D2.3 Final DE4A Trust Management Models and Self-Sovereign Identity Supporting Framework Design

Document Identification			
Status	Final	**Due Date**	30/11/2021
Version	1.3	**Submission Date**	24/06/2022

Related WP	WP2, WP5	**Document Reference**	D2.3
Related Deliverable(s)	D2.1, D2.2, D5.7	**Dissemination Level (*)**	PU
Lead Participant	ATOS	**Lead Author**	Javier Presa (ATOS)
Contributors	Alberto Crespo (ATOS), Alexander Bielowski, Harold Metselaar (MinBZK/ICTU); Tomaž Klobucar (JSI); Carl-Markus Piswanger (BMDW); Ana Rosa Guzmán (SGAD); Francisco J. Aragó (UJI); Damjan Bojović (SI-MPA); Muhamed Turkanović (UM); Arvid Welin (SU);	**Reviewers**	Gérard Soisson (CTIE) Dennis Reumer (RVO) Ivar Vennekens (RVO)

Keywords :
Trust, challenges, blockchain, patterns, eDelivery

Document Information

List of Contributors	
Name	Partner
Alberto Crespo	ATOS
Alexander Bielowski	MINBZK /ICTU
Ana Rosa Guzmán Carbonell	SGAD
Arvid Welin	SU
Carl-Markus Piswanger	BMDW
Damjan Bojović	SI-MPA
Francisco José Aragó	UJI
Harold Metselaar	MINBZK /ICTU
Muhamed Turkanović	UM
Sofía Paredes	AMA IP
Tomaž Klobučar	JSI

Version	Date	Change editors	Changes
0.1	25/05/2021	Javier Presa (ATOS)	Initial version of document
0.2	04/06/2021	Javier Presa (ATOS)	ToC discussed with contributors
0.3	09/09/2021	Javier Presa (ATOS)	Added guidelines
0.4	09/09/2021	Muhamed Turkanović (UM)	Sections 4.2
0.5	20/09/2021	Javier Presa (ATOS)	Section 4.1
0.6	28/09/2021	Alexander Bielowski, Harold Metselaar (MinBZK/ICTU)	First draft of section 2.1.1
0.7	05/10/2021	Tomaž Klobucar (JSI); Carl-Markus Piswanger (BMDW)	Section 2.1.2 and 2.1.3 Section 2.2
0.8	22/10/2021	Ana Rosa Guzmán (SGAD); Francisco J. Aragó (UJI); Alexander Bielowski, Harold Metselaar (MinBZK/ICTU	Section 3 Section 2.14 Section 2.1.5
0.9	08/11/2021	Javier Presa (ATOS)	Chapter 1
0.10	15/11/2021	Alberto Crespo (ATOS); Ana Rosa Guzmán (SGAD)	Review Section 3
0.11	17/11/2021	Damjan Bojović (SI-MPA)	Section 2.1
0.12	18/11/2021	Sofia Paredes (AMA)	Section 2.3
0.13	07/12/2021	Arvid Welin (SU)	Contribution to conclusions section
0.14	07/12/2021	Gérard Soisson (CTIE); Dennis Reumer, Ivar Vennekens (RVO)	Internal review
0.15-19	08/12/2021	Javier Presa (ATOS)	Update after internal review
0.2	10/12/2021	Julia Wells (Atos)	QA
1.0	15/12/2021	Ana Piñuela (Atos)	QA, Final version for submission

List of Contributors			
1.1	06/06/2022	Javier Presa (ATOS) Muhamed Turkanović (UM)	Updated "Introduction" and section 4 considering recommendations from period 2 review report
1.2	13/06/2022	Javier Presa, Alberto Crespo (ATOS)	Update after internal review
1.21	23/06/2022	Julia Wells (ATOS)	Revision for submission
1.3	24/06/2022	Ana Piñuela Marcos (ATOS)	Final for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Javier Presa (ATOS)	09/12/2021 and 13/06/2022
Quality manager	Julia Wells (ATOS)	10/12/2021 and 23/06/2022
Project Coordinator	Ana Piñuela Marcos (ATOS)	15/12/2021 and 24/06/2022

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AP	Access Point
API	Application Programming Interface
CA	Competent Authority
(C/B)2G	Consumer/Business-to-Government
(C/B2)G2G	Consumer/Business-to-Government-to-Government
DC	Data Consumer
DE	Data Evaluator
DID	Decentralized IDentifier
DO	Data Owner
DP	Data Provider
DR	Data Requestor
DT	Data Transferor
Dx.y	Deliverable number y, belonging to WP number x
EBP	European Blockchain Partnership
EBSI	European Blockchain Services Infrastructure
EDCI	European Digital Credential Infrastructure
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
ESSIF	European Self-Sovereign Identity Framework
GDPR	General Data Protection Regulation
LSP	Large Scale Pilot
MS	Member State
QR (code)	Quick Response code
OOP	Once-Only Principle
OOP TS	Once-Only technical system for evidence exchange in the DE4A project
PSA	Project Start Architecture
SDGR	Single Digital Gateway Regulation
S&N	Subscription and Notification
SSI	Self-Sovereign Identity
TIR	Trusted Issuer Registry
TLS	Transport Layer Security
TSR	Trusted Schema Registry
VC	Verifiable Credential
WP	Work Package

Executive Summary

This deliverable is the final version of the design of the DE4A Trust Management Models and Self-Sovereign Identity Supporting framework produced in the context of Task 2.2 “Trust Management Models” in “WP2 Architecture vision and framework”.

The present document has addressed multiple aspects related with the establishment and maintenance of trust needed in relation to the five different evidence exchange patterns (intermediation, user support intermediation, verifiable credential, lookup, subscription & notification) defined and being implemented in DE4A in the context of the Single Digital Gateway and Once-Only Principle.

The deliverable describes the implementation of the trust models in the DE4A project from the perspective of each of the patterns applied in the respective pilots and use cases. After the detailed analysis of the different alternatives on trust management methods to be applied on the different scenarios included in the previous deliverable “D2.2 Initial DE4A Trust Management Models and Blockchain Support” [1], D2.3 explains how the mechanisms and functionalities of the CEF eDelivery Building Block are used over the well-known four-corner model adopted by DE4A infrastructure. A brief overview of the five patterns described in the “D2.5 Project Start Architecture (PSA) 2nd iteration” [6] that are being adopted by the participants of the pilots is also included as a quick reference to the high-level details of each pattern.

This definition of the valid trust solutions framework includes the approach of powers of representation and mandates, to be piloted in the related Doing Business Abroad use cases, being the SEMPER project the base of the implementation. SEMPER project provides coherent definition of powers and e-mandates in alignment with and proposing extensions to the eIDAS Interoperability Framework, enhancing the scope of powers or representation and mandates beyond cross-borders.

CEF eDelivery Building Block, used by all the DE4A patterns except Verifiable Credentials, provides technical specifications and standards to secure the interaction between different actors through a network of nodes for protected evidence exchange. Each of the eDelivery components are configured to work with a client PKI certificate, that ensures the integrity and confidentiality of exchanged data payloads. The process to be followed by each pilot participant is also described, following the process described on the “CEF eDelivery PKI Service Offering” document produced by DIGIT [12].

The deliverable also provides a comparison regarding the trust factor between the three patterns that have been implemented in most of the pilot use cases (Intermediation, User-supported Intermediation and Verifiable Credentials). A conclusion that results from this exercise is that there is no better or worse pattern in general, but all have specific considerations and points to be taken care of for their trustworthy deployment and operation . Also, the selection of a pattern depends on the careful consideration of other factors besides trust, e.g. the level of legal harmonisation, the mutual recognition of stakeholders, the interoperability agreements and barriers, the sensitivity of information to exchange, the security of the networks, etc.

The last part of the document describes how the DE4A Self-Sovereign Identity Supporting Framework has been updated since the previous deliverable and also the use of European standards and frameworks with which DE4A integrates the framework (EBSI-ESSIF) and the issues that arise from this. This is a valuable input for future adopters as it provides concrete details from a technical perspective of how this Self-Sovereign Identity Supporting Framework also acts as a trust solution to realize the Verifiable Credentials pattern.

1 Introduction

1.1 Purpose of the document

The present document is the second and final deliverable produced by "Task 2.2 Trust Management Models" in the context of "WP2 Architecture vision and framework" and describes the improvements of the DE4A multi-faceted trust management model which in turn builds upon a rich and solid foundation of underlying trust models (e.g. from existing CEF Building Blocks and DSIs like eIDAS and eDelivery as well as new paradigms like Self-Sovereign Identity) and was already described in deliverable D2.2 "Initial DE4A Trust Management Models and Blockchain Support Framework" [1].

It is worthwhile to mention that DE4A does not implement a blockchain infrastructure of its own but a Self-Sovereign Identity solution that is piloted in the Diplomas recognition use case of the Studying Abroad pilot and which is integrated with EBSI through the use of ESSIF v2.0 APIs. EBSI provides the highly trustworthy underlying blockchain infrastructure that is specifically adequate for DE4A as a Large-Scale Pilot in the context of cross-border services for the public sector and the participation of DE4A in the EBSI Early Adopters programme (aimed at similar projects with participation of Member States that also belong to the European Blockchain Partnership) will help to achieve the integration with it.

D2.3 also explains how the integration of different trust-supporting mechanisms and anchors is being performed for already trusted services managed by competent authorities both requesting and providing evidences about users, building on the guidelines resulting from the in depth study conducted in the previous deliverable D2.2 [1] with the DE4A MS and their available infrastructures and Government Agencies.

1.2 Structure of the document

This document is divided into the following sections:

- Section 2 "DE4A pilots trust models" reports how the trust models are implemented in the different DE4A patterns used in the pilots.
- Section 3 "Evidence exchange comparing traditional and emerging patterns: challenges and technical anchors" provides a broad comparative analysis on common trust challenges across the three main evidence exchange patterns used in DE4A from the trust factor perspective.
- Section 4 "Self-Sovereign Identity supporting Framework design" describes the final implementation of the interoperable Self-Sovereign supporting solution used in the Verifiable Credential use case of the Studying abroad pilot and the integration performed with EBSI/ESSIF infrastructure.
- Section 5 "Conclusions" outlines the main findings in the deliverable.

2 DE4A Pilots Trust models

After the extensive study and analysis of the existing trust models in D2.2 "Initial DE4A Trust Management Models and Blockchain Support Design" [1], the following section describes the trust solutions framework that is adopted for validation in the pilots of the DE4A project from the perspective of the respective patterns used in their use cases. After an introductory overview highlighting key relevant aspects of the five patterns defined by DE4A for evidence exchange, each of them is addressed in turn providing detailed analysis from organisational (including trust requirements) and technical (including components and trust anchors) perspectives.

2.1 DE4A Patterns

This section aims to highlight in a high manner the important aspects of each pattern designed for evidence exchange in DE4A, as a reference to understand the subsequent sections related to trust models. Further details about the patterns can be found in chapter 3 of D2.5 "Project Start Architectures (PSA), second iteration"[6].

The intermediation pattern (IM) supports a direct interaction flow among different entities in the process: user, Data Consumer (Data Evaluator and Data Requestor) on one side and communication with Data Provider (Data Owner and Data Transferor) on the other side. All cross-border communication is organized around a secure network system of eDelivery Access Points (AP) which handle the secure exchange of Evidence Requests and Evidence Response and which act as trusted proxies in each MS also serving as abstraction elements for the trust management following a 4-corner model and (from the perspective of specific certificates issued from CEF PKI Service to DE4A domain) a shared domain PKI trust model (as the issuing CA issues certificates for other domains, although the certificates issued to DE4A will not be shareable with domains outside DE4A).

This secure communication system represents the general approach to the trust in DE4A pilots with the establishment of an explicit Circle-of-Trust among participants in the domain, which is a well-known concept in federated cross-border networks, with eIDAS being a prominent example. As much this is implemented over X.509 PKI certificates (whereby receivers of AS4 messages can validate the certificate's trust by traversing the certificate path to a trusted certificate authority), this concept can be a valid and scalable approach to manage trust between stakeholders interacting through the Once-Only Technical System (OOTS) in the context of Single Digital Gateway Regulation (SDGR).

A prerequisite for Circle-Of-Trust is a trusted and secure communication channel which is built from technical solutions (based on the Once-Only Principle) from each MS and also from dedicated eDelivery AP network with the use of CEF PKI infrastructure (see more details in section 2.1.1.1 below). Each Member State is also responsible for establishing a secure and trusted system inside the Data Consumer entity (between Data Evaluator and Data Requestor) on one side and Data Provider (between Data Owner and Data Transferor).

Access to this secure network at the cross-border level is allowed only to competent authorities and an adequate vetting process (onboarding conditions) should be considered as part of the Governance framework.

User-supported Intermediation pattern (USI) is similar to Intermediation Pattern. In this pattern, the process has similar actors and security and trust assurances (Circle-of-Trust mentioned above) but user, Data Consumer (Data Evaluator and Data Requestor) on one side and with Data Provider (Data Owner and Data Transferor) on the other side interact in a different manner. Key differences touch on processes like identity matching (the user authenticates at the data provider), record matching (direct interactions with user are possible in case of not direct match) and the Preview (user verifies the evidence at the Data Provider side instead of doing so at the Data Consumer).

All cross-border communication is again organized around secure network system of eDelivery Access Points (AP) which handle the secure exchange of Evidence Requests and Evidence Responses.

Verifiable Credential pattern (VC) leverages the concept of Decentralized Identifiers (DID)[2] in combination with User (eIDAS) eIDs. These DIDs are used for setting direct, i.e. DID communication between entities and associated DID documents hold relevant entity pieces of information about entities to which DIDs are issued, such as associated cryptographic keys, endpoints, etc. that can be used to authenticate them. The data presented in the form of a set of claims about the user, namely Verifiable Credential, is issued by a competent Data Owner (issuer) authority towards the User (which is previously authenticated with their eIDAS eID) and stored in a personal wallet. It is presented in a separate communication to the Data Evaluator (verifier) that cryptographically verifies the authenticity of the data using the Issuer DID that is previously registered on a blockchain registry (i.e. EBSI's Trusted Issuer Registry).

An Edge agent (DE4A mobile wallet) includes the evidence Preview functionality and all secure interchanges are managed (i.e. Initiate DID connection, Accept DID connection, Accept Verifiable Credential, Present Verifiable Credential). Moreover, the managing of DID connections, VC issuing and verifying operated by DPs and DCs is handled through a dedicated cloud agent (Authority Agent) which includes an EBSI Connector which facilitates integration towards EBSI and ESSIF frameworks.

Lookup pattern in general means simple Request – Response interaction between Data Consumer part of the process and Data Provider part as they know each other upfront, without any User involvement (it applies only in cases where the exchange has a legal basis and can be executed without explicit request or consent from the User). It is meant to be more lightweight than Intermediation pattern and enable Near Real Time use of information for repetitive interactions over time. This pattern is used in the second iteration of DE4A Doing Business Abroad pilot.

Trust is organized around secure network system of eDelivery Access Points (AP) which handles secure exchange like in previous patterns. The pilot also uses established A4S infrastructure and canonical message definitions.

This pattern is triggered directly by Data Consumer in terms of providing a public service. Because there is no user intervention, all trust models rely on Data Consumer procedures which the Data Provider needs to rely upon. Evidence and Attribute Lookup variants are considered as explained in section 3.5.1 of D2.5 [6].

Due to a lack of user requests and authentication, the trust challenges are addressed mainly in the Authorization Check procedure which should be included in the Lookup pattern implementation.

Subscription and Notification pattern (S&N) uses eDelivery Access Points (AP) and comprises two processes (an initial subscription that is triggered by Data Consumer, subsequent notifications triggered by a specific business event of the company which is registered in the Data Provider registry).

This pattern is using processes similar to the Intermediation pattern, meaning during the collection of requests from users, Data Evaluator is needed and User intervention is not needed as notifications are sent automatically.

Challenges that are involved in this pattern are linked with user consent, authorization, and organisational trust measures (audits). Moreover, an implicit trust exists on Data Providers by subscribed Data Consumer to receive Notification upon information updates.

The following table depicts the use cases of the pilots where the evidence exchange patterns described above are used:

Table 1: Evidence exchange patterns in Pilots' Use Cases

	Studying abroad pilot			Doing business abroad pilot		Moving abroad pilot		
PATTERNS	UC1: Application to public higher education	UC2: applying for study grant	UC3: diploma/certs/studies/professional recognition	UC1: starting a business in another MS	UC2: Doing business in another MS	UC1: request change address	UC2: request an extract of a civil state certificate	UC3: request pension information
Intermediation (IM)				✓				✓
User supported Intermediation (USI)	✓	✓				✓	✓	
Verifiable Credential (VC)			✓					
Subscription & Notification (S&N)				✓	✓			
Lookup					✓			

The following subsections provide the organisational and technical description of the model for each pattern.

2.1.1 Intermediation pattern

2.1.1.1 Organisational description of the model

What is specific to the Intermediation pattern is that the user, i.e. company in the case of the DE4A Doing Business Abroad (DBA) pilot, exclusively interacts with the Data Consumer (DC), more specifically the Data Evaluator (DE) as explained in the PSA [6]. The cross-border Data Exchange in DE4A is provided by a network of eDelivery[3] Access Points (AP) that handles the secure exchange of Evidence Request and Evidence Response. Irrespective of the Member State (MS) specific assignment of the four roles (Data Evaluator (DE) and Data Requestor (DR) on the Data Consumer (DC) side of the exchange and Data Owner (DO) and Data Transferor (DT) on the Data Provider (DP) side of the exchange) to Competent Authorities, the general approach to trust in the DE4A pilots is the establishment of a Circle of Trust between domain participants. DE4A has verified alignment of this pattern with the current proposal for a Once-Only Technical System (OOTS) in context of the Single Digital Gateway Regulation (SDGR) [4] and the Circle-of-Trust concept follows the same logic as Pan-European Public Procurement Online (PEPPOL) [5]. This section discusses the extension of this trust between participating organisations and how part of this trust is delegated to a closed eDelivery network.

A prerequisite of establishing a circle of trust is a trusted, secure communication channel between the participants. The end-to-end communication can be split in three legs (following the eDelivery 4-corner model; Numbered below for the Evidence Request, the Evidence Response would be the exact mirror image):

1. From the DE to the AP (i.e., corner 1 to corner 2)
2. From AP to AP (i.e., corner 2 to corner 3)
3. From AP to DO (i.e., corner 3 to corner 4)

The first and third leg is in the responsibility of each Member State (MS), building on existing, national OOP solutions and using national certificates and trust anchors. The participants trust all MS, their competent authorities and data intermediaries (if applicable) that their national OOP infrastructure is secure. Please refer to chapter 2 of D2.2 [1] for trust model studies of all DE4A MS.

The second leg is covered by a dedicated eDelivery network, using the CEF PKI as technical multi-domain trust anchor (see 2.3. for technical details). Essentially the access to that network projects the Circle of Trust onto the technical level. Only competent authorities allowed to request or provide evidence via the system are connected via the DE4A connector to the eDelivery AP. The participants trust all MS that their AP is correctly set up and only the right competent authorities are connected. Please note that this approach results in an "encryption gap", as explained section 2.3.10 of the PSA [6], which assumes a high level of trust in the organisations running the AP and Connector.

The specificities and especially the legal basis of the use of the system, i.e. Article 14 of the SDGR [4] and GDPR add to the extent of trust that is required between participants. These trust requirements do not have a specific representation on the technology layer and are procedural agreements on lawful behaviour. In essence one MS is meant to trust the competent authorities of another MS to act in a lawful way:

1. The Cross-border exchange is tied to an explicit request of the user (Article 14.4 SDGR[4])[1]. The DP trusts the DC that Evidence Requests are only sent, based on the explicit request of the user (or exceptions based on national or Union law). Note that the user may be representing a legal person.
2. The Cross-border exchange is also tied to a user preview and approval[2]. In the case of the Intermediation pattern, this preview is provided by the DC. Consequently, the DP trust the DC to only use the evidence if approved by the user and for the purpose intended, hence that the DC handles the evidence in a lawful way. Note that the user may be representing a legal person.

