D2.2 Initial DE4A Trust Management Models and Blockchain Support Framework

Document Identification			
Status	Final	**Due Date**	31/10/2020
Version	1.0	**Submission Date**	17/11/2020

Related WP	WP2	**Document Reference**	D2.2
Related Deliverable(s)	D2.1, D2.4	**Dissemination Level (*)**	PU
Lead Participant	Atos	**Lead Author**	Nacho González (Atos)
Contributors	Alberto Crespo (Atos), José Antonio Eusamio (MPTFP-SGAD), Ana Rosa Guzmán Carbonell (SGAD), Alexander Bielowski (MINBZK/ICTU), Mavi Cristache (MINBZK /ICTU), Harold Metselaar (MINBZK/ICTU), Francisco José Aragó (UJI), José Traver (UJI),	**Reviewers**	Gérard Soisson (LU) Sven Rostgaard (DIGST)

Disclaimer for Deliverables with dissemination level PUBLIC
This document is issued within the frame and for the purpose of the DE4A project. This project has received funding from the European Union's Horizon2020 Framework Programme under Grant Agreement No. 870635 The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.
[The dissemination of this document reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains. This deliverable is subject to final acceptance by the European Commission.
This document and its content are the property of the DE4A Consortium. The content of all or parts of this document can be used and distributed provided that the DE4A project and the document are properly referenced.
Each DE4A Partner may use this document in conformity with the DE4A Consortium Grant Agreement provisions.
(*) Dissemination level: PU: Public, fully open, e.g. web; CO: Confidential, restricted under conditions set out in Model Grant Agreement; CI: Classified, Int = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

	Markus Triska (BMDW), Arvid Welin (SU), Patrick Öberg (SU), Sofía Paredes (AMA IP), Tiago Mendoça (AMA IP), Tanja Pavleska (JSI), Tomaž Klobučar (JSI), Muhamed Turkanovic (UM), Martina Šestak (UM), Blaž Podgorelec (UM), Boštjan Tovornik (SI-MPA), Alenka Zuzek Nemec (SI-MPA), Katarina Čepon (SI-MPA), Ales Pelan (SI-MPA)		

Keywords:
Trust, blockchain, eIDAS, architecture, SSI

Document information

List of Contributors	
Name	Partner
Alberto Crespo	Atos
Alenka Zuzek Nemec	SI-MPA
Ales Pelan	SI-MPA
Alexander Bielowski	MINBZK /ICTU
Ana Rosa Guzmán Carbonell	MPTFP-SGAD
Arvid Wellin	SU
Blaž Podgorelec	UM
Boštjan Tovornik	SI-MPA
Francisco José Aragó	UJI
Harold Metselaar (MINBZK/ICTU),	MINBZK /ICTU
José Antonio Eusamio	MPTFP-SGAD
José Traver	UJI
Katarina Čepon	SI-MPA
Markus Triska	BMDW
Martina Šestak	UM
Mavi Cristache (MINBZK /ICTU),	MINBZK /ICTU
Muhamed Turkanovic	UM
Nacho González	Atos
Patrick Öberg	SU
Sofía Paredes	AMA IP
Tanja Pavleska	JSI
Tiago Mendoça	AMA IP
Tomaž Klobučar	JSI

Document History			
Version	Date	Change editors	Changes
0.1	23/03/2020	Nacho González (Atos)	Initial version of document
0.2	25/03/2020	Nacho González (Atos)	First draft of ToC
0.2	28/04/2020	Nacho González (Atos)	Refined version of the table of contents
0.3	18/05/2020	Nacho González (Atos)	Refinement of table of contents according to GA discussions
0.4	20/05/2020	Nacho González (Atos)	Updated sections assignements to UM and IJS
0.5	03/06/2020	Nacho González (Atos)	Refined sections 4.2 and 4.3 structure
0.6	04/06/2020	Maria Winter (BMDW)	Case of study: Austria contribution
0.6	06/06/2020	José Eusamio (SGAD)	Case of study: Spain contribution
0.6	07/06/2020	Mavi Cristache (MinBZK)	Case of study: Netherlands contribution
0.6	07/06/2020	Francisco José Aragó (UJI)	eIDAS background

