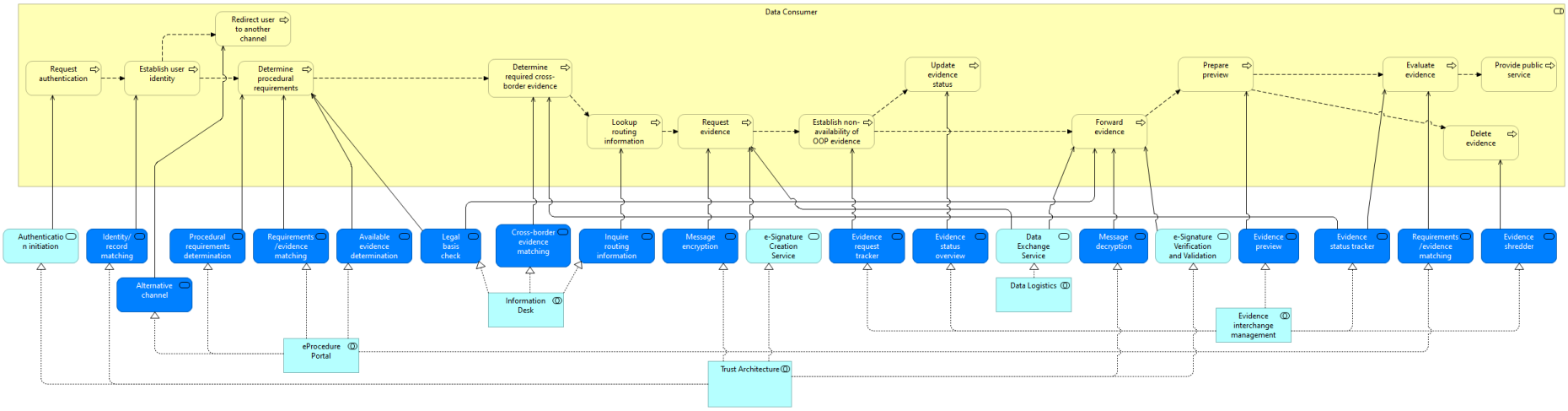


Figure 6 Process Realization of the DC Process

The diagram underneath shows how the Data Provider process (cf. Figure 4) is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by application collaborations which are presented in section 4.2.4 below. In Table 9 the application services are described.

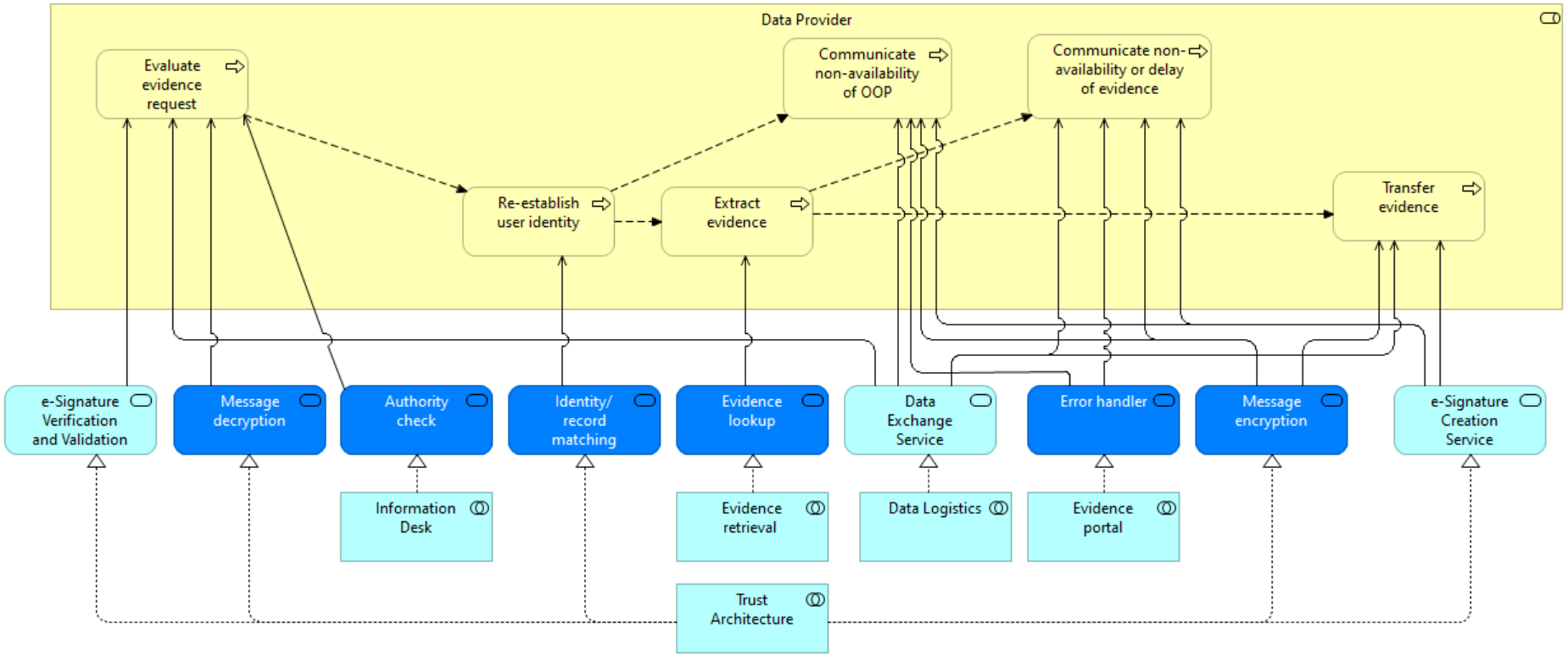


Figure 7: Process Realization of the DP Process

Table 9 describes the Application Services required to execute the Intermediation Pattern. An application service defines an explicitly exposed application behaviour. An application service exposes the functionality of components to their environment. This functionality is accessed through one or more application interfaces or user interfaces.

Table 9: Application Services of the Intermediation Pattern

Application Service	Serves Role	Description	Specialization of Source	Realized by Application Collaboration
eProcedure Initiation	U	Generic service, see 17.	DE4A specific	eProcedure Portal
User Authentication (UI)	U	Generic service, see 11.	EIRA	Trust Architecture
eProcedure termination	U	Generic service, see 16.	DE4A specific	eProcedure Portal
Explicit request	U	Generic request, see 34.	DE4A specific	eProcedure Portal
Evidence status overview	U, DC	Generic service, see 2.	DE4A specific	Evidence interchange management
Evidence preview	U, DC	Generic service, see 18.	DE4A specific	Evidence interchange management
eProcedure save and resume	U	Generic service, see 8. Also see the application collaboration in Figure 8.	DE4A specific	eProcedure Portal
eProcedure confirmation	U	Generic service, see 20.	DE4A specific	eProcedure Portal
eProcedure submission	U	Generic service, see 19.	DE4A specific	eProcedure Portal
Receive (public) service result	U	The user process end (happy flow) with receiving the result of the (public) service. This service takes care of this.	DE4A specific	
Authentication initiation	DC	Generic service, see 6.	EIRA	Trust Architecture
Identity/record matching	DC, DP	Generic service, see 5.	DE4A specific	Trust Architecture
Alternative channel	DC	Generic service, see 22.	DE4A specific	eProcedure Portal
Procedural requirements determination	DC	Generic service, see 21.	DE4A specific	eProcedure Portal

Application Service	Serves Role	Description	Specialization of Source	Realized by Application Collaboration
Requirements/evidence matching	DC	Generic service, see 4.	DE4A specific	eProcedure Portal
Available evidence determination	DC	Generic service, see 23.	DE4A specific	eProcedure Portal
Cross-border evidence matching	DC	Generic service, see 31.	DE4A specific	Information Desk
Legal basis check	DC	Generic service, see 12.	DE4A specific	Information Desk
Inquire routing information	DC	Generic service, see 28.	DE4A specific	Information Desk
Message encryption	DC, DP	Generic service, see 9.	DE4A specific	Trust Architecture
e-Signature Creation Service	DC, DP	Generic service, see 3.	EIRA	Trust Architecture
Evidence request tracker	DC	Generic service, see 27.	DE4A specific	Evidence interchange management
Data Exchange Service	DC (2x), DP (2x)	Generic service, see 1.	EIRA	Data Logistics
Message decryption	DC, DP	Generic service, see 14.	DE4A specific	Trust Architecture
e-Signature Verification and Validation Service	DC, DP	Generic service, see 15.	EIRA	Trust Architecture
Evidence shredder	DC	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.	DE4A specific	Evidence interchange management

Application Service	Serves Role	Description	Specialization of Source	Realized by Application Collaboration
Evidence status tracker	DC	Generic service, see 13.	DE4A specific	Evidence interchange management
Authority check	DP	The DP establishes that the DC can request the evidence. This service handles the lookup of authorisation. 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 (cf. Authority to evidence matrix in Table 13).	DE4A specific	Information Desk
Evidence lookup	DP	Generic service, see 7.	DE4A specific	Evidence retrieval

4.2.4 Application Collaboration

The Application Collaboration views show how different functional application components interact via interfaces in order 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. Solution Building Blocks (SBBs) must be identified or developed for each of these elements. In the Pilot's sections, e.g. chapters 6,7 and 0 there are specific sections addressing the selection of candidate SBBs.

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 chose to terminate it if he/she wishes. 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 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 DP(s).

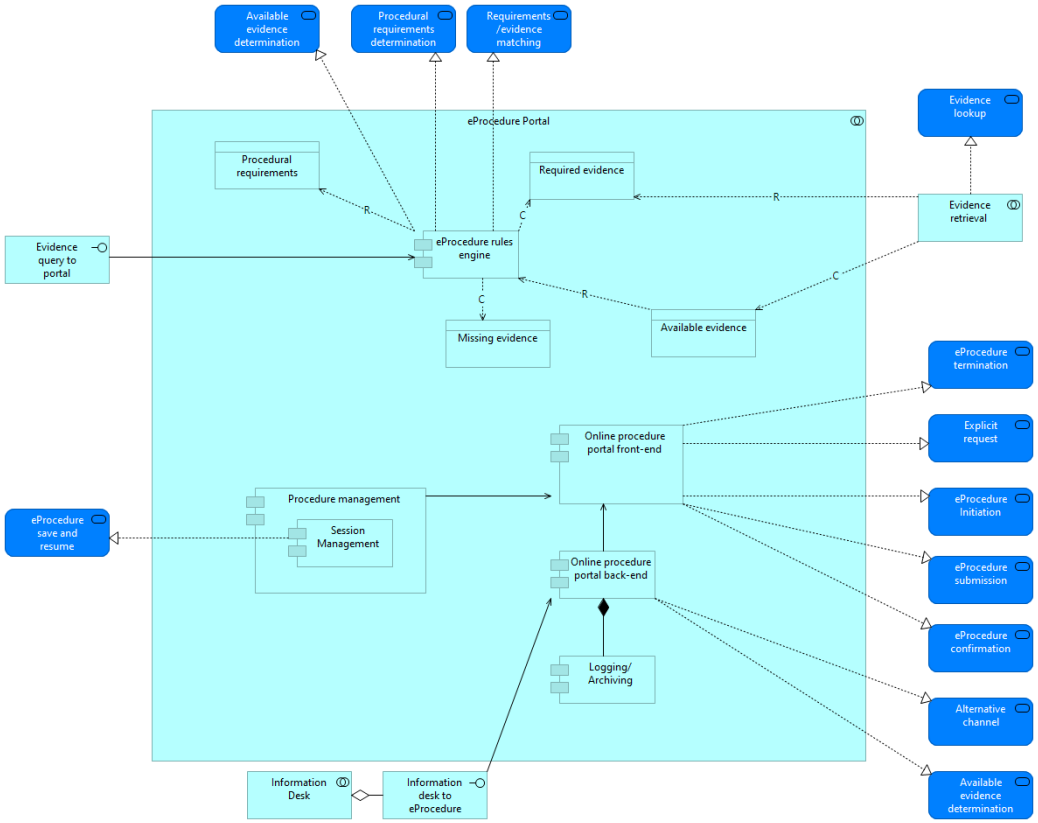


Figure 8: eProcedure Portal

Table 10: Application Components of the eProcedure Portal

Application Component	Description	Application Service
Online Procedure Portal Front-End	Generic component, see o.	• eProcedure initiation • Explicit request • eProcedure termination • eProcedure submission • eProcedure conformation
Online procedure portal back-end	Generic component, see n.	•
Session management	Generic component, see r.	• eProcedure save and resume
eProcedure rules engine	Generic component, see f.	• Procedural requirements determination • Requirements/evidence matching
Logging/Archiving	Application component managing logging and archiving of data. Also, to support the audit trail.	• All services

Table 11: Data objects eProcedure Portal

Data object	Description
Procedural requirements	The requirements applicable to a procedure
Required evidence	The evidence required to fulfil a requirement
Available evidence	The evidence that is already available to a DC and can be (re)used
Missing evidence	The evidence that is missing

The Information desk application collaboration combines multiple co-operating application components. It offers generic functionality used by DC and DP to facilitate the OOP exchanges. It offers functionality to do the cross-border evidence matching, i.e. using an evidence map, mapping required evidences to equivalent evidences in another MS. The DC uses the information desk to lookup routing information, i.e. where to request a piece of evidence. DC can use it

to do a legal basis check in case no user request or approval is needed. The DP consults the information desk to establish that the DC is authorized/allowed to request some evidence type.

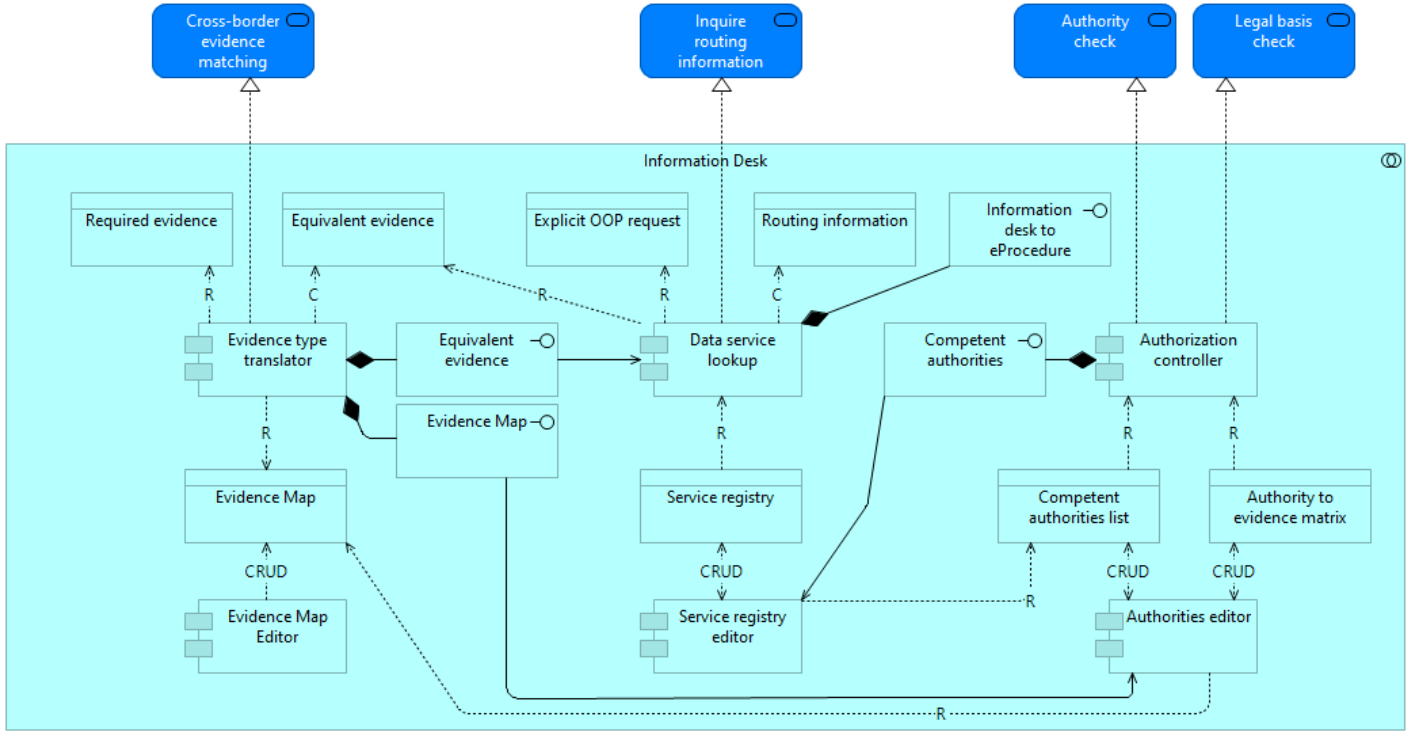


Figure 9: Information Desk

Table 12: Application Components of the Information Desk

Application Component	Description	Application Service
Evidence type translator	Generic component, see l. There are currently several approaches under investigation by WP3.	• Cross-border evidence matching
Evidence Map Editor	Application component maintaining the evidence mappings.	
Data service lookup	Generic component, see e.	• Inquire routing information
Service registry editor	Application component maintaining the service registry.	
Authorization controller	Generic component, see b.	• Authority check • Legal basis check
Authorities editor	Application component maintaining the list of competent authorities and the relationships between those authorities and evidences.	
Equivalent evidence	Evidence type translator exposes an interface in order to be called by other components, e.g. inquire about equivalent evidences.	
Evidence Map	Evidence type translator exposes an interface in order to be called by other components, e.g. request some mapping of evidences.	
Competent authorities	Authorization controller exposes an interface in order to be called by other components, e.g. to establish authorization for a competent authority.	

Table 13: Data objects Information Desk

Data object	Description
Required evidence	The evidence required to fulfil a requirement
Equivalent evidence	A piece of evidence that is equivalent to another piece of evidence in another member state

Data object	Description
Evidence Map	A mapping of evidence to equivalent evidences
Explicit OOP request	A representation of the explicit request for OOP transfer by the user.
Routing information	Information where (what end point) to request a piece of evidence, i.e. what DP
Service registry	A registry containing services for lookup purposes
Competent authorities list	A store containing the competent authorities
Authority to evidence matrix	A store containing for each authority the evidences it can provide and it is allowed to request

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 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. 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.

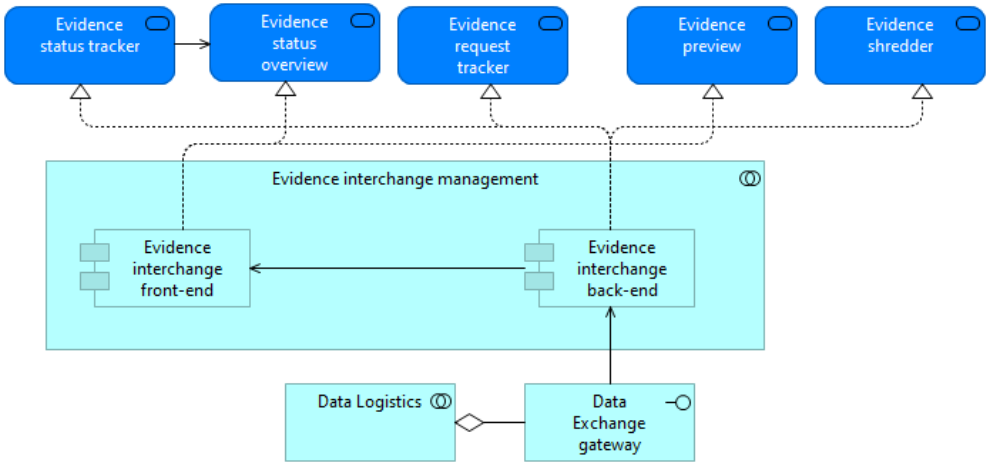


Figure 10: Evidence Interchange Management

Table 14: Application components of Evidence Interchange Management

Application Component	Description	Application Service
Evidence interchange front-end	Generic component, see h.	• Evidence status overview • Evidence preview
Evidence interchange back-end	Generic component, see g .	• Evidence status tracker • Evidence shredder

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 by the DC to initiate the authentication process and it implements functionality so the user can authenticate him/herself. 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 messages2. 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.

[2] Usage of eSeals TBD.

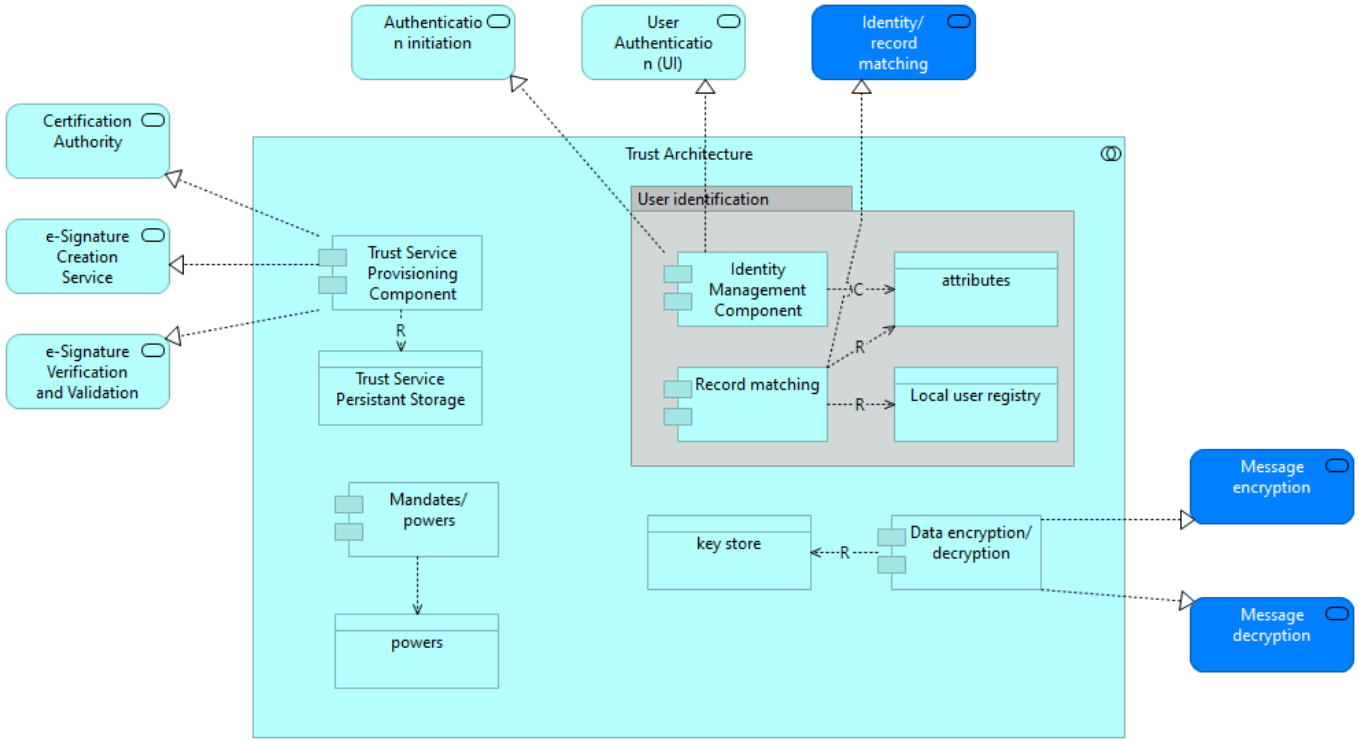


Figure 11: Trust Architecture

Table 15: Application components of Trust Architecture

Application Component	Description	Application Service
Trust Service Provisioning Component	Generic component, see v.	• e-Signature Creation Service • e-Signature Verification and Validation Service
Identity Management Component	Generic component, see m.	• Authentication initiation • User Authentication (UI)

Application Component	Description	Application Service
Record matching	Generic component, see q.	• Identity/record matching
Data encryption/decryption	Generic component, see c.	• Message encryption • Message decryption
Mandates/powers	Handles the mandates/powers for legal and natural persons, i.e. persons representing other persons.	TBD in context of DBA pilot.

Table 16: Data objects Trust Architecture

Data object	Description
Trust Service Persistent Storage	Place to store certificates, e-signatures, e-timestamps and e-seals.
Powers	Electronic powers of representation and mandates. Allow natural persons to act on behalf of other natural or legal persons
Attributes	eIDAS attributes (mandatory or optional) and possibly non-eIDAS attributes used for identity matching
Local user registry	The local registry of the DP against which the attributes are compared
Key store	A store (hardware and/or software) used for securely managing keys (store, retrieve)

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.

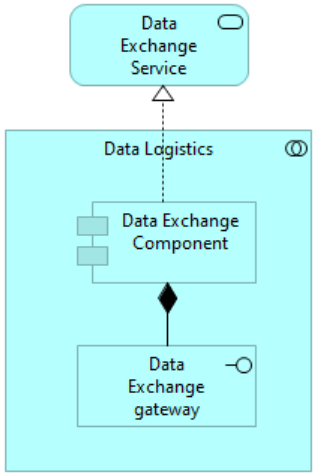


Figure 12: Data Logistics

Table 17: Application components of Data Logistics

Application Component	Description	Application Service
Data Exchange Component	Generic component, see d.	• Data Exchange Service
Data Exchange gateway	The Data Exchange Component exposes an interface in order for other components to make use of it.	

The Evidence portal application collaboration constitutes back-end functionality implementing error handling for the DP. It interfaces with Evidence retrieval and Data logistics.

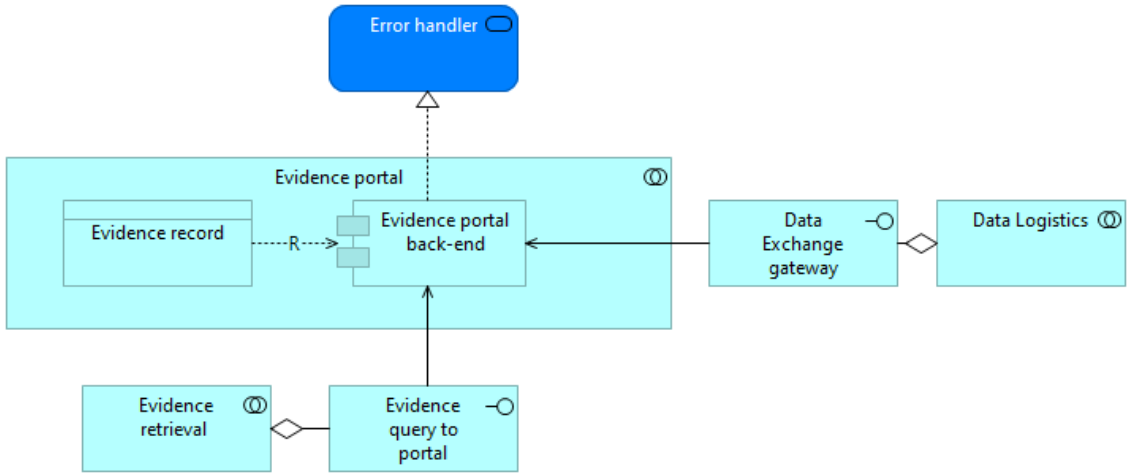


Figure 13: Evidence portal

Table 18: Application components of Evidence portal

Application Component	Description	Application Service
Evidence portal back-end	Generic component, see i.	Data Exchange Service

Table 19: Data objects Evidence portal

Data object	Description
Evidence record	This data object represents the storage of evidence so it can be used by the back-end.

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.

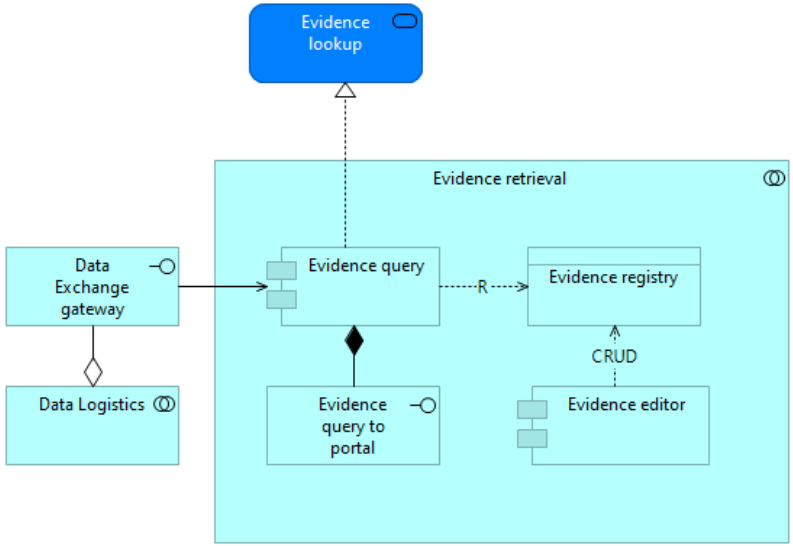


Figure 14: Evidence Retrieval

Table 20: Application components of Evidence retrieval

Application Component	Description	Application Service
Evidence query	Generic component, see k.	• Evidence lookup
Evidence editor	Application component to manage creation/insertion, modification? and deletion of evidences in an evidence registry.	
Evidence query to portal	An interface to expose the query functionality so external components can use it e.g. eProcedure.	

Table 21: Data objects Evidence Retrieval

Data object	Description
Evidence registry	A place where official records are kept, or a book or system for keeping an official record of evidences.

4.3 User-supported Intermediation

4.3.1 Working Hypothesis 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 members of DE4A.

Table 22: User-supported Intermediation pattern working hypothesis 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 PD evidence retrieval processes. The control of the overall process is thus not transferred to the user.
Multiple, complementary, overlapping or conflicting evidence equivalents	Multi-evidence cases must in principle be supported – Identical to Intermediation (see 4.2.1)	Identical to Intermediation (chapter 4.2)

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Interrupted vs. Uninterrupted exchange	The assumption can be slightly relaxed in comparison to Intermediation (chapter 4.2), as the direct interaction between U and DP makes it easier to communicate delays transparently. In order to prevent that process instances, need to be kept alive across multiple platforms in multiple MS, we treat the interdependencies as 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, arguably, more important, because of the higher probability that the eProcedure session hits a time-out during the addition time involved in the direct interaction of the U with the DP in comparison to the Intermediation pattern.	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 evidence that resides still in paper archives. We might 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 [..].
Explicit request and transitivity between actors	The assumption can be relaxed in comparison to the Intermediation pattern (see 4.2.1)	The user authenticates himself 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 (see 4.2.1)	The preview is provided by the DP.
Identity and Record Matching	The assumption can be relaxed in comparison to the Intermediation pattern (see 4.2.1)	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 U to perform the match.
Transitivity of user identity	The assumption can be relaxed in comparison to the Intermediation pattern (see 4.2.1)	The user authenticates himself at the DP.

Interdisciplinary Topic	Hypothesis / Principle	Implications and Limitations
Hand-on of UI between actors	The DP provides an UI to the DC that the user can navigate to.	
Mandate and Proxy	Identical to Intermediation (chapter 4.2), however not relevant for the PSA	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 (see 4.2.1)	
Structured data vs. unstructured data	Identical to Intermediation (see 4.2.1)	
Automated re-use of data	Identical to Intermediation (see 4.2.1)	
Production system and real-life cases	The direct interaction between U and DP allows the pilot to go live in production under current national legal constraints	There might still be unforeseen technical, organisational or legal barriers that make a full production use of the pilot systems impractical for some MSs. DE4A Deliverables. D1.7 [4] [forthcoming] will be an important input into this investigation.

4.3.2 Business Process Collaboration

Figure 15 models the user-supported intermediation pattern in BPMN [2] 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) show the interactions – the conversation – between these participants.

In Table 23 the activities of all participants are listed roughly in chronological order across all three processes. The conversations between the participants are described in Table 24, Table 25 and Table 26, listing the messages between the U and DC (Table 24), between DC and DP (Table 25) and between U and DP (Table 26) respectively.

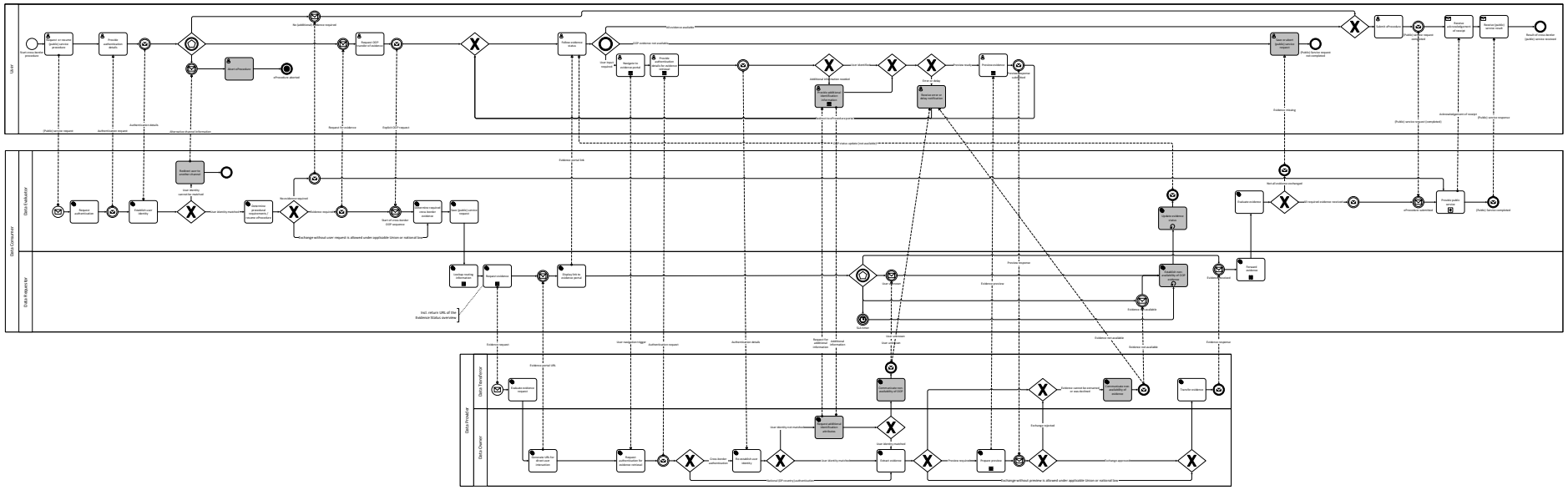


Figure 15: Business Process Collaboration view of the User-Supported Intermediation Pattern

In Table 23 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 15 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[6] 204[6] The third column contains the task type (please refer to the BPMN 2.0 standard specification[2]) as shown in in Figure 4 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 [6] or Article 3(1) of the SDGR [3]. The fourth column describes the business activity in concise language.