In addition, there are several challenges concerning user authentication / identity matching, mandates and record matching that are related to trust. The DP needs to rely on the data provided by the DC, hence must trust the DC to have authenticated the user with an eIDAS eID[3] with the minimum assurance level required for the data provided. In the specific business-use case of DBA, this also includes that the natural person that was authenticated has the powers or mandate to represent for the company in question.

The existence of an EUID for companies, on the other hand alleviates the challenge of matching the request to a record in the business registry. In the citizen domain, the lack of an EUID adds the questions of the quality of the (additional) identification information provided by the DC to the DP and of what constitutes an 'unambiguous' match at the DP; these are not further discussed here as the DE4A pilots in the citizen domain use the User-Supported Intermediation (USI) pattern (see: 2.1.2).

Table 2 below provides an overview of what DC and DP need to be trusted with, for the Intermediation pattern to function as intended in the DE4A DBA pilot. This is very similar to the approach proposed for the OOTS, which relies as well on a circle of trust projected in a closed network.

[1] Note that some interaction patterns used in DE4A e.g. Subscription and Notification, do not require an explicit request of the user. Furthermore, exchanges could take place on other legal bases than Art. 14.

[2] User preview does not necessarily always exist, this depends on the legal basis and even Art. 14 foresees use cases where no preview would be needed.

[3] In DE4A some MS have non-notified eIDs which are accepted for piloting purposes.

Table 2 : Overview of Trust requirements in the Intermediation pattern

The DC is trusted with:	The DP is trusted with:
… maintaining a secure national OOP infrastructure (following applicable security standards in place in the DC Member State)	… maintaining a secure national OOP infrastructure (following applicable security standards in place in the DP Member State)
… setting up a secure eDelivery AP correctly	… setting up a secure eDelivery AP correctly
… providing access to sending Evidence Requests via the AP exclusively to competent authorities that have a legal basis to request evidence (i.e. pertaining to the procedures of Annex II of the SDGR[4] or other procedures covered by Art. 14 or enabled by other legal bases like GDPR)	… providing access to sending Evidence Responses via the AP exclusively to competent authorities lawfully issuing evidence
… the CA requesting only evidence if they have a legal basis to request such evidence	… the CA lawfully issuing the evidence
… the CA collecting the explicit request of the user before sending an Evidence Request	… the CA correctly matching the EUID to the record of the business register
…. the CA providing (when needed) a preview to the user and only using the evidence after approval	
… the CA deleting all received evidence if the user decides not to use the transferred evidence in the respective procedure	
… the CA deleting all received evidence if the Evidence is not anymore needed for the public service and after any (legally) applicable archiving period (related to GDPR obligations)	
… authenticating the user with the minimum assurance level required by the DP	

In a nutshell, the chosen trust model of the Intermediation pattern projects a complex set of trust requirements (Who can request which data for which purposes using which process?) on a closed network approach and the expectation of lawful behaviour on the side of European public authorities. This approach is reasonable for the DE4A pilot environment. It has, however, its limitations, especially if the solution is meant to grow to a wider interoperability platform also involving participants from the private and third sector. In that case, a specific Authorization Check would be needed, i.e. provided by the Information Desk as foreseen in the DE4A Reference Architecture [6]. Further research into this functionality is warranted, but beyond the DE4A pilot scope.

2.1.1.2 Technological description of the model

The following diagram provides an overview of the trust model for the Intermediation Pattern as used in the DBA pilot. The diagram represents one direction from corner 1 (far left) to corner 4 (far right) as indicated by the dashed line as described above (steps 1-3). In the other direction the flow is mirrored (corner 4 becomes corner 1, corner 3 becomes corner 2 etc.).

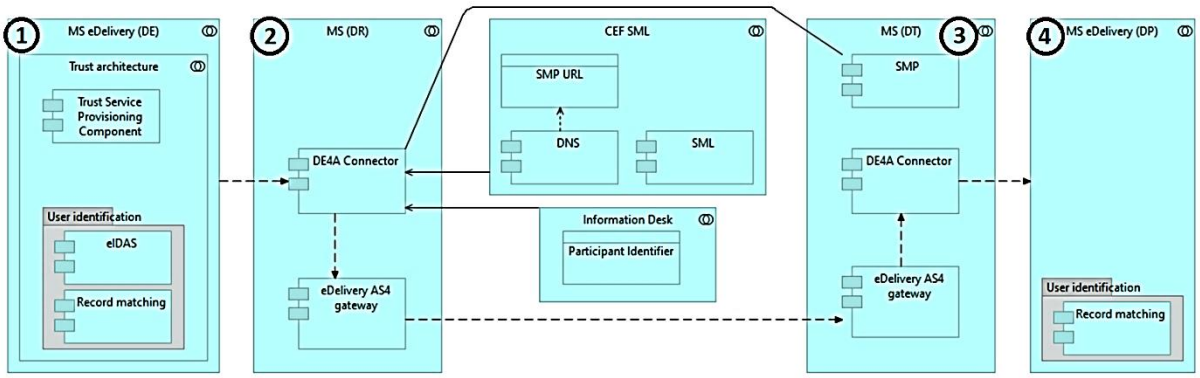

Figure 1: Trust Model Intermediation

2.1.1.2.1 Components of the trust model

The table below list the components that play a role in the trust model. Intermediation relies heavily on the eDelivery infrastructure which is elaborated in more detail in section 2.3.

Table 3 : Overview of Trust components in the Intermediation pattern

Component	Description
Trust Service Provisioning Component	Implements the functionalities encapsulating the trust services functionalities. A 'trust service' means an electronic service which consists of these functionalities: 1. the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or 2. the creation, verification and validation of certificates for website authentication; or 3. the preservation of electronic signatures, seals or certificates related to those services. This component is meant as a generic component and can be used wherever deemed useful. In case of Intermediation, the eDelivery infrastructure takes care of encryption/decryption and signing and signature verification. See also eDelivery AS4 gateway below.
eIDAS	The exact implementation might differ per MS, it supports identity matching. For DE4A in DBA pilot a component that represents a pilot eIDAS network including the SEMPER extension is meant.
Record Matching	Application component that provides matching (finding) of the right evidence based on attributes. Provided attributes are matched against attributes in some local registry.
DE4A Connector	Taking care of eDelivery and IDK interfacing, shielding DR and DT from complexities and facilitating ease of implementation. The connector also takes care of error handling and logging.
eDelivery AS4 gateway	This component – also referred to as AS4 gateway – handles the secure transfer of the data, including encryption and decryption as well as signing/sealing and validating signatures/seals.
DNS/SML	As there can be multiple SMPs, the sending party needs to know where to find the SMP of the receiver to get the actual metadata. This location can be found in the centrally CEF-hosted DNS, that will be queried by the access point of the sending Member State.

Component	Description
	DNS entries will be created from the registration of SMP's: the SML, which is also centrally hosted by CEF. See also SMP below.
Information Desk	The Information desk application collaboration combines multiple co-operating application components. It is used in conjunction with other infrastructural components in order in order to discover which competent data issuing authorities can provide evidence of a certain type for a given administrative procedure, to determine relevant characteristics of data services obtaining descriptive metadata about them and to use identifying information of data services in conjunction with other infrastructural components of the transport layer to obtain reliable routing information, i.e. participant ID.
SMP	For request/response message, information on the receivers Access Point (URL) and its certificates are needed. Each Member State hosts an SMP for this purpose. Before sending a request or response, the sending party queries the SMP of the receiver to get this info. In the scope of DE4A and for testing purposes ("playground") one single centrally hosted DE4A SMP is used.

2.1.1.2.2 Trust Anchors

In the context of Intermediation and usage of the eDelivery infrastructure and from a technical trust perspective, a trust anchor is assumed to be an authoritative entity for which trust is assumed and not derived (e.g. Certification Authorities issuing digital certificates for a given domain or sub-domain). Trust Anchors in Intermediation pattern are:

1. User identity providers. These are trusted third parties that issue identification means within notified eIDAS identification schemes or other national schemes for the Member States that have not yet notified their schemes (in case of DBA pilot Romania, Austria which is pre-notified, Sweden which is peer-reviewed).
2. Providers of TLS certificates (MS specific). Technically speaking a trusted third party from which the certificates are purchased.
3. CEF as provider of the required eDelivery certificates through CEF's PKI. Technically speaking the trusted third party that issues the root certificate for the hierarchy of certificates.
   Because of the encryption gap, the DR and DT need to be trusted as well although technically speaking the trust anchors are the eDelivery certificates deployed to them.
4. SMP as the reliable source of information about the infrastructure and endpoints.

See section 2.3 for more details with respect to certificate usage.

It is to be noted that from a more general perspective other dimensions of trust like legal trust (e.g. cross-border recognition and trust of notified eIDs including accountability), organisational trust (i.e. trust in organisational units responsible for hosting the national eDelivery Access point to properly configure, define and enforce national rules for public authorities that are connected), procedural trust (agreeing on a common governance and set of change and incident management procedures contributing to inter-MS trust). Such non-technical trust dimensions rely on other types of data anchors introduced in section 2.1 of D2.2 [1] .

2.1.2 User Supported Intermediation (USI) pattern

2.1.2.1 Organisational description of the model

In the User-supported intermediation pattern, a user interacts with the Data Evaluator (DE) and Data Owner (DO), as explained in the PSA [6]. Users are identified with their electronic identification means,

issued by Identity providers either within notified eIDAS identification schemes (for the Member States that have already notified their schemes) or other national schemes (e.g. qualified certificates for the Member States who have not yet notified their schemes).

DEs and DOs rely on Identity providers to properly validate users' identities according to the respective minimum assurance levels required (typically substantial and high for eGovernment cross-border services). On the other hand, users authenticate DEs and DOs through TLS certificates issued to the evidence consumers and providers (users interact with DE and DO using secured connections that they can easily verify e.g. browser lock icon). DEs and DOs can obtain TLS certificates at any trust service provider from Trusted List.

For the cross-border evidence exchange and similarly to Intermediation pattern, an eDelivery trust model is used, as presented in D2.2. The evidence requests and evidence responses are exchanged between the Data Consumer (DC), composed of DE and the Data Requestor (DR), and the Data Provider (DP), composed of DO and the Data Transferor (DT). DR and DT include eDelivery access points (AP) that represent corners C2 and C3 in the 4-corner model (encryption and signing are enforced in communication between such APs). DE has a role of corner C1 and DO of C4. This is summarised in the figure below:

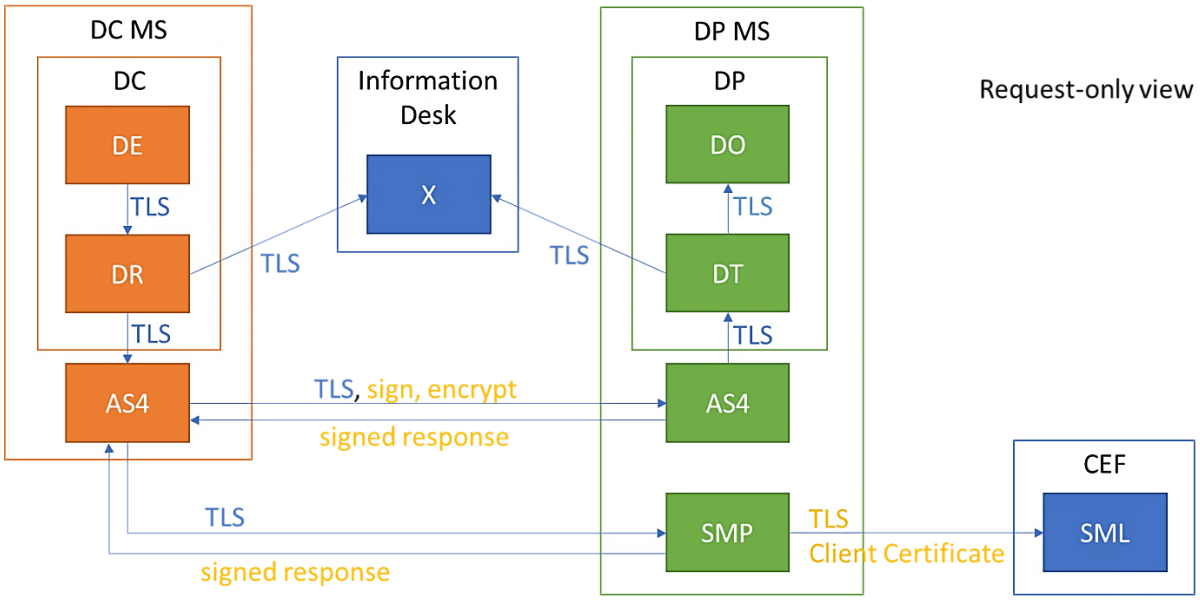

Figure 2: Certificate usage in DE4A

Similar to the Intermediation platform trust model description, the trusted communication between C1 and C2 and between C3 and C4 is responsibility of each Member State. The responsibility of each Member State is also trusted communication between DR and AS4 gateway and between DT an AS4 gateway, regardless of whether the gateways external to DR/DT are used or integrated in the DE4A Connector.

In the case of the SMP component, each SMP has a certificate from the same SMP root certificate (CEF PKI for testing and commercial PKI for production). The production CA for the SMP is aligned with the CEF requirements for use in the SML.

Only competent authorities allowed to request or provide evidence via the system are connected via the DE4A connector to the eDelivery AP. The participants trust all MS that their AP is correctly set up and only the right competent authorities are connected.

The Cross-border exchange is tied to an explicit request and preview requirements from Article 14 of the SDGR [4] when using this legal basis and when other exceptions don't apply[4]. Like in the case of the Intermediation pattern, the DP trusts the DC that evidence requests are sent after the user explicitly requests the use of the underlying system for evidence exchange (unless in case of exceptions based on national or Union law). Specific property of the USI pattern is that the preview is provided by the DP. The DC trusts the DP that a user previewed the evidence and approved its transfer across borders. The user would need to trust the DP that only approved evidence is sent to the DC, however, considering the user can see in the online procedure at DC side which evidence has been transferred, they would have control on this aspect.

The two main differences with the previous pattern are:

1. The DO does not rely on eIDAS authentication coordinated by the DE but coordinates authentication itself.
2. The DE needs to rely on the preview being implemented correctly by the DO instead of the other way around.

Table 4 below provides an overview of what DC and DP need to be trusted with, for the USI pattern to function as intended in the SA and MA pilots.

Table 4 : Overview of Trust requirements in USI pattern

The DC is trusted with:	The DP is trusted with:
… maintaining a secure national OOP infrastructure (following applicable security standards in place in the DC Member State)	… maintaining a secure national OOP infrastructure (following applicable security standards in place in the DP Member State)
… setting up a secure eDelivery AP correctly	… setting up a secure eDelivery AP correctly
… providing access to sending Evidence Requests via the AP exclusively to competent authorities that have a legal basis to request evidence (i.e. pertaining to the procedures of Annex II of the SDGR[4]) or other procedures covered by Art. 14 or enabled by other legal bases like GDPR)	… providing access to sending Evidence Responses via the AP exclusively to competent authorities legally issuing evidence
… requesting only evidence if they have a legal basis to request such evidence	… lawfully issuing the evidence
… requesting only evidence required for the procedure	… correctly matching the user's eID to the unique ID and the records in the registries
… collecting the explicit request of the user before sending an Evidence Request (when exceptions don't apply)	…. providing a preview to the user and only sending an Evidence Response after approval (when exceptions don't apply)
… deleting all received evidence if user cancels procedure	… correctly selecting the evidence in the registry
… authenticating the user with the minimum assurance level required at national level	… authenticating the user with the minimum assurance level required at national level
… correctly redirecting the user to the DP	… correctly redirecting the user back to the DC

2.1.2.2 Technological description of the model

The following diagram provides an overview of the trust model for the USI pattern.

[4] It is to be noted that especially, in the context of the USI pattern, exchange can take place on the basis of consent under GDPR, as the user can decide on DP side to give consent for a transfer of the evidence.

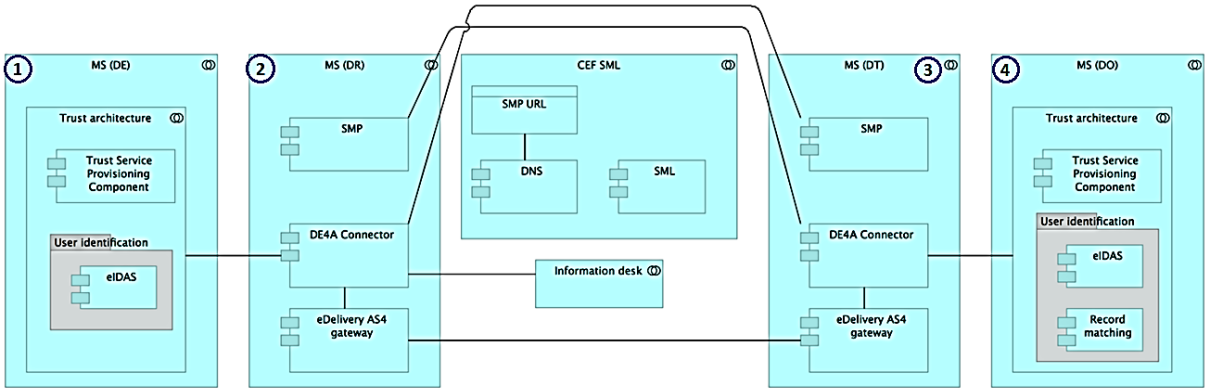

Figure 3 : USI Trust Model Intermediation

2.1.2.2.1 Components of the trust model

The table below lists the components that play a role in the trust model.

Table 5 : Overview of Trust components in the USI pattern

Component	Description
Trust Service Provisioning Component	Implements the functionalities encapsulating the trust services functionalities. A 'trust service' means an electronic service which consists of these functionalities: 1. the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or 2. the creation, verification and validation of certificates for website authentication; or 3. the preservation of electronic signatures, seals or certificates related to those services. This component is meant as a generic component and can be used wherever deemed useful. In case of User Supported Intermediation, the eDelivery infrastructure takes care of encryption/decryption and signing and signature verification. See also eDelivery AS4 gateway below.
eIDAS	For DE4A, the preproduction eIDAS nodes are used until all participant Member States notify their identification schemes.
Record Matching	Application component that provides matching (finding) of the right record based on attributes. Provided attributes are matched against attributes in some local registry.
DE4A Connector	Taking care of eDelivery and IDK interfacing, shielding DR and DT from complexities and facilitating ease of implementation. The connector also takes care of error handling and logging.
eDelivery AS4 gateway	This component – also referred to as AS4 gateway – handles the secure transfer of the data, including encryption and decryption as well as signing/sealing and validating signatures/seals.
DNS/SML	As there can be multiple SMPs, the sending party needs to know where to find the SMP of the receiver to get the actual metadata. This location can be found in the centrally CEF-hosted DNS, that will be queried by the access point of the sending Member State. DNS entries will be created from the registration of SMP's: the SML, which is also centrally hosted by CEF. See also SMP below.

Component	Description
Information Desk	The Information desk application collaboration combines multiple co-operating application components. It is used in conjunction with other infrastructural components in order in order to discover which competent data issuing authorities can provide evidence of a certain type for a given administrative procedure, to determine relevant characteristics of data services obtaining descriptive metadata about them and to use identifying information of data services in conjunction with other infrastructural components of the transport layer to obtain reliable routing information, i.e. participant ID.
SMP	For request/response message, information on the receivers Access Point (URL) and its certificates are needed. Each Member State hosts an SMP for this purpose. Before sending a request or response, the sending party queries the SMP of the receiver to get this info. In the scope of DE4A and for testing purposes ("playground") one single centrally hosted DE4A SMP is used.