Document History			
			eIDAS bridge eIDAS ID
0.6	10/06/2020	Arvid Welin (SU)	Case of study: Sweden contribution
0.7	14/07/2020	Sofía Paredes (AMA IP)	Case of study: Portugal contribution
0.8	17/09/2020	Tomaz Klobucar (UM)	INATBA and CEF Building Blocks contributions
0.9	10/10/2020	Muhamed Turkanovic (UM) Nacho González (Atos)	Blockchain Support Framework contribution
0.10	11/10/2020	Nacho González (Atos)	General sections (executive summary, introduction and conclusions)
0.11	13/10/2020	Nacho González (Atos)	Format corrections
0.12	27/10/2020	Nacho González (Atos) Alberto Crespo (Atos) Gerard Soisson (CTIE) Sven Rostgaard (DIGST)	Internal review check and changes implementation
0.13	29/10/2020	Nacho González (Atos) Alberto Crespo (Atos)	Consolidation of pre-final version
0.14	29/10/2020	Nacho González (Atos) Alberto Crespo (Atos)	Review of links with references, cross-document references and minor changes.
0.15	30/10/2020	Nacho González (Atos) Alberto Crespo (Atos)	Typos, language correction, spelling & grammar.
0.16	30/10/2020	Nacho González (Atos) Alberto Crespo (Atos)	Sections 3 and 4 corrections. References added.
0.17	05/11/2020	Alberto Crespo (Atos)	eIDAS matching contribution extensión. Format corrections.
0.18	09/11/2020	Nacho González (Atos) Alberto Crespo (Atos)	Finishing conclusions. References adjustements. Format corrections. Text review.
0.19	13/11/2020	Julia Wells (Atos)	Final version for submission
1.0	17/11/2020	Ana Piñuela Marcos (ATOS)	Approval for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Nacho González (ATOS)	29/10/2020
Quality manager	Julia Wells (ATOS)	13/11/2020
Project Coordinator	Ana Piñuela Marcos (ATOS)	17/11/2020

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
ABB	Architecture Building Block
BB	Building Block
CA	Consortium Agreement
CEF	Connecting Europe Facility
CFS	Certificate on the Financial Statements
DoA	Description of Action
DIP	Digital Identity Provider
DLT	Distributed Ledger Technologies
DSI	Digital Service Infrastructure
DSM	Digital Single Market
Dx.y	Deliverable number y, belonging to WP number x
EBSI	European Blockchain Services Infrastructure
EC	European Commission
eIDAS	electronic IDentification, Authentication and trust Services
EIF	European Interoperability Framework
EIF-IS	European Interoperability Framework – Interoperability Strategy
EIRA	European Interoperability Reference Architecture
ERDS	Electronic Registered Delivery Service
ESSIF	European Self-Sovereign Identity Framework
GA	Grant Agreement
IDP	Intermediation Data Platform
ISA	Interoperability Solutions for European Public Administrations
KPI	Key Performance Indicator
LoA	Level of Assurance
MS	Member State
NIF	National Interoperability Framework
OIDC	OpenID Connect
OOTS	Once Only Technical System
PC	Project Coordinator
PKI	Public Key Infrastructure
PM	Person-month
QA	Quality Assurance
QM	Quality Manager
RA	Registration Authority
RASCI	Responsible/Accountable/Supportive/Consulted/Informed
RP	Reporting Period
SAT	Solution Architecture Template

Abbreviation / acronym	Description
SBB	Solution Building Block
SI-CAS	Slovenian Central Authentication System
SI-CeS	Slovenian Central Server-based eSignature system
SI-PEPS	Slovenian eIDAS Node
SML	Service metadata locator
SMP	Service metadata publisher
SOA	Service Oriented Architecture
TES	Trans-European Solution
TL	Task Leader
TOGAF	The Open Group Architecture Framework
TOOP	The Once-Only Principle Project
TSP	Trust Service Provider
VC	Verifiable Credential
WP	Work Package
WPL	Work Package Leader

Executive Summary

This deliverable is a first version of the design of the Trust Management Models and Blockchain Support framework produced in the context of Task 2.2 “Trust Management Models” in “WP2 Architecture vision and framework”. This framework sets the basis in terms of trust management and disruptive technologies adoption (such as blockchain) in DE4A. This deliverable serves as the key design guidelines for the implementation of the DE4A Trust Management Model and Blockchain Framework (D5.7 First Release of DE4A Blockchain Supporting Framework– Initial version).

Firstly this deliverable analyses the implementation of different regulatory frameworks (eIDAS, SDG, national…), Digital Service Infraestructure, and interoperability status in a representative sample of MS (those involved in the Trust Management Models task) which shows a highly heterogeneous landscape in terms of trust models across the MS, with many initiatives aimed at the digital transformation of public services in line with strategic national and EU-level policy instruments and some major common trends which offer best practices and experiences valuable on the wider level of pan-European interactions between public administrations including the relevance of electronic identification and authentication schemes which are also mapped to eIDAS trust assurance levels and notified for the effect of mutual cross-border recognition under the provisions of the eIDAS regulation and the establishment of trust models within national Once-Only data exchange platforms.

Furthermore, the deliverable also provides a high-level picture of a valid trust solutions framework that includes different alternatives taken from the CEF Building Blocks and Digital Services Infrastructure trust management approaches, able to be adapted to different scenarios and technical situations. In particular, we have considered the CEF eID and eDelivery building blocks offer a delegated trust model which is relevant for DE4A, as they both feature “nodes” that act as trusted proxies in each MS and serve as abstraction elements for the trust management, allowing endpoints that request or provide data to interact just with their national nodes to which they are connected and trust but where an effective trust chain is also established across borders by virtue of this trust delegation and common standards and specifications in place at European level.