Table 23: 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, see Table 6

Activity / UC	Role	Type	Description
Request authentication	DE	Service	Identical with the Intermediation Pattern, see Table 6
Provide authentication details	U	User	Identical with the Intermediation Pattern, see Table 6
Establish user identity	DE	Service	Identical with the Intermediation Pattern, see Table 6
Redirect user to another channel	DE	Service	Identical with the Intermediation Pattern, see Table 6
Abort eProcedure	U	User	Identical with the Intermediation Pattern, see Table 6
Determine procedural requirements	DE	Service	Identical with the Intermediation Pattern, see Table 6
Request OOP transfer of evidence	U	User	Identical with the Intermediation Pattern, see Table 6
Determine required cross-border evidence	DE	Service	Identical with the Intermediation Pattern, see Table 6
Save (public) service request	DE	Service	The eProcedure and all information provided by the U 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 U 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 U 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.

Activity / UC	Role	Type	Description
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 U 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. This might not be generalized to all potential cases (cf. OOTS target architecture), not the least for exchanges that do not require user preview and approval
Generate URL for direct user interaction	DO	Service	The DP generates a URL as landing place for the U to navigate that is specific for the required evidence type.
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 U 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 U has the national eID of the DP country available (case 1 and 2 in Table 4). The case of using the national eID scheme would consequently be quite common. The DP provides both options to the U.
Provide authentication details for evidence retrieval	U	User	The U uses the means available to him 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.
Re-establish user identity	DO	Service	The DO matches the information about the user (i.e. eIDAS mandatory and optional 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.

Activity / UC	Role	Type	Description
Provide additional identification information	U	User	Exception handling activity: Interactive form- of 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, see Table 6
Extract evidence	DO	Service	Identical with the Intermediation Pattern, see Table 6
Communicate non-availability of evidence	DT	Service	Identical with the Intermediation Pattern, see Table 6
Prepare preview	DO	Service	The DO prepares a preview for the U 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.
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 U 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, see Table 6
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 and OOP transfer of evidence is not be 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

Activity / UC	Role	Type	Description
			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, see Table 6
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, see Table 6
Save or abort (public) service request	U	User	Identical with the Intermediation Pattern, see Table 6
Submit eProcedure	U	User	Identical with the Intermediation Pattern, see Table 6
Receive acknowledgement of receipt	U	Receive	The U 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.

Activity / UC	Role	Type	Description
Provide public service	DE	Subprocess	Identical with the Intermediation Pattern, see Table 6
Receive (public) service result	U	Receive	Identical with the Intermediation Pattern, see Table 6

In Table 24 describes the conservation between U and DC by listing the exchanged messages in chronological order. Table 25 does the same for the conversation between DC and DP and Table 26 for U and DP.

Table 24: User-Supported Intermediation - Conversation between User and Data Consumer

From	Message	To	Description
U	(Public) service request	DC	Identical with the Intermediation Pattern, see Table 24
DC	Authentication request	U	Identical with the Intermediation Pattern, see Table 24
U	Authentication details	DC	Identical with the Intermediation Pattern, see Table 24
DC	Alternative channel information	U	Identical with the Intermediation Pattern, see Table 24
DC	Request for evidence	U	Identical with the Intermediation Pattern, see Table 24
U	Explicit OOP request	DC	Identical with the Intermediation Pattern, see Table 24
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, see Table 24
U	(Public) service request (completed)	DC	Identical with the Intermediation Pattern, see Table 24

From	Message	To	Description
DC	Acknowledgement of receipt	U	Identical with the Intermediation Pattern, see Table 24
DC	(Public) service response	U	Identical with the Intermediation Pattern, see Table 24

Table 25: User-Supported Intermediation - Conversation between Data Consumer and Data Provider

From	Message	To	Description
DC	Evidence request	DP	Identical with the Intermediation Pattern, see Table 25
DP	Evidence portal URL	DC	Identical with the Intermediation Pattern, see Table 25
DP	User unknown	DC	Identical with the Intermediation Pattern, see Table 25
DP	Evidence not available	DC	Identical with the Intermediation Pattern, see Table 25
DP	Evidence response	DC	The evidence in electronic format – Identical with the Intermediation Pattern, see Table 25

Table 26: 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 identify 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

4.3.3 Process Realization

The following diagram shows how the User process (cf. Figure 15) is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by application collaborations which are presented in section 4.3.4. In Table 27 the application services are described.

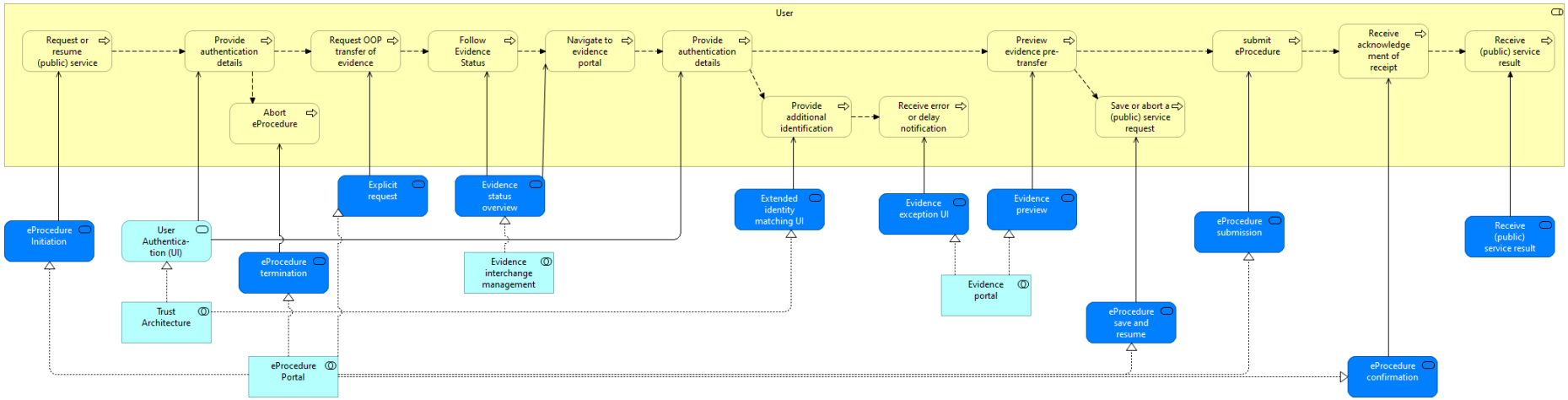


Figure 16: Process Realization of the User process

The following diagram shows how the Data Consumer process (cf. Figure 15) is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by application collaborations which are presented in section 4.3.4. In Table 27 the application services are described.

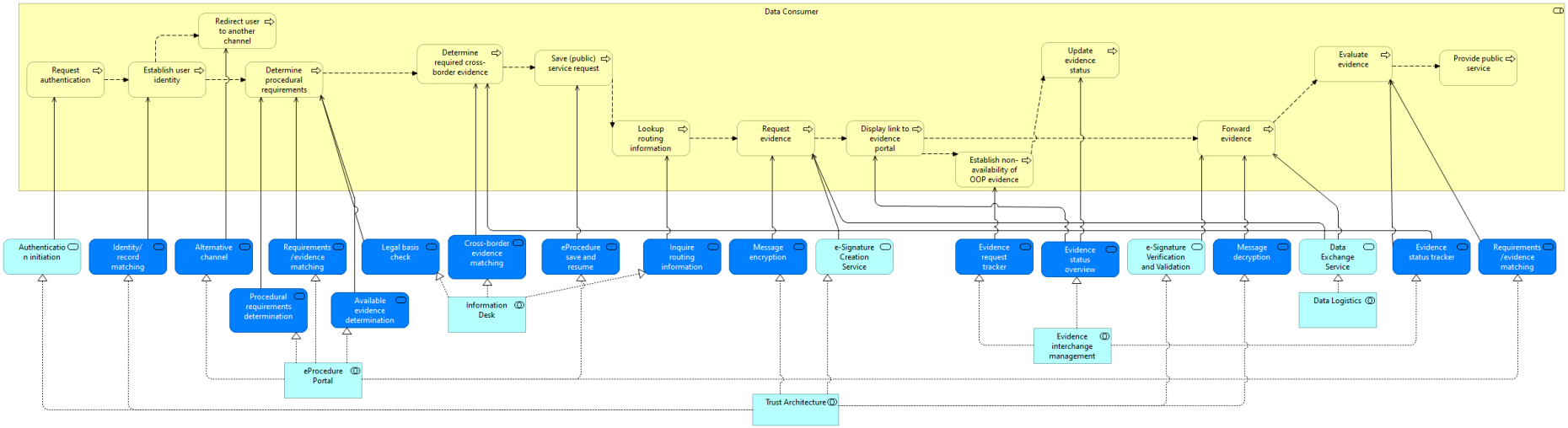


Figure 17: Process Realization of the Data Consumer process

The following diagram shows how the Data Provider process (cf. Figure 15) is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by application collaborations which are presented in section 4.3.4. In Table 27 the application services are described.

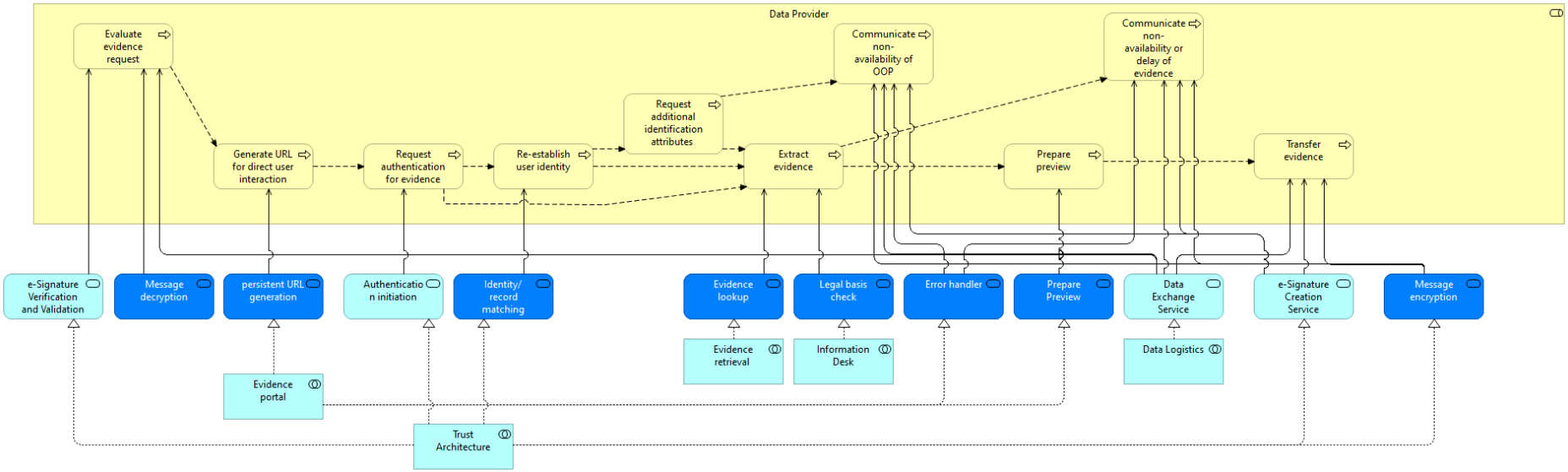


Figure 18: Process Realization of the Data Provider Process

Table 27: Application Services of the User Supported Intermediation Pattern

Application Service	Serves Role	Description	Specialization of Source	Realized by Application Collaboration
eProcedure Initiation	U	Generic service, see 17.	DE4A specific	eProcedure Portal
User Authentication (UI)	U	Generic service, see 11.	EIRA	Trust Architecture
eProcedure termination	U	Generic service, see 16.	DE4A specific	eProcedure Portal
Explicit request	U	Generic service, see 34.	DE4A specific	eProcedure Portal
Evidence status overview	U (2x), DC (2x)	Generic service, see 2.	DE4A specific	Evidence interchange management
Extended identity matching UI	U	Generic service, see 24.	DE4A specific	Trust Architecture

Application Service	Serves Role	Description	Specialization of Source	Realized by Application Collaboration
Evidence exception UI	U	Generic service, see 33.	DE4A specific	Evidence Portal
Evidence preview	U	Generic service, see 18.	DE4A specific	Evidence interchange management
eProcedure save and resume	U	Generic service, see 8.	DE4A specific	eProcedure Portal
eProcedure submission	U	Generic service, see 19.	DE4A specific	eProcedure Portal
eProcedure confirmation	U	Generic service, see 20.	DE4A specific	eProcedure Portal
Receive (public) service result	U	Identical to Intermediation pattern, see section 4.2.3	DE4A specific	eProcedure Portal
Authentication initiation	DC, DP	Generic service, see 6. The difference for USI is that the DP now also initiates user authentication.	EIRA	Trust Architecture
Identity/record matching	DC, DP	Generic service, see 5.	DE4A specific	Trust Architecture
Alternative channel	DC	Generic service, see 22.	DE4A specific	eProcedure Portal
Procedural requirements determination	DC	Generic service, see 21.	DE4A specific	eProcedure Portal
Requirements/evidence matching	DC	Generic service, see 4.	DE4A specific	eProcedure Portal
Available evidence determination	DC	Generic service, see 23.	DE4A specific	eProcedure Portal
Cross-border evidence matching	DC	Generic service, see 31.	DE4A specific	Information Desk
Legal basis check	DC	Generic service, see 12.	DE4A specific	Information Desk
Inquire routing information	DC	Generic service, see 28.	DE4A specific	Information Desk

Application Service	Serves Role	Description	Specialization of Source	Realized by Application Collaboration
Evidence status tracker	DC	Generic service, see 13.	DE4A specific	Evidence interchange management
Message encryption	DC, DP	Generic service, see 9.	DE4A specific	Trust Architecture
e-Signature Creation Service	DC, DP	Generic service, see 3.	EIRA	Trust Architecture
Evidence Request tracker	DC	Generic service, see 27.	DE4A specific	Evidence interchange management
Data Exchange Service	DC (2x), DP (3x)	Generic service, see 1. In the USI pattern the DP has an extra usage of this service.	EIRA	Data Logistics
Message decryption	DC, DP	Generic service, see 14.	DE4A specific	Trust Architecture
e-Signature Verification and Validation Service	DC, DP	Generic service, see 15.	EIRA	Trust Architecture
persistent URL generation	DP	A persistent URL is generated for the purpose of navigation. Based on this URL the DC can forward/redirect the U to the portal of the DP for the required evidence.	DE4A specific	Evidence Portal
Prepare Preview	DP	The DP prepares a preview for the U and displays it in the UI of the evidence portal.	DE4A specific	Evidence Portal
Evidence lookup	DP	Generic service, see 7.	DE4A specific	Evidence retrieval
Error handler	DP	Generic service, see 10.	DE4A specific	Evidence Portal

4.3.4 Application Collaboration

The Application Collaboration views show how different functional application components interact via interfaces in order 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. Solution building blocks must be identified or developed for each of these elements.

This eProcedure portal is basically the same Application Collaboration as for the Intermediation pattern, see section 4.2.4.

The difference is that an additional occurrence of Available evidence determination, realized by the Online procedure portal back-end application component, is not present for USI. The data objects are the same.

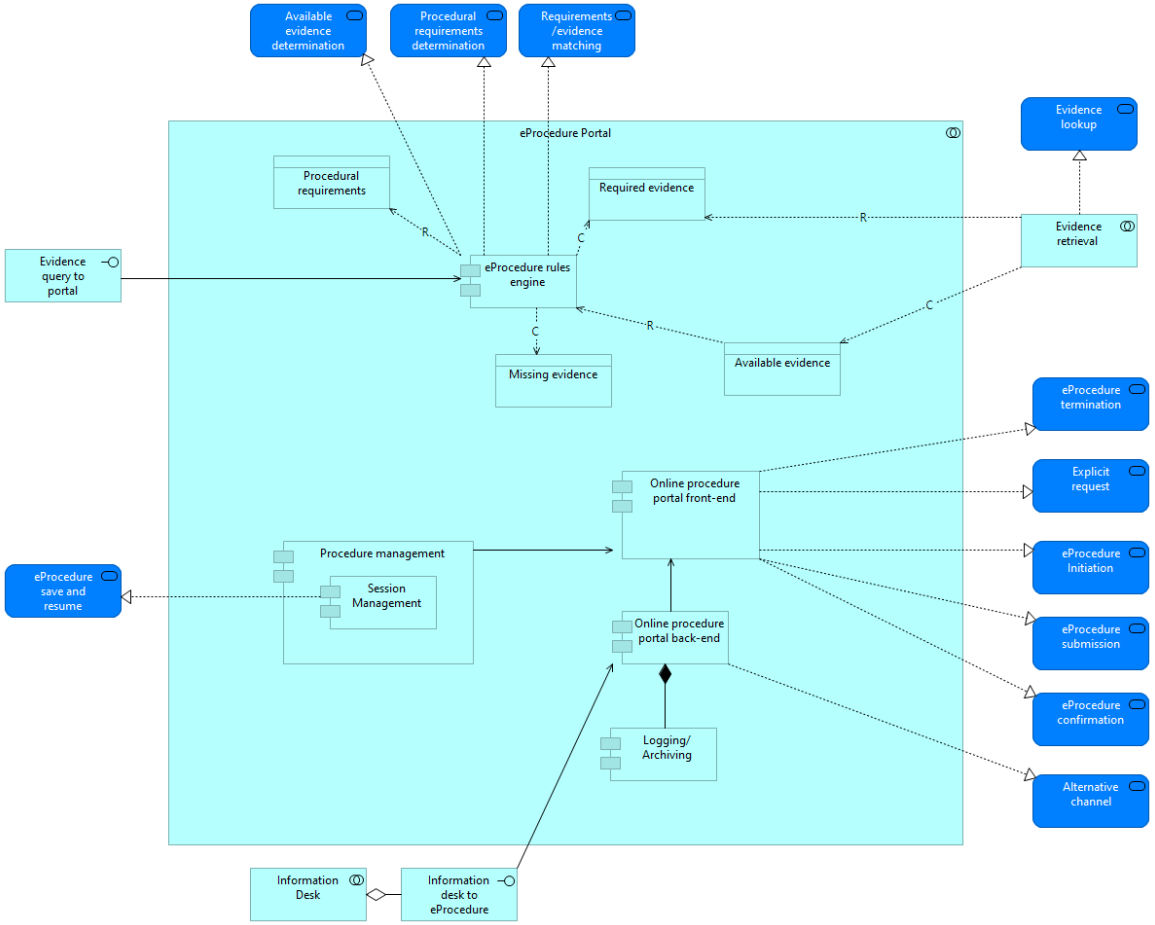


Figure 19: eProcedure Portal

The Evidence portal application collaboration constitutes front-end and back-end functionality. The back end implements the generation of a persistent URL and error handling for the DP. Furthermore, it supports preparing a preview of the evidence for the user. The front-end provides an UI for exception handling and the UI for previewing the evidence. The collaboration interfaces with Evidence retrieval and the Data Exchange gateway.

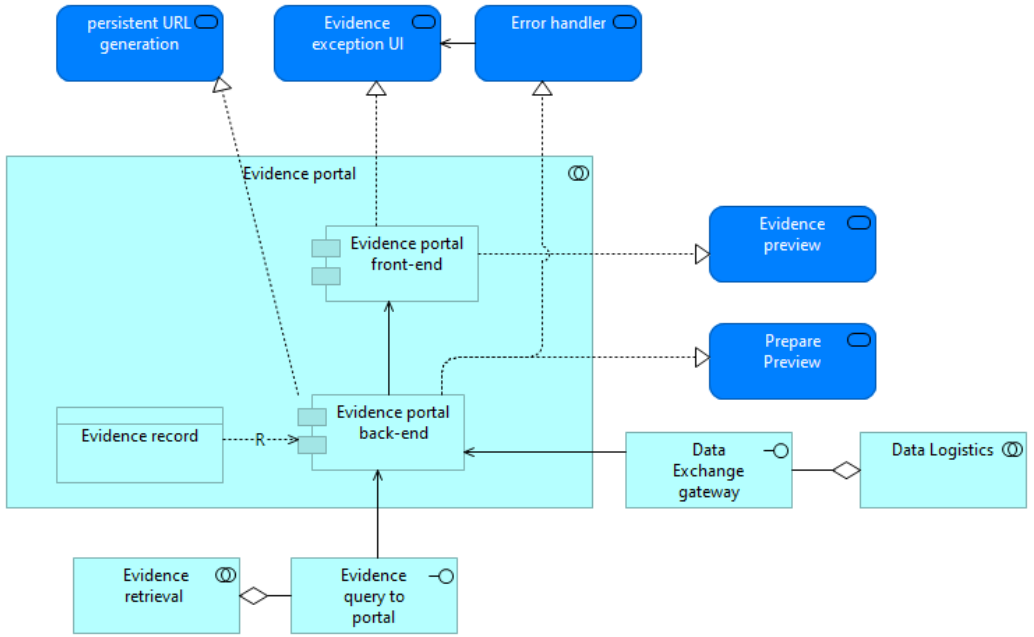


Figure 20: Evidence Portal

Table 28: Application components of the Evidence Portal

Application Component	Description	Application Service
Evidence portal front-end	Generic component, see j	• Evidence Exception UI • Evidence Preview
Evidence portal back-end	Generic component, see i.	• Persistent URL generation • Error handler • Prepare preview

Table 29: Data objects Evidence portal

Data object	Description
Evidence record	

The Evidence Interchange Management application collaboration aggregates two high-level application components providing all functionality to manage the interchange of evidences. The back-end component supports keeping track of the requests and status of evidence(s). The front-end component provides an evidence status overview. Evidence Interchange Management application collaboration interfaces with the information desk.

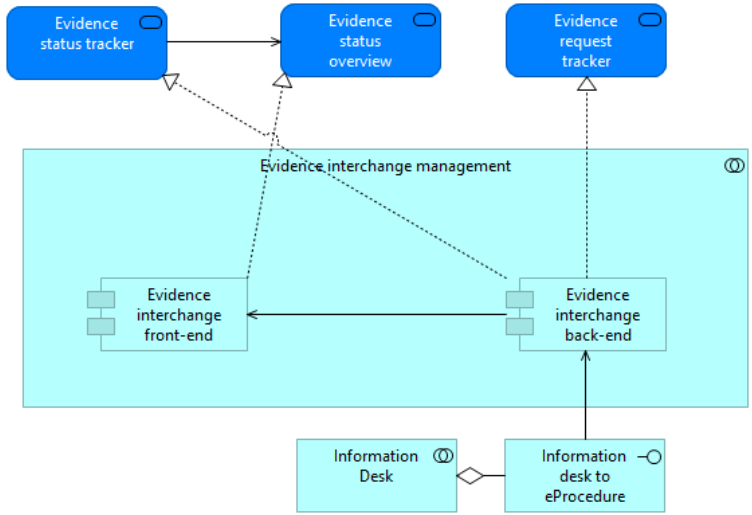


Figure 21: Evidence Interchange Management

Table 30: Application components of Evidence Interchange Management

Application Component	Description	Application Service
Evidence interchange front-end	S Generic component, see h.	• Evidence status tracker • Evidence status overview

Application Component	Description	Application Service
Evidence interchange back-end	Generic component, see g.	• Evidence request tracker

Note: difference compared to Intermediation is two application service less: no Evidence Preview and no Evidence shredder.

The Trust Architecture application collaboration is the same as for the Intermediation pattern, see section 4.2.44.2.4.

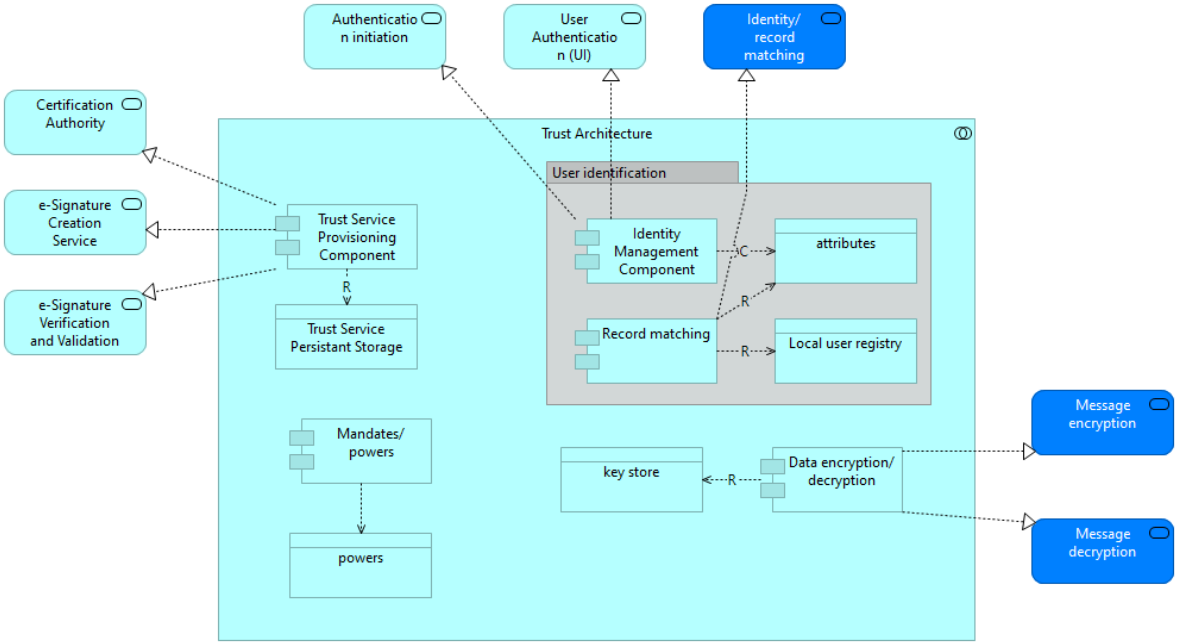


Figure 22: Trust Architecture

Table 31: Application Components Trust Architecture

Application Component	Description	Application Service
Trust Service Provisioning Component	Generic component, see v.	• e-Signature Creation Service • e-Signature Verification and Validation Service
Identity Management Component	Generic component, see m.	• Authentication initiation • User Authentication (UI)
Record matching	Generic component, see q.	• Identity/record matching
Data encryption/decryption	Generic component, see c.	• Message encryption • Message decryption
Mandates/Powers	Same as for intermediation pattern, see section 4.2.4	

Table 32: Data objects Trust Architecture

Application Component	Description	Application Service
Same as for the Intermediation pattern, see section 4.2.4.		

The Data logistics application collaboration is the same as for the Intermediation pattern, see section 4.2.4.

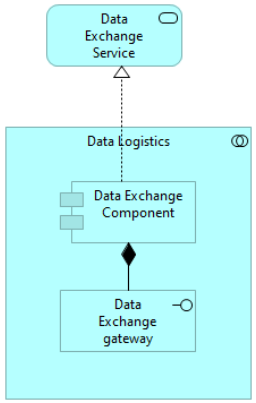


Figure 23: Data Logistics

Same as for Intermediation pattern, see section 4.2.44.2.4.

The Evidence retrieval application collaboration is the same as for the Intermediation pattern, see section 4.2.44.2.4.

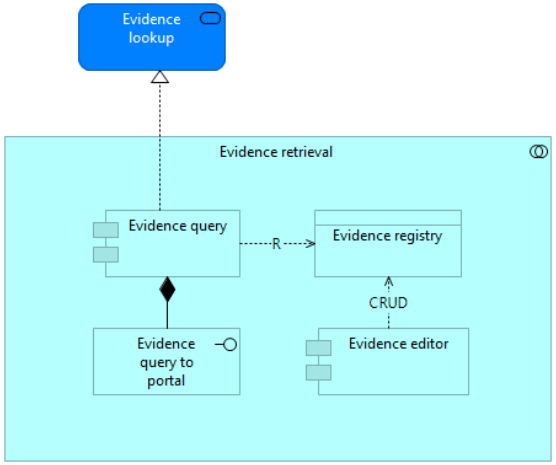


Figure 24: Evidence Retrieval

4.4 Subscription and Notification

Postponed.

Needed by DBA. This pattern will be elaborated in the September/October 2020 timeframe. TBC

4.5 Lookup

Postponed

Needed by DBA. This pattern will be elaborated in the September/October 2020 timeframe. TBC

4.6 Verifiable Credentials

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).

The Verifiable Credentials pattern (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) under his possession. Edge agent serves as an instrument with which 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.

4.6.1 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 members of DE4A.

Table 33: Verifiable Credentials pattern working hypothesis 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 [6]
Multiple, complementary, overlapping or conflicting evidence equivalents	Multi-evidence cases must in principle be supported – Identical to Intermediation (see 4.2.1)	Identical to Intermediation (see 4.2.1)

Interdisciplinary Topic	Hypotheses / Principle	Implications and Limitations
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 becomes 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-manages 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 (handing it on).	We are not considering the exchange without user request and approval in the VC pattern (i.e. based on national or Union law).
Identity and Record Matching	The assumption can be relaxed in comparison to the Intermediation pattern (see 4.2.1)	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 U to perform the match.
Transitivity of user identity	The assumption can be relaxed in comparison to the Intermediation pattern (see 4.2.1)	The user authenticates themselves 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 rooting 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.
Mandate and Proxy	Identical to Intermediation (chapter 4.2), however not relevant for the PSA	The matching of interaction pattern to pilot use cases means that the DBA pilot is not intending to use the VC pattern, hence mandates and powers are not in scope.
Encryption Gap	The assumption can be relaxed in comparison to the Intermediation pattern (see 4.2.1)	Encryption is handled by the DID connection between U and DC and between U 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 will need to be agreed.

Interdisciplinary Topic	Hypotheses / Principle	Implications and Limitations
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 user case this means, for example, that the VC is an evidence that a diploma is existing, meaning was 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 issues a diploma in form of a VC that corresponds to the VC schema adopted by DE4A. This case should be compatible with the VC pattern proposed in this document.

4.6.2 Business Process Collaboration

Figure 25 models the Verifiable Credential pattern in BPM notation. Using the colouring of the tasks in the BPMN, the different point 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, while the blue colour represents the activities performed in the DP portal. In Table 34 all business activities are described.

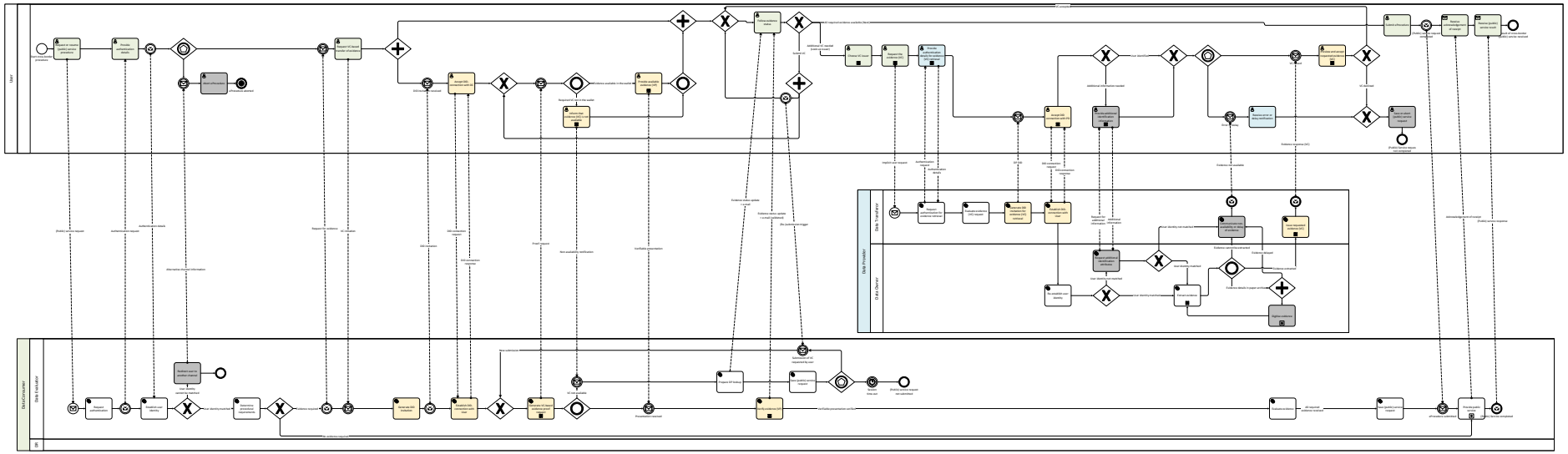


Figure 25: Business Process Collaboration view of the Verifiable Credential Pattern

The business collaboration diagram can be roughly divided in three section: The first section shows the dialogue between the User and the DP 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 data consumers. 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 the Figure 25 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 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 his (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 34: Business Activities of the Verifiable Credential Pattern

Activity / UC	Role	Type	Description
Request or resume (public) service procedure	U	User	Identical with the Intermediation Pattern, see Table 6
Request authentication	DE	Service	Identical with the Intermediation Pattern, see Table 6
Provide authentication details	U	User	Identical with the Intermediation Pattern, see Table 6
Establish user identity	DE	Service	Identical with the Intermediation Pattern, see Table 6
Redirect user to another channel	DE	Service	Identical with the Intermediation Pattern, see Table 6
Abort eProcedure	U	User	Identical with the Intermediation Pattern, see Table 6
Determine procedural requirements	DE	Service	Identical with the Intermediation Pattern, see Table 6
Request VC-based transfer of evidence	U	User	The U 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 U and DE.
Generate DID invitation	DE	Service	The DE generates an invitation for a DID connection with a U. The invitation is represented 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 U agent.
Accept DID connection with DC	U	User	The U responds with accepting or rejecting an invitation for a DID connection generated by DE by scanning a QR code presented on the eProcedure portal.