2.1.2.2.2 Trust Anchors

Trust anchors in the USI pattern from a technical perspective:

1. User identity providers. These are trusted third parties that issue identification means within notified eIDAS identification schemes or other national schemes for the Member States that have not yet notified their schemes (for MA/SA pilots, Romania, Slovenia, Sweden which is peer-reviewed).
2. Providers of TLS certificates (MS specific). Technically speaking a trusted third party from which the certificates are purchased.
3. CEF as provider of the required eDelivery certificates through CEF's PKI. Technically speaking the trusted third party that issues the root certificate for the hierarchy of certificates. Because of the encryption gap, the DR and DT need to be trusted as well although technically speaking the trust anchors are the eDelivery certificates deployed to them.
4. SMP (and organisation responsible for it) as the reliable source of information about the infrastructure and endpoints.

2.1.3 Verifiable Credential (VC) pattern

2.1.3.1 Organisational description of the model

In the Verifiable credentials (VC) pattern, a user interacts with the Verifier (Data Evaluator) and Issuer (Data Owner), as explained in the PSA [6]. Users are identified with their electronic identification means, issued by Identity providers either within notified eIDAS identification schemes (for the Member States that have already notified their schemes) or other national schemes (e.g. from the Member States who have not yet notified their schemes).

Issuers and Verifiers rely on Identity providers to properly validate users' identities with the minimum assurance level required. On the other hand, when accessing their portals users authenticate Issuers and Verifiers through TLS certificates issued to the evidence consumers and providers. The Issuers and Verifiers can obtain TLS certificates at any trust service provider from Trusted List. They also have DIDs for securing communication with the users, while the Issuer generates also a so-called public DID, which is EBSI (European Blockchain Service Infrastructure) compliant. Issuers' public DIDs are registered in the EBSI DID registry and added to the Trusted Issuers Registry that contains information about the competent authorities that issue evidence of certain type (diplomas in the case of the SA pilot). It is important to note that no personal information is stored in EBSI infrastructure as the mentioned DIDs refer to competent authorities (organisations).

For the cross-border evidence exchange, the DID communication is used. The evidence requests and evidence responses are exchanged between the user and the Issuer, or between the Verifier and the user.

Table 6 below provides an overview of what Issuer and Verifier need to be trusted with, for the VC pattern to function as intended in the SA pilot.

Table 6 : Overview Trust requirements in VC pattern

The Verifier is trusted with:	The Issuer is trusted with:
… requesting only evidence if they have a legal basis to request such evidence	… lawfully issuing the evidence
… deleting all received evidence if user cancels procedure	… correctly matching the user's eID to the unique ID and the records of the registries
… authenticating the user with the minimum assurance level required at national level	… authenticating the user with the minimum assurance level required at national level

2.1.3.2 Technological description of the model

2.1.3.2.1 Components of the trust model

The table below list the components that play a role in the trust model.

Table 7 : Overview of Trust components in the VC pattern

Component	Description
Trust Service Provisioning Component	Implements the functionalities encapsulating the trust services functionalities. A 'trust service' means an electronic service which consists of these functionalities: 1. the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or 2. the creation, verification and validation of certificates for website authentication; or 3. the preservation of electronic signatures, seals or certificates related to those services. This component is meant as a generic component and can be used wherever deemed useful.
eIDAS	For DE4A, the preproduction eIDAS nodes are used until all participant Member States notify their identification schemes.
Record Matching	Application component that provides matching (finding) of the right record based on attributes. Provided attributes are matched against attributes in some local registry.
SSI Authority Agent	Implements functionalities necessary to register Issuer's DID in the EBSI ledger, as well as establishing a DID connection between the user's SSI Mobile Agent and the Issuer/Verifier.
SSI Mobile Agent	Implements functionalities necessary for the user to establish a DID connection with the Evidence (Issuer)/eProcedure (Verifier) portal.
EBSI ledgers (API)	For DE4A, EBSI ledgers store information about Issuer DIDs (DID Registry) and Trusted Issuers and the types of VCs they issue (Trusted Issuers Registry) in a

Component	Description
	trustworthy manner. The ledgers are then queried to validate the user's diploma evidence submitted to the Verifier.

2.1.3.2.2 Trust Anchors

Trust anchors in the VC pattern:

1. User identity providers. These are trusted third parties that issue identification means within notified eIDAS identification schemes or other national schemes for the Member States that have not yet notified their schemes (i.e. Slovenia in case of SA Pilot, Diplomas Recognition use case).
2. Providers of TLS certificates (MS specific). Technically speaking a trusted third party from which the certificates are purchased.
3. EBSI. Trusted Issuer Registry (TIR) as the reliable source of information about which competent authorities are allowed to issue verifiable credentials in a given domain (diplomas in the case of the SA pilot).

2.1.4 Lookup pattern

2.1.4.1 Organisational description of the model

As explained in the PSA [6] in much more detail, the basic logic of the Lookup pattern is a simple Request-Response interaction between DC and DP without any user involvement. For the DE4A pilot an evidence lookup is implemented, with a message exchange very similar to the Intermediation pattern described above, however, without user interaction and consequently without explicit request or preview. This allows the pilot to leverage the AS4-infrastructure and message definitions which are already put in place.

Therefore, and not surprisingly, the trust logic is very similar to the one explained in section 2.1.1.1 relying on a closed AS4-based eDelivery Network including the encryption gap in the gateway between Corner 1 and 2 as well as Corner 3 and 4 respectively.

Whereas the Intermediation pattern is directly related to a user requesting the transfer of evidence in context of a public service request, the lookup pattern is triggered directly by the DC in context of providing a public service (i.e. subsidy), typically over a longer period of time. This influences the trust model in so far that the DP needs to rely on procedures of the DC ensuring that evidence is only requested if it is actually required for the (continuation) of the public service.

In addition, the lack of a user authentication, i.e. via eIDAS, means that the lookup, including record matching by the DP, needs to rely on identification attributes stored by the DC. Assigning an assurance level to this identification attributes is not making much sense, introducing an additional element to the trust model. In the case of the DE4A DBA pilot this is a minor issue, as the EUID of companies is used for identification purposes.

Overall, the lack of a user request and authentication brings the need for an Authorization Check to the forefront, which should be included in any implementation of the Lookup pattern. In the case of the DE4A DBA pilot, the total number of participants is small enough to be captured in a simple whitelist.

Table 8 below provides an overview of what DC and DP need to be trusted with, for the Lookup pattern to function as intended in the DE4A DBA pilot.

Table 8 : Overview Trust requirements in Lookup pattern

The DC is trusted with:	The DP is trusted with:
… maintaining a secure national OOP infrastructure (following applicable security standards in place in the DC Member State)	… maintaining a secure national OOP infrastructure (following applicable security standards in place in the DC Member State)
… setting up a secure eDelivery AP correctly	… setting up a secure eDelivery AP correctly
… providing access to sending Evidence Requests via the AP exclusively to competent authorities that have a legal basis to request evidence	… providing access to sending Evidence Responses via the AP exclusively to competent authorities lawfully issuing evidence
… maintaining correctly the competent authority listing in the Authorization Controller based on an agreed national governance	
… the CA requesting only evidence if they have a legal basis to request such evidence	… the CA lawfully issuing the evidence
… the CA requesting only evidence if the public service they provide with regards to the subject of the evidence requires them to do so	… the CA correctly matching the EUID to the record of the business register (DBA Pilot)
… the CA having previously collected and safely stored the identification information of the subject (e.g. EUID in case of DBA Pilot)	
… the CA deleting all received evidence if the Evidence is not anymore needed for the public service and after any (legally) applicable archiving period	

2.1.4.2 Technological description of the model

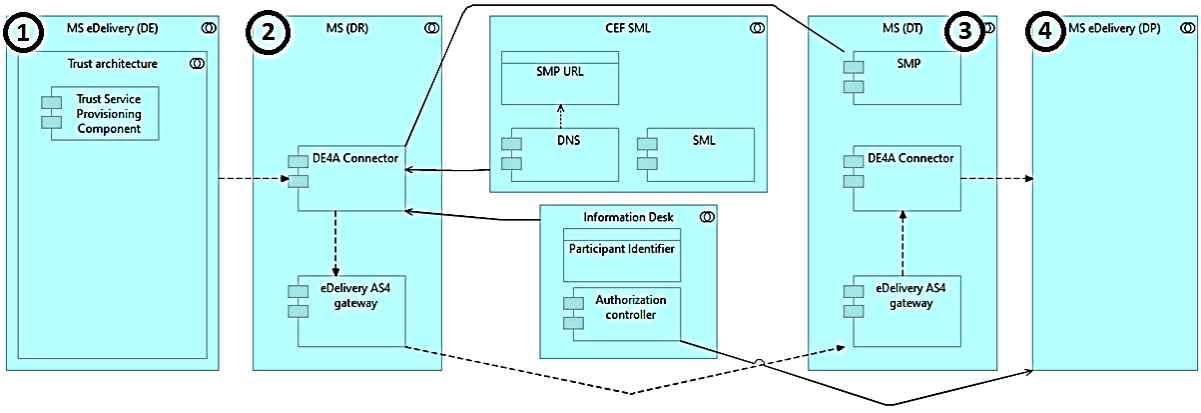

Figure 4 : Trust Model Lookup

2.1.4.2.1 Components of the trust model

The table below list the components that play a role in the trust model. Lookup relies on the eDelivery infrastructure which is elaborated in more detail in section 2.3.

Table 9 : Overview of Trust components in the Lookup pattern

Component	Description
Trust Service Provisioning Component	As for Intermediation, see 2.1.1.2.1. In case of Lookup, the eDelivery infrastructure takes care of encryption / decryption and signing and signature verification. See also eDelivery AS4 gateway below.
DE4A Connector	As for Intermediation, see 2.1.1.2.1.
eDelivery AS4 gateway	As for Intermediation, see 2.1.1.2.1.
DNS/SML	As for Intermediation, see 2.1.1.2.1.
Information Desk / Data Service Lookup	The Information desk application collaboration combines multiple co-operating application components. It is used in conjunction with other infrastructural components in order in order to discover which competent data issuing authorities can provide evidence of a certain type for a given administrative procedure, to determine relevant characteristics of data services obtaining descriptive metadata about them and to use identifying information of data services in conjunction with other infrastructural components of the transport layer to obtain reliable routing information, i.e. participant ID.
Authorization Controller	Application component to establish whether a DC is allowed to receive updates for companies.
SMP	As for Intermediation, see 2.1.1.2.1.

2.1.4.2.2 Trust anchors

In the context of Lookup and usage of the eDelivery infrastructure and from a technical trust perspective, a trust anchor is assumed to be an authoritative entity for which trust is assumed and not derived (e.g. Certification Authorities issuing digital certificates for a given domain or sub-domain). Trust Anchors in the Lookup pattern:

1. User identity providers. These are trusted third parties that issue identification means within notified eIDAS identification schemes or other national schemes for the Member States that have not yet notified their schemes (in case of DBA pilot Romania, Austria which is pre-notified, Sweden which is peer-reviewed).
2. Providers of TLS certificates (MS specific). Technically speaking a trusted third party from which the certificates are purchased.
3. CEF as provider of the required eDelivery certificates through CEF's PKI. Technically speaking the trusted third party that issues the root certificate for the hierarchy of certificates. Because of the encryption gap, the DR and DT need to be trusted as well although technically speaking the trust anchors are the eDelivery certificates deployed to them.
4. SMP as the reliable source of information about the infrastructure and endpoints.
5. The Authorization Controller

See section 2.3 for more details with respect to certificate usage.

2.1.5 Subscription & notification

2.1.5.1 Organisational description of the model

The Subscription & Notification (S&N) Pattern described in the Project Start Architectures [6] reuses the closed eDelivery network, similar to the Lookup pattern described in section 2.1.4. This pattern consists of two separate processes:

1. The subscription process is triggered by the DC, which sends a subscription request to the DP. The DP registers the subscription to the event catalogue of a specific company and returns a subscription confirmation. A subscription application component manages all the lifecycle of subscriptions.
2. The notification is triggered by a business event of a company, recorded in the registry of the DP. The DP sends a notification, containing identifiers and event type, to the DC. It is worth noting that the DP does not receive a business confirmation, but only the confirmation that the event message was well received by the eDelivery Gateway. A cross-border event handler filters all domestic events for relevant cross-border events and takes care of preparing a notification message and compiling a subscribers list to which the notification must be sent.

In this section, the trust model spanning both processes is discussed, irrespective of their triggering logic, timeliness and multiplicity.

The S&N pattern uses a closed network approach to project the network of trust between participants on the technical level and, similarly to the Lookup-pattern, no current legal trust anchor could be identified at this moment. For the DBA pilot this is resolved in two ways: Firstly, the subscription is coupled to an initial evidence exchange, performed using the Intermediation pattern (see section 0). During the collection of the explicit request from the user by the Data Evaluator (DE), the user is asked to provide their consent to the subscription. Secondly, a whitelist is additionally used as authorization control.

This approach works for the pilot, but it is very restrictive in so far that it only works in conjunction with a prior evidence exchange through the same system, hence cannot be triggered from an administrative procedure, and relies on user consent. As one of the potential use cases for a wider roll-out of the S&N pattern is fraud prevention, a different legal basis would need to be created. This topic will be discussed in more detail in the forthcoming DE4A deliverable “D7.2 Initial report on legal and ethical recommendations and best practices”. Another consequence of not using the user request and consent is that it would again require a more fine-grained Authorization Check, most likely on the level of the event set that a competent authority may subscribe to, e.g.: “Municipality can subscribe to company change events”. The authorization rules would need to be derived from the legal basis.

Similarly to the other pattern, the Data Requestor has some trust requirements to be fulfilled that are directly related to the functionality being implemented and operated correctly. This is straight-forward in a pilot setting, but might require some additional, organisational trust measures, such as audits or peer reviews in a broader context. The DP is trusted to register a subscription correctly in the Subscription System before sending a Subscription Confirmation. Furthermore, the DP is trusted to implement and operate the Cross-border Subscriptions in such a way that the DC can actually depend on receiving a notification.

Table 10 : Overview Trust requirements in Subscription and Notification pattern

The DC is trusted with:	The DP is trusted with:
… maintaining a secure national OOP infrastructure (following applicable security standards in place in the DC Member State).	… maintaining a secure national OOP infrastructure (following applicable security standards in place in the DC Member State).
… setting up a secure eDelivery AP correctly.	… setting up a secure eDelivery AP correctly.

The DC is trusted with:	The DP is trusted with:
… providing access to Subscription Requests via the AP exclusively to competent authorities that are allowed to request Subscriptions.	… providing access to sending Subscription Confirmations and Event Notifications via the AP exclusively to competent authorities allowed and able to provide the notifications.
… maintaining correctly the competent authority listing in the Authorization Controller based on an agreed national governance (i.e. in pilot scope: the whitelist in the pilot).	
… requesting only subscriptions if there is a legal basis to request such evidence (i.e. in pilot scope: the consent of the user collected in context of the explicit request, during the initial transfer of evidence).	
… having previously collected and safely stored the identification information of the subject (e.g. EUID in case of DBA Pilot).	… correctly matching the EUID to the record of the business register and registering the subscription correctly (DBA Pilot).
	.. correctly registering the subscription.
	.. identifying the events correctly and actually sending a notification if a subscription to the event exists.

The Notification has an additional aspect within the DC Member State in case the DE and DR roles are played by different organisation that is worth mentioning. No business confirmation is returned from the DE to the DO, but only an acknowledgement that the message was received the DR eDelivery AP. The DP consequently does not know whether the DR correctly routed the event notification further to the DE. We do not consider this a cross-border trust requirement as the responsibility and the interest for this to happen both reside in the DC country, between the DR and the DE. Nevertheless, it is important that the DR takes full responsibility that the notification they acknowledge receiving from the DT is correctly delivered to the DE.

2.1.5.2 Technological description of the model

The diagram depicting the S&N trust model is an exact copy from the Lookup pattern and repeated hereunder. It is basically a simplified form of the Intermediation trust model with an added component called Authorization Controller.

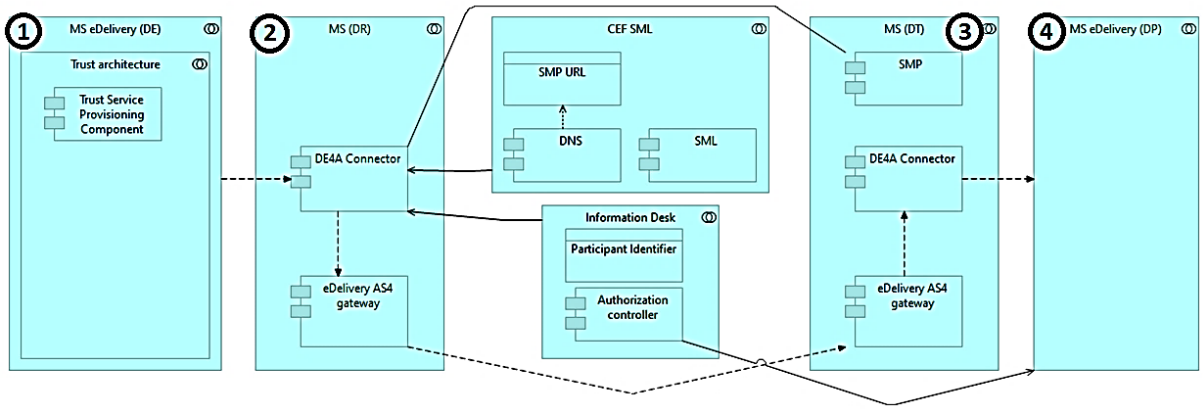

Figure 5 : Trust Model Subscription & Notification

2.1.5.2.1 Components of the trust model

Table 11 : Overview of Trust components in the Lookup pattern

Component	Description
Trust Service Provisioning Component	As for Intermediation, see 2.1.1.2.1. In case of S&N, the eDelivery infrastructure also takes care of encryption/decryption and signing and signature verification. See also eDelivery AS4 gateway below.
DE4A Connector	As for Intermediation, see 2.1.1.2.1.
eDelivery AS4 gateway	As for Intermediation, see 2.1.1.2.1.
DNS/SML	As for Intermediation, see 2.1.1.2.1.
Information Desk / Data Service Lookup	The Information desk application collaboration combines multiple co-operating application components. It is used in conjunction with other infrastructural components in order in order to discover which competent data issuing authorities can provide evidence of a certain type for a given administrative procedure, to determine relevant characteristics of data services obtaining descriptive metadata about them and to use identifying information of data services in conjunction with other infrastructural components of the transport layer to obtain reliable routing information, i.e. participant ID.
Authorization Controller/Subscription System	Application component to establish whether a DC (DE) can subscribe (is allowed) to updates for companies and whether a DP (DO) can send notifications. Subscription system manages lifecycle of subscriptions (creation, validation, confirmation, changes…).
Cross-border Event Handler	Application component handling the cross-border events. It filters all domestic events for relevant cross-border events and takes care of preparing a notification message and compiling a subscribers list to which the notification must be sent.
SMP	As for Intermediation, see 2.1.1.2.1.

2.1.5.2.2 Trust anchors

Technical Trust Anchors in the S&N pattern:

1. Providers of TLS certificates (MS specific). Technically speaking a trusted third party from which the certificates are purchased.
2. CEF as provider of the required eDelivery certificates through CEF's PKI. Technically speaking the trusted third party that issues the root certificate for the hierarchy of certificates. Because of the encryption gap, the DR and DT need to be trusted as well although technically speaking the trust anchors are the eDelivery certificates deployed to them.
3. The Authorization Controller

See section 2.3 for more details with respect to certificate usage.

2.2 Powers of Representation & Mandates

Electronic business processes from private or public sector are often delegated to third persons, who act on behalf of other persons (legal persons and natural persons). Often, persons such as professional representatives are assigned with such role(s). Beside of non-digital powers of representation and mandates, electronic equivalences for electronic business activities have to be established to support business processes. Such mandate management systems, overall in an integrated national setup, are not widespread in Europe nowadays. The study "Study about cross-border interoperability of powers

and mandates" within the ISA2 2016-12 action proved evidence of this fact; the most advanced countries in terms of e-mandates offerings are Austria with its "Online Mandate System" and Netherlands with its "DigiD Machtigen" [7].