Activity / UC	Role	Type	Description
Establish DID connection with User	DE	Service	Both parties (agents) create a DID connection in case none-existed before, otherwise the DID connections is just initialised. The DE informs U 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 U.
Provide available evidence (VP)	U	User	The U is informed about available evidence (VC's) 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 (VC's) 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. rooting 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 amount of time window in which the user can provide required evidence in the form of VP.
Follow evidence status	U	User	After the U chooses to provide the evidence required in the form of a VC and establishes a DID connection with the DE, the eProcedure portal shows him 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 U has the option to PROVIDE the EVIDENCE or LOOK UP THE VC-ISSUER.

Activity / UC	Role	Type	Description
Choose VC issuer	U	User	The U chooses a DP in an interactive way that is capable to provide evidence in the form of VC's that are needed for U to submit eProcedure.
Request the evidence (VC)	U	User	The user informs a DP that he requests the evidence in the form of VC's by way of following the link displays in the Procedure portal. This action starts the process of the preparation for a DID Connection process between U and DT.
Request authentication for evidence (VC) retrieval	DT	Service	The DO requests the U for to authenticate themselves. This can happen in two ways, either using eIDAS (default) or using the eID of the DP MS, in case that the U has the national eID of the DP country available (case 1 and 2 in Table 4). The case of using the national eID scheme would consequently be quite common. The DP provides both options to the U.
Provide authentication details for evidence (VC) retrieval	U	User	The U uses the means available to him 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 U 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 U. 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 U agent.
Accept DID connection with DP	DT	Service	The U responds with accepting or rejecting an invitation for a DID connection generated by DE by scanning a QR code presented on the DT portal.

Activity / UC	Role	Type	Description
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 initialised. The DT informs U about the success of the connection establishment.
Re-establish user identity	DO	Service	Identical with the User -supported Intermediation pattern, see Table 23
Request additional identification attributes	DO	Service	Identical with the User -supported Intermediation pattern, see Table 23
Provide additional identification information	U	User	Identical with the User -supported Intermediation pattern, see Table 23
Extract evidence	DO	Service	Identical with the Intermediation Pattern, see Table 6
Digitise evidence	DO	Subprocess	The DO digitize 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 U 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, see Table 23
Save or abort (public) service request	U	User	Identical with the Intermediation Pattern, see Table 6
Issue requested evidence (VC)	DT	Service	The DT issue evidence in the form of VC to a U
Preview and accept requested evidence (VC)	U	User	The U 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 his digital wallet.
Verify evidence (VP)	DE	Service	The DC 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) • U verification (is authenticated U 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, see Table 6

Activity / UC	Role	Type	Description
Submit eProcedure	U	User	Identical with the Intermediation Pattern, see Table 6
Provide public service	DE	Subprocess	Identical with the Intermediation Pattern, see Table 6
Receive acknowledgment or receipt	U	Receive	Identical with the User-supported Intermediation pattern, see Table 23
Receive (public) service result	U	Receive	Identical with the Intermediation Pattern, see Table 6

Table 35: Verifiable Credentials Pattern Conversations

From	Message	To	Description
U	(Public) service request	DC	Identical with the Intermediation Pattern, see Table 7
DC/DP	Authentication request	U	Identical with the Intermediation Pattern, see Table 7
U	Authentication details	DC/DP	Identical with the Intermediation Pattern, see Table 7
DC	Alternative channel information	U	Identical with the Intermediation Pattern, see Table 7
DC	Request for evidence	U	Identical with the Intermediation Pattern, see Table 7
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 users' 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.

From	Message	To	Description
U	Evidence (VC) Verifiable presentation	DC	Evidence (VC) in the form of a Verifiable Presentation.
DC	Evidence status update with DP lookup (VC not provided)	U	The information, which holds the status of required evidence and the information, also includes a list of DPs, 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, see Table 26
U	Additional information	DP	Identical with the User-Supported Intermediation Pattern, see Table 26.
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

4.6.3 Process Realization

Figure 26 below shows how application services serve the User process (cf. Figure 25). The application services are realized by application collaborations, which are presented in section 4.6.4. In Table 36, the application services are described.

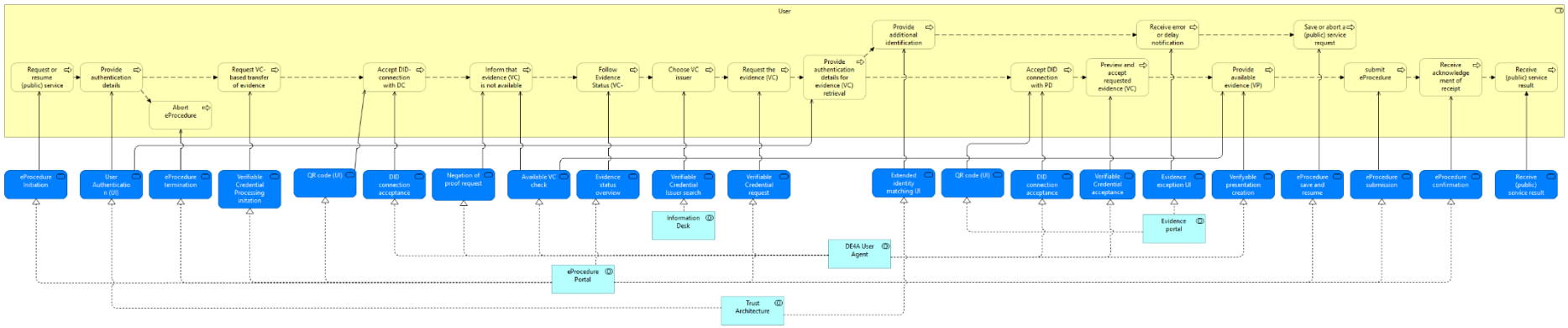


Figure 26: Process Realization of the User Process

Through the eProcedure Portal, the User requests or resumes public service, and via Trust Architecture provides his authentication details. At this point, the User can decide to abort the process or choose the form of evidence needed for (public) service. Besides different options, the User can request to provide evidence in the form of a VC, which are (if already acquired) stored in his 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 DE4A User Agent the pieces of 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 DE4A 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 in DE4A User Agent. Moreover, the User can follow evidence status to check which evidence has already been provided to the DC. In the case that the User does not hold the required evidence, through the Information Desk, the User can perform a search for the Data Provider who can contribute relevant evidence (in the form of a VC).

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 shows the User QR code, which includes all information about the DID connection establishment with DP. Now, the User's DE4A User Agent can accept DID connection with DP.

In the 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 on DE4A User Agent. Now the User can provide available evidence in the form of Verifiable Presentation to the DC, and in the case that all required pieces of evidence are successfully presented to DP, submit the eProcedure. After this, the User receives an acknowledgment of receipt and finally receive (public) service result.

Figure 27 below shows how the DC process (cf. Figure 25) is served by application services (dark blue: DE4A specific, light blue: EIRA). The application services are realized by application collaborations, which are presented in section 4.6.4. In Table 36, the application services are described.

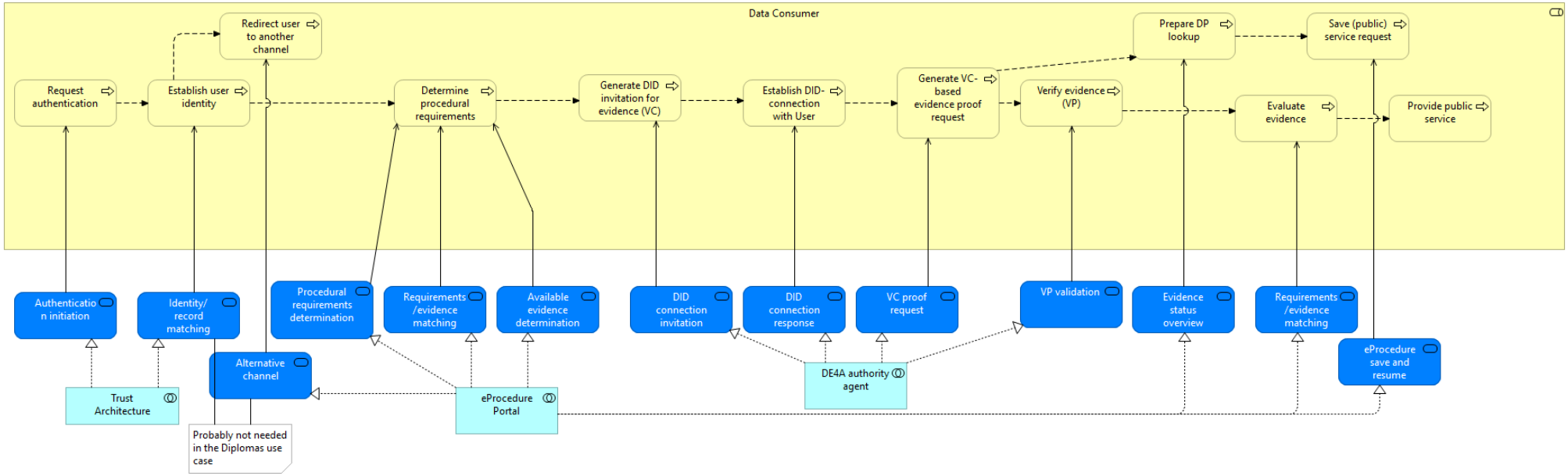


Figure 27: Process Realization of the Data Consumer Process

Data Consumer, through the Trust Architecture, authenticates and establishes the User's identity. Next, through the eProcedure Portal, the determination of procedural requirements is performed, and the later through 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. In the case that all required pieces of evidence are provided and successfully validated and evaluated, the public service is provided.

If the user does not hold all the necessary pieces of evidence, a DP lookup where the missing evidence can be acquired is prepared.

Figure 28 below shows how the DP process (cf. Figure 25) is served by application services. The application services are realized by application collaborations, which are presented in section 4.6.4. In Table 36, the application services are described.

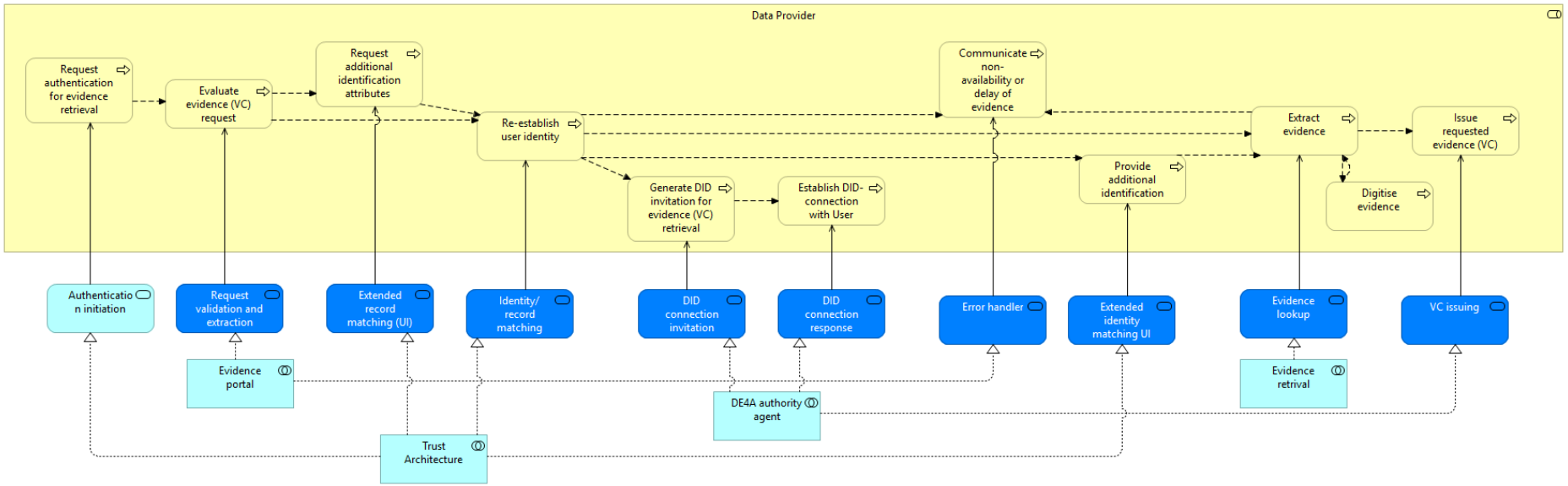


Figure 28: Process Realization of the Data Provider Process

Data Provider authenticates the User through the Trust Architecture, and if needed, request for additional identification attributes and re-establish 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. DE4A authority agent), 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. In the case of an error or delay within the process mentioned above, the User is informed through the Evidence portal.

Table 36: Application Services of the Verifiable Credentials Pattern

Application Service	Serves Role	Description	Specialization of Source	Realized by Application Collaboration
eProcedure Initiation	U	Generic service, see 17.	DE4A specific	eProcedure Portal

Application Service	Serves Role	Description	Specialization of Source	Realized by Application Collaboration
User Authentication (UI)	U	Generic service, see 11.	EIRA	Trust Architecture
eProcedure termination	U	Generic service, see 16.	DE4A specific	eProcedure Portal
Verifiable Credential Processing initiation	U	The U 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 U and DC.	DE4A specific	eProcedure Portal
QR code (UI)	U	Generic service, see 29.	DE4A specific	eProcedure Portal / Evidence portal
DID connection acceptance	U	Generic service, see 25.	DE4A specific	DE4A User-Agent
Negation of proof request	U	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.	DE4A specific	DE4A User-Agent
Available VC check	U	Generic service, see 30.	DE4A specific	DE4A User-Agent
Evidence status overview	U, DC	Generic service, see 2.	DE4A specific	eProcedure Portal
Verifiable Credential Issuer search	U	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.	DE4A specific	Information Desk
Verifiable Credential request	U	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.	DE4A specific	eProcedure Portal
Extended identity matching UI	U, DP	Generic service, see 24.	DE4A specific	Trust Architecture

Application Service	Serves Role	Description	Specialization of Source	Realized by Application Collaboration
Verifiable Credential acceptance	U	Service offers users the ability of a preview and acceptance of evidence (VC), which was issued from DP to him. Furthermore, the service manages the storing of provided evidence in a user-managed digital wallet, which is part of his agent.	DE4A specific	DE4A User-Agent
Evidence exception UI	U	Generic service, see 33.	DE4A specific	Evidence portal
Verifiable presentation creation	U	The service supports the creation of Verifiable Presentation (VP) from the evidences (VC) selected by the user.	DE4A specific	DE4A User-Agent
eProcedure save and resume	U, DC	Generic service, see 8.	DE4A specific	eProcedure Portal
eProcedure submission	U	Generic service, see 19.	DE4A specific	eProcedure Portal
eProcedure confirmation	U	Generic service, see 20.	DE4A specific	eProcedure Portal
Receive (public) service result	U	Identical with the Intermediation Pattern, see Table 9	DE4A specific	eProcedure Portal
Authentication initiation	DC, DP	Generic service, see 6.	EIRA	Trust Architecture
Identity/record matching	DC, DP	Generic service, see 5.	DE4A specific	Trust Architecture
Alternative channel	DC	Generic service, see 22.	DE4A specific	eProcedure Portal
Procedural requirements determination	DC	Generic service, see 21.	DE4A specific	eProcedure Portal
Requirements/evidence matching	DC	Generic service, see 4.	DE4A specific	eProcedure Portal
Available evidence determination	DC	Generic service, see 23.	DE4A specific	eProcedure Portal
DID connection invitation	DC, DP	Generic service, see 26.	DE4A specific	DE4A authority agent

Application Service	Serves Role	Description	Specialization of Source	Realized by Application Collaboration
DID connection response	DC, DP	Generic service, see 32.	DE4A specific	DE4A authority agent
VC proof request	DC	The service, dependant on procedural requirements, generates a request for evidence in the form of verifiable credentials (VCs). It requires evidences to be aligned with a specific VC schema.	DE4A specific	DE4A authority agent
VP validation	DC	This service checks whether a received VP complies with schema requirements, specifications, or other technical conditions. It includes the following activities: • Evidence (VC) issuer is checked (is evidence issuer competent in issuing such evidence?) • evidence issuer digital signature is validated (is provided evidence issued from stated evidence issuer) • subject 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., is not revoked, etc.).	DE4A specific	DE4A authority agent
Request validation and extraction	DP	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 U.	DE4A specific	Evidence portal
Error handler	DP	Generic service, see 10.		
Evidence lookup	DP	Generic service, see 7.	DE4A specific	Evidence retrieval
VC issuing	DP	The service provides functionalities related to (re)issuing of requested evidence in the form of VC. The VC is issued through an established DID connection.	DE4A specific	DE4A authority agent

4.6.4 Application Collaboration

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. Solution building blocks must be identified or developed for each of these elements.

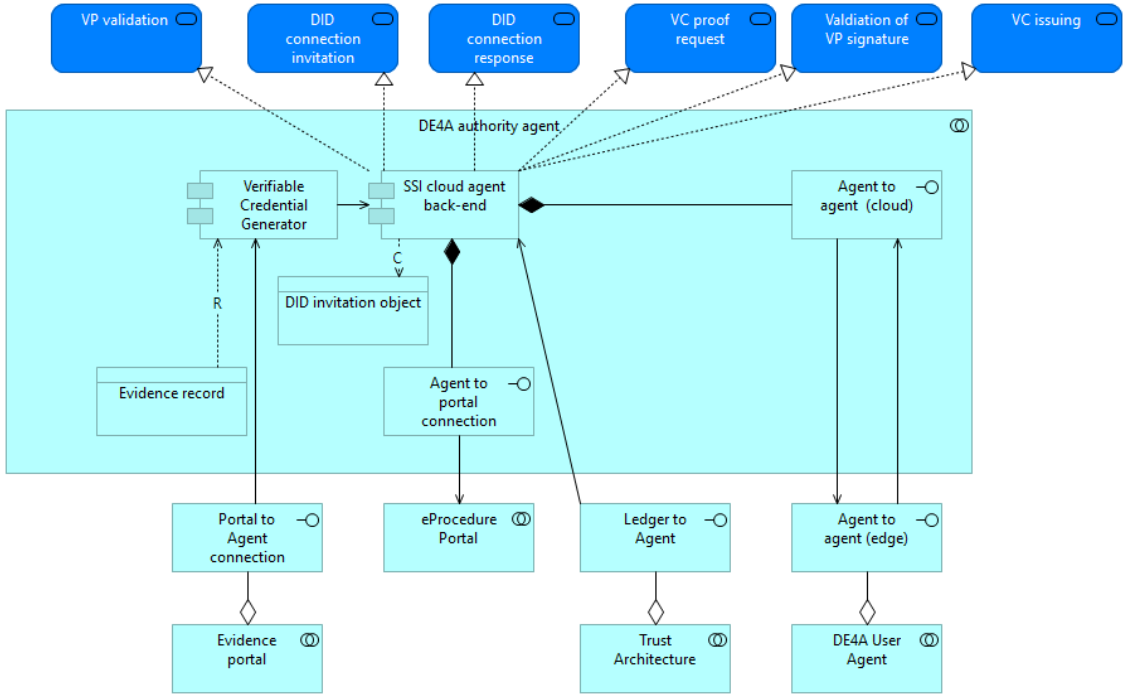


Figure 29: Authority agent

The Authority agent shown in Figure 29 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.

Table 37: Application components of Authority agent

Application Component	Description	Application Service
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.	
SSI cloud agent back-end	Generic component, see s.	• VP validation • DID connection invitation • DID connection response • VC proof request • Validation of VP signature • VC issuing

Table 38: Data objects of Authority agent

Data object	Description
Evidence record	The structured data set extracted by the DO in terms of the data definitions and structure specific to the national framework – this evidence must then be translated into the common VC schema to be issues as VC
DID invitation object	The data object with attributes required for the DID connection establishment between the DP and user.

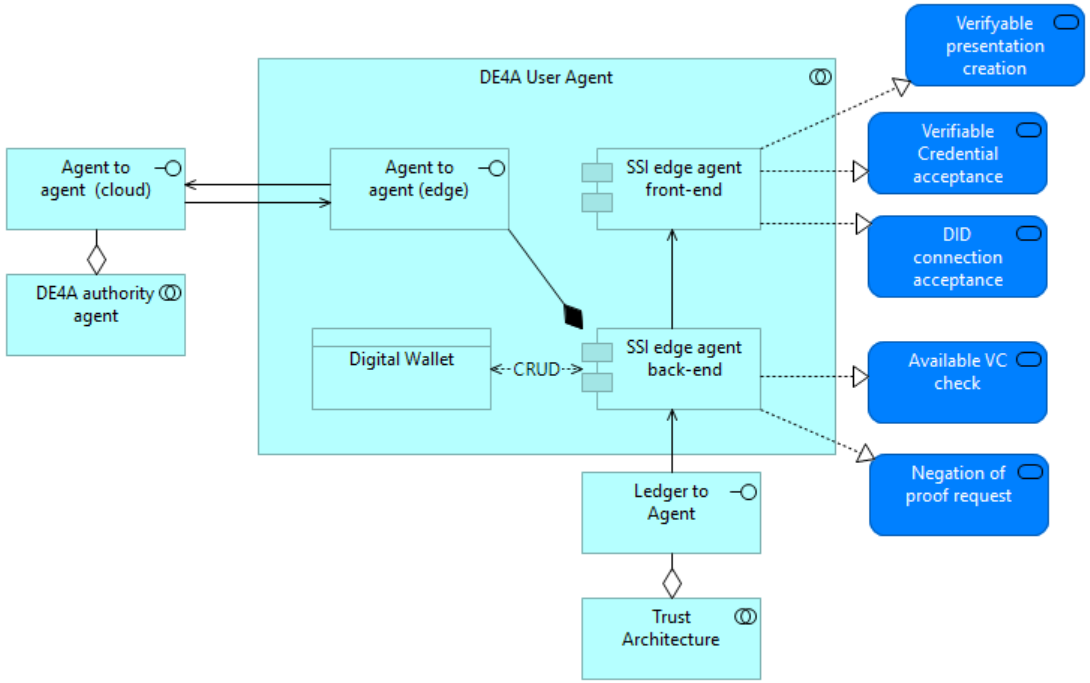


Figure 30: User agent

The User Agent presented in Figure 30 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 SSI edge agent back-end.

Table 39: Application components of User agent

Application Component	Description	Application Service
SSI edge agent front-end	Generic component, see u.	• Verifiable presentation creation • Verifiable Credential acceptance

Application Component	Description	Application Service
		• DID connection acceptance
SSI edge agent back-end	Generic component, see t.	• Available VC check • Negation of proof request

Table 40: Data objects of User agent

Data object	Description
Digital Wallet	The storage for VCs that are under user (i.e. VC holder) control.

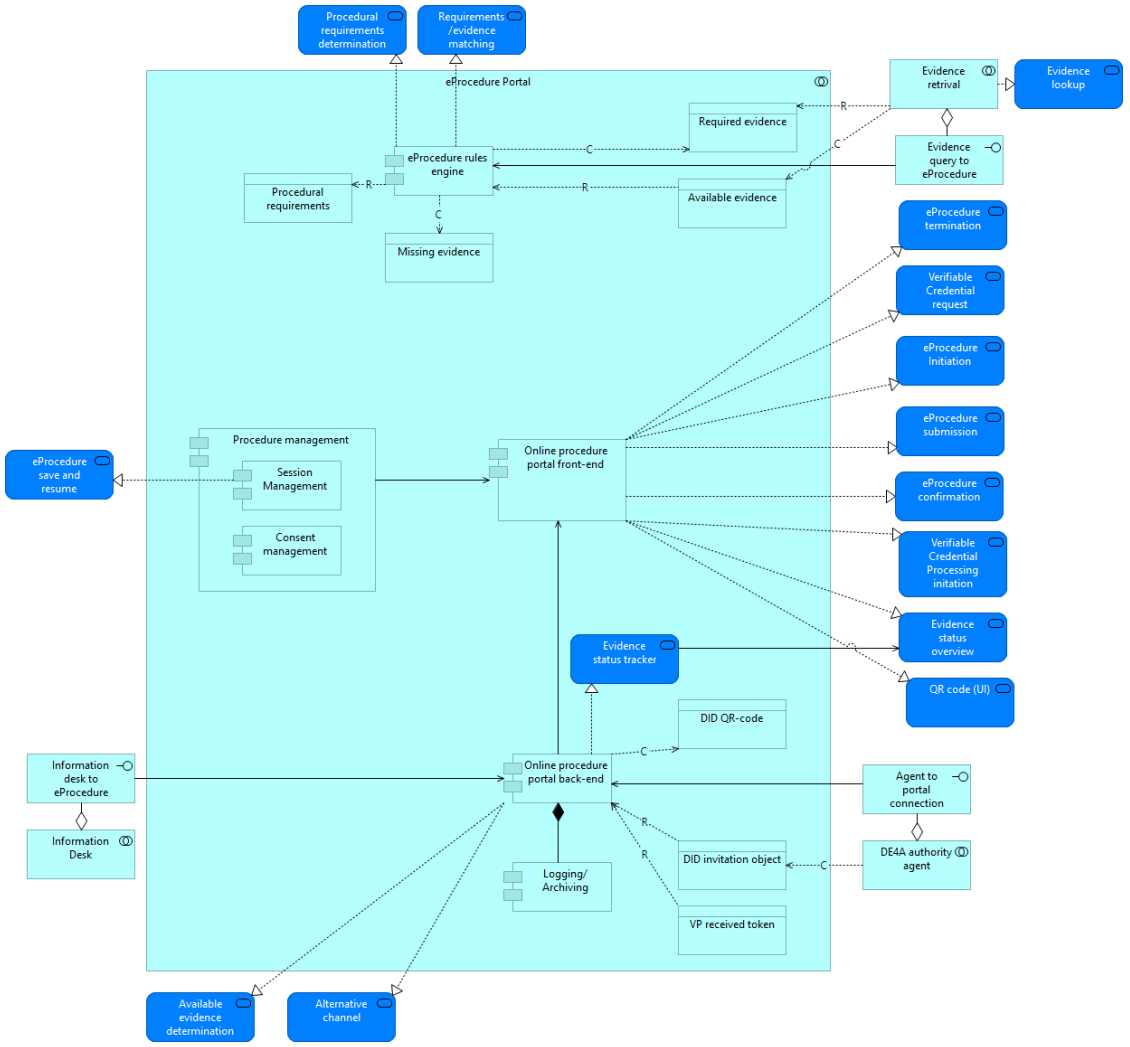


Figure 31: eProcedure Portal

As shown in Figure 31, the eProcedure Portal includes the collaboration between the application components necessary to manage the interaction between the User and the DC. 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 Session Management subcomponents. On the other side, the eProcedure back-end component communicates with the Authority Agent 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.

Table 41: Application components of eProcedure Portal

Application Component	Description	Application Service
Online procedure portal front-end		• eProcedure termination • Verifiable Credential request • eProcedure Initiation • eProcedure submission • eProcedure confirmation • Verifiable Credential Processing initiation • Evidence status overview • QR code (UI)
Online procedure portal back-end	Generic component, see n.	• Available evidence determination • Alternative channel • Evidence status tracker
Logging/Archiving	Identical with the Intermediation Pattern, see Table 10.	• All services
Procedure management	Generic component, see p.	• eProcedure save and resume
eProcedure rules engine	Generic component, see f.	• Procedural requirements determination • Requirements/evidence matching

Table 42: Data objects of eProcedure portal

Data object	Description
Procedural requirements	Identical with the Intermediation Pattern, see Table 11.
Required evidence	Identical with the Intermediation Pattern, see Table 11.
Available evidence	Identical with the Intermediation Pattern, see Table 11.
Missing evidence	Identical with the Intermediation Pattern, see Table 11.
DID QR-code	The graphical representation of the DID invitation object.
DID invitation object	The data object with attributes required for the DID connection establishment between the DP and user.
VP received token	The evidence in the form of verifiable presentation (VP) generated by VC holder.

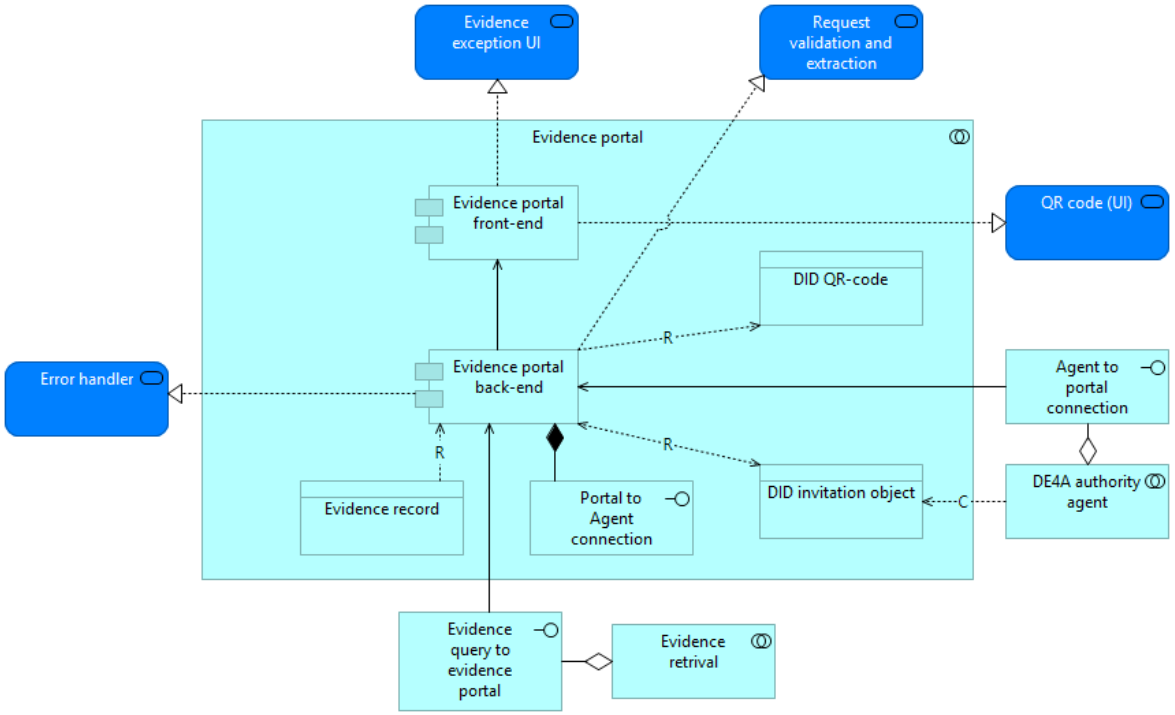


Figure 32: Evidence Portal

The Evidence Portal shown in Figure 32 depicts the collaboration between the portal front-end and back-end components responsible for managing evidence records provided by DPs and establishing secure DID connections between the DP and the User. The portal front-end component provides user interfaces for displaying any exceptions that might occur during establishing the connection or handling of evidences, as well as displaying QR code for establishing DID connection to the User. The back-end component collaborates with the Authority Agent to retrieve the generated QR code and DID invitation object from the Agent, which is then displayed to the User. By reading the Evidence Records, which contain evidence data schema specified by the DO, the back-end component provides responses regarding the evidence schema to the Evidence retrieval, and helps to validate incoming requests for evidences and map them to the appropriate Evidence record.

Table 43: Application components of Evidence Portal

Application Component	Description	Application Service
Evidence portal front-end	Generic component, see j	• Evidence exception (UI) • QR code (UI)
Evidence portal back-end	Generic component, see i.	• Evidence validation and extraction • Error handler

Table 44: Data objects of Evidence portal

Data object	Description
DID QR-code	The graphical representation of the DID invitation object.
Evidence record	The structured data set extracted by the DO in terms of the data definitions and structure specific to the national framework – this evidence must then be translated into the common VC schema to be issues as VC
DID invitation object	The data object with attributes required for the DID connection establishment between the DP and user.

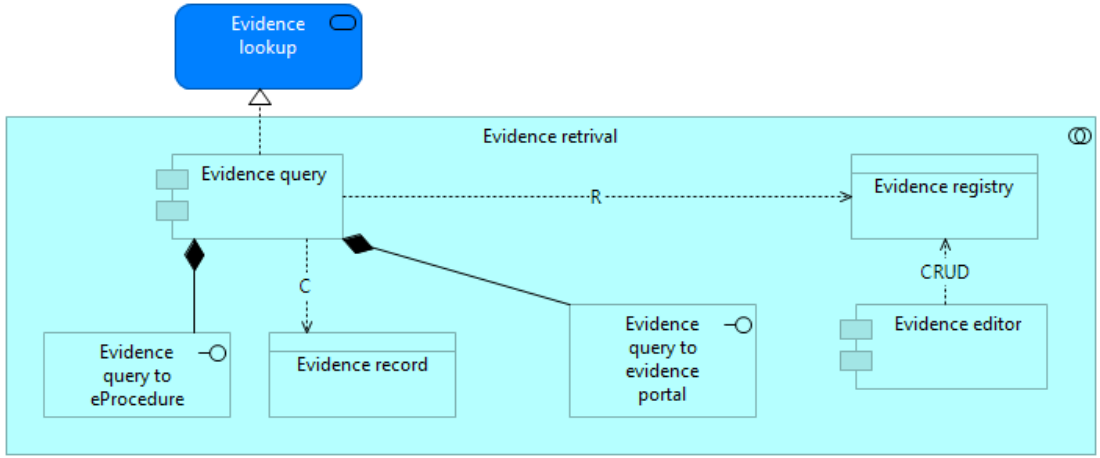


Figure 33: Evidence Retrieval

Figure 33 represents the Evidence Retrieval collaboration between the Evidence query and Evidence editor components to manage evidence in the evidence registry and retrieve evidence records. This collaboration exists both at the DP and at the DC side. In the DC country, it is used to check whether evidence required by the eProcedure is readily available in their national registry. On DP side it is used to retrieve an evidence record that was requested in order to issue it subsequently in form of a VC. The Evidence query components consequently has consequently interfaces for communicating with both the eProcedure (DC) and the Evidence portal (DP).