Powers of representation and mandates can be realised in different ways for electronic use. Two variants are most often mentioned in the recent discussions on that topic:

1. Powers validation as part of the authentication phase (eIDAS oriented – pre-procedure) and
2. Powers validation as part of the evidence gathering and assessment phase (OOP TS/wallet-oriented – in procedure).

The following section describes in detail the SEMPER approach since this solution will be part of DE4A Doing Business Abroad pilot.

The SEMPER project [8] provides a solution for a digital determination of cross-border powers of representation and e-mandates[9]. It developed a harmonized definition of powers and e-mandates in alignment and as an extension of the eIDAS Interoperability Framework. With the SEMPER solution Service Providers are able "…to allow the representation of legal or natural persons within their eIDAS services and on the other hand eIDAS node operators will be able to not only connect to their national identity providers but to also access national mandate management infrastructures as Attribute Providers"[8]. SEMPER extends the eIDAS nodes with the functionality of a semantic translation of powers of representation from a Member State specific format to the SEMPER format[9].

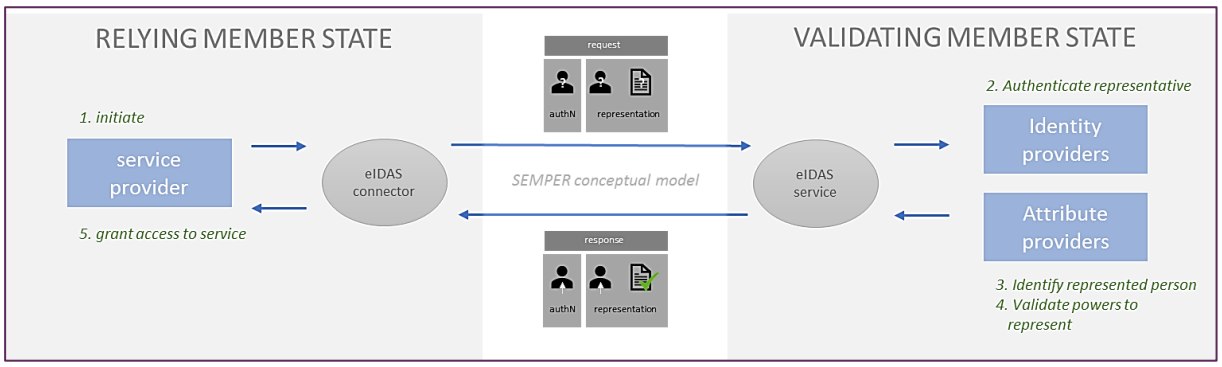

Figure 6 : Overview of SEMPER scenario

Figure 6 shows the overall conceptual model of the SEMPER solution, with the functionality of the request of person authentication and the request of the representation discovery between the actors' service provider (with eIDAS connector) at the relying Member State side and the identity providers and attribute providers via the eIDAS service at the validating Member State side.

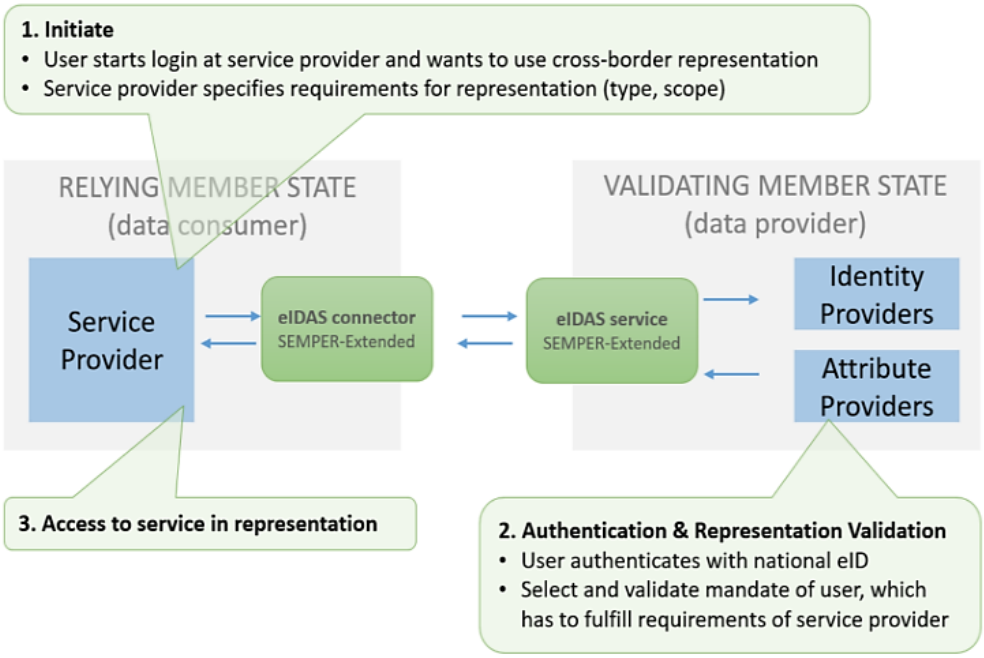

Figure 7 : eIDAS context of SEMPER solution

Figure 7 depicts a finer granularity of the processes, which are shown in Figure 6 with the overall interactions between the actors in the SEMPER process. It comprises the three main process areas:

- Initiation of the SEMPER transaction with (1) User interaction at service provider and request to use representation and (2) definition of specific requirements for the representation at the service provider side
- Authentication and validation of representation with the (1) the eIDAS authentication of the user and (2) the processes of the selection of the mandates and the validation of those, regarding the requirements set from the service provider.
- Finally, the service provider receives the information of the users' authentication and mandates of the user and grants access to the eService.

In SEMPER, it is up to the validating Member State to define the rules for validation, based on the specific requirements. These rules specify whether powers are valid or not; for example, the guidelines for registering mandates at level of assurance (low, substantial and high) and the (type of) services for which the representative has to accept the mandate. National law, principles, and policy of the validating Member State also determine the setting of appropriate rules. The validating Member State has to answer to a powers' validation request with a response, expressed in ok/not-ok, according to national validation rules. The relying Member State trusts the validating Member State, and its processes, and accept the response without any control mechanism, e.g. the relying Member State does not start any redo- or checking-processes. SEMPER's trust system intends that the validating Member State stays with the legal liability for the validation of powers. Like in eIDAS, the relying Member State accepts the powers validation result from eIDAS-notified Member State and the validating Member State is responsible for validating a person's powers, the relying Member State is responsible for granting access according to the set rules.

SEMPER validates the powers within the authentication process (or directly after this process), as it works within the eIDAS-process definition (system architecture). Therefore, it is actually not in the scope of SEMPER to validate powers in a later stage in or beyond the service fulfilment process; this would require functional extensions in the future[10].

SEMPER uses the trust mechanism and the trust management of eIDAS, to reach the goal of a high grade of interoperability. This also corresponds with the RPaM scenario 1.12 of the ISA2 2016.12 action[10]. The trust system comprises of the following system requirements:

- Trust system from the eIDAS framework and architecture
- Trust between relying Member State and validating Member State on powers and mandates for representations. Regarding this aspect it relies on the eIDAS trust-arrangement as specified in the regulation: the peer reviews. For cross-border exchange of powers information in the eIDAS-context, the national mandate management solution should be notified under eIDAS as well[5].
- Trust in the HTTPS (TLS) communication protocol on transport security

DE4A DBA pilot intends to test SEMPER in the second iteration of the pilot that is planned for 2022. The eIDAS node's implementation from the first iteration already exhibits a base functionality for the discovery and the determination of mandates (implicit mechanism for full powers). Nonetheless, the aim of the second iteration of this pilot is to extend this functional scope with the above-described SEMPER functional scope towards fine-grained powers validation. Since SEMPER offers an application (within eIDAS-architecture) with national dependencies - because it relies on national systems interconnection for mandates and powers management -, the DBA Pilot has taken this into account regarding integration and interoperability with such national infrastructures. Furthermore, it is necessary to evaluate the national requirements on the needed level of assurance for the regarding procedure to establish an appropriate setup of SEMPER in the DBA pilot; a challenge which comes along with the rules applied (as described above). The SEMPER application is intended to be used by all participating pilot partners in the DBA pilot within the Use Case 1 [11].

2.3 eDelivery

2.3.1 eDelivery trust models

DE4A is using the CEF eDelivery building blocks to support the secure interaction of the different actors. Some of the eDelivery components need to be operated by Member States directly, some of them are part of the Information Desk (IDK) and some of them are even operated outside of the project. The eDelivery components are always used, except in the case of VC pattern.

The exchange of a single document between a DE and a DO always requires two eDelivery exchanges: the first one initiated by DE and targeted for DO, and the second one is initiated by DO and targeted for the DE. Technically speaking both transmissions are "requests" even though their semantics are "request" and "response".

The basic model underlying eDelivery document exchange is the "4-corner model" mentioned in section 0, and in the project the "DE4A Connector" (sometimes just "Connector") can play the role of both DR and DT and therefore acts as C2 or C3, depending on whether a message is sent or received.

Figure 8 (right side) depicts the structural message exchange initiated by DE (C1), sent by DR (C2), received by DT (C3) and forwarded to DO (C4). The message exchange between C1 and C2 as well as the message exchange between C3 and C4 are not specified by eDelivery, even though AS4 may be used for this, but they must be defined by the DE4A Connector.

[5] However, this arrangement of trust is currently lacking when implementing powers validation in the OOP TS (requesting PoR-evidence over the OOP-TS).

If DO sends a message back to DE, the order of the messages change as well as the corner assignment, as shown in Figure 8(left side): the DO becomes C1, forwarding the response to DT which is now C2. The AS4 transmission targets DR as C3 who in turn forwards the payload to DE which is the C4 in this scenario.

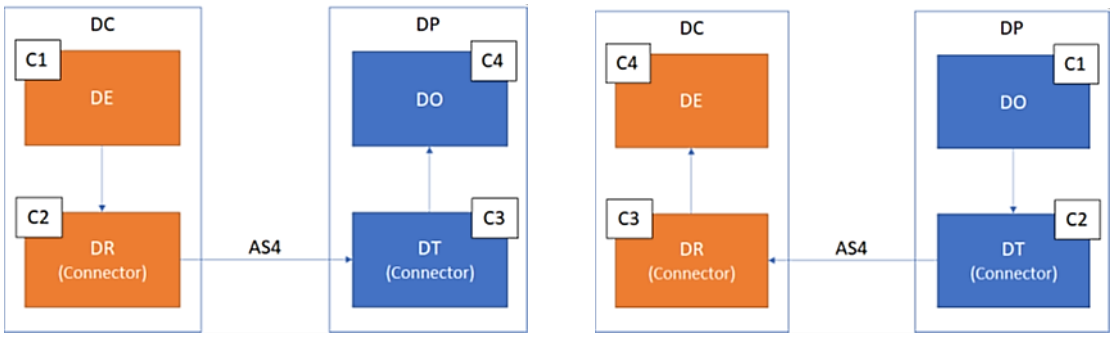

Figure 8 : eDelivery business request and response between DE and DO

2.3.2 Configuration and management of certificates

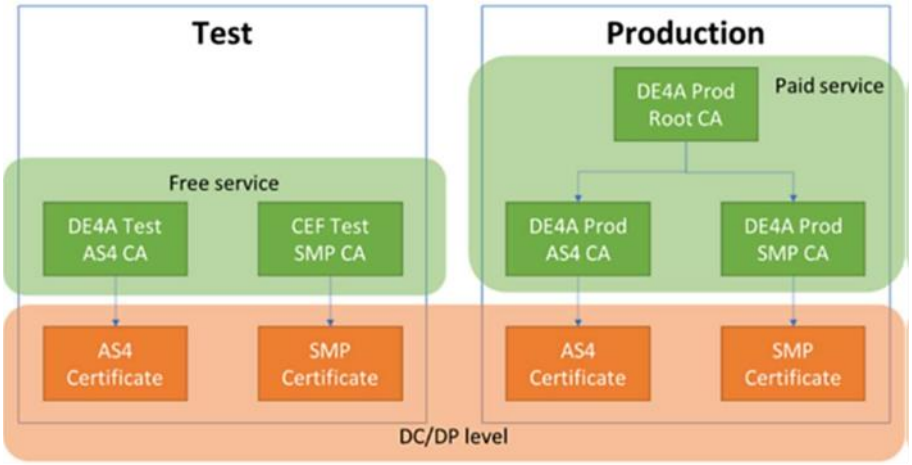

Figure 9 : Test and Production Certificates

The existing eDelivery components are designed to work with a single PKI. That means, that all SMP certificates MUST be based on a single SMP root certificate, and all AS4 certificates MUST be based on a single AS4 root certificate. This rule only applies to the SMP and AS4 signing/encryption certificates, but NOT to TLS certificates used for transport security.

Test certificates are emitted by the WP5 team upon request, but production certificates are managed with the process described on the CEF eDelivery PKI Service Offering Document [12].

The usage of a single root certificate provides an easy way to check if a certificate is valid or not. It requires a functioning OCSP or CRL revocation check to work properly. For a production PKI to function, it needs a strong governance and appropriate controls and measures.

The CEF eDelivery PKI service enables issuance and management of the digital certificates used on the deployed CEF eDelivery components, e.g. between CEF eDelivery Access Points (AP) and Service Metadata Publishers (SMP), to ensure confidentiality, integrity and non-repudiation of the data moving across systems. This service is provided only to the European Union, European Economic Area and United Kingdom public administrations that wish to be established as PKI domain owners in the PKI service and that are interested in creating a circle of trust for information exchange using the

technical specifications and components of CEF eDelivery. The use of the CEF eDelivery PKI is optional; policy domains may choose to use any other PKI service or mutual trust mechanism.

Every legal entity that acts as a service provider or uses one of the CEF eDelivery components is denoted as "Organisation" in the rest of this document, they will be Competent Authorities in the case of DE4A.

A competent authority Organisation that wants to make use of the PKI service needs to request the issuance of a digital certificate per CEF eDelivery component it operates. The certificate usage is two-fold: signing a message and encrypting a message.

Figure 10 shows the CA architecture on which the CEF eDelivery PKI service relies. The Root CA is the T-Telesec GlobalRoot Class 2. The Sub-CA is TeleSec Business CA 1, which issues/signs the certificates for Access Points (AP) and Service Metadata Publishers (SMP).

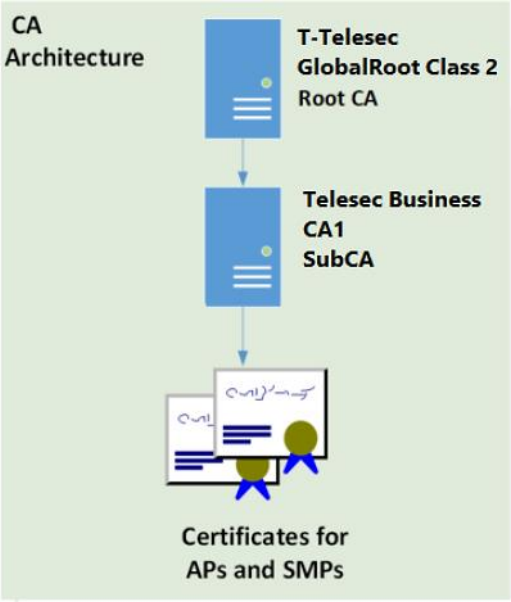

Figure 10 : CA Architecture [12]

The CA architecture information is important for the certificate validation process, in order to ensure that the certificates are issued by the trusted CA (Deutsche Telekom).

In addition to the CA, an important part of the CEF eDelivery PKI service is the Registration Authority (RA), which registers and approves the requests of issuance, revocation and renewal of certificates. Figure 11 shows the architecture of the CEF eDelivery Registration Authority.

Master RA is assigned to the CEF eDelivery domain. It serves to register and manage multiple sub-RAs, i.e. areas of responsibilities that correspond to different CEF eDelivery PKI domains, e.g. BRIS or e-Justice. The sub-RAs are used to register and approve the requests of issuance, revocation and renewal of certificates performed by the operators of CEF eDelivery components (AP and SMP) that operate in the corresponding PKI domain.

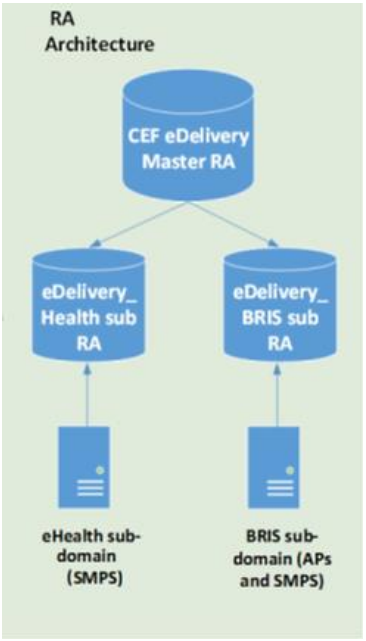

Figure 11 : Example of RA Architecture [12]

Finally, the certificates for APs and SMPs that are issued to Organisations are separated using "Department" field, which is part of the certificate metadata.

Note: It is important to note that the public keys included in the certificates and the corresponding private keys are generated by the requestors of certificate i.e. the operators of CEF eDelivery components (AP and SMP). The private keys need to be kept in a secure place by the requestors of the certificate. There is no backup of the keys provided by Deutsche Telekom.

2.3.3 Infrastructure

Each MS can implement the infrastructure from a set of six configuration ("Set Up") alternatives as per the following figure, although in DE4A the participating Member States actually only use two of such possible configurations (see table 11 below).