Table 45: Application components of Evidence Retrieval

Application Component	Description	Application Service
Evidence query	Generic component, see k.	Evidence lookup
Evidence editor	Identical with the Intermediation Pattern, see Table 20.	

Table 46: Data objects of Evidence Retrieval

Data object	Description
Evidence registry	Identical with the Intermediation Pattern, see Table 21.
Evidence record	The structured data set extracted by the DO in terms of the data definitions and structure specific to the national framework – this evidence must then be translated into the common VC schema to be issues as VC

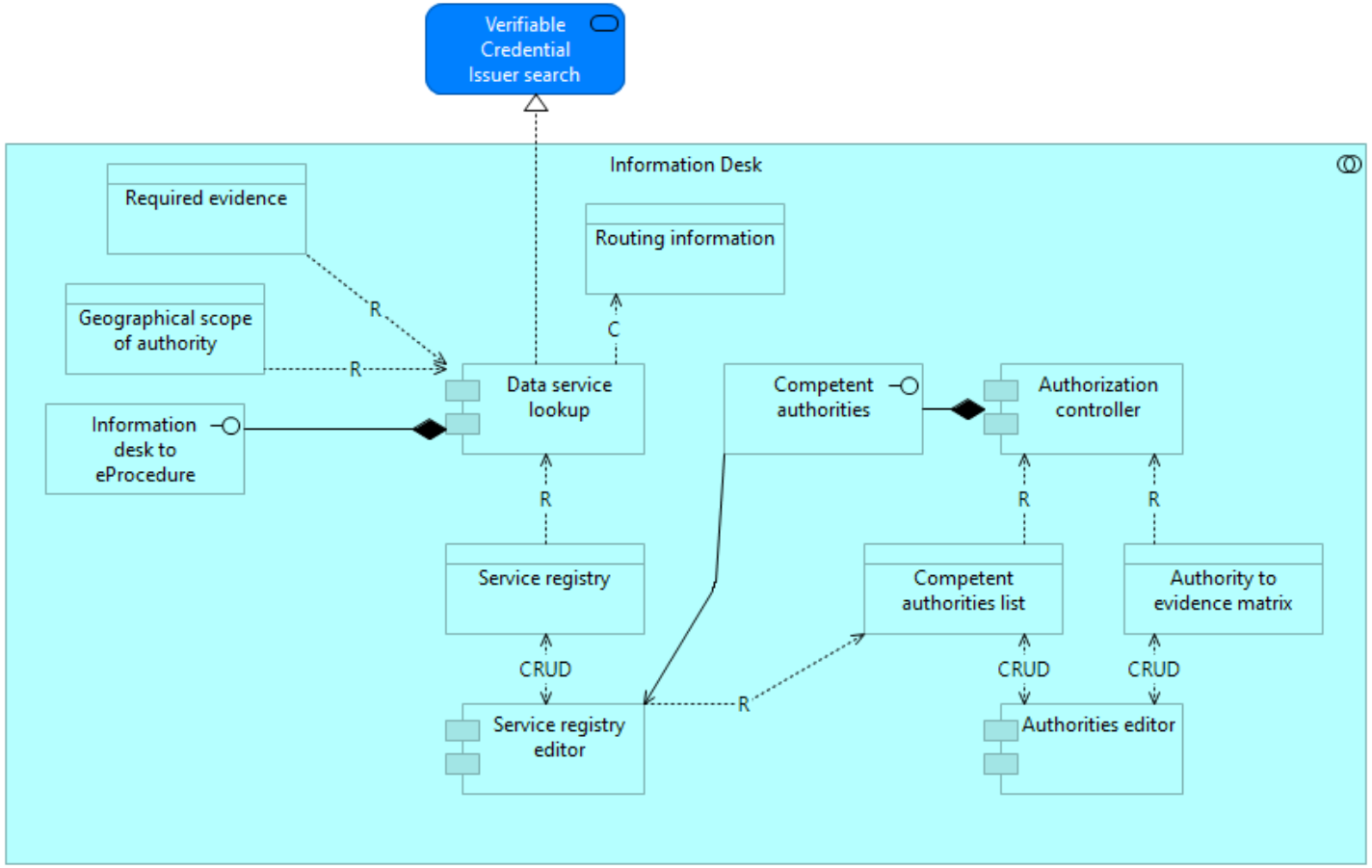


Figure 34: Information Desk

The Information Desk (Figure 34) serves as a supporting mechanism for the User, which can help him find the relevant VC issuer (i.e. possible DP) in case he is missing any evidence for the procedure. The information desk 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 he 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.

Table 47: Application components of Information Desk

Application Component	Description	Application Service
Data service lookup	Generic component, see e.	• Verifiable Credential Issuer search
Service registry editor	Identical with the Intermediation Pattern, see Table 12.	
Authorization controller	Generic component, see b	
Authorities editor	Identical with the Intermediation Pattern, see Table 12.	

Table 48: Data objects of Information Desk

Data object	Description
Required evidence	Identical with the Intermediation Pattern, see Table 13.
Geographical scope of authority	Definition of where the evidence can be retrieved. In simplest case this is only the statement of the MS, but it can be a hierarchical structure including lower-level administrative areas, such as federal states, regions or municipalities depending on the evidence and the member state administrative framework
Routing information	Routing information in the VC pattern are navigable URLs for the User to follow. This is a clear difference to the Intermediation and USI pattern where the rooting is endpoints of the messaging infrastructure.
Service registry	Identical with the Intermediation Pattern, see Table 13.
Competent authorities list	Identical with the Intermediation Pattern, see Table 13.
Authority to evidence matrix	Identical with the Intermediation Pattern, see Table 13.

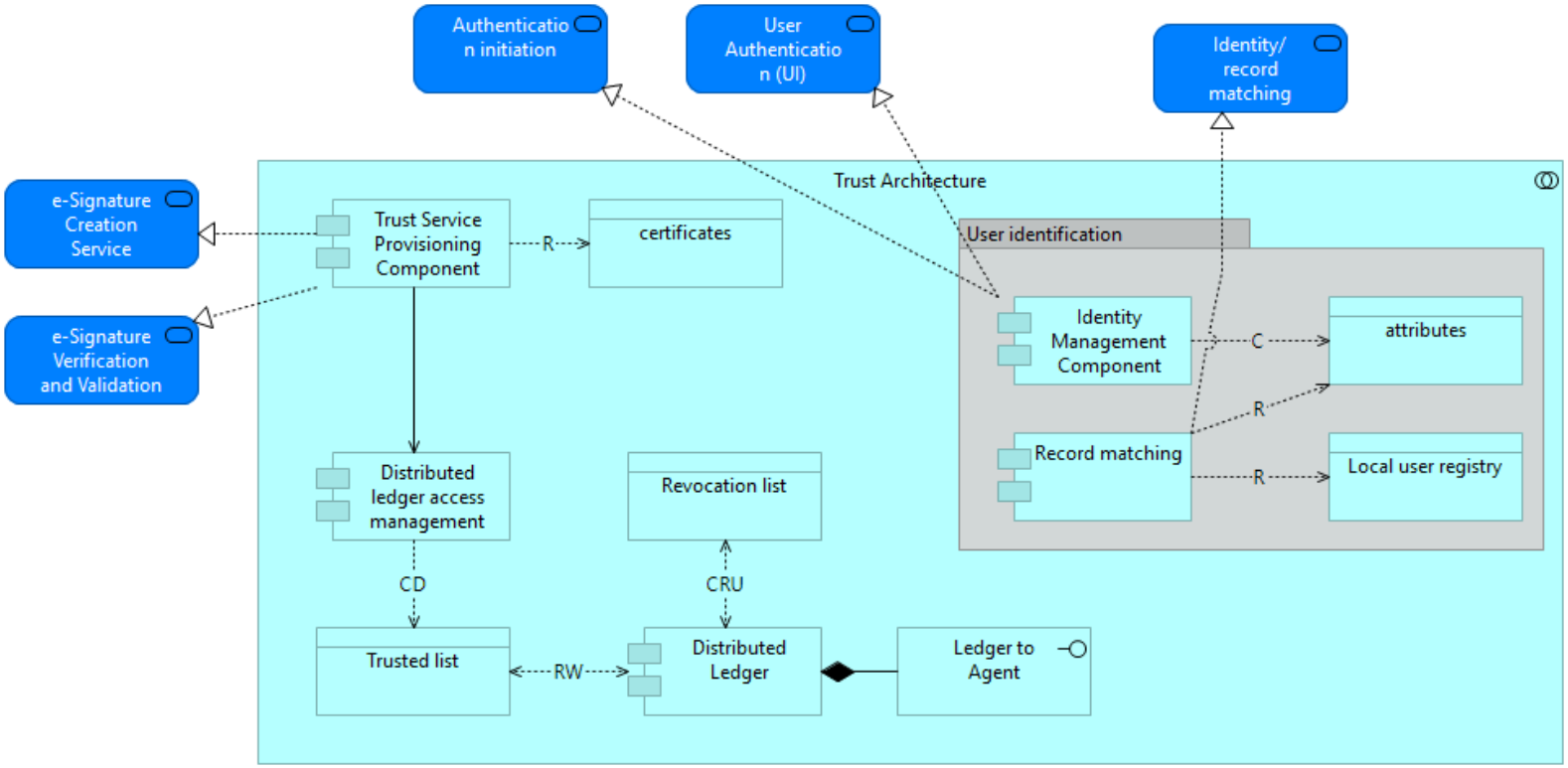


Figure 35: Trust Architecture

Figure 35 depicts the collaboration between application components of the Trust architecture. The collaboration between these components in the VC pattern is achieved similarly as in the Intermediation pattern (cf. Figure 11). The interaction between the user identification components remains the same. In addition to creating, verifying and validating digital signatures, the Trust Provisioning Component now also needs to retrieve the DP certificates and communicates with the Distributed ledger access management component to store the certificates to the Trusted list stored/retrieved to/from the Distributed Ledger (instead of persistent storage in the Intermediation pattern).

Table 49: Application components of Trust architecture

Application Component	Description	Application Service
Trust Service Provisioning Component	Generic component, see v.	• e-Signature Creation Service • e-Signature Verification and Validation Service
Distributed ledger access management	Application component that manages the access management related to Write/Read access into distributed ledger storage.	
Distributed ledger	Application component that handles connections and operations related to the distributed ledger.	
Identity Management Component	Generic component, see m.	• Authentication initiation • User Authentication (UI)
Record matching	Generic component, see q.	• Identity/record matching

Table 50: Data objects of Information Desk

Data object	Description
Certificates	Identical with the Intermediation Pattern, see Table 16
Attributes	Identical with the Intermediation Pattern, see Table 16
Local user registry	Identical with the Intermediation Pattern, see Table 16
Trusted list	The data object required for handling access management operations related to the permissioned distributed ledger.
Revocation list	The data object with attributes/identifiers of evidences (VCs) that were, for some reason, revoked.

5 Business Risk Register

This section lists and details the business risks, both functional and operational, that could be found in the DE4A project and that could also be present in the implementation of the technical system of the SDG.

The risk analysis[3] is based on the experience developed over more than 10 years providing data and evidence exchange services to thousands of public administrations on tens of thousands of final procedures or services for citizens and companies.

In general, business risks will always be related to the quality of the data to be exchanged, for intrinsic reasons (fundamentally lack of data or errors in them) or extrinsic reasons (fundamentally due to interoperability problems, when handling different concepts or values that need to be handled univocally).

One of the problems that must be considered in any project is risk analysis and management. In an interoperability project, a series of basic elements to be considered in this analysis emerge, related to the dimensions of interoperability:

- Legal
- Technical
- Semantics
- Organisational

These dimensions are going to combine with each other, especially in a project like this one with many relationships and actors that complicate the situation much more. Identified risks will impact business risks in different ways, affecting the usability, the security of personal data or the entire process providing a service to an unqualified user.

Risks have a probability. As it is almost impossible to quantify it will be assigned a relative value (e.g. high, medium, low). The same for the impact if the risk materialises (e.g. high, medium, low).

A ***risk score*** will be provided as the result of ***probability x impact***.

Impact and probability values will be: high=5, medium=3 and low=1, so a risk with probability (medium= 3) and impact (high = 5) has a risk score of 3x5=15.

Further entries will be included or taken into consideration as needed.

: Business Risk RegisterTable 51: Business Risk Register below : Business Risk Registershows the proposed risk register.

[3] The DE4A project maintains an internal document with the analysis of the business risks which can be provided on request.

Table 51: Business Risk Register

ID	Risk Description	Probability (desc)	Impact (Desc)	Risk score	Mitigation
RSK0001	Identity Fraud	Low	High	5	Improve Identity matching mechanism and powers details Implement a voluntary Registry for SDGR services for moving people. Could be under eIDAS project or just DE4A.
RSK0002	Poor or variable data quality of records at Data Providers	Medium	Medium	9	Improvement plans for Data Quality, digitization and automation
RSK0003	Absence of data according to a temporal criterion or event occurred	High	Low	5	Improvement plans for Data Quality, digitization and automation
RSK0004	Interface requires additional data plus National ID	Medium	Low	3	Implies a deep invest in development services adapted to evidence interchange
RSK0005	Evidence service with several data parameters requested (without National ID)	Medium	Low	3	Implies a deep invest in development services adapted to evidence interchange
RSK0006	Citizen cannot be cross-border uniquely identified	Medium	Medium	9	An Identity registry for moving people would improve a lot interoperability. This registry would be volunteer but very practical
RSK0007	Fraudulent misrepresentation of persons or companies	Medium	High	15	Improve Identity matching mechanism and powers details Double factor mechanisms to verify mandates and powers.
RSK0008	Collecting benefits across different Member States	Low	Medium	3	Harmonize European policies regarding aids and benefits.
RSK0009	Alternative sources of the same data	High	Low	5	Quality Interoperability score for a data source
RSK0010	Real problems associated with the lack of "common interface"	Medium	Low	3	Harmonize machine-machine interfaces based on canonical evidences
RSK0011	Tax abuse	Low	High	5	Efficient and effective data exchange system is set up between member States. In order to have this done, two conditions must be fulfilled: 1) Availability of a reliable and seamless identification system.

ID	Risk Description	Probability (desc)	Impact (Desc)	Risk score	Mitigation
					2) Systems for “anomaly” detection and data exchange that do not depend on the citizen’s will
RSK0012	Benefit from unemployment aids in one country and working in another in the union.	Low	High	5	Implement controls on the actual procedures to provide new data or evidence to fulfil the requirements
RSK0013	Collect pensions in a country incompatible with other payments in the country of residence.	Low	Medium	3	Implement controls on the actual procedures to provide new data or evidence to fulfil the requirements Harmonize European policies regarding aids and benefits.

6 Studying Abroad Pilot

The Studying Abroad (SA) use cases are centred around the students and prospective students who are studying, have studied or will be studying in another Member State. The following use cases will be piloted:

1. Use case 1: application to public higher education:
   Submission of an application by a prospective student for admission to public higher education in another Member State.
2. Use case 2: application for a study grant:
   Submission of an application by a student for a study grant in another Member State.
3. Use case 3: diploma/certs/studies/professional recognition:
   Cross-border procedure of recognition of academic and professional studies in order to facilitate the use of such information by government and other sectors.

6.1 Selection of interaction patterns

6.1.1 Use case #1: Application to public higher education

The pilot defined some requirements for cross-border data exchange (D4.1, Section 4.2.3) for UC#1:

- STA01-MFLE-04 (Selection of data providers): As a student could have studied in the past in any (can be more than one) of the EU Member States, it is necessary to involve the student in the process of the DPs selection. It is also not expected that the student is aware of all DPs where his evidence is stored, so the system should facilitate selection of competent authorities where the required evidence might be stored.
- STA01-MFLE-05 (Data collection and aggregation): Different competent authorities in MS might own evidence required for the procedure. Depending on the selected communication pattern It could be possible to retrieve and aggregate evidence from several data providers.
- STA01-PRI-01 (Data minimization): The data exchanged between the student, data consumer, and data providers should be limited to the data required by the procedure with the aim to not process evidence beyond what is technically necessary for the exchange of evidence, and then only for the duration necessary for that purpose.
- STA01-SEC-02 (Identity matching): Data provider can uniquely match presented electronic identity of a student with the person to whom evidence belongs.
- STA01-SCA-03 (Member States): The procedure can involve data providers or evidence issued from several (more than two) Member States.

The pilot has also identified several challenges that can affect the procedure:

- Restrictions of direct access to the registries' data by foreign competent authorities in certain Member States: some pilot countries, e.g. Belgium do not allow direct access to the user data stored in base registries.
- Re-authentication: It can happen that mandatory eIDAS data set is not sufficient for a Data provider to uniquely match presented electronic identity of a student with the person to whom evidence belongs in a registry. In some countries, it is also not allowed to share across borders unique national identifiers, such as citizen numbers. Therefore, the student may need to authenticate more than once when evidence also comes from third countries and DP requires the student to authenticate again at DP.

For this purpose, the following interaction pattern is considered suitable:

User-supported intermediation pattern: This pattern is suited as it solves the two challenges mentioned above and still mostly follows the preferred intermediation pattern. As the requirements of UC#1 are similar to those in UC#2, it is envisaged to implement the same pattern in both use cases. Due to the legal restrictions on direct access to user's data in some of the participating Member States in UC#2 (e.g. Belgium), it is only possible to conduct piloting in production if re-authentication is supported at the DP, which is allowed by the User-supported intermediation pattern.

6.1.2 Use case #2: Applying for study grant

The pilot defined some requirements for cross-border data exchange (D4.1, Section 4.3.3) for UC#2:

- STA02-MFLE-04 (Selection of data providers): As a student could have studied in the past in any (can be more than one) of the EU Member States, it is necessary to involve the student in the process of the DPs selection. It is also not expected that the student should be aware of all DPs where his evidence is stored, so the system should facilitate selection of competent authorities where the required evidence might be stored.
- STA02-MFLE-05 (Data collection and aggregation): Different competent authorities in MS might own evidence required for the procedure. Depending on the selected communication pattern It could be possible to retrieve and aggregate evidence from several data providers.
- STA02-PRI-01 (Data minimization): The data exchanged between the student, data consumer, and data providers should be limited to the data required by the procedure with the aim to not process evidence beyond what is technically necessary for the exchange of evidence, and then only for the duration necessary for that purpose.
- STA02-SEC-02 (Identity matching): Data provider can uniquely match presented electronic identity of a student with the person to whom evidence belongs.
- STA02-SCA-03 (Member States): The procedure can involve data providers or evidence issued from several (more than two) Member States.

The pilot has also identified several barriers that need to be removed:

- Restrictions of direct access to the registries' data by foreign competent authorities in certain Member States: some pilot countries, e.g. Belgium do not allow direct access to the user data stored in base registries.
- Re-authentication: It can happen that mandatory eIDAS data set is not sufficient for a Data provider to uniquely match presented electronic identity of a student with the person to whom evidence belongs in a registry, so the student may need to authenticate more than once when evidence also comes from third countries and DP requires the student to authenticate again at DP.

For those reasons, the same interaction pattern has been selected as in UC#1:

User-supported intermediation pattern: This pattern is suited as it solves the two challenges mentioned above and still mostly resembles the preferred intermediation pattern. Due to the legal restrictions on direct access to user's data in some of the participating Member States in UC#2, it is only possible to conducting piloting in production if re-authentication is supported at the DP, which is allowed by the User-supported intermediation pattern.

6.1.3 Use case #3: Diploma/certs/studies/professional recognition

One of the goals of the DE4A project is to pilot new concepts and technologies in the higher education context, in particular self-sovereign identities, verifiable credentials, and distributed ledger technologies (e.g. blockchain). European Commission has already seen added value of more user-centric approaches for recognition of educational achievements, as evident for example from the

European Digital Credentials Infrastructure (EDCI) and European Blockchain Services Infrastructure (EBSI). The first implements a Europass framework for digitally signed credentials aimed at fostering the adoption of verified, trustworthy digital certificates, and at promoting the recognition of qualifications, competences and skills acquired, while EBSI aims at delivering EU-wide cross-border public services using ESSIF (European Self-sovereign Identity Framework use case) and blockchain technology also for higher education (Diploma use case).

As UC#3 has similar scope, it is envisioned that the **Verifiable Credentials pattern** will be implemented in the Diploma recognition use case.

6.2 Implications and exceptions to principles

The table below highlights derived principles and the main implications of these principles when worth mentioning. In case the SA pilot will deviate from the principle, this is mentioned as well.

Table 52: Architecture log SA

#	Principle	Implication/Exception	Use case
1	Only exchange of structured and authentic evidence that can be automatically and reliably be linked to the right person	**Implication: reauthentication** This principle assumes automated data exchange on the basis of automatic match of the used person eID with the unique identifiers used in the authentic sources. Automatic identity matching is not always possible and may require re-authentication of the users at DP.	UC1, UC2, UC3
2	Data minimisation	**Implication: selection of the appropriate pieces of evidence** Multiple pieces of evidence of the same type can exist at a DP, for example when a student has two diplomas in different fields and only one of them is suitable to be submitted to the DC as part of the application.	UC1, UC2, UC3
3	Data minimisation	**Deviation: additional data in evidence** Lack of common evidence schemes across EU means that more data than necessary might be included in evidence, e.g. certificate of completion of secondary education.	UC1, UC2, UC3
4	Authentic sources under the sole control and responsibility of the competent evidence providing authority	**Implication: multiple authorities** The evidence can be stored at several places, for example universities issue diplomas to students, however the competent authorities for this type of evidence can also be national or regional registries of diplomas operated by Ministries or other relevant bodies.	UC1, UC2, UC3
5	Authentic sources under the sole control and responsibility of the competent evidence providing authority	**Implication: single request** Member States can establish brokers that connect to different competent authorities, for examples those issuing academic (record of academic results) and non-academic (household status) evidence. In such cases, there can be only one request and transfer required for	UC1, UC2, UC3

#	Principle	Implication/Exception	Use case
		several pieces of evidence owned by different competent authorities.	

6.3 Candidate Solutions and Building Blocks

Please note that the information in this section is an informed sketch only and is by no means final.

6.3.1 User-supported intermediation pattern

The main solution building blocks envisaged to be used for UC#1 and UC#2 of the SA pilot are:

- eIDAS infrastructure for eID
  - All SA Member States have national eIDAS nodes up and running. As one of them (Slovenia) has not yet notified their identification scheme, it is still open which eIDAS infrastructure (production, preproduction, DE4A-specific) will be used for the piloting, as recognition of non-notified identification schemes in this case is still an issue.
- eDelivery (and subcomponents, like AS4 gateway, SMP and SML) for the information desk and for data logistics
  - The main functions of the information desk as well as the data transport will be handled by the eDelivery components. WP5 needs to consolidate mature eDelivery components and improve the immature ones.
- CEF eSignature for digital signatures
  - The SA pilot will use the CEF eSignature building block for creation and validation of digital signatures. Depending on signature component in use by eDelivery.
- eProcedure Portal
  - The eProcedure Portals of the DC's handle most of the service-related activities. The portals need to connect to eIDAS and to the OOP technical system.
- GUI standard and shared component for evidence preview
  - All DPs need to give the user the opportunity to preview the evidence. If possible, it is preferable if this is done on the DP MS level, in order not to force every DP to change its system. The project's user centric approach requires WP5 to develop a default GUI as well as a software component for previewing evidence that the DP (or DP MS) can implement.

The table below presents the solutions / software building blocks for implementing the user-supported intermediation pattern in the SA pilot.

Table 53: SBBs for User-supported Intermediation Pattern

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
eProcedure Portal	• eProcedure Initiation • eProcedure termination • eProcedure save and resume	eProcedure Portal OOTS connector	The DC portal needs a connection to the OOP technical system. For this connector the	The services to pilot are already existing, but they will need to be customized.

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
	• eProcedure confirmation • eProcedure submission		TOOP connector might be used.	For connecting to the OOTS, WP5 needs to examine whether the TOOP connector can be used.
	Receive (public) service result	eProcedure Portal	No changes to current DC implementation expected.	
	Explicit request	OOP GUI standard and reference implementation	To be developed by DE4A WP5. To be deployed by each MS/DC.	Might be implemented by each DC or as a DC MS central component.
	Alternative channel	eProcedure Portal	To be developed by DC.	
	Procedural requirements determination	eProcedure Portal	No new functionality required.	
	Requirements/evidence matching	eProcedure Portal	Might require adaptation by the DC, as the DC will be confronted with new types of evidence.	
	Available evidence determination	eProcedure Portal	No new functionality required.	
Trust Architecture	User Authentication (UI)	eIDAS node	To be set up by DC MS and DP MS.	
	Extended identity matching UI	Evidence Portal	To be developed by DP if not existing already.	
	Authentication initiation	eProcedure Portal / Evidence Portal	To be developed by DC and DP if not existing already.	Connect to the national eIDAS node (eIDAS connector).

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
	Identity/record matching	eProcedure Portal / Evidence Portal	To be developed by DC or DC MS, and DP or DP MS if not existing already.	
	Message encryption	eDelivery AS4 / ebXML / TOOP connector	Needs to be developed by WP5.	Might use TOOP connector as a starting point.
	Message decryption	eDelivery AS4 / ebXML / TOOP connector	Needs to be developed by WP5.	Might use TOOP connector as a starting point.
	e-Signature Creation Service	eDelivery AS4 / ebXML / TOOP connector		MS might want to follow different strategies, the central infrastructure to provide the support to use eSignature Building Block would be preferred.
	e-Signature Verification and Validation Service	eDelivery AS4 / ebXML / TOOP connector		
Evidence interchange management	Evidence status overview	eProcedure Portal	To be developed by DC.	Basic functionality to be implemented by the eProcedure portal.
	Evidence request tracker	Reference component (not available)	Matches request to evidence (to be) received.	Gap, needs examination by WP5.
	Evidence preview	OOP GUI standard and reference implementation	To be developed by DE4A WP5. To be deployed by each MS/DP.	Might be implemented by each DP or as a DP MS central component. For better user experience, the latter option is preferred, i.e. to have a single

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
				preview point per MS.
	Evidence status tracker	Not to be implemented in first iteration of the SA pilot.		
	Evidence status overview	Not to be implemented in first iteration of the SA pilot.		
Information desk	Cross-border evidence matching	EB/CCCEV?	Needs advise from WP3.	Degree of harmonisation of evidence schemes varies across the EU and between the SA use cases. This is especially relevant for the non-academic data for UC#2.
	Legal basis check	eDelivery / SMP / SML	Probably needs adaptation by WP5.	
	Inquire routing information	DSD eDelivery / SMP / SML	Probably needs adaptation by WP5.	
Data logistics	Data Exchange Service	eDelivery / AS4	Probably needs adaptation by WP5.	
Evidence Portal	Evidence exception UI	Evidence Portal	To be developed by DP.	
	Persistent URL generation	Evidence Portal	To be developed by DP based on a common approach defined by WP5.	
	Prepare preview	Evidence Portal	To be developed by DE4A WP5. To be deployed by each MS/DP.	
	Error handler	Evidence Portal	To be developed by DP.	

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
Evidence retrieval	Evidence lookup	DP data service	DP specific	

6.3.2 Verifiable credentials pattern

The main solution building blocks envisaged to be used for UC#3 of the SA pilot are:

- eIDAS infrastructure for eID
  - All SA Member States have national eIDAS nodes up and running, however one of them (Slovenia) has not yet notified their identification scheme. Therefore, it is still open which eIDAS infrastructure (production, preproduction, DE4A-specific) will be used for the piloting, as recognition of non-notified identification schemes in this case is still an issue.
- eProcedure Portal
  - The eProcedure Portals of the DCs handle most of the service-related activities. The portals need to connect to eIDAS.
- DE4A authority agent
  - All DCs and DPs will have to extend their existing functionalities with an authority agent in order to be able to communicate with the user agent and the underlying trust architecture (EBSI-based ledgers). The project's user centric approach requires WP5 to develop a software component that DCs and DPs can integrate in their systems.
- DE4A user agent
  - A dedicated mobile application (user wallet) that connects with the DC and DP authority agents and stores user's verifiable credentials needs to be developed by WP5.
- Blockchain service infrastructure
  - The DE4A authority and user agents as well as the information desk connect to the trust architecture, for example to check who is allowed to issue verifiable credentials, which verifiable credentials they can issue, which evidence schemes have been registered, or which credentials have been already revoked. It is envisaged that the required registries/ledgers (e.g. domain ledger that includes trusted accreditation registry, trusted issuer registry, and trusted schema registry) will be provided as part of the European Blockchain Service Infrastructure v2 and not developed/set up by the DE4A project. In the case that EBSI will not be able to provide for the DE4A project necessary functionalities in time, the EBSI, i.e., ledger related functionalities, will be mocked.

The table below presents the solutions / software building blocks for implementing the verifiable credentials pattern in the SA pilot.

Table 54: SBBs for SA Verifiable Credentials Pattern

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
eProcedure Portal	• eProcedure Initiation • eProcedure termination	eProcedure Portal	The DC portal needs a connection	The services to pilot are already existing, but

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
	• eProcedure save and resume • eProcedure confirmation • eProcedure submission	OOTS connector	to the OOP technical system.	they will need to be customized. For connecting to the OOTS, WP5 needs to examine the most appropriate approach.
	Verifiable credential processing initiation	Authority agent	To be developed by WP5. To be deployed by each DC.	
	QR code (UI)	eProcedure Portal	To be developed by WP5. To be deployed by each DC.	
	Verifiable Credential request	Authority agent	To be developed by WP5. To be deployed by each DC.	
	Receive (public) service result	eProcedure portal	No changes to current DC implementation expected.	
	Alternative channel	eProcedure Portal	To be developed by DC.	
	Procedural requirements determination	eProcedure Portal	No changes to current DC implementation expected.	
	Requirements/evidence matching	eProcedure Portal	Might require adaptation by the DC, as the DC will be confronted with new types of evidence.	
	Available evidence determination	eProcedure Portal	No new functionality required.	

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
	Evidence status overview	eProcedure Portal	To be developed by DC.	Basic functionality to be implemented by the eProcedure Portal.
Trust Architecture	User Authentication (UI)	eIDAS node	To be set up by DC and DP if not existing already.	
	Extended identity matching UI	Evidence Portal	To be developed by DP if not existing already.	
	Authentication initiation	eProcedure Portal / Evidence Portal	To be developed by DC and DP if not exsiting already.	Connect to the national eIDAS node (eIDAS connector).
	Identity/record matching	eProcedure Portal / Evidence Portal	To be developed by DC and DP if not existing already.	
Information desk	Verifiable credential issuer search	EBSI	To be developed by WP5.	Connect to the ledger provided by EBSI.
DE4A Authority agent	DID connection invitation	Authority agent / EBSI	To be developed by WP5. To be deployed by each DC and DP.	Backend agent based on an open source framework or libraries provided by EC.
	DID connection response	Authority agent / EBSI	To be developed by WP5. To be deployed by each DC and DP.	
	VC proof request	Authority agent / EBSI	To be developed by WP5. To be deployed by DC.	
	VP verification	Authority agent / EBSI	To be developed by WP5. To be deployed by DC.	Connect to the ledgers provided by EBSI.

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
	VC issuing	Authority agent / EBSI	To be developed by WP5. To be deployed by DP.	EC plans to implement libraries that can be used for issuing VCs.
DE4A User agent	DID connection acceptance	User agent / EBSI	To be developed by WP5.	Edge agent based on an open source framework.
	Negation of proof request	User agent	To be developed by WP5.	
	Available VC check	User agent	To be developed by WP5.	
	Verifiable credential acceptance	User agent	To be developed by WP5.	
	Verifiable presentation creation	User agent	To be developed by WP5.	
Evidence portal	QR code (UI)	Evidence Portal	To be developed by WP5. To be deployed by each DP.	
	Evidence exception UI	Evidence Portal	To be developed by DP.	
	Request validation and extraction	Evidence Portal	To be developed by WP5. To be deployed by each DP.	
	Verifiable credential processing initiation	Authority agent	To be developed by WP5. To be deployed by each DP.	
	Error handler	Evidence Portal	To be developed by DP	
Evidence retrieval	Evidence lookup	DP data service	DP specific	

7 Doing Business Abroad Pilot

The Doing business abroad use cases of all the participating Member States have the entity concerned in common: a company. Some pilot scenarios focus on company enrolment in another Member State, like initial registration at a company portal and registration for – and assessment of – tax obligations. Others are more "doing business"-oriented, like annually declaring corporate tax. For both use cases the main source of company data will be the business registers in the other Member State.

The following generic use cases will be piloted:

1. **Use case 1: starting a business in another Member State:**
   initial registration of the company and assessment of the right to do business and of obligations to file tax in the Member State the company wants to do business in – at the core of this use case is the fulfilment of procedural obligations to start doing business in the Member State.
2. **Use case 2: doing business in another Member State:**
   applying for specific services in the Member State the company is operating in – at the core of this use case is updating company information by the service provider. This use case may include fulfilling corporate tax duties as well[4].

7.1 Selection of interaction patterns

The two use cases correspond with two cross-border interaction concepts:
1. Use case 1: cross-border querying the foreign business register (pull);
2. Use case 2: cross-border notification of changes by the foreign business register in case of an event or change in company data (push).

7.1.1 Use case #1: Starting a business in another member state

The pilot defined some requirements for cross-border data exchange ([8], section 3.2.5):

- DBA01-MFLE-03 (Support for synchronous data retrieval): The Doing Business Abroad pilot needs a synchronous process for data retrieval. The process 'waits' for information to be retrieved and then processed by the data consumer. When information is not available in a synchronous manner, the process needs to be terminated and started over.
- DBA01-MFLE-04 (Support for data discovery): In some scenarios, the data consumer processes information from any Member State. The OOP technical system should facilitate the retrieval of company data from sources unknown to the data consumer.
- DBA01-MFLE-05 (Support for direct retrieval): In some scenarios, almost all data will be retrieved from a specific source. E.g. in the MijnRVO.nl scenario, by far most of the companies will be Belgian or German. The data consumer (RVO) is familiar with the data source and the way to retrieve data. By far the most efficient way to implement the once only principle will be direct retrieval of data from the data provider by the data consumer. This pattern is often referred to as the "look-up pattern".
- DBA01-MFLE-07 (subscription service): The data consumers in the Doing Business Abroad pilot need to be notified of updates in company data. Therefore, the data consumer needs to be able to subscribe to changes at the data provider. This needs to be facilitated by the OOP technical system.

[4] Please note that use case (1) and (2) can be part of one logical process flow. Digitally filling corporate tax (doing business), for example, may be a process resulting from the conclusion at initial registration (starting a business) that the company has corporate tax duties.

- DBA01-MFLE-09 (Three Member State scenario): Although piloting focusses on a two Member State scenario, the piloting partners see the need for a three Member States scenario in the future: a representative from Member State A represents a company from Member State B to apply for a service in Member State C.
- DBA01-INT-03 (Evidences need to be exchanged and processed with a high level of security): This requires end-to-end encrypting of the data to exchange. Only the data provider (as sending entity) and the data consumer (as receiving entity) should be able to decrypt the evidence and 'read' the attribute values.

For this purpose, two primary interaction patterns are suitable:

1. **Intermediation pattern:** This pattern is most suited for the DBA pilot scenarios the request company data from potentially any business register. These pilot scenarios therefore should be able to rely on discovery and semantic transformation functionality to retrieve data.
2. **Lookup pattern:** This pattern is most suited for the DBA pilot scenarios in which there is a limited set of business registers that provide all (or almost all) company data to the data consumer, e.g. because of geographical positioning. This pattern is most apparent in the RVO pilot scenario. The RVO portal hosts several border region services.

The lookup pattern should allow for a light-weight implementation of the Once Only principle. Although technically both patterns can be used together (lookup pattern for a selected set of data providers and intermediation for the others), there does not seem to be much business value in combining both.

Other interaction patterns may have been suitable for piloting as well, like the user-managed access pattern. The piloting partners chose the two patterns mentioned as:

- They minimise efforts for users to register or apply for the service. In all patterns requiring the user to retrieve the evidence, the user additionally has to authenticate to the data provider. This reduces business value for companies due to the additional time needed (and in some Member States costs of authenticating).
- They minimise the impact on the piloting data providers. Starting point of the Doing Business Abroad pilot is the re-use of the data providers' data service that are in place today. In the user managed patterns, the data providers have to adapt their data services to allow access by the user (instead of the data consumer).

Finally, this first use case may end with the data evaluator subscribing to notifications on changes in company data of the company concerned. This requires the **subscription and notification pattern**. Please note that this concerns the subscription functionality of this pattern only, the notification functionality of this pattern is required for the second use case.

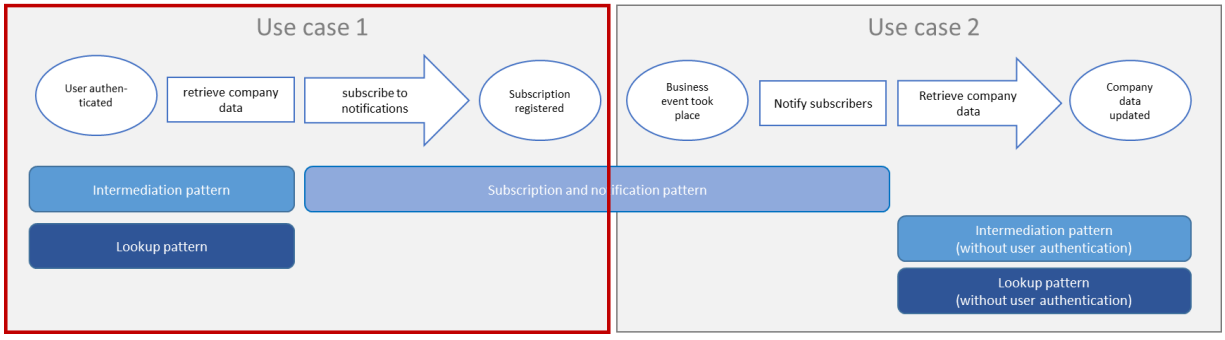


Figure 36 DBA UC1 in context

Table 55: DBA UC1 in context

Process	Interaction patterns
1. Authenticate user	Intermediation pattern & lookup pattern
2. Identify company and validate powers to represent	Intermediation pattern & lookup pattern
3. Request company data	Intermediation pattern & lookup pattern
4. Provide company data	Intermediation pattern & lookup pattern
5. Enrol to the company portal	Subscription and notification pattern (for subscribing to updates)
6. Establish right to do business and determine (tax) obligations	No interaction pattern

As most of the DBA-pilot scenarios require the intermediation pattern (and this pattern is of DE4A-wide importance) the DBA pilot will start with implementing the intermediation pattern. The lookup pattern and the subscription & notification pattern will follow.

7.1.2 Use case #2: Doing business in another member state

This use case is starts with a notification from the data provider that some company data has changed.

The pilot defined a couple of requirements regarding this use case:

- DBA02-MFLE-01 (The data provider should be able to send 'fire-and-forget'-style notifications): The processes of the data provider may not depend on availability and response times of all the data consumers it must inform. Possibly a central notification queue needs to be implemented in the OOP technical system.
- DBA02-MFLE-02 (The OOP technical system should facilitate instant delivery of notifications): Some of the business events may require action of the data consumer without delay. The data consumer requires to receive notification instantly.
- DBA02-MFLE-03 (The OOP technical system should facilitate delayed/batch delivery of notifications.): Some of the business events may not require any swift response from the data consumer. For these data consumers it is more efficient to process notifications once a while, like once a day or week. The OOP technical system should facilitate this.

Implementation of these requirements require the **subscription and notification pattern**. After receiving the notification, the data consumer needs to fetch the updates data itself. It can do so by the intermediation pattern or the lookup pattern. It is very likely a data consumer will select the same pattern for fetching the updates data as it selected for implementing the first use case.

Please note that contrary to the first use case, there will be no authenticated user in this use case. As this is typical for the subscription and notification pattern, it is not for the intermediation and lookup patterns. These two patterns normally start with authenticating the user.

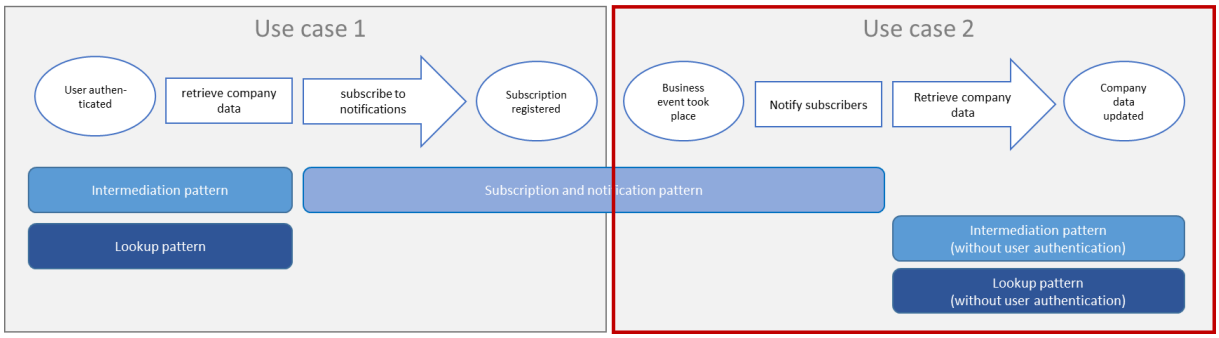


Figure 37: DBA UC2 in context

Table 56: DBA UC2 in context

Process	Interaction patterns
1. Notify	Subscription and notification pattern
2. Update company data	Intermediation pattern & lookup pattern
3. Unsubscribe	Subscription and notification pattern

7.2 Implications and exceptions to principles

The table below highlights derived principles and the main implications of these principles when worth mentioning. In case the DBA pilot will deviate from the principle, this will be mentioned as well.

Table 57: Architecture log DBA

#	Principle	Implication/Exception	Use case
1	Only exchange of structured and authentic evidence that can be automatically and reliably be linked to the right person	**Implication: sending an image for previewing** The DBA pilot focusses on exchange of structured and machine processable data. In some cases, for previewing purposes, the DC will present the user with the official document on screen as well. This is an image of the document the user is familiar with in current practise (like unstructured data in a PDF). As an implication of this architectural principle, the image should be integrated in the exchange of structured data. In other words, DBA expects the image to be one of the data elements in the evidence definition. The data provider should guarantee that the data incorporated in the image is identical to the structured data sent. Furthermore, the technical system should allow for swift transport of such images to prevent unacceptable waiting times for the user.	UC1
2	Only exchange of structured and authentic evidence that can be automatically and	**Deviation: data is not concerning the user**	UC1 UC2

#	Principle	Implication/Exception	Use case
	reliably be linked to the right person	This principle assumes the data exchanged is on the user itself and the user has authenticated with his/her eID. In the DBA pilots there are two deviations: 1. The data exchanged is on the company and not on the user (the representative). 2. Not in all cases the user will be authenticated, e.g. when updating company data after receiving a notification from the data provider. No matching of the natural person eID with the unique identifier from the authentic source is foreseen.	
3	Only exchange of structured and authentic evidence that can be automatically and reliably be linked to the right person	**Implication: company identification via eIDAS** It is of course crucial that information from the correct company will be provided. The member state identifying the company should provide a company identifier that the business register uses to identify the company as well. Translated to eIDAS: the eIDAS LegalPersonIdentifier should be the company identifier in the business register of the data providing member state. This way, the data consumer can send the eIDAS LegalPersonIdentifier to the data provider 1-on-1. The DBA pilot assumes no 'company identity matching'.	UC1 UC2
4	Digital by default	**Deviation: paper-based procedures are not accepted** This principle states 'this does not mean that the user should be obliged to use the online administrative procedure'. This is obviously true for services to citizens, but not to companies. Some Member States, like NL, require companies to use digital services. Digital is not only default, but mandatory as well.	UC1
5	One-Only Principle	**Implication: re-design of customer journey** This principle states that multiple administrative procedures must be re-analysed in the context of the complete customer journey. Fortunately, this approach has been widely adopted by many Member States already for services to companies. Company portals (business portals / PSC) offer services to companies to be fulfilled by several service providers.	UC1
6	Authentic sources under the sole control and responsibility of the competent evidence providing authority	**Deviation: some authentic data will be copied** This principle states that data from authentic sources should preferably not be copied by the data consumer. In the doing business abroad cases, it is – for the foreseeable future – inevitable that basic company information will be copied. This information is needed for multiple services and service providers, at the time of use as well as later in the process. These DV processes cannot rely on external	UC1 UC2

#	Principle	Implication/Exception	Use case
		sources of company data fully. Fortunately, basic company information does not change often. To keep the company as updated as possible, the doing business abroad architecture defined two mechanisms for updating data: 1. Each time the user authenticates to the company portal, the company portal will retrieve up-to-date company data to check whether company attributes have been changed. 2. When supported by the data provider: a notification mechanism from the data provider to the data consumer will be sent in case of a change in company data (subscription & notification pattern).	
7	Mobile first	**Deviation: desktop first implementation** Most of the administrative tasks performed by companies doing business abroad are performed using desktop pc's. That will not change soon. The DBA pilot will learn from mobile design and implement mobile design elements whenever useful, e.g. implement a responsive design. But, in case mobile-first-elements may weaken the desktop-experience, the latter prevails.	UC1
8	Data control by the user	**Deviation: when updating company data, the user should not be in control** The subscription & notification pattern doesn't involve users. In a sense, when notifying and updating in this pattern the user is not controlling the data at that point in time. Furthermore, sending data from the data provider to the data consumer is not necessarily in the interest of the user/company, e.g. when the company portal needs to be updated in order to prevent fraud, end financial support, impose additional taxes, etc. Additional legal analysis is required to examine the conditions under which use of the OOP technical system is allowed for updates.	UC2
9	Reuse before build	**Deviation: BRIS will not be used** There is a difficulty in reusing existing components built under different directives/regulations. Existing components must be extended/changed and retested. This is not always cheaper and might lead to unwanted compromises and complexity. Furthermore, this is not always legally possible. BRIS has been developed for inter-business register communication only and has been – legally – limited to certain pre-defined data-elements. Furthermore, the commission is assessing new concepts to replace the BRIS network that exists today.	UC1 UC2

#	Principle	Implication/Exception	Use case
		The DBA pilot will not use the BRIS network but will use the BRIS semantics as much as possible.	
10	Data control by the user	**Implication: requested evidences might contain user data for other natural persons than the requestor.** This principle states the user has a maximum degree of control over his personal data. In case of self-employed / sole traders / single person entities, company data will be personal as well. The company address may be the home address of the person running the company for example. The user will not be in control of this personal data in all cases. The importance of data exchange for safe economic operation might prevail over personal privacy (e.g. to prevent fraud). In any case, data exchange on any company must always comply with the GDPR requirements.	UC1 UC2

7.3 Candidate Solutions and Building Blocks

This implementation of SBB's will be fit for purpose of the DBA pilot and will not be a full swing implementation of the OOP technical system. For example, record matching is not required for the DBA pilot and will not be implemented and piloted.

Please note that the information in this section is an informed sketch only and is by no means final.

7.3.1 Intermediation pattern

The main solution building blocks to use for the DBA pilot are:

- eIDAS infrastructure for eID
  - Although SDGR does not oblige the use of eIDAS for cross-border eID, the eIDAS regulation does. Most of the Member States have national eIDAS nodes up and running. The Member States that are in the process of setting up their national eIDAS nodes, need to complete this work before piloting. Setting up an alternative eID infrastructure does not make sense for the DBA pilot nor is it feasible within the pilot timeframe.
- eDelivery (and subcomponents, like AS4 gateway, SMP and SML) for the information desk and for data logistics
  - The main functions of the information desk as well as the data transport will be handled by the eDelivery components. The TOOP Project has seriously progressed in the development and integration of eDelivery for Exchange of company data. WP5 needs to consolidate mature eDelivery components and improve the immature ones.
- GUI standard and shared component for evidence preview
  - All DC's need to give the user the opportunity to preview the evidence. The projects user centric approach requires WP5 to develop a default GUI as well as a software component for previewing evidence that the DC (or DC member state) can implement.
- CEF eSignature for digital signatures

- The DBA pilot will use the CEF eSignature building block for creation and validation of digital signatures. Depending on signature component in use by eDelivery.

- eProcedure portal
  - The eProcedure portals of the DC's handle all service-related activities. The portals need to connect to eIDAS, to the OOP technical system and implement – among others – the preview functionality.

The table below presents the solutions / software building blocks to use in the DBA pilot for implementing the intermediation pattern.

Table 58: SBBs for DBA Intermediation Pattern

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
eProcedure Portal	• eProcedure Initiation • eProcedure termination • eProcedure save and resume • eProcedure confirmation • eProcedure submission	DC Company portal OOTS connector	The DC company portal needs a connection to the OOP technical system. For this connector the TOOP connector might be used.	The services to pilot are already existing within the company portals of the data consumer. For connecting to the OOTS, WP5 needs to examine whether the TOOP connector can be used.
	Receive (public) service result	DC Company portal	No changes to current DC implementation expected.	
	Explicit request	OOP GUI standard and reference implementation	To be developed by DE4A WP5. To be implemented by each MS/DC.	Might be implemented by each DC or as a DC MS central component.
	Alternative channel	eProcedure Portal	To be developed by DC.	Current paper-based procedures will be the alternatives to using the OOP technical system. The eProcedure portal will refer the user to these existing procedures in case evidence is

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
				not available digitally or the user does not want to use the technical system.
	Procedural requirements determination	eProcedure Portal	No new functionality required.	
	Requirements/evidence matching	eProcedure Portal	Might require adaptation by the DC, as the DC will be confronted with new types of evidence.	
	Available evidence determination	eProcedure Portal	No new functionality required.	
Trust architecture	User Authentication (UI)	eIDAS node	To be implemented by DC MS.	In case of use of reference software: version 2.3.1 or higher.
	User Authentication (UI)	SEMPER extension to eIDAS	To be implemented by DC MS.	For participants that are able to validate powers / that can interpret a declaration of powers. The SEMPER extension might need updating to the latest version of the eIDAS reference software by WP5.
	Authentication initiation	eProcedure Portal	To be developed by DC.	Connect to the national eIDAS node (eIDAS connector).
	Identity/record matching	-	Not required	

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
	Message encryption	eDelivery AS4 / ebXML / TOOP connector	Needs to be developed by WP5.	Might use TOOP connector as a starting point.
	Message decryption	eDelivery AS4 / ebXML / TOOP connector	Needs to be developed by WP5.	Might use TOOP connector as a starting point.
	e-Signature Creation Service	eDelivery AS4 / ebXML / TOOP connector		
	e-Signature Verification and Validation Service	eDelivery AS4 / ebXML / TOOP connector		
Evidence interchange management	Evidence status overview	DC Company portal	To be developed by DC.	Basic functionality to be implemented by the eProcedure portal.
	Evidence request tracker	Reference component (not available)	Matches request to evidence (to be) received.	Gap, needs examination by WP5.
	Evidence preview	OOP GUI standard and reference implementation	To be developed by DE4A WP5. To be implemented by each MS/DC.	Might be implemented by each DC or as a DC MS central component.
	Evidence status tracker	Not to be implemented in first iteration DBA pilot.		
	Evidence status overview	Not to be implemented in first iteration DBA pilot.		
	Evidence shredder	DC Company portal	To be developed by DC.	Basic functionality to be implemented by the eProcedure portal.
Information desk	Cross-border evidence matching	CERB/CCCEV?	Needs advise from WP3.	Evidence in the company domain is very much

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
				harmonised across the EU in initiatives like EBR and BRIS. Light weight evidence matching seems most suitable for DBA.
	Legal basis check	eDelivery / SMP / SML	Probably needs adaptation by WP5	
	Inquire routing information	DSD eDelivery / SMP / SML	Probably needs adaptation by WP5	
	Authority check	eDelivery / SMP / SML	Probably needs adaptation by WP5	
Data logistics	Data Exchange Service	eDelivery / AS4	Probably needs adaptation by WP5	
Evidence retrieval	Evidence lookup	DP data service	DP specific	

7.3.2 Lookup pattern

The lookup pattern needs to be designed first.will be added in a future release of this document.

7.3.3 Subscription and notification pattern

The subscription and notification pattern need to be designed first.will be added in a future release of this document.

8 Moving Abroad Pilot

The Moving Abroad (MA) Pilot is to deliver fully functional procedures that will support the EU-citizen to request and exchange information between member states participating in the pilot. The pilot will address the situation when the citizen needs to provide evidence that is required (in a procedure) to register (and change his address), to prove the citizen birth, marriage, death, as well as when the citizen is requesting pension information and claiming pension from a member state.

The approach selected by the pilot is to establish a solid understanding of the current situation within the participating member states and the goals set by the DE4A project. To close the gap between the current situation and the project goals, agile and exploratory methods will be used. The reasoning behind this approach is that an upfront analyse and design is considered too complex to be done within the scope of the pilot.

The ambition of the Moving Abroad Pilot is to deliver accordingly to the goals set by the European Commission and the DE4A project. The exploratory part of the pilot may however come to the conclusion that some part of the identified challenges might not be resolved within the time span of the pilot. There might also be gaps in member state specific regulations and the technical solution that needs to be resolved outside of the scope of the pilot. These are however important findings that add value to the pilot deliverables.

8.1 Architectural Drivers & Requirements

The Moving Abroad Pilot has identified the following architectural challenges that need to be addressed and resolved to reach the goals of the DE4A project.

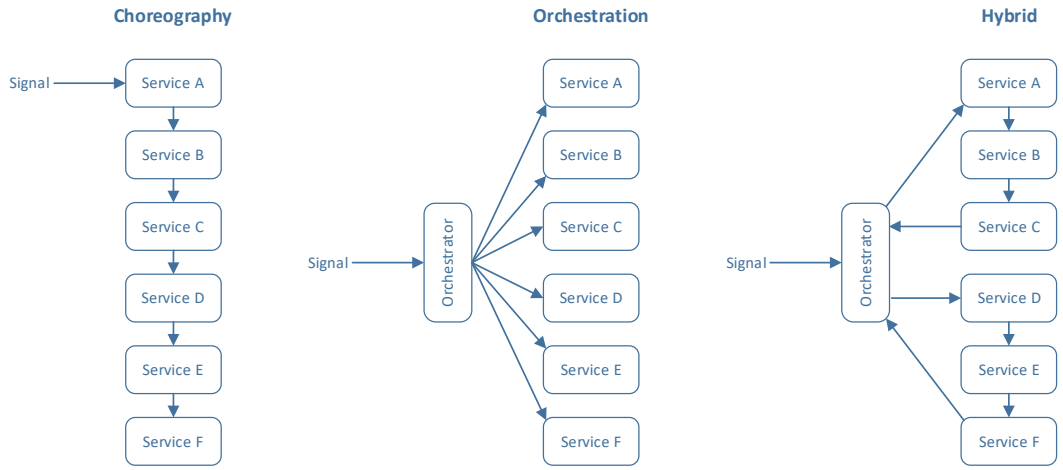
- Evidences may not be readily available via online services
- Provision of evidences require civil servant decision-making
- Identities cannot be established due to lack of full support for eIDAS
- Record-matching cannot be completed due to lack of identity-mapping mechanism
- Evidences do not hold the same legal value in all MS

The basis for selecting interaction pattern, candidate solutions and building block is the analysis done so far for the Moving Abroad pilot. Here follows a summary of the analysis in relation to the interdisciplinary questions in section 2.3.

Orchestration / Choreography

A hybrid approach to orchestration and choreography may prove to be a more viable solution and should therefore be the preferred option for the pilot.

In an ideal world, the cross border exchange of evidence is supported by well-structured processes were actors collaborate in an orderly manner. However, the real world scenarios and preconditions in participating MS show many differences between processes and the order of execution. Existing processes both include decision-making executed by civil servants and evidences in paper format. Thus, it is hard to find one mode of interaction that fits all procedural variants that exists in the MS. The pilot hypothesis is therefore a hybrid approach as described in the picture below.



Further analysis and deeper understanding of the pilot use cases may shift the balance towards either orchestration or choreography.

Multiple, complementary, overlapping or conflicting evidence equivalents

The approach is to work toward a generic data model to which each MS can map relevant information. A civil state certificate is a type of evidence commonly used in many member states. However, in the Nordic countries, it is more common to use an extract from the population registry. An extract from the population registry in Sweden do not have the same legal value in Belgium as a civil state certificate. This may have legal implications that limits the use of evidence in specific MS.

Interrupted vs. Uninterrupted exchange

The pilot intent is to allow multiple consecutive requests for the exchange of evidences. In some situations, relevant evidences may be unavailable to online services. For example, when national law requires a civil servant decision or evidences has a paper-based source. One solution is to allow for an interrupted exchange of evidence where necessary actions can take place before completing the procedure. For example, a sub-process at the DP that digitizes the requested evidence and informs the user when the evidence is available in a digital format.

There may also be ongoing digitalization initiatives on a national level that mitigates these challenges. If such initiatives deliver within the timeframe of DE4A would be a bonus but is out of the pilot control.

Explicit request and transitivity between actors

Support is required for explicit request and transitivity between authorities. The DP cannot rely solely upon user validation at the DC side and will not allow this type of evidence exchange between authorities within the DE4A timeframe. National law requires requests for evidence coming from the citizen provided that he can authenticate himself with an eIDAS notified mean, an authority that was granted access explicitly in the law, or an authority that was granted access after a formal access procedure.

Preview & Approval UI

The DP will manage preview and approval. The explicit request and transitivity between actors implies that the preview and approval will be the responsibility of the DP. However, this may affect the DP in a number of ways; existing user interfaces need changes, new user interfaces developed, new lifecycle dependencies between DP and DC at the user interface level.

Identity & Record Matching

Because of supporting explicit request and transitivity, the DP must do the identity and record-matching. This mitigates some of the problems documented in the interdisciplinary questions, section 2.3. Identity and record matching relates to the problem with transitivity of user identity.

Transitivity of user identity

Transitivity of user identity will require further analysis. The problem arises with eIDAS since piloting MS lack ability to link to national identity. This will prevent retrieval of evidences at the national level.

Hand-on of UI between actors

User interface references are required in the evidence exchange because of supporting explicit request and transitivity. This also implies the need for interrupted procedures.

Mandate and Proxy

Support for mandate and proxy is an assumed requirement in the pilot that will probably not be resolved within the pilot timelines. For example, in life events where national law allows a natural person to represent another, for example a parent representing a child.

Encryption Gap

Since evidences may contain sensitive personal information encryption is a requirement. MS will not allow sending evidences unencrypted over the Internet.

This will likely be a complicating factor when establishing common solutions on a national level.

Structured data vs. unstructured data

The pilot approach is to provide evidence described both in a structured format (XML) and in a multilingual pdf form based on the metadata provided by the DP. A canonical evidence model is a vision but may be hard to achieve within the scope of the pilot.

In the current situation, evidences include:

- Digitalized evidences (paper-based) not machine-readable
- Evidence as electronic document with prefixed structured contents allowing some machine-readable capabilities
- Evidence as electronic document with machine-readable metadata
- Evidence as datasets with prefixed data schemas fully machine-readable

The following use cases are descibed in detail in the Moving Abroad Use Case Specification [9].

8.2 Use Case #1: Request address change

Preliminary work has showed that it is necessary to include the registration process with the use case for request address change. The reason is that a citizen cannot live in a country on a permanent basis and request a change of address before the registration process is completed.

The registration process is more complex than requesting a change of address and requires more evidences as well as physical presence in the country to be completed. The required evidences include both personal and sensitive information, and it is of great importance to establish identity of the user.

However, a significant part of the required information is stored in the national/population registry where the citizen is currently registered. The order of steps/activities may also vary between procedures in different MS.

Based upon current legislation, the best fit for UC1 is a user-supported process together with the architectural requirements presented in section 8.1.

Use Case Description

Preconditions

The citizen that requests a change of address must have a “To” address in a foreign MS.

Step 1: A citizen initiates the procedure for registering a change of address via the “From” DC.

The citizen provides the “To” address on the DC portal.

When moving abroad, the citizen should inform the population service of the municipality where he is registered, before or on the day of his departure.

The citizen can request to change the address for several family members. (ReqNbr MVA01-MFLE-05), which may be beyond the pilot scope.

If the address change is valid for the whole family, it is enough that only the adult reference person of the family does the declaration. An adult of the family can request an address change only for himself and a minor person with the explicit approval from the adult reference person.

Step 2: The "From" DC portal sends a request 'Deregister' to the "From" DP to deregister the citizen from the "From" (municipality of) the National (population) Register.

(ReqNbr MVA01-MFLE-01) [9]

Step 3: In parallel with step2, the "From" DC sends a request to the DP of the "To" MS to register the citizen.

Step 4: The DP of the "To" MS could go immediately through the administrative procedure and do the necessary checks required by the DP. Please note that in some MS this is done post factum.

(ReqNbr MVA01-MFLE-02) [9]

Step 5: The DP of the "To" MS does the registration and confirms 'Registered' to the "From" DC. (ReqNbr MVA01-MFLE-03) [9]

Step 6: The "From" DC notifies the citizen of the completion of his registration in the "To" MS.

Step 7 (optional): The citizen registers to the embassy or consulate.

Once moved abroad, it is recommended to register the new address to the embassy or consulate.

The embassy or consulate can help the citizen to provide an eID card or consulate attests.

Postconditions

For example, the municipality must ask the local police to check if the citizen has moved and lives on the "To" address. In case the citizen still lives at the "From" address, then the de-registration must be cancelled.

In case the citizen is a foreigner and lives on the "To" address, the municipality will deliver a foreigner card to the citizen.

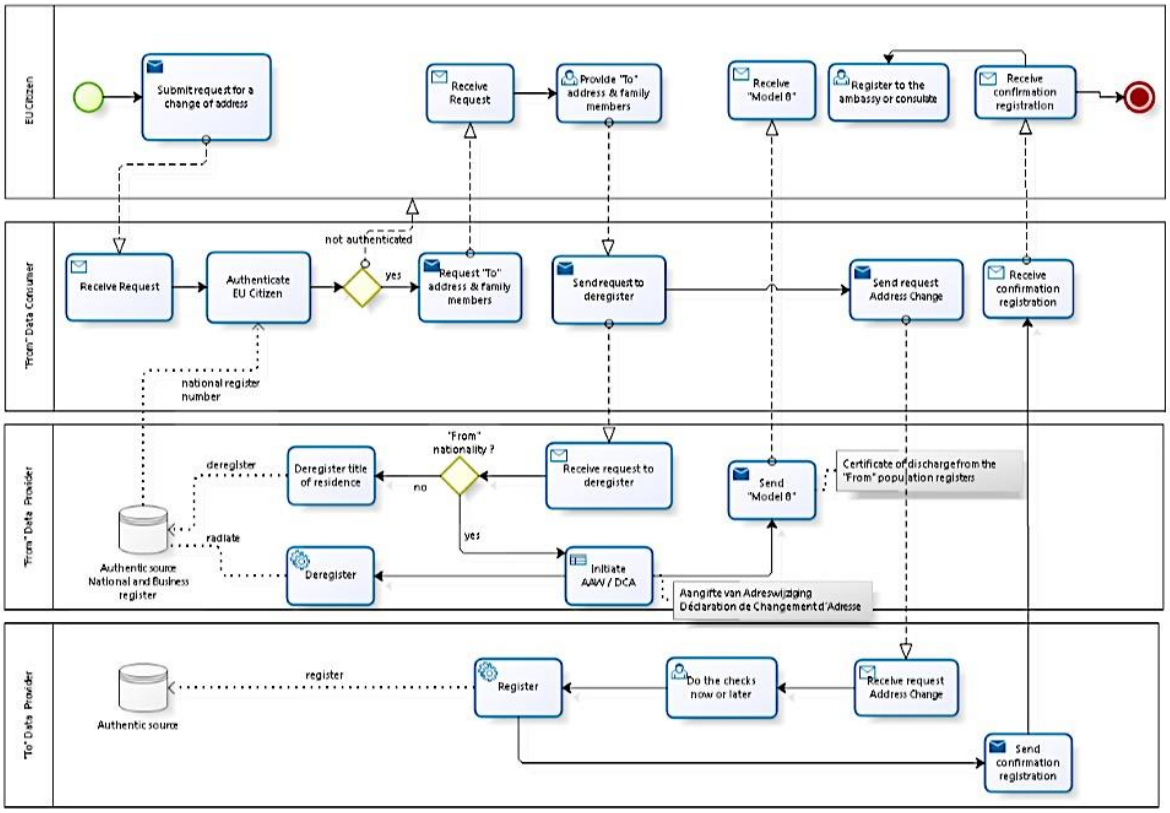


Figure 38 -BPM Model, Request address change

8.3 Use case #2: Request an extract or copy of civil state certificate

A civil state certificate is a type of evidence commonly used in many member states. However, in the Nordic countries, it is more common to use an extract from the population registry. In member states using civil state certificates, the certificate may need to be digitized before it is made available via online services. The Nordic countries, already have a solution available to exchange evidence information. However, it is unlikely that this solution can be integrated with the OOP-system within the scope of the pilot.

The approach taken for UC2 is similar with UC1, and a user-supported process is considered the best fit for UC2 together with the architectural requirements presented in section 8.1.

Use Case Description

Preconditions

The citizen that requests a copy or extract of a civil state certificate must be authenticated prior to the request and be linked to the identification number of the authentic source containing the evidence.

Step 1: A citizen initiates the procedure for a copy or extract of a civil state certificate via a foreign DC portal.

The citizen is authenticated prior to the request and linked to the identification number of the DP (authentic source containing the certificates). (ReqNbr MVA02-PREV-01) [9]

Step 2: The foreign DC sends a 'Request for copy/extract' to the DP.

The system must deliver fully electronically a copy or extract of a birth or marriage certificate for the requesting citizen himself. (ReqNbr MVA02-MFLE-01) [9]

The system should deliver fully electronically a copy or extract of a birth or death certificate for the people for whom he is legally allowed to request the copy or extract (children, wife, father/mother, …). (ReqNbr MVA02-MFLE-02) [9]

The system could deliver fully electronically a copy or extract of other type of civil state certificates (nationality, …). (ReqNbr MVA02-MFLE-03) [9]

Step 3a: Scenario 1: the certificate is (already) present in the civil status register

In case the certificate is available in an electronic format (i.e. has already been migrated to the Register), the DP must deliver a signed copy or extract in real time. (ReqNbr MVA02-MFLE-04) **Error! Reference source not found.**

The foreign DC replies with a confirmation of receipt.

The foreign DC delivers the copy or the extract to the citizen/civil servant.

Step 3b: Scenario 2: the certificate is not yet present in the civil status register

In case the certificate is not available in an electronic format (i.e. has not yet been migrated to the Register), the DP must inform the foreign DC.

The DP sends a request for information to the population register to determine the municipality that has created the certificate (in some MS).

The DP sends a request to migrate the certificate to the civil status registry of the municipality that has created the certificate.

The DP notifies the foreign DC that the certificate is being migrated and asks for an email address of the requester.

Once the certificate has been migrated to the civil status registry of the municipality, this authority will provide an electronic copy or extract of the certificate to the requester by email (this could be an eBox). (ReqNbr MVA02-MFLE-05) [9]

Postconditions

In case the requested certificate is not present in the national registry and needs to be migrated first, a mechanism needs to be in place to notify the user of this and to send the (link to) the copy or extract once the certificate is migrated.