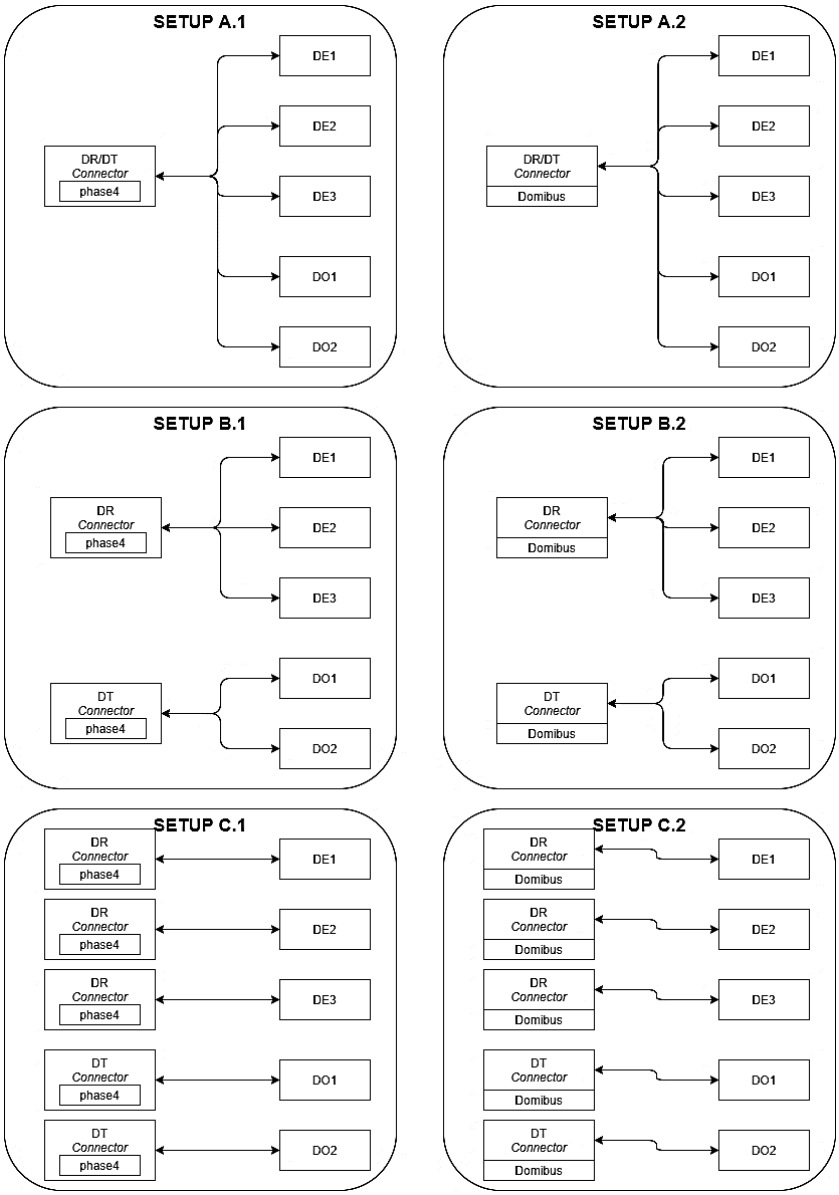

Figure 12 : Alternative infrastructure setups

The following table details the choices of the DE4A Member States:

Table 12 : Examples of configuration on MS Gateway

COUNTRY	SET-UP	CONNECTOR AS4 Gateway
Austria	A.1	Internal Phase 4
Luxembourg	A.1	Internal Phase 4
Portugal	A.1	Internal Phase 4
Romania	C.1	Phase 4
Slovenia	A.1	Internal Phase 4
Spain	A.1	Internal Phase 4
Sweden	A.1	Internal Phase 4
The Netherlands	A.1	Internal Phase 4

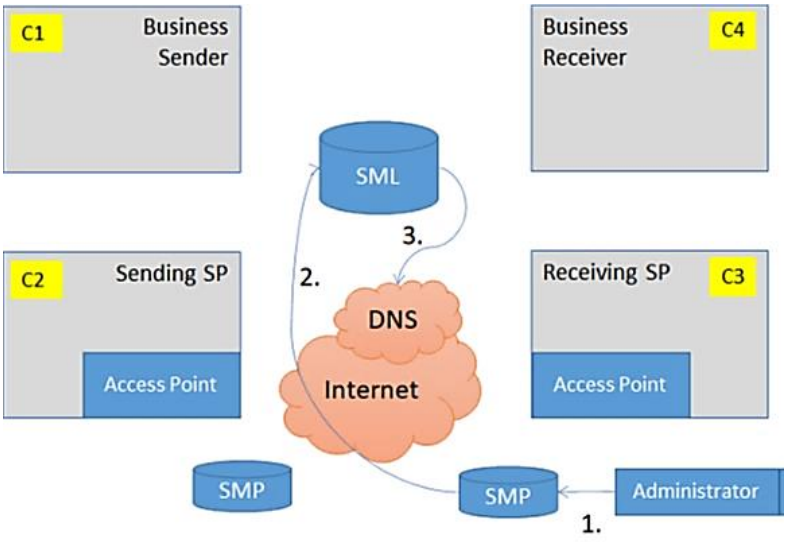

Figure 13 : SMP Registration

The initial registration of an SMP to the SML is depicted in the above figure. It requires a trusted SMP certificate which is used as a client certificate when invoking the SML's API.

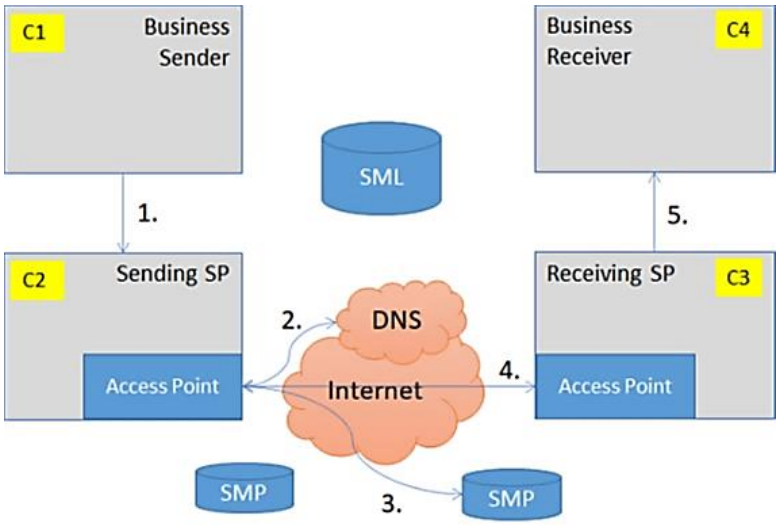

Figure 14 : eDelivery Message Exchange

The figure above shows the big picture of a message exchange. Two certificates are used:

a. the SMP Endpoint X.509 Certificate to connect to and
b. the origin's AS4 certificate to sign and encrypt the AS4 message.

2.3.4 Process for obtaining a Certificate

To obtain a Certificate, an organisation must follow the process described on the "CEF eDelivery PKI Service Offering Document" [12].

The following diagram summarizes the existing processes.

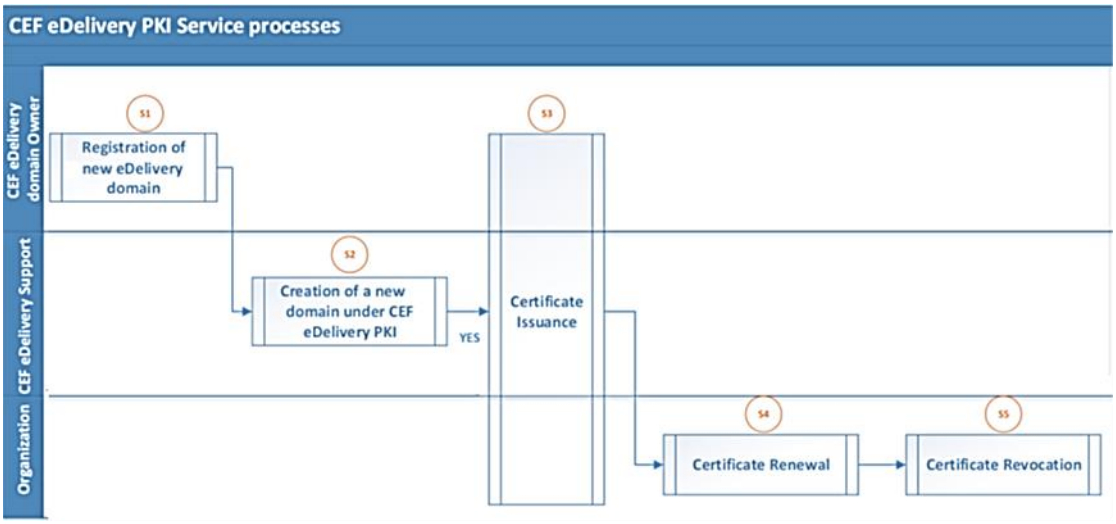

Figure 15 : CEF eDelivery PKI Service processes

The processes can be summarized as follows:

1. Registration of a new CEF eDelivery PKI domain

   Start: A policy domain owner wants to use the CEF eDelivery PKI service to establish trust in the domain, contacts CEF eDelivery Support and provides required information and documents
   Result: CEF eDelivery registers the new PKI domain

2. Creation of a new PKI domain under CEF eDelivery PKI

   Result: CEF eDelivery Support delivers a smart card with the certificate needed to log in to the sub-RA page

3. Certificate Issuance

   Start: Organisation contacts domain owner to express interest in a PKI certificate
   Result: Organisation retrieves approved certificates

4. Certificate renewal

   Start: CEF eDelivery Support alerts Organisation on certificate expiration date proximity
   Result: Organisation renews and retrieves new certificate

5. Certificate revocation

   Start: either Organisation or CEF eDelivery PKI Domain Owner request certificate revocation to CEF eDelivery Support
   Result: Certificate enters the CRL of the PKI domain

Note: It is the responsibility of the Organisation to configure the Certificate on the chosen Access Point or SMP software.

3 Evidence exchange comparing traditional and emerging patterns: challenges and technical anchors

This chapter presents a comparison of the three major evidence exchange patterns –Intermediation (IM), User-supported Intermediation (USI) and Verifiable Credentials (VC)- regarding the trust factor. The comparison presented in this chapter highlights the differences in trust challenges and technical trust anchors, to help on the selection of the more suitable pattern for a specific use case of evidence exchange to implement.

The next sections describe the differences among the three evidence exchange patterns regarding the trust factors without any assessment about which pattern is better or worse. Besides, the trust factor is just one of the several critical factors to consider for selecting one of the evidence exchange patterns that suits better for a specific use case, such as the level of legal harmonisation, the mutual recognition of stakeholders, the extent of participants, the interoperability agreements and barriers, the sensitivity of information to exchange, the security of the networks…, among others.

3.1 Overall comparison of trust models

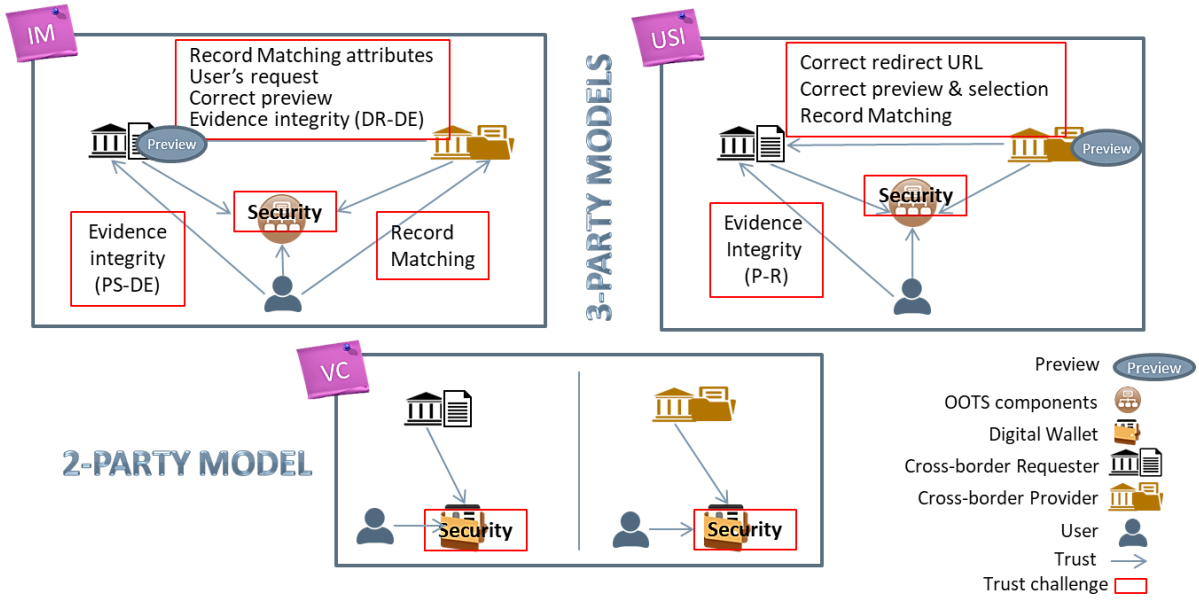

Figure 16: Overall Comparison of Trust Models

IM and USI are patterns where one exchange involves three stakeholders simultaneously: user, cross-border Data Requestor (DR) and cross-border Data Transferor (DT)[6]; they are (C/B)2G2G models. However, VC is a pattern where one exchange only involves two stakeholders at a time (excluding validations): the user and the cross-border Data Transferor when the evidence is requested by the user to be stored in his/her eWallet, and the user and the cross-border Data Requestor when such an evidence is incorporated to a procedure; this is a (C/B)2G model. While in the three models the trust factor requires in general a systemic security approach, in this chapter only the trust provided by the peculiarities of each pattern is analysed.

[6] Note that in this section, the terms Data Requestor and Data Transferor are used with a generic meaning referring to the entities requesting and providing evidence in the respective Member States in cross-border exchanges.

On the whole, trust issues in the IM pattern arise due to the intermediation of the cross-border Data Requestor between the user and the cross-border Data Transferor for collecting evidence required by the procedure. Among different trust issues detailed further below, the cross-border Data Transferor needs to trust the cross-border Data Requestor in regard to the attributes for record matching, the user's request to use the system, the user's preview of the provided evidence and the integrity of the evidence while it is transmitted from the two corners at the requestor side, data requestor and data evaluator. Besides, the user needs to trust that the cross-border Data Transferor has properly conducted the record matching because, otherwise, the user will not try the exchange through the system even with the preview guarantee. The user also needs to trust that the preview -there are discussions as well on how to keep it separate from the rest of the eProcedure Portal- will protect the integrity of the previewed evidence when it is finally incorporated to the procedure.

Trust requirements in general are reduced in the USI pattern, since the requestor is not acting on behalf of the user to interact with the provider[7]. However, the user needs to trust the integrity of the evidence when it is transmitted from the provider's portal to the requester's portal; besides, the requester needs to trust on the user is correctly redirected to the provider and the provider has correctly conducted the record matching, the selection and the preview of the evidence required by the procedure.

Regarding the VC pattern, the user is always in control of the data flows, i.e. the user is in the middle of the flow and is in control of it as they ask to receive the evidence in their wallet and choose where to present it also controlling which amount of attributes to disclose. The issuer (provider) delivers the data directly to the user's wallet, and the verifier (requester) obtains the data from the wallet. Neither the provider nor the requester acts on behalf of the user, so there are not trust issues due to this. The trust aspects that need to be considered here are more centred on the user: the model needs to be carefully defined to avoid delegating any trust on the user (e.g. mechanisms including the signing of data to ensure its provenance and integrity / non-tampering while stored in the wallet). Main risks are related with the offline nature of the data transfer (freshness of the data is not optimal, unless a data revocation mechanism can be checked fully online by the consumer), the potential holes in the model that would allow the user to tamper the data (for example, using a flawed verifiable presentations model), or confusing the subject and holder concepts if the wallet implementation does not properly prevent holding data from different users[8]. This will be developed in the next sections.

3.2 Trust challenges

In this section relevant trust challenges for the evidence exchange are analysed by comparing the three trust models regarding each challenge. The identified trust challenges have been grouped under the following concepts:

- Transitivity of explicit request
- Transitivity of identity
- Preview
- Delegation of evidence disambiguation
- Evidence validity
- Powers and Mandates

[7] It is to be noted that in some cases public authorities may be obliged by law to use information currently available, for example in base registries. Retrieving this information – even under approval of the user – may not be interpreted in such cases as acting on behalf of the user.

[8] Regarding wallet implementations, the user will also need to be given proper assurance that the wallet they use is genuine and certified in order to trust it.

3.2.1 Transitivity of explicit request

According to the SDGR Article 14, the user has to explicitly request to use the evidence exchange system; the alternative to use this system is for the user to directly upload the evidence lawfully issued in a digital form by the corresponding competent authority. This explicit request should not be confused with the user's consent on a personal data treatment, since this user's consent inheritably implies the right set by the GDPR Article 7(3) to withdraw the consent at any time, which is not applicable to the processing of personal data that has been lawfully established by a public service regulation, as foreseen in the GDPR Article 6(1)(e)[9].

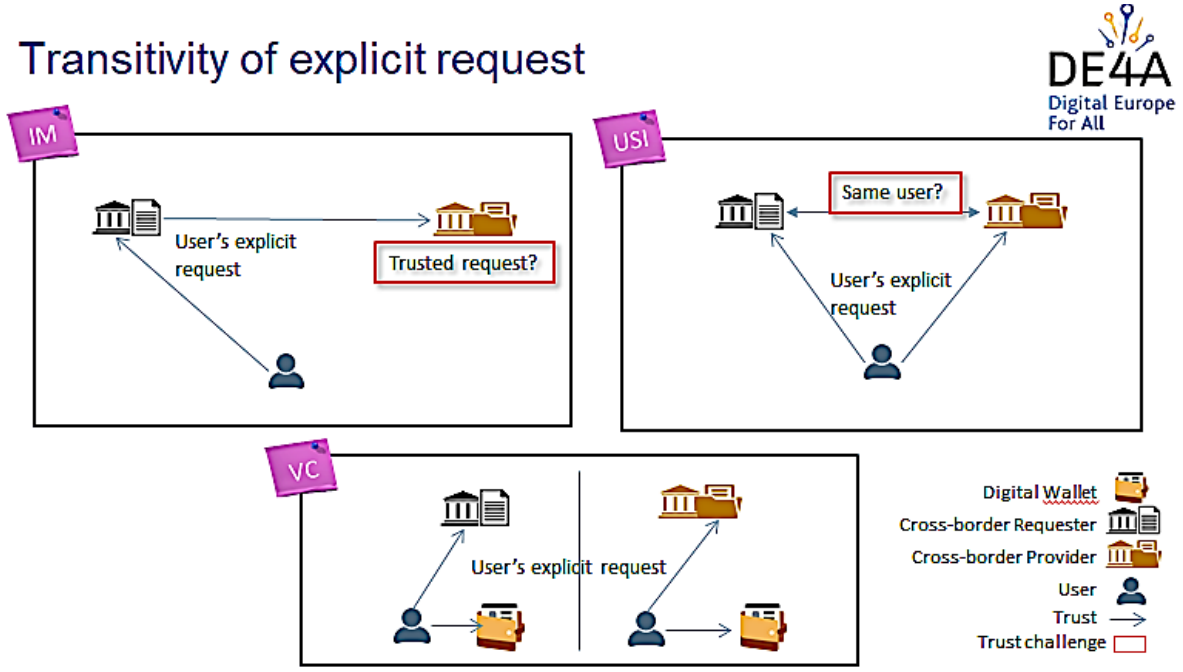

Figure 17: Transitivity of Explicit Request

The IM model poses a trust challenge regarding the explicit request, since the provider needs to trust the requester has properly obtained the user's explicit request to use the system (a flawed or rogue requester could query information from unknowing citizens, which makes securing the business logic of the requester a highly critical task). This situation is not easily overcome, since authenticity, integrity and non-repudiation guarantees pose to users an extra burden and difficulty for using the system that should be avoided. Section 0 explains in detail this specific trust challenge.

In the case of the USI model, users are redirected to the provider's portal under their explicit request but then they are freely interacting with such a portal, and they can cancel that interaction at any time. In this sense, there is no doubt that they really want to use the system, but there is an open question on whether the user that interacts with the provider is the same user that interacts with the requester. This is caused by the fact that both the requester and the provider need to authenticate the user, the user may use the same or different electronic identities and both sides might identify a different person with such identities. This problem will be developed at length in the next section.

In the case of the VC model, the user (Holder) is directly requesting either the storage of evidence in the digital wallet or the use of evidence stored in the digital wallet, so the explicit authorization of the user is given in every nuclear data transfer operation.

[9] A more detailed discussion from a legal perspective of the differences between two concepts can be found in section 3.1.7 "Data protection and legal basis" of D4.5 "Doing Business Abroad - Use Case Definition & Requirements".

3.2.2 Transitivity of identity

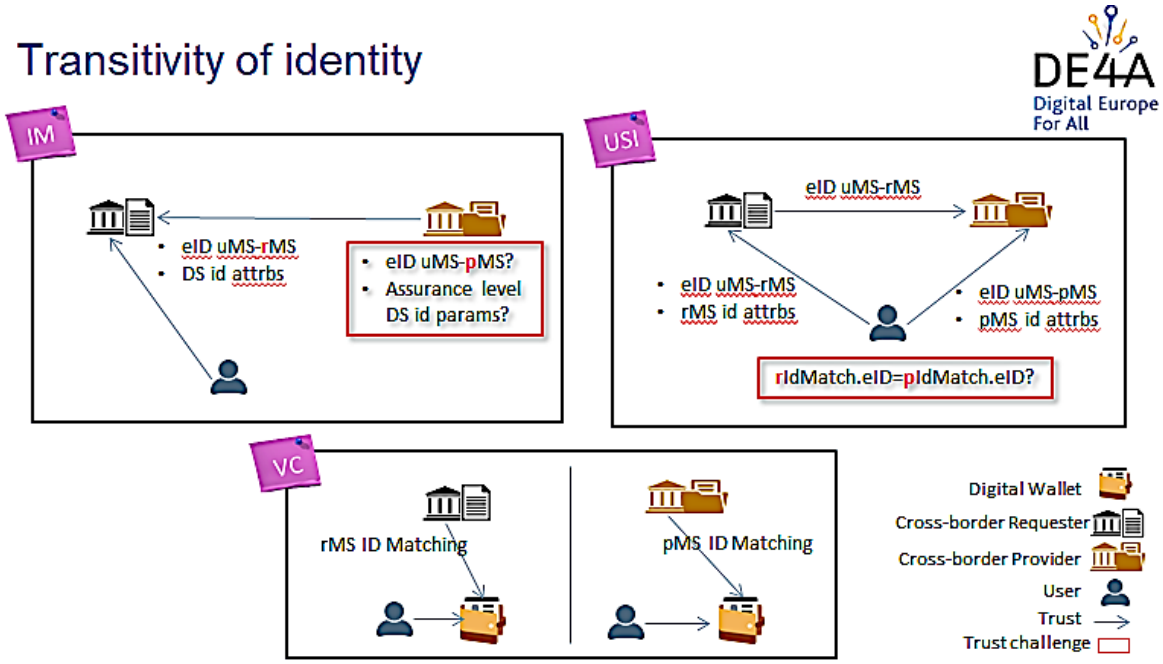

Figure 18: Transitivity of Identity

The IM model also poses an important trust challenge regarding the transitivity of the user's identity because the user is identified at the requester's portal and the provider has to work with this identification outcome. However, this is a challenge because the eIDAS identifier (PersonIdentifier) of the user's digital identity may change depending on the country that requires the identification and differs from the identity issuing country[10].