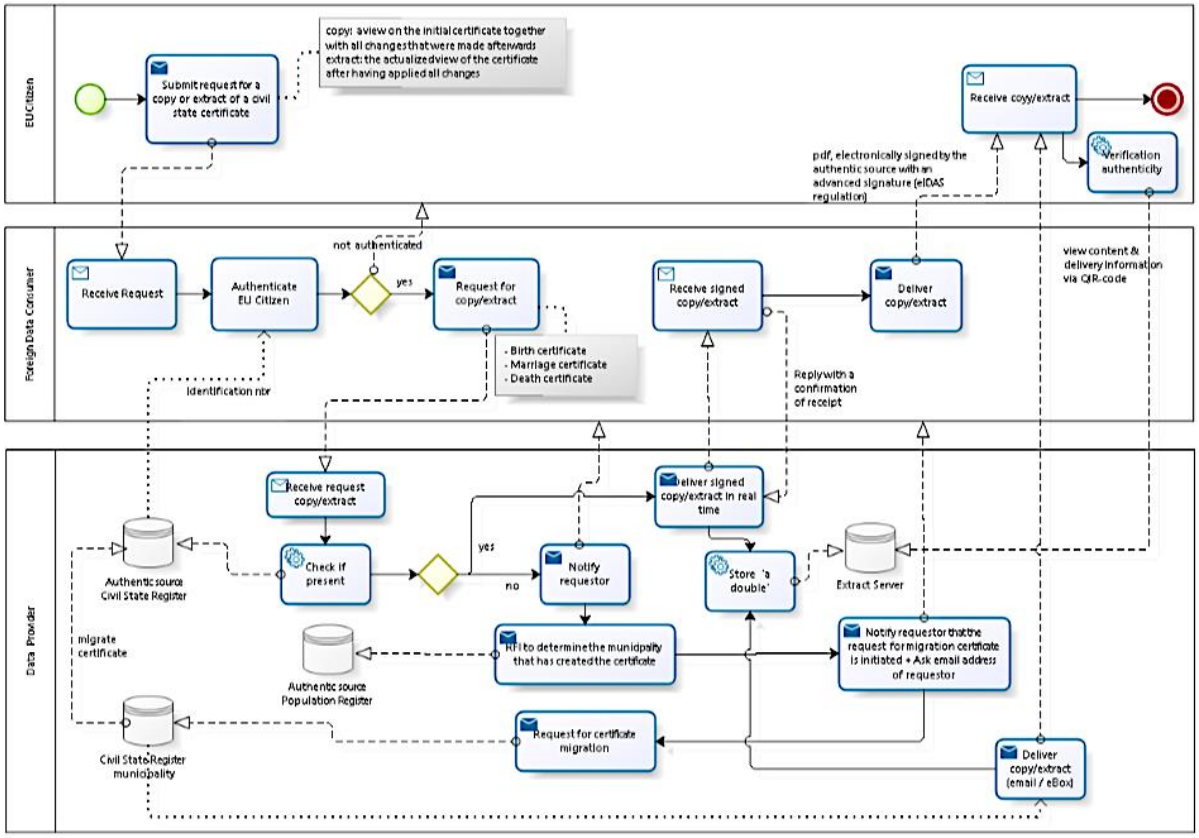


Figure 39 -– BPM Model, Request an extract or copy of civil state certificate

8.4 Use case #3: Request Pension Information – Claim Pension

At the time of writing, a working hypothesis is to reuse the Electronic Exchange of Social Security Information (EESSI). The reasoning is that no additional business value would be achieved by creating new procedures on top of the existing service interfaces provided by EESSI. The existing EESSI solution can instead linked directly to the procedure portal as needed.

Use Case Description (Request Pension Information)

Preconditions

The EU Citizen wants to get an overview of his/her career eligible for pension across the EU MS where he/she has worked to verify whether his/her entire career is known for the calculation of his/her pension.

The EU Citizen launches the request either in the EU MS of last employ or the EU MS of residence.

The EU Citizen exists in the pension registers of the EU MS where the request was made and can be linked to credentials in EIDAS for identification in the other EU MS.

Step 1: EU Citizen initiates the procedure for requesting career information via a DC.

The EU Citizen is authenticated prior to the request and linked to the identification number of the EU MS's pension system. (ReqNbr MVA03-PREV-01) [9]

Step 2: EU Citizen requests the overview of his/her career

The EU Citizen launches a demand to the EU MS DC for information on his/her career. (ReqNbr MVA03-MFLE-01) [9]

The EU Citizen indicates in which of the participating countries he has worked, so broadcasting is only done to these countries.

Step 3: DC collects additional information for identification.

The DC collects additional information on the EU Citizen that is required for identification by the other MS, i.e. names and birth date (These 2 fields are in eIDAS MDS)**Error! Reference source not found.**

Step 4: DC sends the request for information.

The DC sends the request for information to the various EU MS DP where the EU Citizen has worked. (ReqNbr MVA03-MFLE-02) [9]

Step 5: DP investigates the EU Citizen's career

Each EU MS DP consults its backend to investigate whether it holds career information for the EU Citizen. This backend will be different for each EU MS. In some EU MS's the investigation might be fully automated; in some it might be largely manual and in the hands of a civil servant of the EU MS's pension institution. (ReqNbr MVA03-MFLE-03) [9]

Step 6: each DP replies to the DC with career information

After investigation, each DP replies to the DC with a structured table containing an overview of the EU Citizen's career in the DP's EU MS. This is done in a fixed format per insurance/residence period. The answer may be per insurance/residence period or aggregated per type of period, depending on the facilities at hand in the DP's EU MS's system. (ReqNbr MVA03-MFLE-03) [9]

Step 7: DC aggregates all replies

The DC aggregates all replies (one line per insurance/residence period) received from DP into one aggregated career structured table across EU MS, ordered in chronological order. The table is prepared for the EU Citizen in a translated form, i.e. with all codes replaced by their respective descriptions in the EU Citizen's preferred language and sent as such to the EU Citizen. (ReqNbr MVA03-MFLE-02) [9]

Step 8: EU Citizen receives career information

The EU Citizen receives the information on his/her cross-border career in all MS.

Postconditions

The EU Citizen has received the career overview in accordance to the facilities available in the EU MS where the request was made.

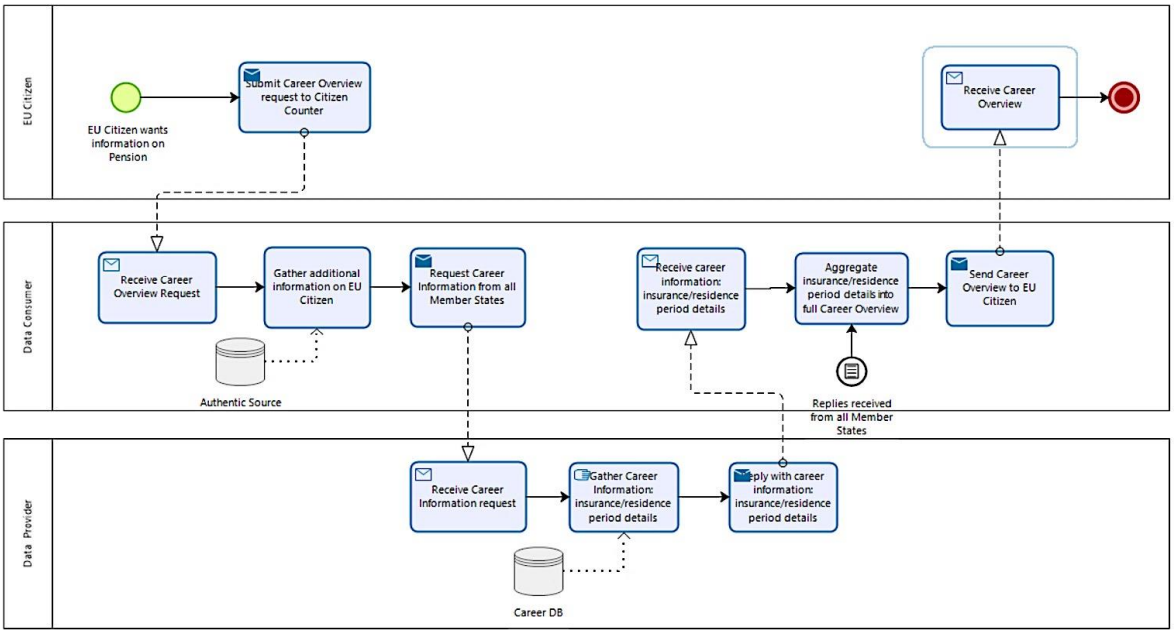


Figure 40 -– BPM Model, Request pension information

Use Case Description (Claim Pension)

Preconditions

The EU Citizen wants to simulate the remainder of his/her career until a given (hypothetical) pension date and find out what acquired rights this would result in.

The EU Citizen launches the request either in the EU MS of last employ or the EU MS of residence.

The EU Citizen exists in the pension registers of the EU MS where the request was made and can be linked to credentials in EIDAS for identification in the other EU MS's.

Step 1: EU Citizen initiates the procedure for requesting a pension simulation via a DC.

The citizen is authenticated prior to the request and linked to the identification number of the DP (authentic source containing the certificates). (ReqNbr MVA03-MFLE-01)**Error! Reference source not found.**

Step 2: EU Citizen requests a pension simulation

An EU Citizen launches a demand to the EU MS DC to perform a simulation on his/her career. He/she provides a desired retirement date to base the simulation on, and whether the current period needs to be extended to that date for the simulation or not. (ReqNbr MVA03-MFLE-05, ReqNbr MVA03-MFLE-05) [9]

The EU Citizen indicates in which of the participating countries he has worked, so broadcasting is only done to these countries.

Step 3: DC collects additional information for identification.

The DC collects additional information on the EU Citizen that is required for identification by the other MS, i.e. names and birth date (These 2 fields are in eIDAS MDS).

Step 4: DC sends the request for simulation.

The DC broadcasts the request for simulation to the various EU MS DP in the DE4A network where the EU Citizen has worked. (ReqNbr MVA03-MFLE-06) [9]

Step 5: DP investigates the EU Citizen's career and calculates the acquired rights

Each EU MS DP consults its backend to investigate whether it holds career information for the EU Citizen. This backend will be different for each EU MS. In some EU MS's the investigation might be fully automated; in some it might be largely manual and in the hands of a civil servant of the EU MS's pension institution.

The DP calculates the acquired rights based on the career information. If required, the DP of the EU MS where the EU Citizen is currently working will extrapolate this insurance/residence period to the desired retirement date and calculated the acquired rights based on that period. (ReqNbr MVA03-MFLE-07) [9]

Step 6: each DP replies to the DC with simulated acquired rights

After investigation, each DP replies to the DC with a structured table containing an overview of the EU Citizen's career in the DP's EU MS, with the acquired rights for that period. This is done in a fixed format per insurance/residence period. The answer may be per insurance/residence period or aggregated per type of period, depending on the facilities at hand in the DP's EU MS's system. (ReqNbr MVA03-MFLE-07) [9]

Step 7: DC aggregates all replies

The DC aggregates all replies (one line per insurance/residence period) received from DP into one aggregated career structured table across EU MS's, ordered in chronological order. The table is prepared for the EU Citizen in a translated form, i.e. with all codes replaced by their respective descriptions in the EU Citizen's preferred language, and the total of the acquired rights is calculated. This is sent as such to the EU Citizen. (ReqNbr MVA03-MFLE-06) [9]

Step 8: EU Citizen receives pension simulation

The EU Citizen receives the simulation of his/her acquired rights related to his/her cross-border career in the DE4A participating MS.

Postconditions

The EU Citizen has received the pension simulation in accordance with the facilities available in the EU MS where the request was made.

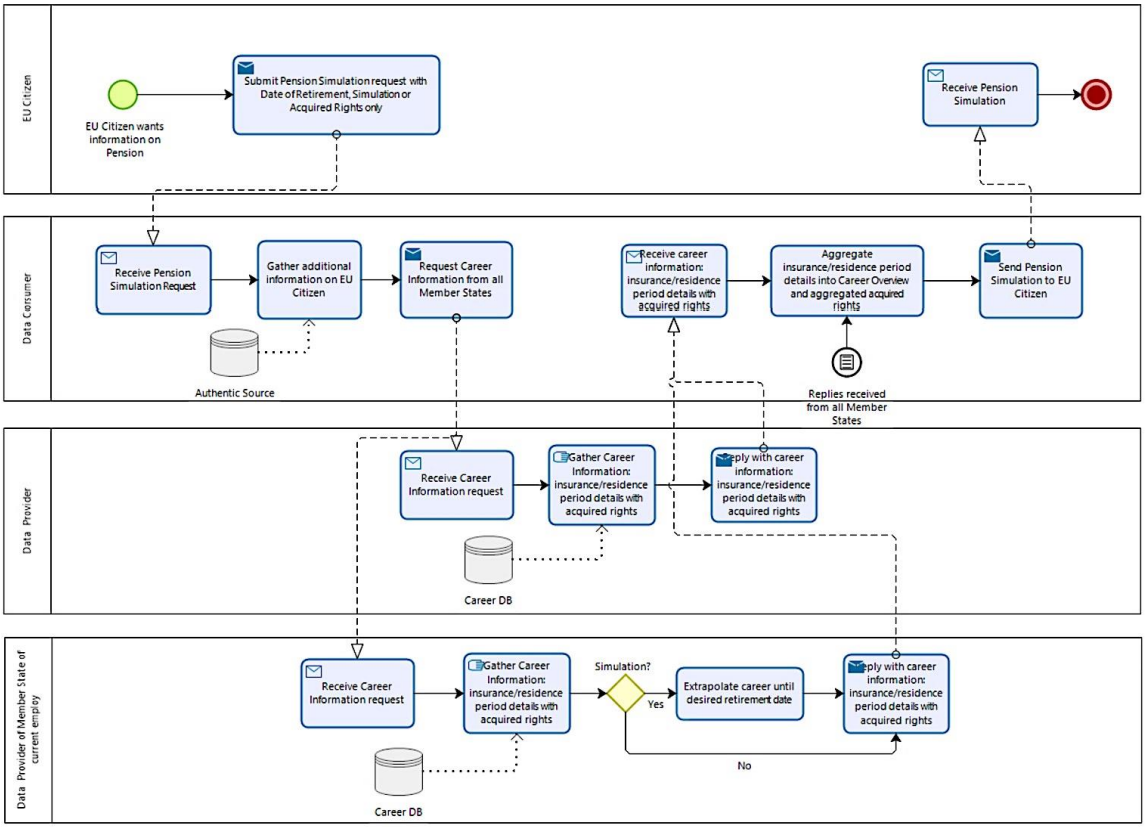


Figure 41 – BPM Model, Claim pension

8.5 Interaction Pattern Selection

Based upon the analysis the best fit for UC1 and UC2 is the User-Supported Intermediation (USI) pattern.

For UC 3 further discussion with the EESSI team is needed. In this UC an intermediation pattern might be considered given the fact that there exists an international regulation in the social security sector that allows to exchange pension information directly between trusted authorities.

8.5.1 User-Supported-Intermediation Pattern

The USI-pattern schematic can be found in section 4.3.

The main reasons to select the User Supported Intermediation pattern as the best fit are:

- The national laws do not allow the direct exchange of the UC 1 and UC 2 evidences with foreign authorities. The use of the standard intermediation pattern would mean that the pilots could not operate in production in the DE4A timeframe. This constraint is bypassed by involving the user in the request process. The national laws in all member states authorize direct requests for evidence by the citizen themself.
- By the fact that the pilots can operate in production, the real business value for the citizens will be realized already in the DE4A timeframe before the launch of SDG in Dec 2023.
- The pattern offers a solution in case a citizen intervention is needed at DP side. An example of this is the identity linking in cases where unique linking cannot be automatically base on eIDAS alone. Further interaction with the citizen is required to establish the link, by asking additional

information such as the natural identity (NatId), the place of birth, the first names of the parents, etc.

- Also to preview the evidence as well as approve and to share it with the foreign procedure an intervention is needed. This is especially important for the evidence of UC1 and UC2 that is both sensitive and include personal information. Placing the check as close to the source will increase safety.
- Further, most of the MS have already a solution for citizens to request and preview their evidences.
- The user is actively involved in the process and has a good view on / control over what is happening with his evidence.
- The pattern simplifies the implementation and offers a reuse of components already existing in the member states, for example, most member states have already a solution for the citizen to request his evidence and preview it.

8.5.1.1 A phased implementation approach

For the implementation, we recommend a phased approach.

In a **first phase** it will be possible to exchange evidence that is available and can be provided electronically in real time.

In a **second phase** the solution is further extended with the possibility to interrupt the procedure in case the evidence is not yet available for electronic exchange. After preparing the evidence for electronic exchange, the citizen is informed of this and can re-enter the procedure. This extension is very important to further increase the percentage of evidence that can be exchanged cross border. In several member states the evidence needs an intervention of a civil servant before it can be exchanged electronically, i.e. produce a digital version of a paper-based document, migrate it to a central repository, , enter the metadata, …)

Once a digital version is produced and available online, the citizen can restart the procedure.

Here follows a mapping of the pilot use cases for Moving Abroad mapped to the User-Supported Intermediation Pattern.

Activity / UC	Role	Type	Comments	Use Case
Request or resume (public) service procedure	U	User	OK	UC1, UC2
Request authentication	DE	Service	OK	UC1, UC2
Provide authentication details	U	User	OK	UC1, UC2
Establish user identity	DE	Service	OK	UC1, UC2
Redirect user to another channel	DE	Service	OK	UC1, UC2
Abort eProcedure	U	User	OK	UC1, UC2
Determine procedural requirements	DE	Service	OK	UC1, UC2
Request OOP transfer of evidence	U	User	OK	UC1, UC2
Determine required cross-border evidence	DE	Service	OK	UC1, UC2

Activity / UC	Role	Type	Comments	Use Case
Save (public) service request	DE	Service	OK	UC1, UC2
Lookup routing information	DR	Service	OK	UC1, UC2
Request evidence	DR	Service	A prerequisite is that data exchange between involved member states is supported by national law. In some cases, the procedure cannot be completed online, and may require physical presence as well as some manual activity or decision by a civil servant. In these cases, the DP may confirm that a request has been received and a response message be sent at a later moment and possibly through another channel. Note that for a full roll-out, more than one evidence may be required to complete a procedure, for example, a parent may request to move together with children.	UC1, UC2
Evaluate evidence request	DT	Service	The authority check may be omitted in pilot use cases (can be managed by agreement between participating pilot partners).	UC1, UC2
Generate URL for direct user interaction	DO	Service	OK	UC1, UC2
Display link to evidence portal	DR	Service	OK	UC1, UC2
Navigate to evidence portal	U	User	OK	UC1, UC2
Request authentication for evidence retrieval	DO	Service	OK	UC1, UC2

Activity / UC	Role	Type	Comments	Use Case
Provide authentication details for evidence retrieval	U	User	OK	UC1, UC2
Re-establish user identity	DO	Service	OK	UC1, UC2
Provide additional identification information	U	User	OK	
Communicate non-availability of OOP	DT	Service	OK	UC1, UC2
Extract evidence	DO	Service	OK	UC1, UC2
Communicate non-availability of evidence	DT	Service	OK	UC1, UC2
Prepare preview	DO	Service	OK	UC1, UC2
Receive error or delay notification	U	User	OK	UC1, UC2
Preview evidence pre-transfer	U	User	OK	UC1, UC2
Transfer evidence	DT	Service	OK	UC1, UC2
Establish non-availability of OOP	DR	Service	OK	UC1, UC2
Update evidence status	DE	Service	OK	UC1, UC2
Follow evidence status	U	User	OK	UC1, UC2
Forward evidence	DR	Service	OK	UC1, UC2
Evaluate evidence	DE	Service	OK	UC1, UC2
Save (public) service request	U	User	OK	UC1, UC2
Abort (public) service request	U	User	OK	UC1, UC2
Submit eProcedure	U	User	OK	UC1, UC2
Receive acknowledgement of receipt	U	Receive	OK	UC1, UC2
Provide public service	DE	Subprocess	OK	UC1, UC2
Receive (public) service result	U	Receive	OK	UC1, UC2

8.6 Implications and exceptions to principles

The table below highlights derived principles and the main implications of these principles when worth mentioning. In case the Moving Abroad pilot will deviate from the principle, this will be mentioned as well. Further insights done by the pilot might discover more exceptions to the principles.

Table 59: Architecture log Moving Abroad (MA)

#	Principle	Implication/Exception	Use case
4	Digital by default	**Deviation: Paper-based procedures are sometimes necessary** In some member states, evidences are no readily available via online services. The reasons may be national law or lagging digitalization. Evidences must in some cases be digitized from paper-based sources before they can be made available in online services.	UC1, UC2
5	Once-Only Principle	**Implication: re-design of customer journey** This principle states that multiple administrative procedures must be re-analysed in the context of the complete customer journey. There are ongoing activities in many member states to take a more user-centric approach when designing services. However, much work remains to be done.	UC1
7	Mobile first	**Deviation: no mobile first implementation** Designing for mobile first may not be the best solution for users where there is a lot of information to enter or preview.	UC1

8.7 Candidate Solutions and Building Blocks

The moving abroad pilot will rely on the OOP technical system for exchange of evidences, though some parts of the procedure may be omitted for sake of simplicity and to cut corners to be able to deliver within the pilot timeframe.

Please note that the information in this section is an informed sketch only and is by no means final.

The main solution of the Moving Abroad pilot consist of the following parts:

- eProcedure Portal
- Evidence Portal
- Trust Architecture
- Evidence Interchange Management
- Information Desk
- Data Logistics
- Evidence Retrieval

The table below presents the solutions and software building blocks to use in the MA pilot for implementing the User-Supported Intermediation pattern.

Table 60 SBBs for the Moving Abroad Pilot Use Cases 1 and 2

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
eProcedure Portal	eProcedure initiation eProcedure submission eProcedure confirmation eProcedure termination Explicit request	Portal Front-End Portal Backend-End Logging/Archiving	UC1 is not complete until the citizen is physically present in the new country. Therefore, the requirements required to	A reference implementation to demonstrate redirection from DC to the DP would be useful. However, it is likely that implementation

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
			complete the registration in the new country is out of scope for the pilot.	details and technical frameworks will vary between MS.
	eProcedure save and resume	Session Management	-	-
	Alternative channel	-	-	Existing procedures will be the alternatives to using the OOP technical system. The eProcedure portal could refer the user to these existing procedures in case evidence is not available digitally or the user does not want to use the technical system.
	Procedural requirements determination	eProcedure Rules Engine	Requires further analysis.	It is clear that requirements vary between MS and may also change after the law has legal basis in each MS.
	Requirements/evidence matching (2x)	eProcedure Rules Engine	Requires adaption to manage new evidence types.	In some cases, civil servants do the matching manually.
	Available evidence determination	Evidence Broker	Requires further analysis	As noted in chapter 4.3.4, available evidence determination is not included in the USI-pattern. How will the DC select the correct DP if there are more than one option?
	User Authentication (UI)	eIDAS	Requires support of notified eIDAS	Authentication at DP will likely make use of national eID as well as eIDAS
Evidence Portal	Evidence Exception Evidence Preview	Evidence Portal Front-End	The User-Supported Intermediation	An assumption is that existing DP procedures can be

Application Collaboration	Application Service	Solutions / Building Block	Requirement Mapping	Fit and Gap (Notes)
			pattern requires each DP to provide means to preview evidences.	used as basis for required development and integration with the OOP-technical system.
	Persistent URL Generation Error Handler Prepare Preview	Evidence Portal Back-End	-	-
Trust architecture	Authentication Initiation User Authentication (UI)	eIDAS with SEMPER extension	Developed by WP5?	National law may vary between MS when a legal representative is allowed the make a request on behalf of another person, e.g. parents request to move with children. Further analysis may exclude this from the pilot scope.
	Identity/record matching	Record Matching	To be implemented by DP.	In case of eIDAS, mapping to NatId may be required to be able to identify the correct data record.
	Message encryption Message decryption	eDelivery		-
	e-Signature Creation Service e-Signature Verification and Validation Service	Trust Service Provisioning Component	Developed by WP5	-

Application Collaboration	*Application Service*	*Solutions / Building Block*	*Requirement Mapping*	*Fit and Gap (Notes)*
		Mandate/Powers (extension of SEMPER to natural person representation?)	Required as a legal representative may be allowed the make a request on behalf of another person, e.g. parents request to move with children.	Potentially out of scope of pilot implementation
Evidence interchange management	Evidence status tracker Evidence status overview	Evidence Interchange Front-End	Developed by WP5?	-
	Evidence request tracker	Evidence Interchange Front-End	Developed by WP5?	-
Information desk	Legal basis check Authority check	Authorization Controller	Developed by WP5?	-
	Inquire routing information	Data service loopup	Developed by WP5?	-
	Cross-border evidence matching	Evidence type translator	Developed by WP5	-
Data logistics	Data Exchange Service	eDelivery	Developed by WP5	-
Evidence retrieval	Evidence lookup	Evidence query Evidence editor	DP specific	-

9 Building Blocks

9.1 Introduction

The purpose of the BB assessment is to assess the suitability of the BBs identified and catalogued in Task 1.5 for use within the DE4A project. Thus, it bridges outputs from WP1 and requirements from WP4 to provide input for the technical, operational and administrative considerations in the architectural assessments carried out here. Over 40 BBs have been considered for this assessment, 31 of which are assessed at the first phase of this work. The results of the assessment show that there is a mature and acceptable stock of solution building blocks that can be considered as potential candidates for implementation by the pilots, either in their entirety or partially, with the needed upgrades.

9.2 Theoretical background

9.2.1 Objectives and scope

To reach the goal outlined above, this section delves into the architectural evaluation of the building blocks catalogued as useful for DE4A. It is important to note that the term “building block” (BB) in the context of this assessment refers to a Solution Building Block in TOGAF sense.

The most important step in assessing the BBs is determining the methodology that would support a common description framework of the BBs, while providing means for determining the quantitative and/or qualitative evaluation criteria of the considered BBs. The outcome of the assessment is a succinct list of recommendations for BB use by the pilots in WP4. In addition to defining the methodology, gap analysis is performed based on both the pilots’ requirements and the common description framework of the BBs, considering the results from the assessment, the project requirements and the common PSA principles. The overall process of conceptual considerations, empirical evaluation, gap analysis and piloting recommendations are denoted as a DE4A generic methodology for architecture building blocks evaluation.

9.2.2 Available methodologies

In order to provide continuity and justification of the methodology that is being developed, we first outline and assess the suitability of the currently available methodologies in view of the implementation context and the objectives of the DE4A project. To that end, both generic EU/EC assessment methodologies and past LSP project-specific methodologies are considered.

9.2.2.1 Common assessment method for standards and specifications (CAMSS)

CAMSS [12] is part of the ISA² interoperability solutions evaluation toolkit for public administrations, businesses and citizens. It provides a method to assist in the assessment of ICT standards and specifications. The main objective of CAMSS is achieving interoperability and avoiding vendor lock-in. In that sense, CAMSS criteria evaluate (among other things) the openness of standards and specifications. This is done by employing the CAMSS tools and adapting the evaluation according to the needs of an individual Member State.

In the context of DE4A, relying solely on CAMSS does not provide the means for BB suitability and gap analysis in relation to the piloting needs. Moreover, it does not provide any selection criteria or a taxonomy for consistent mapping of the different BBs onto a common comparable framework.

9.2.2.2 Past project-specific methodologies

eSENS

eSENS has developed its own methodology for BB assessment, which is mainly an adaptation of CAMSS and Asset Description Metadata Schema (ADMS), supported by inputs of the eSENS deliverable D6.1 (see Table 5 in eSENS D3.1). Its objective is to propose a documentation of format and defining criteria for the maturity and sustainability assessment of building blocks. The overall framework consists of three steps: 1) The Consideration step; 2) The Assessment step; and 3) The Recommendation step and produces a list of assessment criteria to be used for BB evaluation. These criteria, however, are very general and not architecture-specific – their applicability is valid and valuable only if used in collaboration with the legal, business, organizational, technical and implementation team.

It is important to note that the assessment methodology employed in eSENS is developed with a different aim from ours – its analysis and recommendations refer to the desired BB qualities that are needed to ensure meeting the maturity levels and the sustainability criteria envisaged by the project. Thus, although it produces guidelines for assessment, it does not provide concrete output in terms of actual scores, analysis and recommendations for BBs. Moreover, it does not provide a comparable baseline when multiple BBs have to be considered for the same pilot and it is based on the assumption that the existing BBs represent the exhaustive list of possible solutions from which a suitable match should be chosen. In the case of DE4A, such assumption does not hold, as there may be a case where a certain BB is not mature enough to be recommended for piloting but is also not to be completely disregarded either. More importantly, the methodology developed here is used for actual assessment and is to be fine-tuned at a later stage in connection to the general architecture lifecycle development.

TOOP

Like eSENS, the overall idea of the TOOP assessment methodology is to reuse existing frameworks and building blocks provided by CEF, eSENS, and other initiatives. First, an initial inventory of existing e-Government building blocks is proposed. Then, the principles of selection of building blocks for OOP applications are provided, together with high-level views of the architecture. Finally, an analysis of selected building blocks is done with respect to their relevance, applicability, sustainability, need for further development and external interfaces.

The main criteria for inclusion of a building block in TOOP are:

- The specific project requirements;
- The TOOP pilots' needs;
- Usability in long-term applications (maintenance and support provided).

As a result, the building blocks are categorized into three basic groups:

1. BBs that provide capabilities needed by all or most TOOP Pilot Areas;
2. BBs that provide capabilities needed or probably needed by some TOOP Pilot Areas;
3. BBs that provide capabilities not needed by the TOOP Pilot Areas.

TOOP's criteria are tightly bound to the piloting needs, whereas the rationale behind their choice is OOP-specific rather than generic. The methodology here follows a similar line of reasoning, but differs in the conceptual framework, which is more formally defined and made reusable by other projects as well.

9.2.2.3 ISA2 Interim Evaluation

The interim evaluation [13] aimed to assess how well the ISA² Programme has performed since its start in 2016 and whether its existence continues to be justified. Based on stakeholders' views, opinions and public consultation, it evaluated the implementation of the programme based on seven criteria and identified several points for improvement.

The evaluation criteria considered were: **Relevance** (the alignment between the objectives of the programme and the current needs and problems experienced by stakeholders); **Effectiveness** (the extent to which the programme has achieved its objectives); **Efficiency** (the extent to which the programme's objectives are achieved at a minimum cost); **Coherence** (the alignment between the programme and comparable EU initiatives as well as the overall EU policy framework); **EU added value** (the additional impacts generated by the programme, as opposed to leaving the subject matter in the hands of Member States); **Utility** (the extent to which the programme meets stakeholders' needs); and **Sustainability** (the likelihood that the programme's results will last beyond its completion).

However, the interim evaluation does not provide a specific methodology – either in terms of criteria choice, or in terms of architectural or future piloting recommendations. Its value lies mainly in the identification of possible gaps that exist within the current EU architecture framework even prior to the implementation of the available building blocks. In that sense, the main recommendations for prospective actions are determined in **awareness raising beyond national administrations; moving from user-centric to user-driven solutions;** and **working towards increased sustainability.**

Our work integrates the interim evaluation criteria even at the stage of cataloguing BBs relevant in DE4A context. More importantly, it takes into consideration the methodological gaps identified in the assessment in terms of awareness, user-driven solutions and sustainability prescriptions and integrates specific technical, administrative and operational aspects in the recommendation's extraction for the pilots.

9.2.2.4 EAAF

The Enterprise Architecture Assessment Framework (EAAF) [14] assists the US government in the assessment and reporting of their enterprise architecture activity and maturity, as well as in the advancement of the use of enterprise architecture to guide political decisions on IT investments. In addition to providing the methods for the assessment, EAAF also identifies the measurement areas and criteria by which government agencies are to rely on the architecture to drive performance improvements. This is integrated into the so-called Performance Improvement Lifecycle, where points for improvement are identified and translated into specific actions.

In that sense, the framework provides a good overall methodology for the assessment of DE4A BBs. Following its guidelines, in order to perform the technical assessment, the architects, together with the relevant project partners (mainly from WP1 and WP4):

- Identify and prioritize the BBs considering the pilots' needs and in view of the project goals and objectives;
- Determine specific methodological steps for gap analysis, using common or shared information assets and information technology assets;
- Quantify/qualify and assess the performance to verify compliance with pilots' requirements and provide report on gap closure; and
- Assess feedback on the pilots' performance in order to enhance the architecture and fine-tune the assessment methodology for future implementation decisions.

9.2.3 Methodological considerations

The need to develop a generic methodology that integrates some aspects of the standardized methodologies, but does not rely on a single one, is based on several considerations:

1. The assessment methodologies currently available either focus on alignment of the BB specifications or are only concerned with the maturity of the solution provided by the building blocks;
2. They do not provide a clear definition of the common principles for assessment;
3. They do not allow for a phased-approach to the assessment and are applicable either for a single BB or for a finalized solution architecture (Note: Although EAAF prescribes the principles for a phased assessment, it does not delineate the phases explicitly and only gives a requirement for the overall outcome of the assessment).

As a result, the architect is prevented from developing an assessment for multiple BBs with varying levels of complexity and is also disabled to perform comparative evaluation for determining the best fit for a particular solution architecture.

The methodology developed here is novel in that it addresses the points above and is also generic in the sense that it can be reused by other large-scale projects for similar purposes. It incorporates the assessment principles of existing standards-based methodologies (like CAMSS and EAAF) taking into account the architecture feasibility and sustainability, but it also generalizes these principles over the context of implementation required by DE4A.

9.3 Methodology

In order to account for both the piloting recommendations criteria and the performance assessment criteria, the overall methodology requires a phased approach. Therefore, it consists of two phases:

I) The first phase takes stock of the entire list of BBs that can have potential use in the project and as part of the piloting. Then, a conceptual and an empirical framework for evaluation is developed – the former enables the gap analysis of the BBs, whereas the latter allows for qualitative and comparative analysis of the BBs, as well as extraction of concrete recommendations for piloting. The first phase essentially corresponds to the first three points of the EAAF.