Besides, the proposed additional identity parameters to overcome the eIDAS identifier issue also pose a trust challenge because, in contrast with the eIDAS dataset attributes, these additional attributes have no assurance level since they are manually provided by the user (furthermore, it is not a user centric approach either to ask the user to provide such attributes). This has implications that will depend on the nature and trust requirements of the consumer service, such as the level of assurance of the electronic identity notified according to the eIDAS regulation. Most basic services can be considered safe, as cheating would go against the user's interests, but on others the user might try to cheat by providing false data, if impersonating someone else can result in a benefit. Due to this, both competent authorities –requester and provider-must evaluate the risk and impact of a user having unauthorised access to or unlawfully using data from another citizen, resulting from a faulty identity/record matching. It might happen that the provider service under this situation cannot accept any user-provided input for the record matching process and must rely solely on the eIDAS provided data or raise an error state. This requirement could raise the number of false negatives, affecting the capability to offer service to a substantial share of citizens.

It must be noted that the eIDAS MDS should be enough to resolve most of the matchings, as the chances of a user benefitting from someone else who shares the same name, surname and birth date are small, but the risk is still there. However, a person may have different eIDAS digital identities with small differences in the name and surname, because they can be registered differently depending on the Member State naming rules (second family names, patronymic names, middle names, composed

[10] It is to be noted that the PersonIdentifier ***may*** not only change ***depending on the country***, but changes necessarily for each eIDAS notified eID used, i.e. it can also change for the same country if the user uses different notified eIDs of this country and necessarily always changes if the user is using a notified eIDAS eID of another MS.

names, etc.) Therefore, as some services could not accept this risk, these situations must be analysed by the concerned competent authority specifically under the conditions of the offered service.

In the USI model, the challenge regarding the transitivity of identity is reduced since the user is identifying both at the requester's portal and the provider's portal, so it is not necessary to rely on additional parameters for the record matching to be required by the data consumer. However, both sides need to trust that they have actually identified the same user, considering the possible false negative and false positive cases of identity matching. On one hand, as introduced in the former section, this issue needs to be carefully analysed, as for the IM model. The situation described above for the IM model can be applied here as well, but with less implications. In this case (USI pattern), both the user and the second citizen must collude or act in coordination, as the latter will authenticate on the data provider side after the former has authenticated on the data consumer side. In this case it is the user and the second citizen who are solely liable for the fraud. On the other hand, the same person could be identified as different persons on each side, because of their respective identity matching processes and the electronic identities used by the user in each portal. The risks for the data consumer business logic are the same, but it has less legal implications for the data provider, as it won't be unlawfully accessing citizen data and delivering it to an unauthorised party (unless the collusion attack mentioned above takes place successfully). In any case, from the security and technical point of view, the situation is analogue to the case described above for IM model and the same recommendations should be followed.

In the VC model, since the digital wallet is linked to a user's digital identity and there is not any transitivity of identity, no trust challenges are found in these regards. The only thing that applies is the same as for the USI pattern regarding the risks for double authentication, and the formerly introduced necessary differentiation between holder and subject. If the data consumer does not check that the identity of the citizen that does the authentication and the identity inside the provided VC data are the same, risk exists for data to be obtained in a fraudulent manner. This can be mitigated thanks to the cryptographic capabilities of the wallet, by designing a process where the wallet keys are generated and bound immediately to an identity under a controlled environment. All trusted data providers would need to limit their data issuing only to the wallet associated with the identity of the citizen that authenticated on the issuer; that is, requesting the subject's identity data and checking against the local identity before authorising to issue any data (as in IM/USI cases), making the wallet effectively bound to a single identity (of course, the user can still get data issued from other sources to the wallet, as far as the sources trust it, but those VCs would be out of the trust circle, so any data consumer would discard them)[11]. In any case, this approach would depend on the proper implementation by all the issuers of secure communication protocols with the wallets (in order to avoid man-in-the-middle attacks) and proper identity matching of the wallet holder requesting the evidence, so the first approach of putting the matching effort on the consumer seems easier to deploy and leaves the responsibility on the hands of the party interested on granting this.

3.2.3 Preview

The user should be able to preview the issued evidence to be incorporated to the procedure in order to cancel or confirm that incorporation.

[11] The verifier (requestor) should also always verify the evidences / attestations that it accepts, i.e. verify whether the user authenticated is the same as the one the evidence concerns as well as verifying the integrity and provenance from a trusted issuer (e.g. signature information).

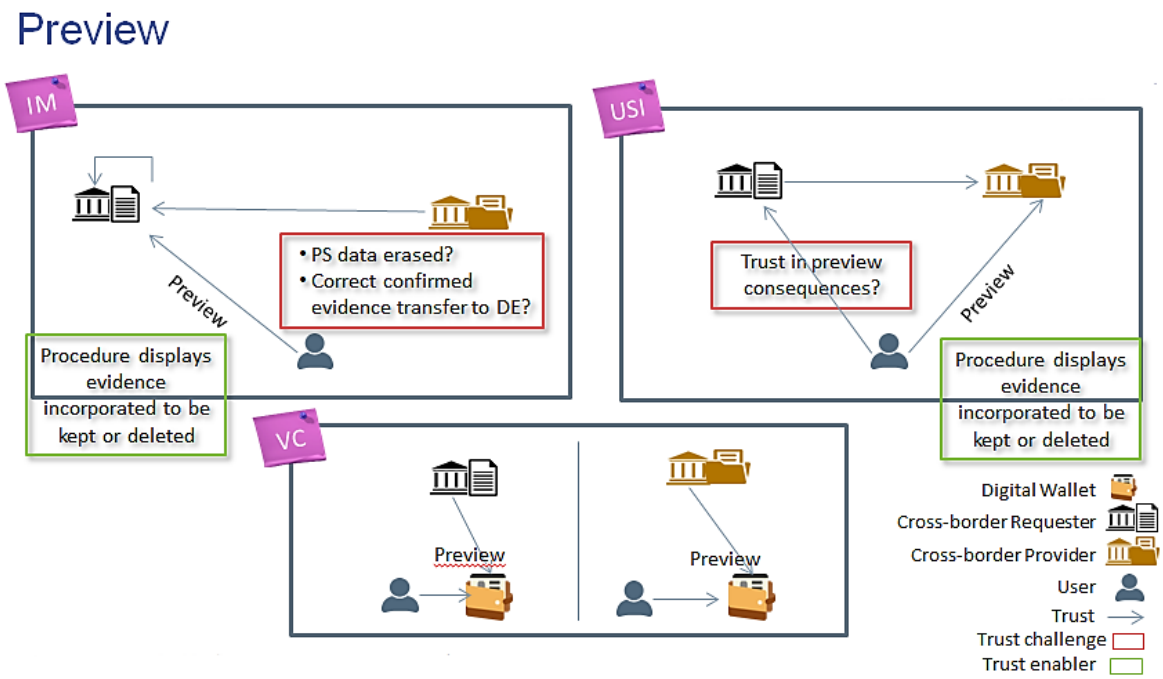

Figure 19: Preview

In the IM model the preview happens in the requester's country, so the data transference abroad has been made before the user decided to transfer the evidence, although the user may cancel the incorporation of the evidence to the application procedure. Besides, in both cases - whether the user confirms or cancels the evidence incorporation to the procedure- the provider and the user need to trust that the evidence data does not remain stored in any temporal space. In the case of the user's confirmation, the provider needs to trust that the evidence is properly incorporated to the application procedure with all due guarantees (i.e. the user needs to trust that the data requestor shows the data exactly as transferred, does not alter any data at any point in time, does not share any data without consent, deletes all personal data as soon as it is not lawfully allowed to keep this data…). This challenge may be mitigated by showing to the user the attached evidence just before submitting the application. However, there is no proper mitigation measure to avoid transferring the evidence abroad when it will not be finally incorporated to the procedure because of the user's cancellation.

In the USI model, the preview is under the provider's control, so there is not a need to keep it as a separate functionality. In this model both user and requester need to trust that the consequences of the preview are correctly transferred by the provider to the requester, since the user loses control on (is expected to rely in such correct transfer of) the evidence after the cancellation or the confirmation of its incorporation to the procedure. This challenge may be also mitigated by finally showing at the requester's portal the cancellation event or the confirmed evidence for the user to double-check.

In the VC model, the use of digital wallet includes a preview functionality both to store and to read the evidence. That is, the preview happens on the user's domain, the wallet, both in the process of the transfer from the issuer that is authorized by the user, and right before asking for authorization to transfer the evidence to a consumer, so there is no trust challenge in these regards because the user is always in the middle and with control of the data flows, although the aspect of user trust in the wallet (correct implementation of preview function not leaking user's information, etc,) is also relevant here.

3.2.4 Delegation of evidence disambiguation

Since the record matching to locate evidence related to cross-border users is not a simple task, sometimes multiple evidences are located for a single request. For instance, when the user has several

tertiary academic diplomas issued by a competent authority but only one is relevant for the procedure. To solve this issue, some solutions rely on the user to disambiguate and select the appropriate evidence relevant to the procedure. For instance, for users to request the birth certificate of one of their children, the user needs to select the one to incorporate to the procedure among all the children's certificates. As a general rule, it must be noted that here there is a theoretical conflict between the data minimization principle - the minimum amount of information to complete the task should be revealed- and the need for the user to examine the evidence to be able to disambiguate (as long as the multiple evidences are only shown to the user himself and not already transferred to a CA there is not an issue with the data minimization principle). The three models have different levels of sensitivity in this regard, so it is important to define a model that allows revealing only the minimum amount of information needed to ensure that all the evidences can be differentiated.

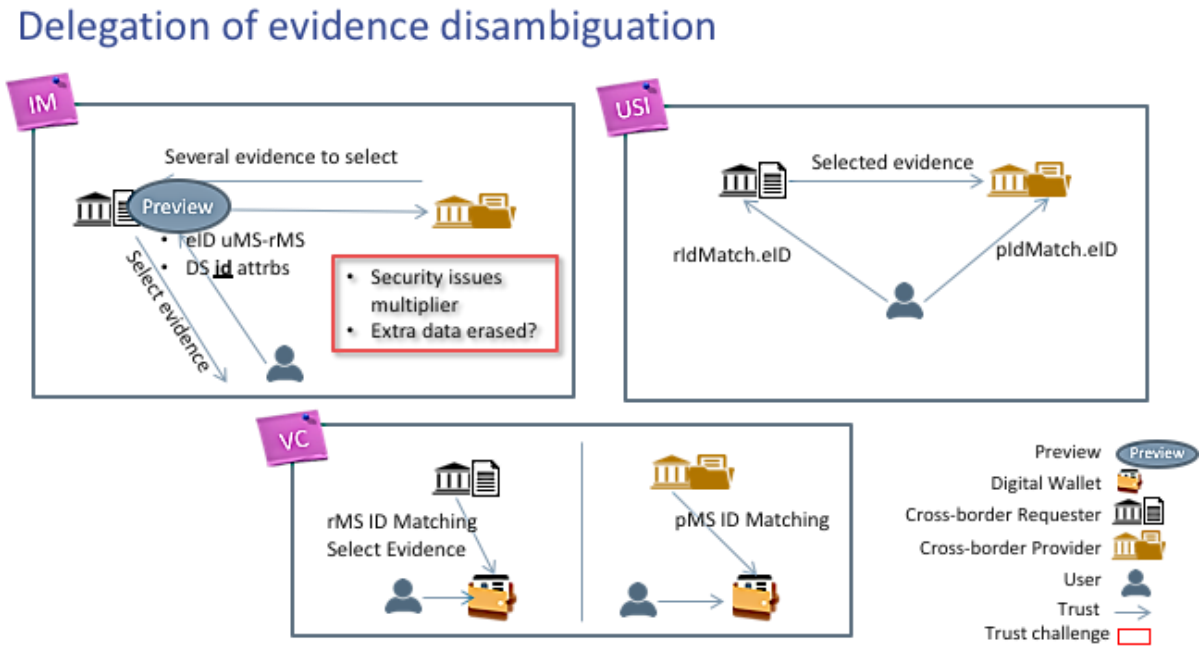

Figure 20: Delegation of Evidence Disambiguation

In the IM model, the SDG proposed solution is sending to the cross-border preview space all the evidences for the user to select the correct one. In this case, all the trust challenges previously highlighted are multiplied by the number of evidences transferred for such selection, so given the sensitivity of the task, strong security measures and a common legal framework to ensure this transfer can happen safely and legally must be established. There could be data services with specific additional parameters to disambiguate a potential multiple record matching, but this solution requires the user to know exactly the values used by the registry in the different records (e.g. the exact qualification name or qualification identifier), which could be difficult to know in advance.

However, this is not the case for the USI and VC models because the user directly selects the evidence before transferring it to the requester's country. As the evidence never leaves the issuing legal domain, those models have less requirements, but they nevertheless need to take care that the information is displayed to the user only after proper authentication and successful record matching.

3.2.5 Evidence validity

The requester needs evidence valid at the time it is required by the procedure. Some types of evidence are valid forever (academic diploma), others have a fixed validity period (annual tax declaration), and others can change on a daily basis (absence of criminal record). But even forever valid evidence might

be revoked in case of any administrative or court decision (fraud detected regarding an academic diploma).

In the case of the IM and USI models, the freshness of the evidence is guaranteed because it is issued at the moment of the request (or is valid at the moment of actual transfer in case of USI pattern and interrupted procedures). However, in the case of the VC model the evidence might be issued in a different time, so the requester needs to trust the evidence is up to date. For mitigating this trust challenge, a verifiable credential should include metadata to check the expiration date or the credential status, for instance with the help of a revocation list allocated in the ledger to avoid creating centralised bottlenecks; its metadata may also provide a reference to a refresh service that eases for users the refreshing of their credential information with only a click for their consent.

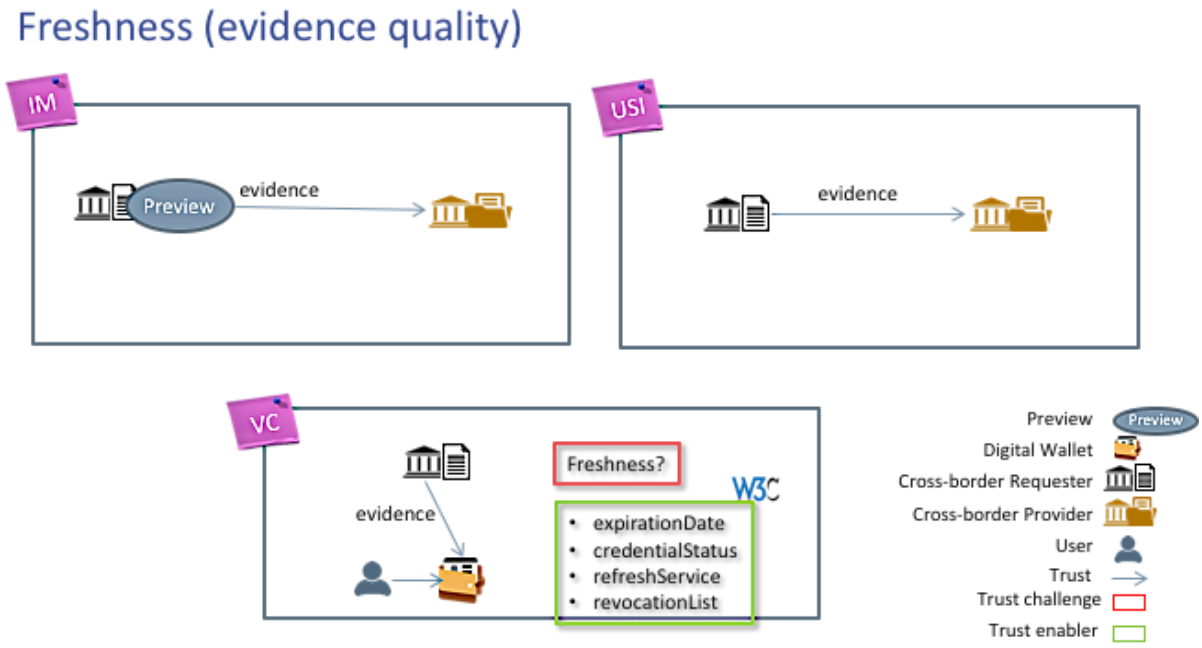

Figure 21: Freshness (Evidence quality)

3.2.6 Powers and Mandates

When the user acts for the representation of legal person or another natural person, as a grandchild acting on behalf of his/her grandmother, the public service needs to know the specific mandates for that representation. DE4A has reused the approach used by the SEMPER project, where mandates are represented as the list of public services that the representative is entitled to access on behalf of the represented person, i.e. the access policy. The access policy is created by the identity provider that grants the representation powers, so in the SEMPER project the access policy is part of the response of the identity provider that uses an eIDAS node for cross-border identification. This access policy could be extended by including as well the canonical evidence types that could be asked by the representative. An alternative is providing the access policy as a type of canonical evidence, which could enable the provision of access policies by a third country. On the hand, the access policy could be also implemented in the VC pattern as part of the DID document associated to the eWallet or as a new credential type.

In any case, the trust challenge is the access policy, since for the mutual recognition of mandates there is a need of commonly agreed semantics and legal grounds. This trust would be provided by extending the response of the identity provider by the eIDAS technical group in charge of the eIDAS node specifications and the eIDAS Toolbox proposed in the eIDAS regulation amendment proposal. If the access policy is implemented as a canonical evidence type, it should be included in some European

regulation to provide the required legal grounds. Nevertheless, the responsibility to decide if a representative has access to an evidence in the name of a represented entity or can proceed with a procedure in their name, stays under the sole responsibility of the respective responsible MS.

DE4A has not analysed the trust challenges and anchors implementing mandates under the USI pattern.

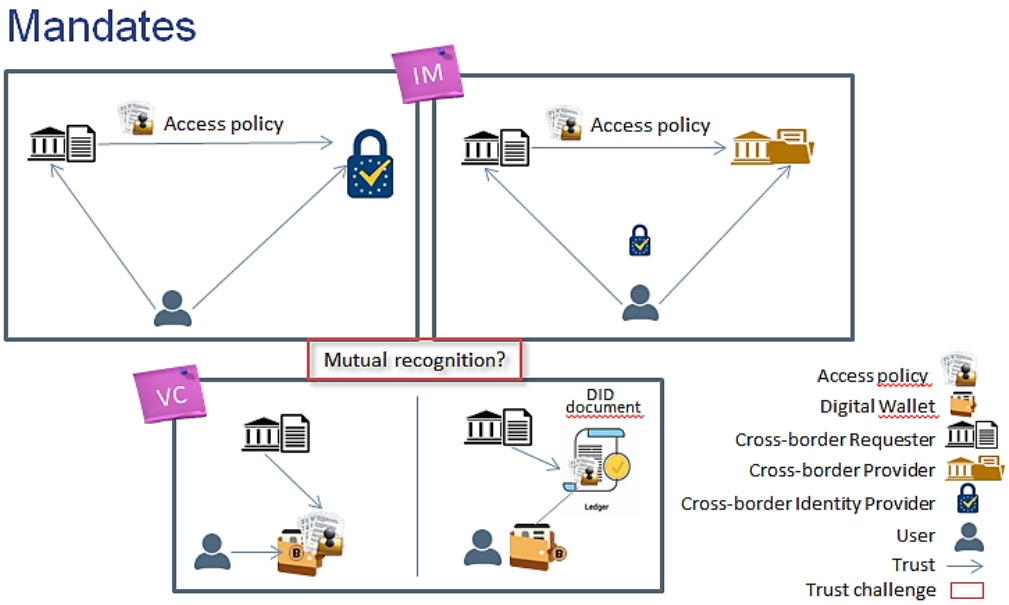

Figure 22: Mandates

3.3 Technical trust anchors

The three models under the comparison analysis –IM, USI, VC- also include some technical assets that acts as trust anchors. In this sense, an architectural pattern relies on these technical anchors for providing trust. In this section there is a comparison between the technical anchors used by the three patterns to provide trust regarding specific aspects.

3.3.1 Identity of participants

Key trust anchors are the technical assets to guarantee the identity of the participants in the evidence exchange.

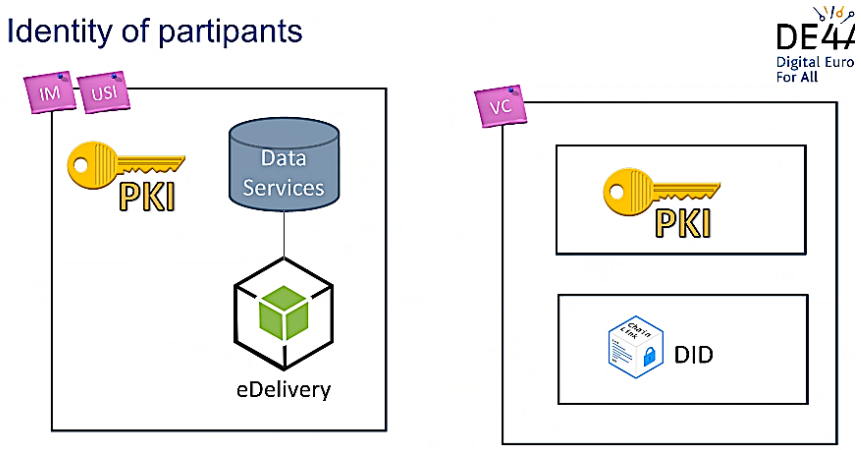

Figure 23: Identity of participants

IM and USI patterns rely on a Public Key Infrastructure (PKI) to guarantee the identity of participants while in VC pattern, stakeholders such as Issuers can have a public DID in a blockchain-based registry (Trusted Issuer Registry in EBSI) that can be verified (PKI is also used in VC pattern when (advanced/qualified) eSeals are used to sign issued evidences). The PKI provides a management structure and mechanisms to allow both data consumers and providers to trustfully publish their identity data and to securely verify the identity of other entities they interact with. For the IM and USI patterns, the identity of participants in the eDelivery network are guaranteed by a vertical PKI, which has a root of trust that issues digital certificates for such participants, for both requesting and providing services. Each participant in the eDelivery network publishes their data on a Service Metadata Provider for the other participants to reach the source of the metadata to verify the identity.

In the case of the VC pattern, the identity of participants such as Issuers or Verifiers relies on the use of Decentralised Identifiers (DID). The DE4A VC implementation, according to the European Blockchain Services Infrastructure (EBSI), is supported by decentralised means of access and verification, as it uses a Decentralised Identifier (DID) infrastructure, allowing for identity metadata and keys of e.g. issuing authorities to be published on a registry in the ledger for any other party to check against.

Regarding the cross-border user identity, the DE4A project uses the current eIDAS network with eIDs issued by Member States for users. The eIDAS notified identity schemes provide the needed trust on the validity of the provided identity attributes according to the corresponding level of assurance.

In the three models, the registration process and the maintenance process of the technical trust anchors for identifying the participants are essential for that trust.

3.3.2 Evidence security

Key trust anchors are also the technical assets that guarantee the security of the evidence during its exchange.

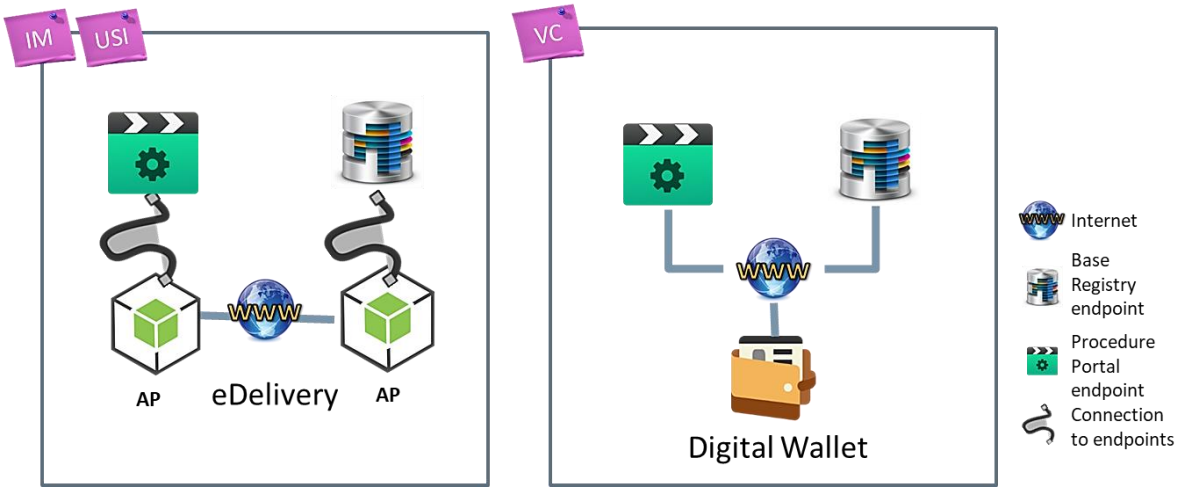

Figure 24: Evidence Security

In the case of the IM and USI patterns, the exchange uses three networks: an internal network between the procedure portal and the requester's eDelivery node, an internal network between the base registry and the provider's eDelivery node, and the Internet connection between both eDelivery nodes. The latter requires greater protection against security threats since resources available through Internet are constantly exposed to cyber-attacks, so services exposed to Internet through the eDelivery nodes and the eDelivery nodes themselves are both technical anchors and assets to protect: for this reason, eDelivery protocol is considered secure as it establishes that payloads exchanged between Access Points are encrypted and signed. In this aspect, the IM model has a better security posture, because all the communications are back-channel machine-to-machine communications, so the interfaces exposed to the internet can be better isolated as the list of trusted requestors is well-known

and limited. The USI pattern has some interfaces that are front channel, which means that they need to be open to any client machine on the Internet (they require user authentication, of course, but they are nevertheless more vulnerable to Denial-of-Service attacks) and thus cannot be as isolated as on the IM model. In any case, the most important point is that the data is never delivered to the user for the transit in any of the two models.

In the case of VC, the evidence security relies heavily on the digital wallet implementation, specifically on the protocols to exchange evidence securely with either procedure portals or base registries, and on the local storage of the evidence. Such exchange always involves the Internet network and the data travels to the user and from the user, so the only defence against eavesdroppers are the secure socket technologies and specific messaging mechanisms to establish trust from wallet to Issuer/Verifier server-side components[12] (whereas IM and USI can add more in-depth security for data leaks). Despite this, it must be noted that the needs are not so critical for this case as for IM and USI because the data that can be transferred on these channels relates only to the authenticating user, not to any requested user. Also, the digital wallet is not implemented as a network resource constantly connected to internet, but only under the user's demand to download or upload evidence. So, the user can choose not to connect to not-trusted requestor/providers, and the attack window on the resource is dramatically reduced.

The other aspect that needs to be commented is the data storage security. For the USI and IM models, data source is always in a remote server under the control of an organisation which is tasked in providing of keeping it. Since they keep large amounts of data for many users, they are first-level targets for attackers, so they need to implement strict data management and security procedures, sometimes even including random audits of the data to check for unnoticed tampering, which is normally the case with governmental-level security infrastructures and procedures. Decentralised storage on the user's domain (wallet) shifts this risk to the client side, but at the same time adds new concerns as vulnerabilities on the wallet technology could be exploited by malicious attackers and for connections established based on reading QR codes risks of 'shoulder-attack' also exist. Sensitivity of the data and procedures involved are also relevant to consider in defining the acceptable uses of wallets or the specific security countermeasures that need to be in place by design. Reaching each user individually has more cost for an attacker, but the usage of automation and targeting thousands of users at a time is still a risk (as phishing campaigns show), and the user is less trained or has the means to keep the data secure and avoid leaks. Tampering is less of an issue, if the data is signed by the issuer, but still requires a good revocation system to make sure any vulnerability detected in the issuer implementation allows to quickly void any flawed issued data and prevent for it to be consumed.

3.3.3 Evidence freshness

In the IM and USI patterns, the evidence validity is guaranteed since it is issued at request time. The technical anchors behind such guarantee are a proper design of the request and response eDelivery messages and the quality of the contents of the Information Desk (IDK), that provides the endpoint for the message exchange.

As explained in the previous section, evidence validity is one of the trust challenges in the VC model, so pure "cold" digital wallets cannot provide the required mitigation to such a challenge, but "hot" or "hybrid" implementations. However, as explained in the previous point, digital wallets permanently connected to the Internet ("hot" wallets) pose a risk to the security of evidences, so hybrid solutions are the most appropriate. Some initiatives exist to define mechanisms to allow fully online wallets where the owner can decide which consumers can have access to which data and at which times.

[12] C.f. DIDComm messaging (http://identity.foundation/didcomm-messaging/spec), OpenID Connect for Verifiable presentations (https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0.html).

Under the W3C VC specification, the freshness service along with the credential status service can be used by hot or hybrid implementations; the expiration date property and the revocation service can be used by any wallet implementation. All of them are essential as technical anchors to guarantee the validity of the evidence in a usable way for users and competent authorities.

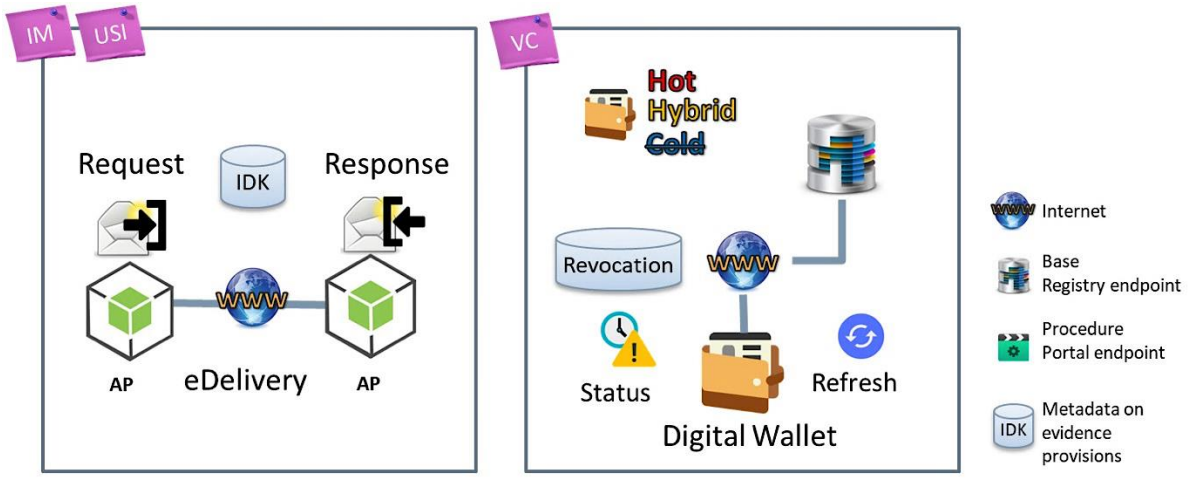

Figure 25: Evidence Freshness (online services)

3.4 Further research questions

This chapter has covered the main trust challenges and technical anchors, but there remain several open questions to compare the three trust models for the evidence exchange.

The first open question regards how the trust model may impact on the perception of trust, because not every trust or mistrust factor is real since it depends on the stakeholder's perception. So, what are the factors to improve the perception of trust in each model? How do they differ?

On the other hand, the interoperability agreements are key factors to improve the trust, since they provide a common framework that is well known by all the stakeholders. So, what are the key interoperability agreements for the trust in each evidence exchange pattern? How do they differ? Are these interoperability agreements enough to provide trust?

Besides, trust needs to be proven, so each architectural pattern for the evidence exchange needs a particular audit model to check the trust challenges and enablers. So, what audit model is needed as a trust anchor for each evidence exchange pattern? How do they differ?

Finally, the new European Digital Identity Wallet proposed in the revision of the eIDAS Regulation could provide further guarantees to the identified trust challenges, so the question arises of which requirements should be adopted by this Wallet and new trust services to minimize trust issues in the evidence exchange between cross-border competent authorities.

4 Self-Sovereign Identity Solution

4.1 DE4A Self-Sovereign Identity supporting framework

This section provides updated information on the Self-Sovereign identity supporting solution beyond that which was previously included in section 4 of D2.2 [1]. Its design can be considered a Solution Architecture for the Verifiable Credentials pattern addressed in section 2.1.3 and previously in section 3.3. of D2.5 [6]. The actual implementation of the Self-Sovereign identity framework has been addressed in related task of WP5 "DE4A Common Component Design & Development Work Package". In particular, this section provides more details on the underlying technology enabling the realization in practice of the VC patterns under the self-sovereign paradigm, the use of European standards, blockchain infrastructure and services with which DE4A integrates EBSI-ESSIF and the issues that arise from this. DE4A follows a subset of the terminology used in EBSI [13].

The Self-Sovereign identity framework implements the exchange of Verifiable Credentials[20], including their user-centric control, and its developed components and services are validated in the Diploma Recognition scenario of "Studying Abroad" pilot within DE4A. The framework relies on the adoption of a Self-Sovereign Identity (SSI) solution as one of the key pillars of the approach. In the following sections, the final architecture that is being implemented and its components are explained.

The purpose of using blockchain technology in DE4A as trust anchor comprises several aspects that DE4A leverages for the benefit of its Verifiable Credentials-based use case and to generate valuable learning for its stakeholders. Those intrinsic features that blockchain provides to DE4A are the following59[1]:

- Immutability: as any blockchain transaction becomes a permanent digital record stored in the ledger.
- Traceability: reference data related to issuers or to exchanges of verifiable attestations, presented as Verifiable Credentials can be notarised in a privacy-preserving manner on blockchain ledger allowing to have trusted digital audit trails that can be reviewed by others (as immutable proof of authenticity/integrity).
- Integrity: the immutability aspect and the traceability with trusted digital audit trail provide the data stored with a high level of incorruptibility that grants data integrity.
- Transparency: as a reliable source of truth which removes any bias and allows instant verifications (in our case about trustworthiness of issuers of Verifiable Credentials)

During the first stages of the project, in the design phase, EBSI infrastructure was selected by the consortium as being very relevant and the most suitable to use as distributed trust anchor to integrate issuer information. One of the main reasons behind this decision is it is strongly supported by MS in the European Blockchain Partnership (EBP). This enables DE4A solution to be more portable and interoperable in case MS decide to adopt these services in the future, aligning the full self-sovereign life-cycle (involving Issuers of Verifiable Credentials, users of 'Edge Client' wallets as Holders of such credentials and Verifiers of Verifiable Presentations) as much as possible with the EBSI specifications (e.g. EBSI Verifiable Credentials Playbook [21]) and APIs [22] through which integration with EBSI is achieved [23].

DE4A also evaluated other advantages of using EBSI-ESSIF for a cross-border pilot for public sector, which can be classified depending on their nature as technical and non-technical. Among the reasons are:

- use of an infrastructure already defined and agreed by all participant MS (those in DE4A Diploma Recognition use case as well as MS in EBSI/ESSIF and in other EBSI Early Adopters Diploma use case projects like DE4A),

- Infrastructure (EBSI nodes) is maintained by key EU stakeholders and ESBI/ESSIF functionalities will continue to be evolved beyond the current v2.0 version, ensuring long-term support beyond DE4A project which is an important factor for sustainability of the work carried out in the project,
- highest level of trustworthiness considering the inherent EBSI blockchain features mentioned further above coupled with strong guarantees of compliance with current (GDPR) and future regulations (revision of eIDAS) and respect to European values,
- documentation and supporting services available (email, regular webinars, wiki…) that helps any adopter,
- robust and tested infrastructure, with a continuous availability (24x7).

Furthermore, the timing of Early Adopters programme and releases of ESSIF v2.0 were verified to be compatible with DE4A development and integration timelines and were included in the solution task planning.

After analysing the reasons and circumstances already mentioned, the Consortium decided to use EBSI infrastructure through ESSIF-provided services and APIs. This use of the ESSIF Services and the underlying EBSI blockchain infrastructure provides clear advantages (as listed above) over other possible solutions, such as the deployment of an ad-hoc blockchain infrastructure by the DE4A project.

It is worth noting that, on one hand, there is an EBSI-ESSIF infrastructure and middle-tier services being used as underlying framework and, on the other hand, that the project is extending this existing framework at application level (or Business Apps as depicted in EBSI architecture[15]) according to the business requirements and logic of DE4A, following the SSI paradigm and standards.

4.1.1 Architecture

Figure 26 represents the architecture of the Self-Sovereign identity supporting framework in DE4A.

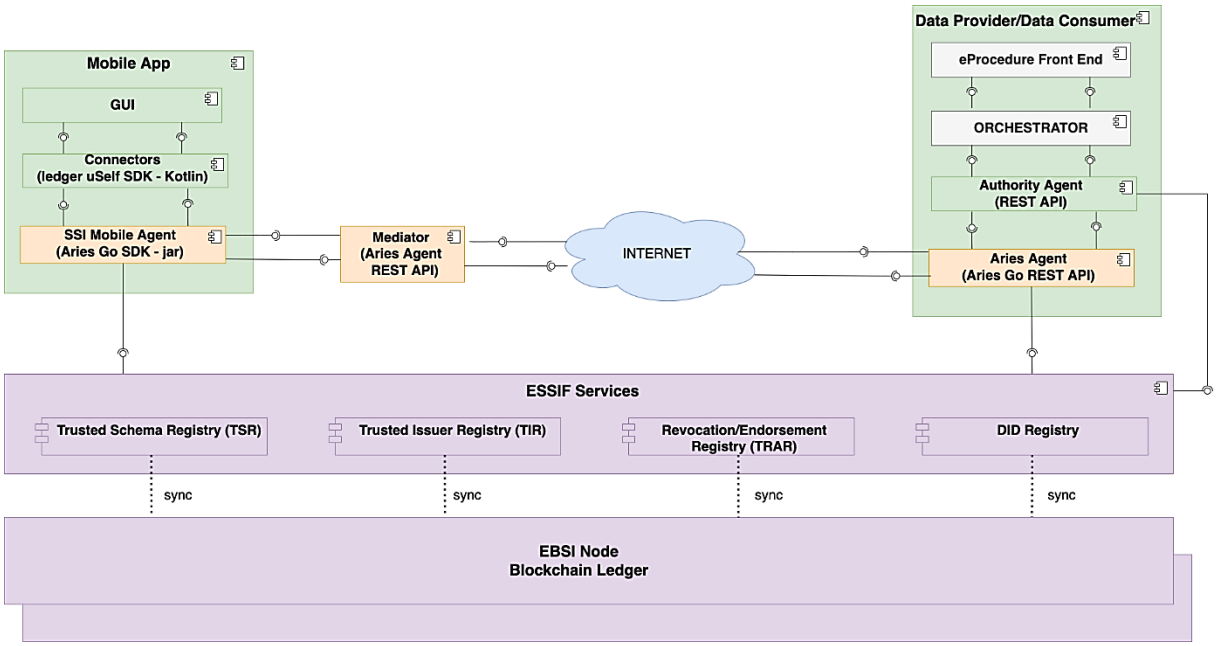

Figure 26: Self-Sovereign identity supporting framework design in DE4A

There are some distinctions to make depending on the background colour. The orange components with the suffix “Aries Agent” are those that are based on the SSI framework Hyperledger Aries (Go version). With green background components that DE4A implemented from scratch are indicated. On the bottom part of Figure 26 the ESSIF components are depicted providing the services with which the DE4A SSI solution is being integrated (see Section 4.2) and which abstract the underlying (complexity of) EBSI blockchain infrastructure, making it effectively transparent to DE4A high-level applications.