II) The second phase will account for the complete list of project artefacts and will provide empirical validation for the results and recommendations from the first phase. In addition, reassessment of the previous gaps will be performed. This phase will mainly be realized in close collaboration with the pilots: direct feedback via surveys and questionnaires on BBs' performance will be obtained and the initial conceptual framework will be fine-tuned accordingly. The second phase corresponds to the last point of the EAAF.

9.3.1 Conceptual framework

In this section, we first catalogue the BBs that are to be considered by the assessment. This step considers the output from D1.5 and establishes a relation to the internal project environment. Then we establish a common conceptualization of the key elements, which is based on the Digital service model, Section 2.2 of the Study on "The feasibility and scenarios for the long-term sustainability of the Large Scale Pilots". With that, a relation to the external project environment is established. Finally, a basic assessment framework is developed to enable the grading of the BBs from several maturity aspects: technical, administrative and operational. The output of the assessment will allow us to perform gap analysis and will also guide the extraction of the piloting recommendations.

The Digital Services Model: A five-layered approach

The LSPs so far have developed building blocks that enable cross-border interoperability based on standards, specifications and common code/components. Therefore, moving beyond the pilot projects and towards actual deployment, it is crucial to develop a structure in which the digital services and the elements they are composed of can be conceptualized.

To establish a conceptual model, it is important to clearly set out the key terminology that is used in relation to the DSI for the provision of cross-border public services. CEF provides an overarching framework suitable for this purpose, called **Digital Services Model** (DSM). It takes into account the deliverables of the LSPs, the stakeholders and roles they can take on, and the drivers behind the dynamics of this complex ecosystem.

The Digital Services Model is not only needed to establish common terminology and framework, but it is also necessary to analyse the needs and requirements for the future deployment of any digital services, enabling a continuity of the developed methodologies with the LSPs. Thus, it presents the different levels of granularity which need to be taken into consideration for the overall management of the DSI for the provision of public Services.

The following elements represent the main part of the DSM taxonomy:

1. Standards and Specifications;
2. Common code or Components;
3. Building Blocks;
4. Core Service Platforms;
5. Generic Services.

Standards and Specifications have been used by all the LSPs for the development of the digital services. These standards and specifications play a central role in interoperability as it means that systems have commonalities in key areas, enabling systems to communicate with one another.

Components are the common code that has been developed for the building blocks. Building blocks are made up of several components (e.g. a timestamp component/functionality). These are often referred to as modules in the deliverables of the LSPs. Component can either be BB-specific or used in several BBs.

Essentially, all the solutions derived from the LSPs are ultimately **building blocks** in the sense that they are services that can be integrated as part of other services. Given the fact that these building blocks have the most obvious potential for reuse across different domains (or Core Service Platforms) these can be seen as a specific layer as part of the set of digital services.

Core Service Platforms enable the provision of cross-border digital services in different domains, like eHealth, eJustice and eProcurement. These are the platforms where all the different BBs for a specific service (e.g. eHealth services or eID services) are brought together and made available, enabling service providers to take up and reuse the services as part of their own services. The Core Service Platform (CSP) level should eventually enable the Member States to interact with other Member States through the use of building blocks (via the Generic Services).

It is important to determine what building blocks have been developed by an LSP, as well as which of these are CSP-specific and which are reusable. The CSP-specific blocks are called *domain blocks* (e.g. ePrescription is specific to eHealth) and the reusable blocks are called *building blocks* (e.g. eID can be reused in various domains).

The reusable building blocks are the strongest common element between the various CSPs. They therefore need to meet the needs and requirements of all the CSPs. This underlines the links between the building blocks and the CSPs, and the need to manage both of these simultaneously.

Generic Services is the level of abstraction at which the Member States integrate or connect to the CSPs. These interconnections are necessary to link up a Member State so it can provide cross-border access and use of national eIDs, electronic health records, national procurement platforms, national eJustice platforms and public services for foreign business. Each Member State has to ensure that these existing systems at national level are linked up with the CSPs through Generic Services in order to be cross-border enabled.

To define a common taxonomy for BB description prior to the actual assessment, the relevant BBs are catalogued in view of the five-layered model described above. This is represented in Figure 42.

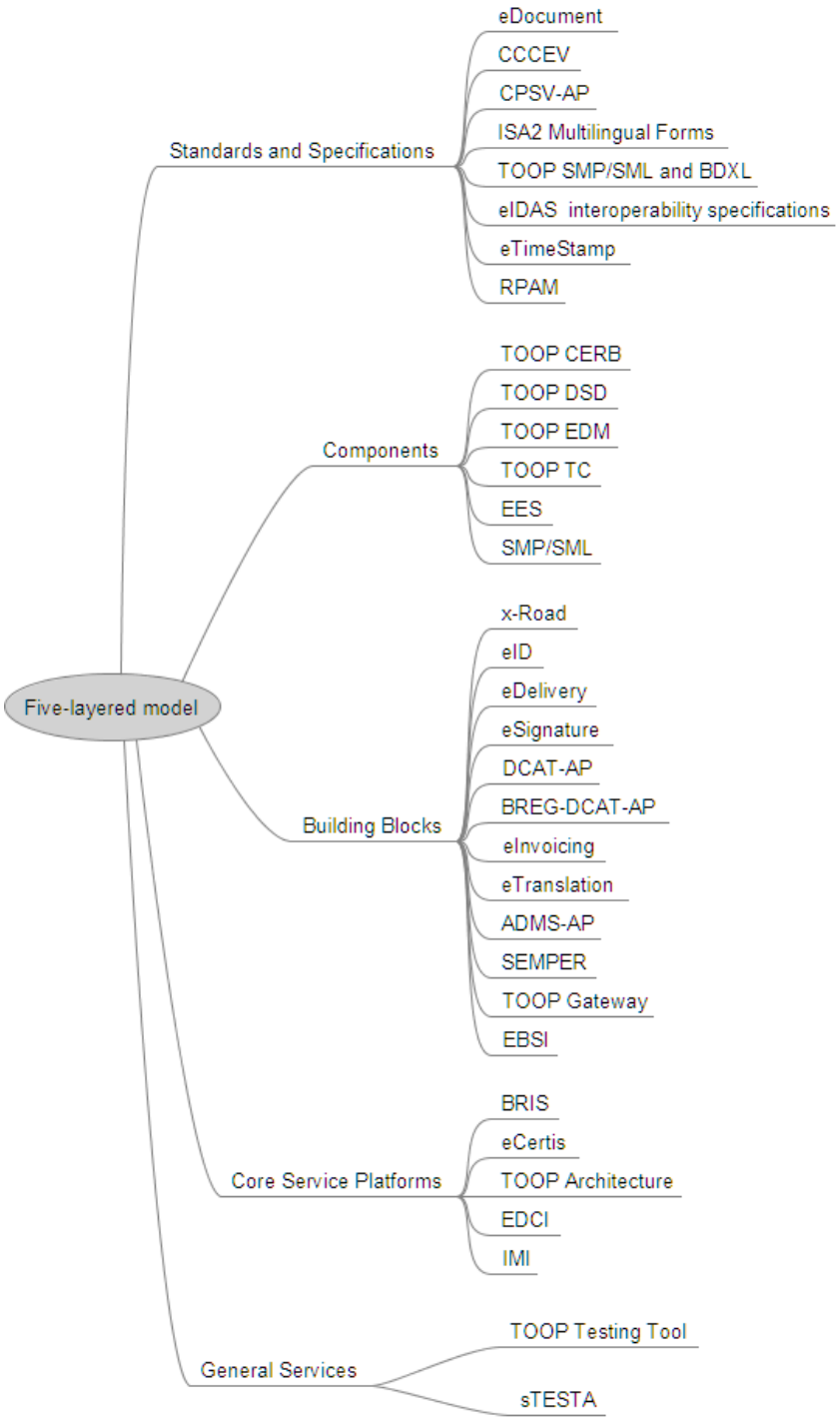


Figure 42: Taxonomy of Building Blocks

Although implicitly understandable, it is worth noting that some BBs can belong to two different categories, as their application is largely context dependent. In other words, whereas in one context a certain BB can be seen as a Standard/Specification, in another context it can be a Component. In those cases, the more general category is assigned to that BB, giving priority to show its potential rather than its most common use. Assessment criteria

In this section, a basic assessment framework is presented composed of the criteria that guide the expert scoring of BBs from the aspect of technical, administrative and operational maturity. The criteria essentially represent a matrix indexed by two dimensions: Score and Maturity aspect. These dimensions, together with the semantics of the criteria (the matrix-cells) are shown in Table 61 For better graphical representation of the empirical assessment that will be performed in the next section, each row is represented by a colour, visually grasping the overall maturity of a certain building block.

Table 61 Conceptual BB assessment framework

Maturity Score	Technical	Administrative	Operational
3 (Highest)	Cutting-edge	Completely aligned with current EU policies	EU infrastructure, broadly accepted
2	Implemented and running	Aligned with national policies, but is yet to be aligned with the EU	runs in production in EU (one or more MS)
1	Not stable/ under development	Acceptable, but subject to improvement	Piloted
0 (Lowest)	Antiquated/to be phased out	Conflicting with current policy/no-GO	Concept

Legend

Recommended	Acceptable	Useful	Discarded

The colouring of the framework is not important only for the visual appeal of the reader; rather, it is meant to serve as a concrete input (an additional dimension) for the prospective formalization of the assessment framework. Such formalization would enable a semi- and, ultimately, a fully automatic maturity and quality attributes assessment of both a set of desired (composable) BBs, as well as a solution architecture representing a Common Service Platform or a General Service per se.

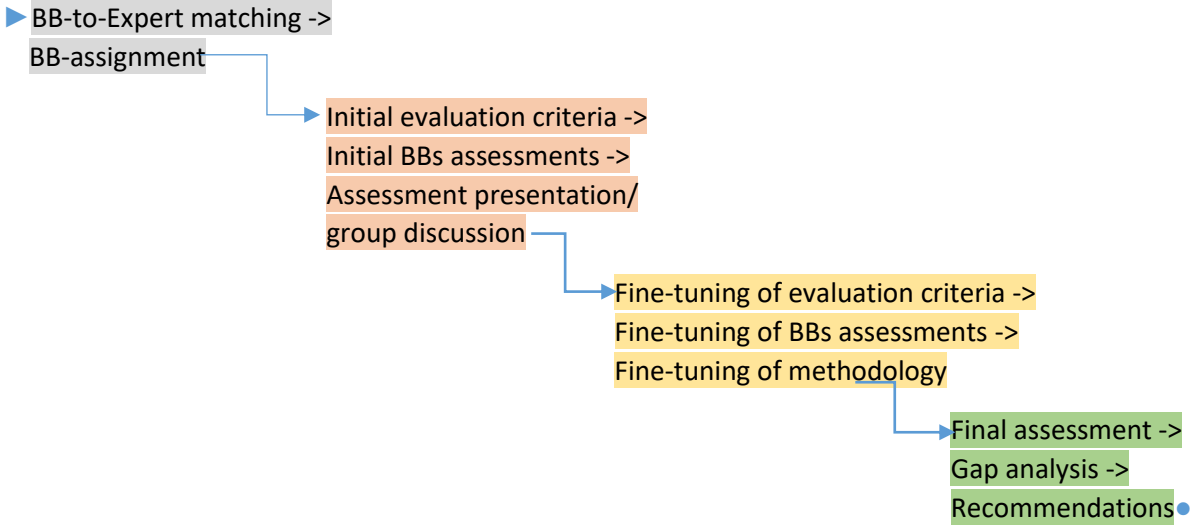
It is important to note that the framework represented above is a simplified version of the generic assessment framework that will be the final contribution by WP2. This is because at this stage it cannot be expected that all necessary information by the pilots is obtained for an overall architecture evaluation to take place. Such assessment will be performed in the second phase of the *BBs' assessment* task, when the framework from Table 2 will also be further revised and fine-tuned. As a result, the gap analysis in the second phase will take into account the exhaustive set of pilots' requirements and the pilots' feedback on the implemented BBs.

9.3.2 Empirical framework

The empirical framework is essentially an implementation of the conceptual framework with concrete recommendations as an output. While the conceptual framework is based on well-standardized assessment methodologies, the (input to the) empirical evaluation of the BBs relies largely on expert opinions and judgements. To close the subjectivity gap between the experts' evaluation criteria, the BB Assessment group defined an internal process of iterative calibration on the evaluation criteria, as represented by the process flow below:

▶ Preparatory step à Assessment step à Fine-tuning à Recommendation step ●

At a more granular level, each step integrated the following actions:



In the **Preparatory step**, the building blocks were matched to the experts' experience and expertise with respect to the capabilities provided by each BB and the architecture principles outlined by the DE4A objectives. One or more groups of BBs with shared capabilities were then assigned to each expert for assessment.

In the **Assessment step**, the initial evaluation criteria were agreed upon and integrated into the basic assessment framework (Table 61). Then, the results from the initial assessments for each BB were presented in front of the BB Assessment group. This allowed for a constructive discussion on the need to fine-tune the evaluation criteria and to revise the evaluation results. These considerations are part of the **Fine-tuning step**, which is essentially an iterative procedure on its own, until the complete set of evaluation criteria is obtained, and the BB scores are approved by all experts of the BB Assessment group.

In the **Recommendation step**, the final scores for each BB were provided for all three maturity aspects: Technical, Administrative and Operational. These are then analysed in view of the piloting requirements and the DE4A objectives as part of the Gap analysis, enabling the extraction of a single Recommendation as an output from the overall process.

The output of the preparatory step is the Taxonomy of BBs, whereas the output of the Assessment step is the conceptual framework – further whose criteria, aspects and semantics were fine-tuned in the third step. The scores and recommendations are obtained as an output from the final (Recommendation) step, supported by the argumentation given in the Gap Analysis. For a more complete overview of the final scores and recommendation, they are succinctly represented altogether in Table 62.

9.3.3 Recommendations and Gap Analysis

This section summarizes the assessment for each building block, by aspect and with an overall recommendation grade. A recommendation is essentially the expert opinion based on the results from the conceptual framework, the gap analysis and in relation to the piloting needs and requirements. The overall list of assessed BBs is catalogued in Table 62.

Table 62: BB recommendations[5]

#	Building Block	Technical Maturity	Administrative Maturity	Operational Maturity	Recommendation
1	eDelivery[6]	Implemented and running	Completely aligned with current EU policies	runs in production in EU (one or more MS)	Recommended
2	eID	Implemented and running	Completely aligned with current EU policies	runs in production in EU (one or more MS)	Recommended
3	eSignature	Cutting-edge	Completely aligned with current EU policies	runs in production in EU (one or more MS)	Recommended
4	CCCEV	Implemented and running	Completely aligned with current EU policies	Piloted	Acceptable
5	CPSV-AP	Implemented and running	Completely aligned with current EU policies	runs in production in EU (one or more MS)	Acceptable
6	eCertis	Implemented and running	Completely aligned with current EU policies	EU infrastructure, broadly accepted	Recommended
7	eIDAS interoperability specifications	Implemented and running	Completely aligned with current EU policies	runs in production in EU (one or more MS)	Acceptable
8	sTESTA	Implemented and running	Completely aligned with current EU policies	EU infrastructure, broadly accepted	Discarded
9	x-Road	Implemented and running	Aligned with national policies, but is yet to be	runs in production in EU (one or more MS)	Useful

[5] The DE4A project maintains an internal register of all assessed BBs which can be provided on request.

[6] For a detailed assessment of eDelivery, eSignature, eID, CCCEV, CPSV-AP see [17].

#	Building Block	Technical Maturity	Administrative Maturity	Operational Maturity	Recommendation
			aligned with the EU		
10	DCAT-AP	Implemented and running	Completely aligned with current EU policies	EU infrastructure, broadly accepted	Acceptable
11	BREG-DCAT-AP	Not stable/ under development	Acceptable, but subject to improvement	Piloted	Acceptable
12	ISA2 Multilingual Forms	Implemented and running	Completely aligned with current EU policies	runs in production in EU (one or more MS)	Acceptable
13	EBSI (CEF Blockchain)	Not stable/ under development	Acceptable, but subject to improvement	Piloted	Useful
14	eInvoicing	Implemented and running	Completely aligned with current EU policies	EU infrastructure, broadly accepted	Recommended
15	eTranslation	Implemented and running	Completely aligned with current EU policies	EU infrastructure, broadly accepted	Recommended
16	SEMPER	Not stable/ under development	Acceptable, but subject to improvement	Piloted	Recommended
17	BRIS	Implemented and running	Completely aligned with current EU policies	EU infrastructure, broadly accepted	Discarded
18	TOOP Architecture[7]	Implemented and running	Aligned with national policies, but is yet to be aligned with the EU	Piloted	Recommended
19	TOOP CERB	Not stable/ under development	Acceptable, but subject to improvement	Piloted	Useful
20	TOOP DSD	Not stable/ under development	Acceptable, but subject to improvement	Piloted	Acceptable

[7] For TOOP BBs see section 9.5 comprising an extensive overview on the TOOP project and – mainly – an introduction of the technical artefacts of the TOOP infrastructure.

#	Building Block	Technical Maturity	Administrative Maturity	Operational Maturity	Recommendation
21	TOOP eDelivery [SMP/SML and BDXL]	Cutting-edge	Aligned with national policies, but is yet to be aligned with the EU	runs in production in EU (one or more MS)	Recommended
22	TOOP EDM	Not stable/ under development	Acceptable, but subject to improvement	Concept	Acceptable
23	TOOP TC	Implemented and running	Aligned with national policies, but is yet to be aligned with the EU	Piloted	Recommended
24	TOOP Gateway	Cutting-edge	Aligned with national policies, but is yet to be aligned with the EU	runs in production in EU (one or more MS)	Recommended
25	TOOP Testing Tool	Not stable/ under development	Acceptable, but subject to improvement	Piloted	Acceptable
26	ADMS-AP	Implemented and running	Completely aligned with current EU policies	EU infrastructure, broadly accepted	Useful
27	EDCI	Not stable/ under development	Acceptable, but subject to improvement	Piloted	Useful
28	EES	Not stable/ under development	Aligned with national policies, yet to be aligned with the EU	Concept	Useful
29	eTimeStamp	Not stable/ under development	Completely aligned with current EU policies	Concept	Recommended
30	eDocument	Not stable/ under development	Acceptable, but subject to improvement	Concept	Discarded
31	RPAM	Implemented and running	Acceptable, but subject to improvement	Piloted	Useful

#	Building Block	Technical Maturity	Administrative Maturity	Operational Maturity	Recommendation
32	SMP/SML	Cutting-edge	Completely aligned with current EU policies	runs in production in EU (one or more MS)	Recommended
33	IMI	Cutting-edge	Completely aligned with current EU policies	EU infrastructure, broadly accepted	Discarded

Following is the analysis of the results from the overall assessment from the aspect of the pilots' needs, the conceptual framework and the overall architectural principles. It is important to note that this is not the exhaustive set of gap analysis, but it serves as a proof of concept for the methodological and assessment choices decisions made.

Pilots needs' considerations

From the table above, it can be noted that, although some of the BB are assessed as immature from some aspect, the final recommendation is still for them to be used by the pilots. This is due to the fact that, regardless of the current state of maturity, when matched with the pilots' requirements, some a BB may still have the necessary architecture capabilities that require adjustment in the DE4A context. For instance, this is the case with SEMPER. The SEMPER extension to eIDAS is not fully mature yet but is the only cross-border functionality for working with proxies that currently mandates successfully piloted. Otherwise, there will be a need to develop a DE4A-specific solution for cross-border powers validation from the scratch, which is bot not useful and not feasible within the project timeframe. In order for SEMPER to gain a broader user-base, it has to be validated by more Member States (currently, it has been piloted with 4 MS). In addition, SEMPER has been piloted with legal persons only. Although this is sufficient to the DBA pilot, this is not the case for the moving abroad and studying abroad, as there is a need for piloting with natural persons. The DE4A pilots themselves may be used for this. Finally, SEMPER extends eIDAS, but has not been handed over to DIGIT yet. Therefore, it has not been incorporated in the eIDAS reference software of DIGIT yet. Integration in eIDAS will improve sustainability of the SEMPER extension. Concretely, SEMPER would benefit from eIDAS-like specifications to allow Member States that do not use the eIDAS reference software to develop their own extension based on these specifications.

In contrast to SEMPER, there is also a case where a BB may be assessed as completely mature in most of the aspects but is still disregarded at the Recommendations stage. This is, for instance, the case with the IMI BB, which despite the overall high maturity in all aspects is out of the scope of the DE4A project. Similarly, the BRIS building block has a scope that is much narrower (especially from an administrative perspective) than the scope of DE4A and is therefore not to be used by the pilots. More concretely, BRIS has been developed for inter-business register communication, which is not the primary focus of the DBA pilot (the functional shortcomings on BRIS for piloting in DBA (D4.5, annex V) have been confirmed by DG DIGIT and there is no BRIS-roadmap foreseen that will deliver a solution to the findings). Furthermore, it is legally not feasible to use the BRIS-network for the DE4A-pilots (currently not allowed for non-business registers). An alternative is being discussed with DIGIT: a message broking platform as a possible future BRIS-wide solution that is piloted in TOOP. However, funding for continuation of the platform is not arranged and the current intention is to bring the (cloud-based) prototype infrastructure down when TOOP testing ends.

Similar reasoning in compiling the overall recommendation score is applied to the other building blocks. These considerations have been discussed in detail at the BB Assessment Group meetings during the Recommendation step of the empirical framework. It is out of scope of the deliverable to present a detailed overview of each BB. However, the subtlety of some of the assessment criteria (such as context dependence) is also an argument to justify the decision to rely only on the experts' evaluations in the first phase of the methodology.

Assessment outcomes considerations

Out of the 33 assessed BBs, 13 BBs are Recommended for implementation, 9 are Acceptable, 7 are Useful and 4 are Discarded (see **Error! Reference source not found.**a). From a maturity point of view (see **Error! Reference source not found.**b): in terms of technical maturity, 5 are cutting-edge, 18 are implemented and running in an operational environment, whereas 10 are not stable or under development. From an administrative maturity aspect, almost half (17) of the BBs are completely aligned with current EU policies; 7 are aligned with national policies but are yet to be consolidated at an EU level, whereas 9 (although acceptable) are still subject to further improvements.

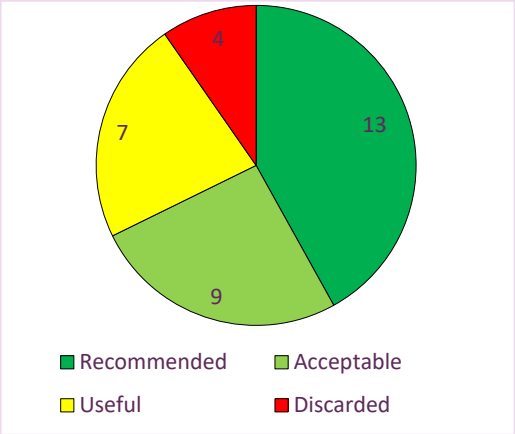


Figure 43 (and figure 44) Taxonomy of assessed BBs with their recommendations

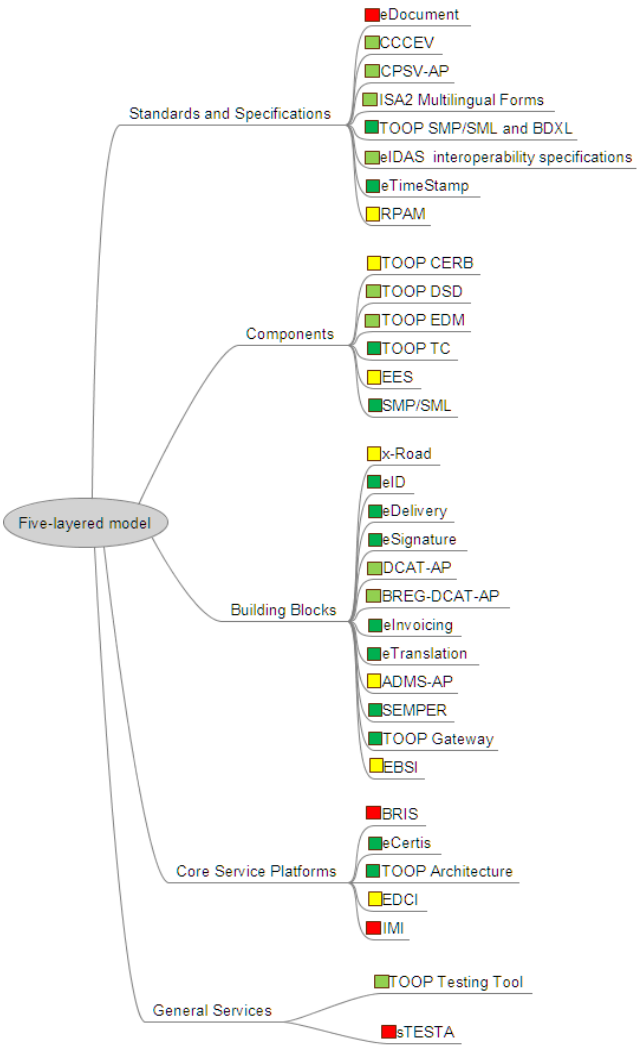


Figure 44

From operational maturity aspect, there are 8 BBs which are broadly accepted as part of an EU infrastructure, 12 that run in production in one or more Member States and 10 that are piloted within some kind of operational or testing environment. It is interesting to note that the only aspect by which a BB has been assessed as immature is the Operational aspect. Thus, there are 4 BBs (TOOD EDM, EES, eTimeStamp and eDocument) that are marked as operationally immature, as they are only at the stage of a Concept and are yet to be developed.

From a BB type aspect (also visible from Figure 44), most of the recommended BBs are of the type 'Building Block' (7 out of 13) and 'Standards and specifications', whereas the 'General services' and the 'Core service platforms' are the least numerous and the most immature. This is expected, as the later are also the most complex ones and only few in number across EU.

It is also notable that most of the BBs considered for use by the pilots are in a mature and useful state that allows reusability and potential upgrades before implementation in the DE4A pilots. Such considerations are already being made (as discussed in the previous subsection) and are part of the piloting requirements to be assessed in the second phase of the methodology.

Architecture framework considerations

As outlined in the methodological considerations in Section 9.2.3, the two phases of the overall methodology follow the Enterprise Architecture Assessment Framework principles, with the additional step of providing recommendations for the pilot in between the two phases. Such an approach allows, in addition to the qualitative evaluation, to obtain e quantitative score for the maturity of the overall architecture as a (sub)set of the assessed BBs. In that sense, while the output of the EAAF is a maturity level assessment of the overall architecture, the phased approach in DE4A creates an intermediate feedback loop between the pilots and the Project Start Architecture, allowing for adaptable integration of the assessment methodology within the WP2 change management.

Regardless of the incomplete overall assessment, it is still possible to have a quantitative assessment for a solution architecture after the first assessment phase. However, this is not to be considered as the overall architecture framework maturity level, but only as a 'current maturity level' of the solution architecture comprised of a given set of BBs. Such value can serve as a reference point to be compared upon a given KPI for the overall maturity, in case there is such requirement.

In order to compile a single value for the current maturity level for a pilot solution architecture, the set of BB assessments and their recommendations shell be compared upon the baseline for the EAAF maturity levels given in Figure 45. EAAF Maturity levels

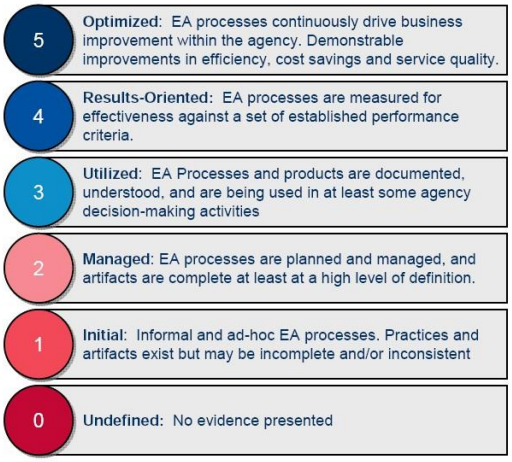


Figure 45. EAAF Maturity levels

In the context of DE4A, we will provide such assessment in the second phase of implementation of this methodology, as currently there is no definite list of BBs matched to the specific pilots.

9.4 Summary

This chapter presented the assessment of BB suitability for integration in the DE4A pilots in terms of technical, administrative and operational maturity of the BBs identified and catalogued in Task 1.5. Thus, the results of the assessment provide a bridge between WP1's outputs and the WP4 requirements. Over 40 BBs have been considered for this assessment, 33 of which are assessed at the first phase of this work. The results of the assessment show that there is a mature and acceptable stock of solution building blocks that can be considered for implementation by the pilots, either in their entirety or partially, with the needed upgrades.

The methodology developed here is generic and reusable by other projects, as it defines the common principles for BB systematization, while providing means for determining the quantitative and/or qualitative evaluation criteria of the considered BBs. With that, it contributes to the overall EU digital strategy for providing sustainable architectural solutions for cross-border public services.

The outcome of the assessment is catalogued as concrete scores and recommendations for BB use by the pilots in WP4. The gap analysis performed provide supports and arguments on the decision for the particular scores and for the final recommendation. Moreover, the possibility for an overall quantitative assessment of the overall project architecture is also considered as part of the gap analysis.

In the second phase of the assessment, the actual implementation and maturity in the context of DE4A will be assessed. Through a continuous collaboration with the pilot, a special survey will be developed to extract the necessary information throughout the whole piloting life cycle. An overall quantitative score will also be provided for the solution architectures for all three DE4A pilots. Finally, the possibility to formalize the overall methodology will be analysed. This is will greatly aid the architects and enable semi- and fully automatic architecture and quality attributes assessments.

9.5 TOOP Infrastructure and Functionalities

This section comprises an overview on TOOP project and – mainly – an introduction of the technical artefacts of the TOOP infrastructure.

9.5.1 Overview on the TOOP

TOOP project itself was confronted with the wage of SDGR and some further challenges, solving data exchange, overall, in the form of "evidence" exchange in an explicit cross-border approach. The TOOP approach was widely not invented within the project, but rather a crystallisation of existing concepts, combined with new complementary system parts. The fact that the baseline components of TOOP stem from existing – and overall implemented and operated – eServices in Europe, proves it ability. The base component of TOOP infrastructure "CEF eDelivery" was developed in "PEPPOL" Large-Scale-Pilot project and further developed in eSENS project. eDelivery building block is since his introduction widely used in OpenPEPPOL, the successor organisation from the PEPPOL project, established in 2012 [33]. Eventually, eDelivery is used since more than 10 years in operational field and was finally introduced as CEF building block, following the CEF initiation in 2014.

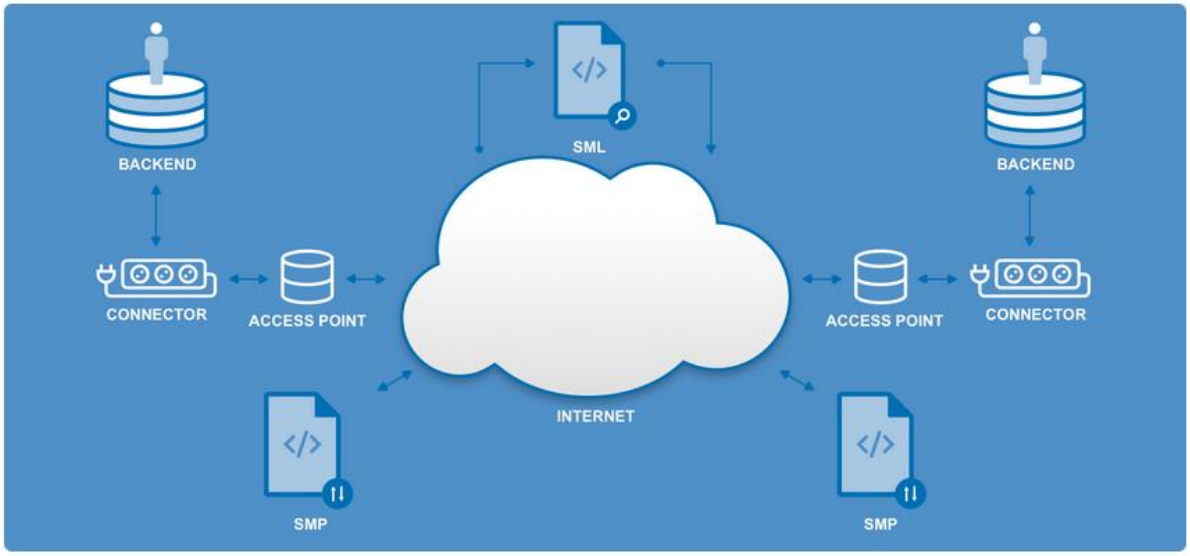


Figure 46 Overview on CEF eDelivery

The main objective of the Large Scale Pilot project "The Once Only Project" (TOOP) [18] is to explore once-only principle across borders, especially to facilitate the evidence exchange between the two main actors of the architecture: The Data Consumer (DC) and the Data Provider (DP). TOOP focus on reusability and interoperability as defined in the European Interoperability Framework (EIF): legal, organizational, semantic and technical.

9.5.2 TOOP Solution Architecture

The Cross-Border Evidence Exchange Process is the core of the Solution Architecture [38]. For the application of the Once-Only Principle, a Data Consumer needs a specific kind of data, in order to properly execute a procedure.

In order to do that, there are several process steps that need to be executed with several interactions that need to take place between the central services of the TOOP infrastructure and the actors' systems.