4.1.2 Components

The components of the DE4A Self-Sovereign identity supporting framework are the following:

Mobile App: Mobile device wallet application that will be used by citizens. It is implemented on Android operating system, and it includes a Graphical User Interface (GUI) for the end users to interact with the SSI solution during the pilot. It must be downloaded in each pilot participant´s mobile device. This application contains:

- **Mobile GUI**: Icons-based interface that allows users to interact with the different components of the solution using their mobile device. It provides students with different screens guiding them through the process, focusing on the usability of the application.
- **Mobile Connectors**: this software layer is devoted to facilitate the use of the internal SSI Mobile Agent (Hyperledger Aries Go) for the GUI described above.
- **SSI Mobile Agent:** component installed on the mobile side based on the underlying technology provided by Hyperledger Aries Go, used by DE4A for adopting an SSI solution**.**

Mediator: another set of components based on Hyperledger Aries Go, needed for adopting the SSI solution that manage the messages (evidence exchanges, notifications, …) between the mobile devices and the end-points (DP/DC). This Mediator will handle all requests of the different mobile devices that are connected to the DP/DC, becoming the gateway of the communications to manage all mobile connections.

Data Provider/Data consumer: any of the endpoints involved in the DE4A environment. For each of them that participates on the VC pattern use case an instance of the following must be installed:

- **Authority Agent:** Component deployed and integrated in the back-end of the service and evidence providers (DP/DC) and which is responsible for the interactions with other SSI-agents on behalf of the endpoints. It wraps all functionalities needed for different protocols used during SSI workflows and simplifies the complex interactions that are necessary for: verifiable credential issuance, verifiable presentation verification and DID communication.
- **Aries Agent:** third component based on the Hyperledger Aries GO needed for the adoption of the SSI approach. This component is deployed and used in the back-end of the evidence providers (DP/DC). As the Mobile Agent, it provides the mechanisms for managing smoothly the communications between the mobile devices and the data provider authority (issuer) or data consumer (verifier).

ESSIF Services: the catalogue of ESSIF services includes: the Trusted Schema Registry (TSR) that contains JSON schemas of VCs, the Trusted Issuer Registry (TIR), that includes information about issuers and which types of VCs they are accredited to issue and the DID Registry, which manages all the DIDs and DID Documents in the platform.

All these four ESSIF services mentioned above are synchronized with the EBSI blockchain ledger infrastructure, communicating with the EBSI nodes.

4.2 EBSI/ESSIF integration

European Blockchain Services Infrastructure (EBSI) and European Self-Sovereign Identity Framework (ESSIF) infrastructure and governance framework represent a single point of truth for EU-wide self-sovereign identity public services compatible with current legal regulations, i.e. GDPR. A public site with detailed functional documentation on EBSI v2 is available online [14] (more technical documentation is available for integrators in a Wiki for community of participants in the Early Adopters programme, not yet public).

The integration with EBSI/ESSIF initiative is addressed through the development of middleware layers (EBSI connector) between their infrastructure (Core Services API, see [15]) and the clients/agents to be connected to the European blockchain infrastructure (shown in Figure 27). For that purpose, both

authority and edge SSI agents can connect to/use the EBSI ledger for the means of identity verification instead of a custom setup distributed ledger. This way, EBSI/ESSIF ledger/framework-based services (such as TIR and TSR) will be leveraged for their use in a real-world DE4A use case.

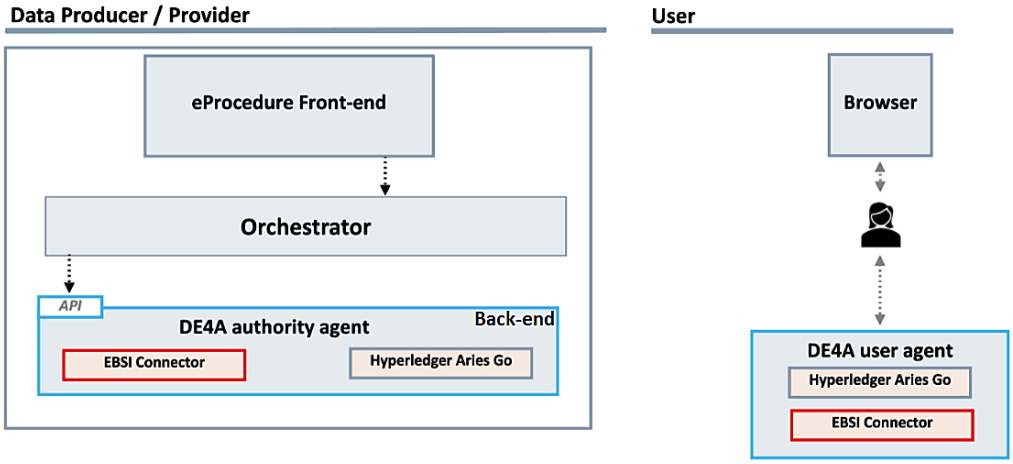

Figure 27: Core technical components of SSI agents

To connect and be interoperable with the EBSI/ESSIF interfaces and compliant wallets, certain actions (e.g. onboarding process) must be taken and existing protocols implemented (e.g. anchoring of DID documents on the EBSI ledger, adding the DID of the Data Provider to the EBSI/ESSIF Trusted Issuer Registry etc.). For that purpose, EBSI/ESSIF requires the so-called onboarding process of actors (Trusted Accreditation Organisations -TAO- and Trusted Issuers TI) to the EBSI Circle-of-Trust.

The SSI agents should therefore, from the user/business side implement all the necessary steps of the onboarding process specified in the EBSI/ESSIF Community Documentation. At the moment, DE4A is leveraging open-source projects developing libraries and products specifically focused on the EBSI/ESSIF integration and protocols, i.e., walt.id (see [16]), integrated in DE4A's EBSI Connector, see figure below depicting the chain of integrations towards EBSI/ESSIF :

Figure 28: DE4A-EBSI/ESSIF Integration Diagram

4.2.1 Alignment with EBSI/ESSIF

Since EBSI/ESSIF is still under development with frequent releases of new versions, many details are subject to change over time. Specifically, DE4A integrates with the following services provided by ESSIF v2.0 [22]:

1. API of ESSIF v2 TIR component
2. API of ESSIF v2 DID registry

DE4A is committed to maintain a high level of alignment with EBSI/ESSIF. This is achieved through the following actions:

- DE4A authority agents generate EBSI-compliant public DIDs and respective DID documents
- DE4A authority agents anchor public DIDs of DP and DC on EBSI ledger/blockchain invoking through walt.id library the ESSIF DID Registry
- DE4A authority agent of DP will register the EBSI-compliant public DID in the TIR by means of the EBSI support services
- DE4A authority agent of DC will verify that EBSI-compliant public DID of DP is registered in the TIR by invoking through walt.id library the ESSIF TIR Registry
- DE4A authority agents of DP will sign evidences in the VC format with the EBSI-compliant public DID

Due to the specifications agreed for DE4A VC pattern implementation, the following differences are noted with the general EBSI/ESSIF approach (not affecting the intended interoperability and presented to and agreed with EBSI/ESSIF as part of the alignment process):

- DE4A edge agent does not generate public DIDs for students
- DE4A edge agent does not anchor student DIDs on the EBSI ledger
- DE4A does not use Verifiable IDs
- DE4A uses eIDAS minimal dataset for the purpose of identifying the holder of the VC
- DE4A uses eIDAS to authenticate students
- DE4A does not use OpenID Connect
- DE4A does not eSeal VCs with eIDAS eSeal certificate

As explained in the previous section, interoperability between Aries Go agent and EBSI/ESSIF is achieved by configuration of Aries Go agent and using open-source library walt.id [17].

Aries Go configuration

Aries Go SSI agent must be connected to the EBSI ledger to resolve and have access to EBSI DID documents. This is achieved through its configuration: EBSI resolver must be added in the configuration file of the Aries agent (HTTP_DID_RESOLVER=ebsi@https://api.preprod.ebsi.eu/did-registry/v2/identifiers). By doing that, the Aries Go agent can resolve DID documents anchored on the EBSI ledger.

walt.id

Open-source library walt.id implements all the specified workflows with the EBSI API and removes the complexity for the user. walt.id library is incorporated in the Aries Go agent within the EBSI connector component. All the calls to the EBSI connector are done during the start-up process of the Aries Go agent, while only EBSI resolver is used during the later ongoing processes, e.g., issuing VCs and validating VPs. All the actions are performed only on authority agents since DE4A does not anchor students' DIDs, i.e., edge agents.

walt.id is used for generating EBSI-compliant DID documents and anchoring them on the EBSI ledger. It is planned that walt.id library can also be used for TIR and TSR actions (see below). The following functionalities of walt.id are used in the start-up process (in chronological order):

1. Generation of two key pairs: Secp256k1 (to sign transactions for EBSI ledger)[18] and Ed25519 [19](for EBSI-compliant DID docs)
2. Creation of EBSI-compliant DID doc using Ed25519 key pair
3. ESSIF onboarding with created DID doc
4. ESSIF authorization with created DID doc
5. ESSIF DID registration with created DID doc - Secp256k1 key pair is used to sign Ethereum-based EBSI transaction
6. Exporting of Ed25519 key pair

Since Aries Go agent needs keys generated in walt.id library, the following calls are performed on Aries agent during start up:

1. Importing Ed25519 key pair into Aries Go internal Key Management Service storage

During the repeating processes of the Aries Go agent, EBSI/ESSIF is used in the following calls:

1. Issuance of a VC-based Diploma: signing VCs with EBSI DID using Aries Go REST API call (resolver fetches the EBSI DID document from EBSI ledger)
2. Diploma verification: validating VPs using Aries Go REST API call (resolver fetches the EBSI DID document from EBSI ledger)

In the second phase of the project (final pilot iteration), walt.id library will be used for the onboarding process of issuers - generating the DID document of the organisation/issuer and anchoring it in the TIR registry. The schema of the VC, based on EDCI, can also be anchored in TSR using walt.id library.

4.2.2 EBSI/ESSIF Integration Challenges

There are several challenges with the EBSI/ESSIF integration, which are being addressed during the different iterations of the development (Agile). These are:

- delays in having EBSI/ESSIF APIs and their final technical documentation available
- dependency on open source walt.id library. The software is going through heavy development and thus many changes and some functionalities, e.g., TSR operations, are yet to be developed
- by validating VCs through an EDCI JSON-LD schema, interdependence with an EDCI model will be established. But such validation is currently a challenge because the EDCI JSON-LD schema is not yet available.

DE4A is currently interoperable with EBSI/EESIF through anchored EBSI-compliant DID documents and signing VCs with EBSI DIDs. While DE4A is advancing successfully to be compliant with the blockchain infrastructure of the European Union and its related SSI framework, there are still a few aspects (see 4.2.1) that may be deemed by future adopters to address (e.g. including support for SIOP standard to facilitate interoperability with stakeholders using federated identity protocols such as OIDC, see section 5 of [23]).

5 Conclusions

This deliverable has addressed multiple aspects related with the establishment and maintenance of trust needed in relation to the five different evidence exchange patterns defined and being implemented in DE4A in the context of the Single Digital Gateway and Once-Only Principle. A key notion that emerges is that trust is a multi-faceted concept which comprises both technical (e.g. trust anchors acting as authoritative sources of information including digitally signed objects like certificates) and non-technical dimensions, including legal provisions in applicable European regulations setting the policy baseline for trust frameworks (covering mutual recognition of the roles of competent authorities, accountability, etc.) as well as organisational and procedural aspects determining how building blocks enabling interoperability are properly configured and maintained by public authorities in charge of their operation also under common governance principles e.g. covering regular assessments as well as incident and change/update management procedures.

In section 2, and taking into account the trust models that were introduced in detail in previous deliverable D2.2[1], these have been further refined by means of a detailed analysis of the trust solutions framework of DE4A, particularized for each of the relevant evidence exchange patterns in the project. It is important to note that in order to understand well the nuances enabling an effective comparison of how the trust-enabling solutions are applied to each pattern, future adopters will need to consider the descriptions provided both from a technical (comprising components and trust anchors) and organisational perspective (e.g. complex sets of trust requirements that need to be satisfied). Common to the majority of the patterns emerges the need to establish and maintain (govern) an explicit and scalable circle of trust, which is a well-established concept underlying the operation of large cross-border federated networks such as eIDAS and which materializes supported on PKI certificates and is projected on a secure communication infrastructure (CEF eDelivery). In this context, the underlying 4-corner trust model of eDelivery is determinant to understand how the trust anchors and technical components are meant to be deployed and function. Given the importance of this trust framework, a specific subsection 2.3 details how DE4A has adopted 4-corner model and the different configuration “set-ups” available to Member States thanks to the flexible design of components like the DE4A Connector and how certificates are configured and managed in DE4A by leveraging as well the CEF PKI Service for the lifecycle of digital certificates used for eDelivery AS4 Gateways and SMPs).

For the Verifiable Credentials pattern, the trust model relies on a somewhat different approach (SSI) where trust anchors are managed in a decentralised manner over reliable pan-European infrastructures and frameworks such as EBSI and ESSIF and will in the future materialize as a new Digital Identity Framework (following the common security and interoperability specifications for digital identity wallets and new ledger-based trust services for certified attestations).

The common structure followed in the analysis of the patterns from the relevant trust perspectives is meant to allow an easy understanding both of the similarities (which are large among patterns relying on eDelivery trust model) as well the differences e.g. in regard to trust assumptions. Furthermore, details are provided in section 2.2 for key trust-enabling functionalities addressed in DE4A pilots like Doing Business Abroad, explaining how trust is enabled and verified for cases of representation through electronic powers and mandates, leveraging results from previous CEF projects like SEMPER[8]. This represents a valuable contribution as it enables future DE4A adopters (e.g. competent authorities) to have at their disposal a more in-depth knowledge of which are the needed trust anchors and components and how they are meant to function together in order to satisfy specific trust requirements in the context of each evidence exchange pattern.

DE4A partners of the Trust Management Models task in which this deliverable is framed, also agreed to include a comparison regarding the trust factor between the three patterns that have been analysed and implemented for the major part of the project (Intermediation, User-Supported Intermediation

and Verifiable Credentials) considering how they can help to address commonly defined trust challenges (Transitivities of explicit request and identity, Preview, Delegation of evidence disambiguation, Evidence validity and Powers and Mandates), as a way of supporting authorities and implementors to select suitable patterns for specific use cases of evidence exchange. The analysis was internally presented for discussion among the partners in two internal workshops and different contributions were incorporated to the final text. A conclusion that results clearly from this exercise is that there is no better or worse pattern in general, but all have specific considerations and points to be taken care of for their trustworthy deployment and operation. Furthermore, selection of a pattern depends on the careful consideration of other factors besides trust, e.g. the level of legal harmonisation, the mutual recognition of stakeholders, the interoperability agreements and barriers, the sensitivity of information to exchange, the security of the networks, etc. This comparative study is highly original and can be further extended in the future by other researchers, as new regulatory and technical developments which can be expected both on the side of the SDGR and the OOTS and the revision of eIDAS regulation for establishing the new EU Digital Identity Framework emerge. This could address some of the identified open questions in section 3.4 regarding factors that can improve the perception of trust in each model, the role of interoperability agreements in each of the trust models and how they can contribute to providing trust, the audit models necessary in each case to verify that trust challenges are being correctly addressed by the different technical components and anchors and, last, but not least, an analysis of requirements relevant in relation to trust-related challenges in the scope of the European Digital Identity Wallets and new trust services enabling trustworthy cross-border exchange of identity and evidences under a user-centric, self-sovereign approach.

In this regard, the deliverable reflects in section 4 how the DE4A Self-Sovereign Identity Supporting Framework has been updated since the previous deliverable (also in the context of work carried out in task of the Common Component and Design Work Package). The provided details on the underlying technology enabling the realization in practice of the VC patterns, the use of European standards and frameworks with which DE4A integrates the framework (EBSI-ESSIF) and the issues that arise from this, is also valuable for future adopters as it provides concrete details from a technical perspective of how this Blockchain Support Framework also acts as a trust solution to realize the Verifiable Credentials pattern.

Considering that sustainability and trust is one of the key factors for DE4A as well as most similar Large Scale Pilots developments and that the goal is for its deliverables to be used also after project end, it becomes relevant to consider the experience in this regard from other similar projects. For example, in LSP STORK there were long discussions between the co-chairs and EC representatives. As a result, EC took responsibility to maintain and update the technical solution / code. It was also agreed that a wide uptake in Member States could not build on bi-lateral agreements between states to trust one another's eID and Level of Trust. That and more was solved by the eIDAS regulation. In DE4A the need for support from EC has been reported, similar to that in LSP STORK.

References

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

[2] D. Reed, M. Sporny, M. Sabadello, D. Longley, C. Allen, Decentralized Identifiers (DIDs) v1.0, W3C Working Draft, W3C, August 2021. https://www.w3.org/TR/did-core/

[3] eDelivery, Connecting Europe Facility (CEF),https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery

[4] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1568968116540&uri=CELEX:32018R1724

[5] Pan-European Public Procurement Online (PEPPOL), https://peppol.eu/

[6] DE4A Deliverable D2.5 Project Start Architecture (PSA) 2nd iteration – also available on the DE4A Wiki, https://www.de4a.eu/project-deliverables

[7] DigiD Machtigen, https://machtigen.digid.nl/

[8] SEMPER project, https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2018-eu-ia-0032

[9] TUG Crossborder Semantic Interoperability of Powers and Mandates, https://graz.pure.elsevier.com/en/projects/eu-semper-crossborder-semantic-interoperability-of-powers-and-man

[10] DE4A Deliverable D4.5 Use Case Definition & Requirements - https://www.de4a.eu/project-deliverables

[11] DE4A Wiki project. DBA use cases, https://wiki.de4a.eu/index.php/DBA_Use_case_definition#Use_cases

[12] CEF eDelivery PKI. Service Offering Document, Version 2.3 (2021) https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service?preview=/82773287/439943709/(CEF%20eDelivery).(PKI).(SOD).(v2.3).pdf

[13] EBSI Terminology. EBSI Documentation. https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/EBSI+Terminology

[14] EBSI Learn section. EBSI Documentation. https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/Learn

[15] Architecture Diagram of EBSI V2. https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/Architecture

[16] SSI Kit for Europe (EBSI & ESSIF). https://docs.walt.id/v/ssikit/ssi-kit/ssi-kit l

[17]walt.id Source Code. https://github.com/walt-id

[18]Ecdsa Secp256k1 Signature 2019. https://w3c-ccg.github.io/lds-ecdsa-secp256k1-2019/

[19]Ed25519 Signature 2018. https://w3c-ccg.github.io/lds-ed25519-2018/

[20]W3C Recommendation. Verifiable Credentials Data Model v1.1. November 2021. https://www.w3.org/TR/vc-data-model/

[21]EBSI Verifiable Credentials Playbook https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Playbook

[22]EBSI API documentation https://api.preprod.ebsi.eu/docs/

[23] DE4A Deliverable D5.8Final Release of DE4A Self-Sovereign Identity Supporting Framework v1.0 https://www.de4a.eu/project-deliverables