Table 63: Process Steps TOOP infrastructure components

Nr	Process Step	Infrastructure Component
1	User Identification and Authentication using a trust mechanism like eIDAS	eIDAS Node (MS A)
2	Identify the proper evidence using the Criterion Evidence Rule Base (CERB)	CERB
3	Discover the DPs that can provide the required evidence for the specific user using the Data Service Directory	DSD
4	The DC requests an explicit consent from the user for requesting the data on its behalf from the chosen DPs	MS Online Portal Application
5	For each selected DP: DP Routing Information Fetching, Data Message Submission	

Nr	Process Step	Infrastructure Component
5.1	DP Routing Information Fetching: Extract the routing information required for secure and reliable Message Exchange	SMP, SML, AS4 Access Point (eDelivery)
5.2	DC Message Submission / Evidence Query Request Submission Create and send a Data Request containing the data required by the DC and the routing information. The following information is passed to the AS4 Access Point	EDM, AS4 Access Point
6	Each DP	
6.1	Receive and Validate the Data Request	EDM
6.2	Verify the Data Consumer	eIDAS Node (MS B)
6.3	DC Routing Information Fetching: Similar to step 5.1 the routing information for the DC is extracted for the Data Response	SMP, SML, AS4 Access Point (eDelivery)
6.4	DC Message Submission Gathering all necessary information to create a Data Response, if possible, otherwise an Error Response is created. The created Data Response is passed to the AS4 Point, back to the DC.	EDM, AS4 Access Point
7	The DC receives the responses, validates and extracts the information for use in the step of the executed procedure	EDM

9.5.3 Criterion Evidence Type Rule Base (CERB)

The Criterion & Evidence Type Rule Base is a central service that will allow Member States to manage and share information about rules relating evidence types to criteria, in particular for standardised types of evidence (e.g. birth certificates) that do not require a detailed substantial assessment.

DG GROW's eCertis [38] is the services that will act as the Criterion & Evidence Type Rule Base system. eCertis provides a REST API [39] that can be used to query various mapping between criteria and evidences. Currently, eCertis is under an updating process of its internal functionalities, in order to become multi-domain, and, when ready, will be used by TOOP as the CERB system in the pilots.

9.5.4 Data Service Directory (DSD)

The Data Services Directory is also a central service that maintains a catalogue of Data Providers with the datasets the DP is able to provide upon request. In the Evidence Exchange Process, the DC uses the DSD for discovering possible DPs, which can provide the required evidences. The information data model is a profile of the BREG-DCAT-AP specification, an application profile of DCAT, profiled by ISA[2], in order to achieve both organizational and semantic interoperability. The Service API is implemented using the OASIS Regrep v4 Query Protocol with the REST API Binding. It also provides a Java client library that implements the REST API for managing the DSD lookup.

9.5.5 SMP/SML and BDXL (eDelivery)

In TOOP the CEF eDelivery building block is used to create a network for digital cross-border communication for evidence exchange in three different pilot domains: 1) eProcurement 2) General Business Mobility 3) Maritime. CEF eDelivery BB is open and free for all, developed by previus LSP's and supported by OASIS standards. eDelivery is based on a distributed model (on the AS4 messaging protocol) where every participant is connected to a node (Access Point) that is using standard transport protocols and security policies.

An Access Point could act on national, organizational or regional level. In TOOP every MS use an Access Point to register the endpoint for the MS application. Therefore, the Service Metadata Provider (SMP) acts as decentralized registry of the eDelivery network to provide the metadata about the Participants business capabilities and the eDelivery access points, which are used by Data Consumers and Data Providers in the MS applications.

As the SMP is a decentralized registry, all participants MUST be registered to the central BDXL (Business Document Exchange Location) instance. BDXL is the successor specification of SML and mostly used interchangeable. The goal of a BDXL instance is to create dynamic DNS (Domain Name System) entries to link participant identifiers to SMPs, so that by knowing the participant identifier and the algorithm to create the DNS name, the URL of the SMP of that particular participant-identifier can easily be retrieved. In a short sentence, The SMP provides participants business capabilities and the Access Point metadata where the BDXL/SML is used to find the location of the SMP.

As standard transport protocol the OASIS BDXR SMP 1.0 profile [32] was defined in TOOP. The following parameter are used to identify an endpoint within the network:

- Participant identifier - technical identifier of the final recipient
- Document type identifier - the kind of document to be exchanged. The document type identifier is predefined for each business domain.
- Process identifier - the orchestration that is to be used. Will be predefined by TOOP.
- The transport protocol ID - to identify AS4 in the e-SENS profile that value is constantly bdxr-transport-ebms3-as4-v1p0 in TOOP.

9.5.6 TOOP Exchange Data Model (EDM)

The TOOP exchange data model specification describes a process providing electronic messaging support for requesting specific data elements or documents and providing adequate data responses or document responses. The Exchange Data Model is designed as an abstract structure to extend the data elements (semantic concepts) for different business domains.

This approach reduces the data model in each application to their application's needs and does not provide a huge, unclear data model for each business domain. EDM is a standardized data model to provide interoperability between the MS and a base for the national mapping adaptions.

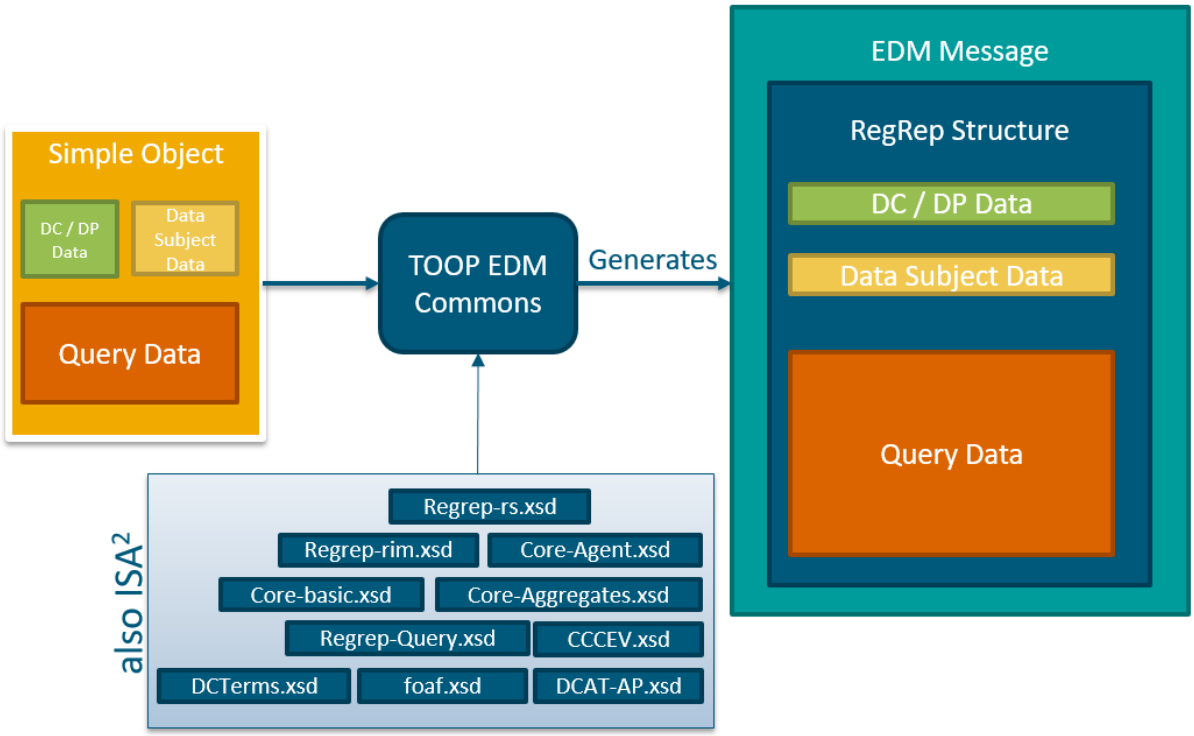


Figure 47 TOOP EDM

9.5.7 TOOP Connector (TC)

The TOOP solution architecture [23] is based on OASIS Standards [23] for exchanging business documents within a 4-corner architecture extended by a component for handling the communication between DC/DP and the central services. It encapsulates the complexity for each interfaces of the central services in a very flexible, exchangeable and extensible manner and provides a default implementation:

- Client implementation for CERB, based on REST API (see chapter CERB)
- Data Provider Queries to discover the DP list, based on REST API
- Fetching the DP Routing Information – SMP [24] client via REST API to DNS [25] (eDelivery)
- AS4 [26] backend using the CEF AS4 profile [28]

The TC ensures that the payload (Data Request and Response) is properly constructed, validated and packed in an envelope, and that the envelope can be successfully sent via AS4. It includes the invocation of dynamic discovery (DSD/SMP/DNS lookup), which is a decentralized metadata exchange system without a single point of failure. The TC is a java library that can be integrated in any MS application via Java API or can be run as a standalone deployable that could be used via REST API. The following figures illustrate the different approaches.

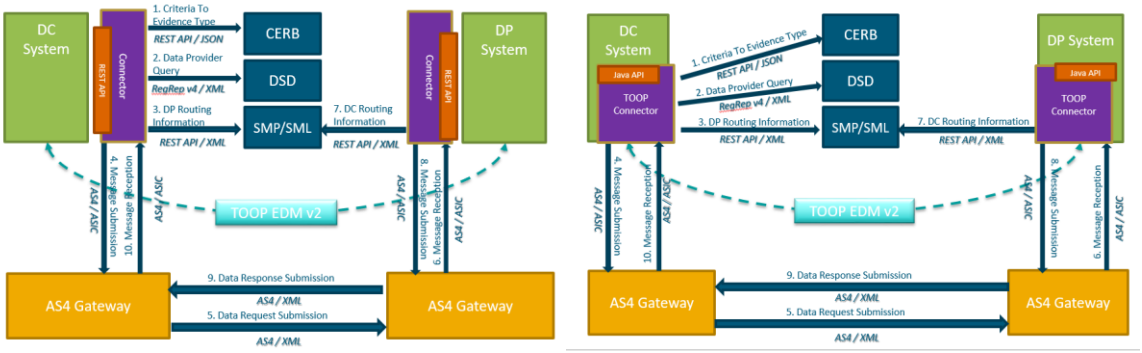


Figure 48 TOOP System Overview (2 different implementations)

The benefit of the API-based interfaces for DC and DP is that every MS can independently implement the sematic mapping on the national level and no other MS has to be involved. The semantic mapping is decentralized organized by the MS to reduce the complexity of using additional central services managing the semantic problems of all MS. Due to the flexibility of the implementation in several libraries it is possible to combine all the components (DC, DP, TC and AS4) in a single deployable artefact. With an additional SMP instance the needs of a MS are fulfilled in the TOOP infrastructure. This approach is up and running in the Austrian TOOP pilot, while other pilot partners manage the components in separate deployables and/or (Docker) containers. The decision is up to the MS, which are responsible for the integration and decision making in Large Scale Pilot projects.

For logging a distributed streaming platform (Apache Kafka [28]) is used to provide a higher level of transparency for all participants.

The conclusion is that the TC combines all the aspects of eDelivery [29] and provides secure, interoperable, trustworthy and non-repudiable message exchange in an adaptable manner reducing the complexity for the MS in a single component.

9.5.8 TOOP Gateway (AS4)

Since TOOP uses the CEF building block eDelivery, which can be implemented following the 4-Corner-Model (as one example of communication methods), it consists of two gateway-instances both on DC and DP side. “The OASIS ebMS3 and AS4 specifications are specifications for point-to-point message exchange between two Message Service Handlers.” The gateway acts as interface protocol between the two Access Points at DC and DP side. The 4-Corner-Model [31] implemented in TOOP uses AS4 interface for the communication between the two inner corners – C2 and C3, which means the request and data transfer between the DC and DP Access Points, not the crucially the communication between the outer corners – the DC and DP itself.

9.5.9 TOOP Testing Tools

The TOOP simulator [31] is a CLI program that mock the behaviour of a DP or DC. It helps the developers to test the MS solution against the reference implementation.

The TOOP playground is a test environment that simulates the behaviour of a running DC as well as a DP of a virtual MS. Each MS can test independently from other MS the message exchange against the virtual instances.

9.5.10 TOOP pilots

The TOOP project is focused on the pilot execution, three different pilot areas are implemented within its Large-Scale-Pilot-approach [31]:

- Cross-border e-Services for Business Mobility (GBM – focus of the article)
- eProcurement
- Online Ship and Crew Certificates

As a model for the pilot realisation the existing model of *Connectathon* of the IHE was chosen and adapted [34]. A Connectathon is a procedure to demonstrate interoperability between ICT systems, to prove that the technical specification has been fully and correctly implemented. Therefore, a Connectathon consists of [1] a planning, [2] specific content, [3] a technical implementation and [4] an execution (…and documentation as shown below). A Connectathon also represents a procedure for identifying errors and improving them.

When used in TOOP no negative effects for an error in the implementation arise to the participating parties, but the incentive for improvement. Therefore, a specific concept of this instrument specifically for TOOP was described and adopted for the project. If such improvement is necessary, it may be results in a refinement of the specification or the specific implementation at the participating organisations' side. However, in TOOP project malfunctions must not affect operative ICT-environment and therefore do not lead to data loss or damage. Thus, the Connectathon in TOOP enables test validation in a controlled and neutral environment; this means that both data providers (called TOOP data providers) and data consumers (called TOOP data consumers) work together on their respective service endpoints in order to establish functional connectivity, but also compatibility with formats and to ensure data attributes and semantics. The Connectathon [34] encourages the partner countries to work closely together to solve the technical problems.

regard it is important to provide a standardised model of documentation of the pilot result for the documentation [35][35]. Hence, a measuring system is necessary to determine the success of each connectivity trials within the former trials. Therefore, TOOP project has developed a threefold division in the result classification: [1] passed, [2] partly passed and [3] failed. All trials between the Member States participants' where graded following this system and also commented with qualified information, which resulted in a traceable and comparable result documentation, as depicted as an example in the figure below.

9.5.11 Recommendation on TOOP re-use capabilities

TOOP has pronounced and established a huge work planning, which was differently wide and deep realised in the project. For example, exhibits the core infrastructure components a significant deep maturity level, which derived from the yet existing base components such as eDelivery building block and the long-lasting experience in the 4 corner model deriving from PEPPOL and openPEPPOL. On the other hand, some components, such as the semantic models and regarding components exhibit a lower maturity level, but exist at least in concepts. Nonetheless, the existing release of the infrastructure and components shows a paved way, overall when it comes to EDM and CERB components.

Core infrastructure elements have been developed and are widely used in the pilots, very narrow shaped along the introduced pilot areas. The use of the infrastructure and the components in the pilots, as described above in chapter 9.5.10, have shown significant progress and improvements within the piloting sessions (Connectathon sessions) and have shown the procedural abilities of the infrastructure as such.

Due to the fact that TOOP infrastructure and components are still under progress it is hard to say how they will perform in a final level, but the concepts follow a well-defined and applicable method, which widely follows the needs of European infrastructures. This kind of infrastructure must show the capability and ability handle with non-functional requirements, such as subsidiarity, openness and re-usage or actuality. Thus, very specific challenges come along, which are more in the field of agreements as on technical requirements. This mirrors the challenges in TOOP. Some system elements/parts are more flexible if implemented as others, but at least follow these important non-functional requirements. One point to highlight in this sense is the method of finding the actors involved and their real addressing, which means the very particular part of "Dynamic Discovery". As a citation: "*The CEF eDelivery Service Metadata Locator (SML) enables Access Points to dynamically discover the location of the destination Access Point. Instead of looking at a static list of IP addresses, the Access Point consults a Service Metadata Publisher (SMP) where information about every participant in the document/ data exchange network is kept up to date, including the IP addresses of their Access Point.*" [40] As an explanation: When looking in the field of the public sectors throughout Europe it is obvious to see that it remains a high dynamic in organisational changes and responsibilities. Thus, results in the need of higher administrative burdens at all, overall, when extrapolated in the European level. Finally, this could result in a challenge of keeping up-to-date all the actors data and their [1] actual and [2] correct addressing. The concept of Dynamic Discovery follows this non-technical requirement with the distribution of the partner management (within the system) - which is located rather centrally - and the addressing of the actor involved – which is located at the actors side and responsibility. Conclusively, this partly distributed approach brings the partner management and the addressing management (locator) in a sustaining system. As another example the 4-Corner-Model of the DC-DP-communication via gateways takes the same line.

10 Conclusions

The Project Start Architecture set out to define a starting point for the three DE4A pilot projects and for WP3 - Semantic Interoperability Solutions and WP5 – Common Components Design & Development, also providing guidance on the 22 interdisciplinary questions listed in 2.32.3. The Reference Interaction Patterns (chapter 44) provide a top-down analysis of cross-border evidence exchange in 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, however, have yet to develop into a full consensus of the DE4A Member States. Continued internal and external validation is required based on the first complete version of this document, not the least in light of further insights during the refinement of features in the technical work packages (WP3 Semantic Interoperability Solutions, WP4 Cross-border Pilots for Citizen and Business and WP5 Common Component Design and Development).

An Architecture Log is initialized per Pilot (see sections 6.2 for the Studying Abroad Pilot, 7.2 for Doing Business Abroad and 8.6 for the Moving Abroad Pilot) to document detailed implications and exceptions classified along the DE4A derived principles (see D2.1 Architecture Framework)). This Architecture log will serve as input for lessons learned and as basis for the update of the PSA to Deliverable D2.5 for the second pilot iteration. The pilot specific chapters also include a first, indicative mapping from Application Services to Building Blocks (BB), based on the quick scan assessment of these BB in chapter 9 and the preliminary mapping of chosen interaction pattern per pilot use-case. Some of the guidance on the interdisciplinary question is provided on the level of the pilots, especially where these questions are domain/sector specific.

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

- 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 and User-supported Intermediation (USI) pattern and to the user themself in the Verifiable Credential pattern. In the first two cases, this means that we attempt to correlate the request of the DC and the response of the DP in context of the DC.
- Multiple, complementary, overlapping or conflicting evidence equivalents are complex cases that are essentially covered by all reference interaction patterns included in the current version of the PSA. Whether such cases are actually in scope of our specific combination of pilot use-cases and participating MS requires further analysis. This need is recognized in the Technical Working Group and is beyond the scope of this document.
- 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 deferred responses 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 digitised, then the complete OOP sequence must be repeated, starting with a new OOP request.

- **Explicit request and transitivity between actors** is a controversial issue and one of the main reason for supporting both the Intermediation and the USI pattern. The Intermediation pattern follows the interpretation that SDGR 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.
- **Preview & Approval** UI is integrated differently in all three patterns: The Intermediation pattern assumes that the preview can be prepared by the DC after the evidence was technically 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. 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.
- **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 actually 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. A perfect match is not possible, but MS experience shows that a reasonably high percentage of users can be matched in this way. The USI and VC pattern include a direct interaction between User and DP, hence can request additional information to improve the matching and reduce the likelihood of false positives.
- **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.
- A **Hand-on of UI 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) mean 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.
- **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.
- 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.
- 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.
- **Automated re-use of data**, meaning fully automated parsing of data contained in exchanged evidences 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. 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.

- 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, organisational 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.
- **EESSI integration** in the MA pilot is still under investigation.
- First investigations showed that a **BRIS integration** is very unlikely in terms of full or partial reuse of the BRIS system. 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
- 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 reasons is that EU citizen living and working in another MS than their country of origin is the user group that might profit the most of the existence of a Once-Only Technical System on European level and often hold eIDs of their host country (population-wise, this user-group amounts to a 28th MS).
- 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 will 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 is under discussion.
- 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, where a memorandum of understanding to this effect appears to be one of the likely alternatives.
- 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 end-points. The Intermediation pattern additionally assumes that an authority check would be needed: a control that the requesting authority has a valid reason to request a specific evidence type. This still needs further investigation and alignment with the CEF Preparatory action. If a true circle of trust could be established across all participating, competent authorities, such an authority check could be obsolete and could be replaced by a simple check against a list of trusted authorities.
- **Legal validity or SSI and block chain technology**: The diploma recognition use case, adopting the VC pattern, is uncertain to reach in production level, because of legal limitations to the use of block chain technology (i.e. in Spain), dependency on EBSI-ESSIF infrastructure and services being ready and the lack of legal validity of Decentral Identifiers (DIDs). DE4A hopes that the

latter limitation might be relaxed through the work of ESSIF and EBSI in time for the second pilot iteration.

- The close relation between DE4A and the efforts of implementing the OOTS in context of the SDGR [3] 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.
- Another ongoing discussion concerns **Matching evidences between MS,** establishing an equivalence between what one MS requests for an eProcedure and what another MS can provide as evidence. Presently there are two, potentially complementary approaches under investigation in the context of the Semantic Framework of WP3: Criterium based (cf. CCCEV) and canonical evidence bases.

The results of the BB assessment (chapter 9) show that there is a mature and acceptable stock of solution building blocks (SBBs) that can be considered for implementation by the pilots, either in their entirety or partially, with the needed upgrades. The Pilots' analysis of SBBs clearly indicates the potential for (re)use of exisiting and emerging BBs on European level, e.g. eIDAS, the SEMPER[8] extension to eIDAS, eDelivery (and subcomponents, like AS4 gateway, SMP and SML), eSignature and TOOP[9] components.

The Pilot's analysis also shows the foreseen usage of DCs eProcedure Portals, DP data services and the need for GUI standards and shared components for evidence preview and explicit request.

The PSA is an important input into the Pilot planning exercise that will culminate in the deliverables D4.2, D4.6 and D4.10 of the Studying Abroad, Doing Business Abroad and Moving Abroad Pilots respectively. 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 all through both pilot iterations. The PSA-team is expected to continue operation in order to provide ongoing guidance to the pilots.

The reference architecture (chapters 3 and 4) and especially the identified Application Service, Application Components and Interfaces are the basis for creating the backlogs for WP3 Semantic Interoperability Solutions and WP5 Common Component Design & Development, e.g. D5.1 First inventory of features for products/components.

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) that will result in D2.7 - Optimal Interoperability Architecture for cross-border procedures and evidence exchange in light of the Singe Digital Gateway Regulation.

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

- Already commenced consolidation of Application Services (with a focus on identified gaps) into a portfolio backlog of WP5 (i.e. D5.1) and the wider Technical Working Group (WP3, WP4 and WP5)
- Project-wide walkthroughs of the reference interaction patterns to maximize the value of the architecture analysis for the overall project (walkthrough of the intermediation pattern was provided internally and to the CEF Preparatory Action already during the process of compiling the document).

[8] SEMPER is still in its piloting phase making a final assessment impossible.

[9] TOOP being again extended until January 2020 making it impossible to assess their final results yet.

- Align the required Application Components and Application Interfaces of the chosen interaction pattern with the deployment and configuration backlog of WP4 pilots and summarize the result in the pilot planning deliverables.
- Use models of the reference architecture and derived models as context for feature refinement sessions in the technical work packages WP3, 4 and 5
- Extension of the PSA with Subscription and Notification and Lookup pattern specifically relevant for the DBA pilot (publication of the extended PSA expected early 2021).

References

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

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

[3] SDGR - 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

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

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

[6] DE4A Deliverable D2.1 Architecture Framework, submitted 01.04.2020

[7] DE4A D4.1 Studying Abroad use cases definition v1.0

[8] DE4A D4.5 Business Abroad Use Case Definition and Requirements v1.0_Final

[9] DE4A D4.9 Moving Abroad use cases definition v1.0

[10] DE4A , WP3 team - DE4A WP3, D3.1: Initial set of requirements,
https://newrepository.atosresearch.eu/index.php/f/409102

[11] D04.01 – Final Report: Study on Data Mapping for the cross border application of the Once-Only technical system SDG, Deloitte, 28/02/2020, Ref. Ares(2020)1876945 - 01/04/2020

[12] CAMMS https://ec.europa.eu/isa2/solutions/camss_en

[13] ISA^2 Interim Evaluation https://ec.europa.eu/isa2/sites/isa/files/190613_synopsis_report.pdf

[14] EAAF
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/fea_docs/OMB_EA_Assessment_Framework_v3_1_June_2009.pdf

[15] Study on "The feasibility and scenarios for the long-term sustainability of the Large Scale Pilots"
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2577

[16] 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)

[17] CEF-ISA BB assessment: eDelivery, eSignature, eID, CCCEV & CPSV-AP Version 0.2

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

[19] Business Register Interconnection System (BRIS)
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2017/09/19/Business+Register+Interconnection+System

[20] EESSI https://ec.europa.eu/social/main.jsp?catId=869&langId=en

[21] EBSI https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

[22] ROV https://www.w3.org/TR/vocab-regorg/

[23] http://toop.eu/sites/default/files/D23_Generic_Federated_OOP_Architecture_3rd_version.pdf

[24] http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html, http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/os/bdx-smp-v1.0-os.html

[25] An OASIS BDXR TC standard; see https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+software for further guidance

[26] According to the OASIS BDXR TC BDXL standard; see https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+service for further guidance

[27] Another OASIS standard based on ebXML Messaging 3.0; see https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+software for further guidance

[28] eDelivery AS4 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.14

[29] KAFKA https://kafka.apache.org/

[30] eDelivery DOC https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Documentation+eDelivery

[31] Four Corner Topology https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.14#eDeliveryAS4-1.14-FourCornerTopology

[32] TOOP simulator https://github.com/TOOP4EU/toop-simulator/

[33] Piswanger, C.-M., & Zehetner, C. (2019) A Shortcut on “The Once Only Principle Project". Jusletter IT 21. Februar 2019 - https://jusletter-it.weblaw.ch/issues/2019/IRIS/a-shortcut-on---the-_d0b9171939.html__ONCE&login=false (IRIS Conference)

[34] IHE Europe (2017) Whitepaper on Connectathon

[35] Lampoltshammer, T., & John, K., & Helger, P., & Piswanger, C.-M. (2019) Connectathons - A Sustainable Path Towards Development in European Large-Scale Pilots. Proceedings of Ongoing Research, Practitioners, Posters, Workshops, and Projects of the International Conference EGOV-CeDEM-ePart 2019, 207-214

[36] SMP http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/os/bdx-smp-v1.0-os.html

[37] OpenPEPPOL https://peppol.eu/about-openpeppol/history-of-openpeppol/

[38] TOOP SA http://wiki.ds.unipi.gr/display/TOOPSA20

[39] eCERTIS https://ec.europa.eu/tools/ecertis/#/about

[40] eCERTIS API https://ec.europa.eu/tools/ecertis/assets/ECERTIS_REST_API.pdf

[41] eDelivery https://ec.europa.eu/inea/sites/inea/files/2018-2_faq_edelivery_starterset_final.pdf

[42] Regulation (EU) 2016/1191 of the European Parliament and of the Council of 6 July 2016 on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the European Union and amending Regulation (EU) No 1024/2012 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R1191

Appendix

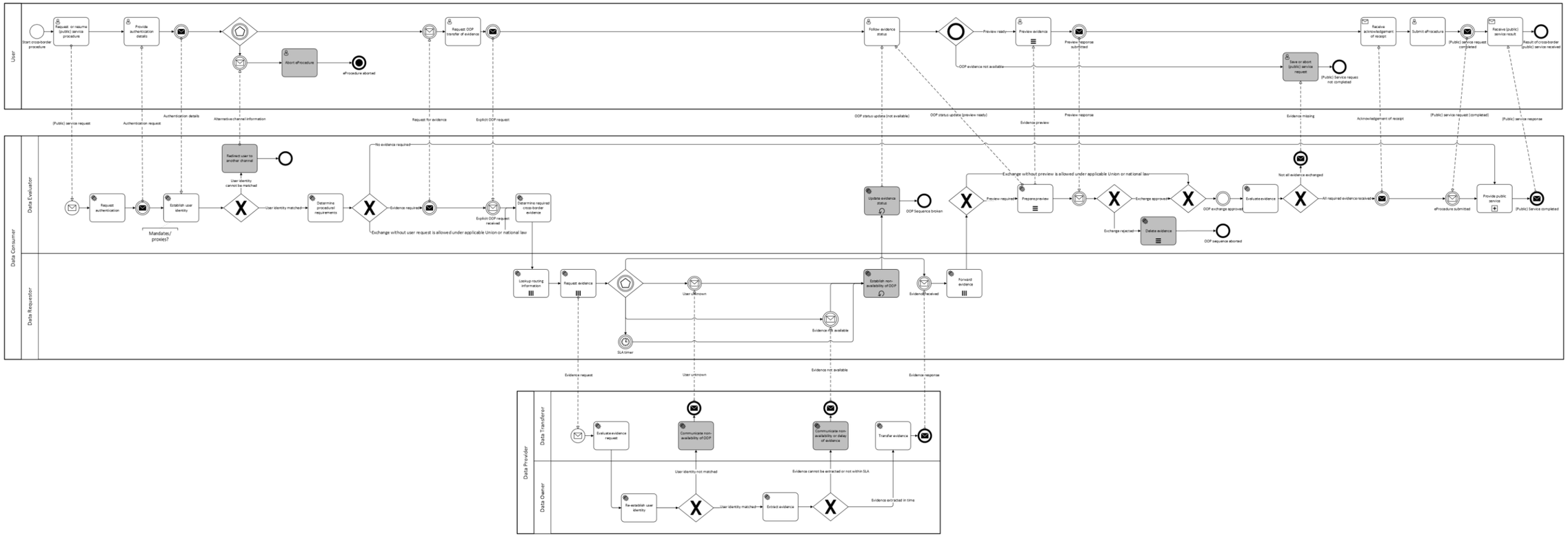


Figure 49 Intermediation pattern

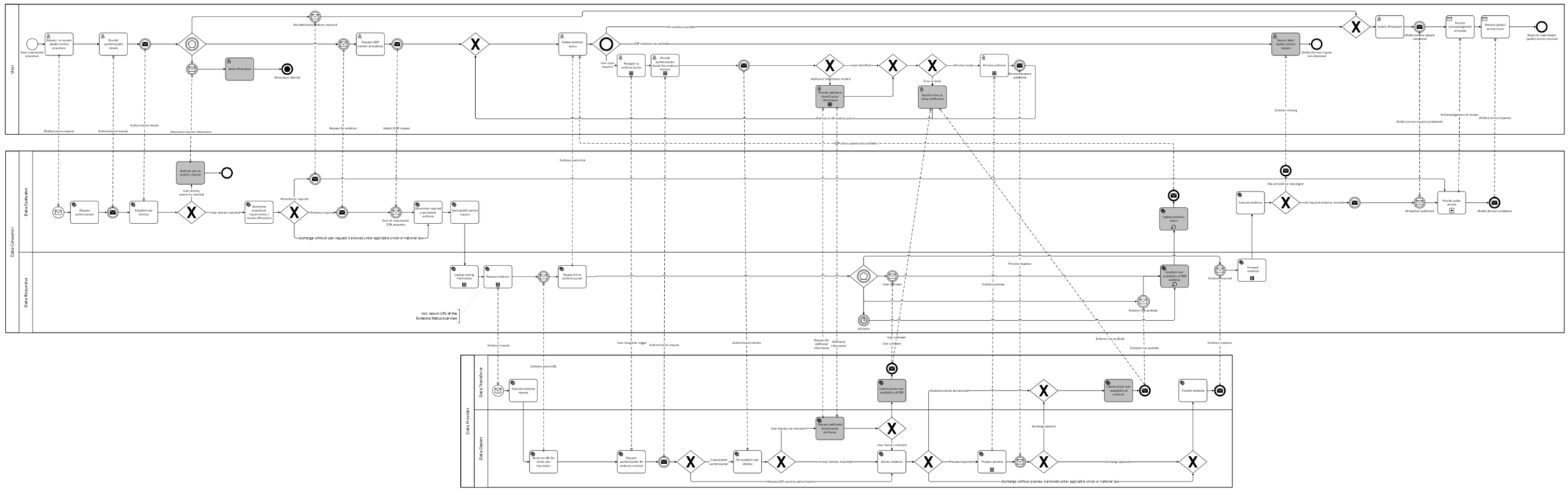


Figure 50 User supported intermediation pattern

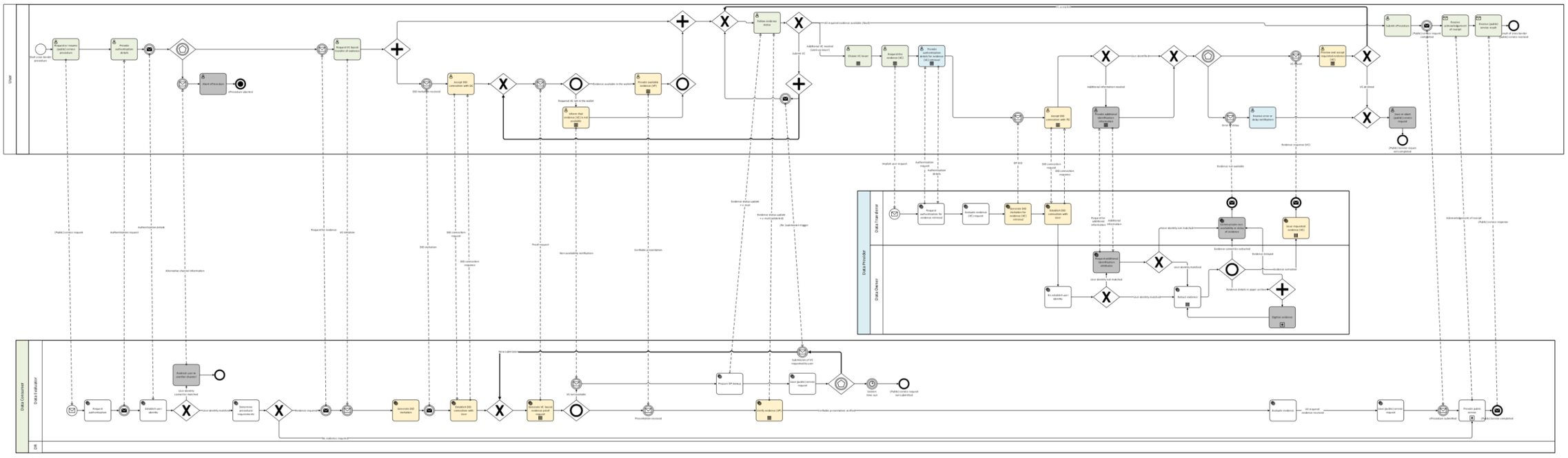


Figure 51 Verifiable Credential Pattern