With regards to aspects related to eIDAS identity/record matching, DE4A will establish some common principles and recommendations to reinforce in this important area between competent authorities (acknowledging that such record matching processes are implemented under specific MS rules). Regarding the intermediation and user-supported intermediation patterns described in D2.4 [2], this deliverable analyses how the implementation can be done making use of functionalities and components of the CEF eDelivery Building Block, considering the default delegation scenario on a four-corner model and providing extensive details on the security model and the proposed approach to address PKI aspects necessary to manage needed digital certificates as trust anchors of this infrastructure, enabling the necessary confidentiality, integrity and non-repudiation of the data exchanged across systems. This is why after the assessment made in the deliverable, including proposed requirement areas and studying the weaknesses and strengths of the four different trust models, the adoption of the Dedicated Domain PKI trust model is proposed for its implementation in DE4A eDelivery infrastructure. This approach also is aligned with the TOOP project [98], where the trust model is being implemented from a dual approach, with the Dedicated Domain PKI model with a single trust anchor for the AS4 gateways (Access Points).

Finally, the deliverable describes the proposed interoperable blockchain-supported solution that will cover certain technological aspects of the trust solution to validate the role of this transformative technology in DE4A e.g. for implementing the Verifiable Credentials interaction pattern needed in the Diplomas Verification use case. Such Blockchain Support Framework is generic in its nature and

designed to be versatile in order to be used for further purposes where Blockchain provide an added value in eGovernment interoperability platforms.

A final version of this deliverable capturing all the improvements trust model findings will be reflected in "D2.3 Final DE4A – Final Trust Management Models and Blockchain Support Framework Design" due to July 2021.

1 Introduction

1.1 Purpose of the document

The present document is one of the deliverables in WP2 (Architecture vision and framework) for the DE4A project. It is delivered in the context of "Task 2.2 Trust Management Models" that aims to come up with an architecture and according procedure so that the any-to-any connection across border can be done in a secure, trusted and genuine way. Thus, this task will verify that a comprehensive approach to trust is built across Europe and that it is in line with already existing circles of trust like the backbone network of eIDAS nodes or the ecosystem of eIDAS Trust Services

This document has two main goals:

- Study and assess from the functional and technical point of view how trust is managed in the different public authorities' procedures in a representative sample of Member States.
- Elicitate an architectural framework for a trust model in the scope of the DE4A project, based on the adoption of disrupting technologies with a blockchain approach.

The main challenge addressed in the scope of the work done in this task is shaping the technical approach to a trust relationship and it inherits interoperability barriers. Therefore, once this problem is solved, a Data Provider (DP) will trust a Data Consumer (DC) from other country to exchange evidences in a trustworthy way. In the deliverable a more detailed analysis of different trust models relevant in the context of DE4A is covered: eIDAS and eDelivery but also in the context of SSI approach. Nevertheless, further considerations are expected to apply as the project progresses in its technical specifications e.g. at the level of eDelivery, the design of the overall message exchange model in the context of the target solution architectures and the discovery model (static or dynamic).

The 2017 Tallinn Ministerial Declaration on eGovernment [3] subscribed by all EU MS contains the principles guiding the European Interoperability Strategy to provide state-of-the-art digital solutions that support EC political priorities, in particular aiming to maximize interoperability across borders and across domains with privacy, security, sustainability, inclusiveness, accessibility, transparency and openness. The European Interoperability Reference Architecture (EIRA) Interoperability Security Viewpoint [4] states that "citizens and businesses must be confident that when they interact with public authorities they are doing so in a secure and trustworthy environment and in full compliance with relevant regulations, e.g. the Regulation on electronic identification and trust services". Thus, trust in DE4A first and foremost results from and rests on their realization at all levels foreseen in the European Interoperability Framework. Therefore, while trust is explored in this deliverable more from a technical perspective, it needs to be supported as well from semantic, legal and organisational (including integrated public service governance) dimensions.

In this deliverable, it is considered that that trust and security need to be integrated as an essential part of the fabric of DE4A Architectural Trust framework that realizes Once-Only and Digital-by-Default principles (c.f. section 7 of D2.1 Architecture Framework), both at the level of its business architecture (WP2 Architecture vision and framework) and in the context of the detailed technical design and implementation of its common specifications and components (WP5 Common Component Design & Development), with the final goal of validating in real life pilots the achievement of increased trust in government and corresponding citizen satisfaction related to better quality, user-centric and more efficient delivery of public services.

As is described in [2], the final objective of this deliverable is a proposal of an architecture compliant with a trust model that will assure that the OOTS will not become unmanageable because of key and certificates management complexities. Mature technologies that have been widely implemented in other initiatives like CEF Building Blocks (paying special attention to eDelivery) have been studied and the basis for extending its capabilities to modern blockchain technology have been set up.

1.2 Structure of the document

This document is divided into three main sections:

- Section 2 “Trust Models Study” reports how the trust challenges are addressed in different eGovernment procedures in the most representative MS’ case studies.
- Section 3 “Technological study” describes the current state of the technologies to address the functional, technical and business requirements for trust management in DE4A.
- Section 4 “Architectural Trust Framework” depicts the Blockchain Support Architecture, the interoperable blockchain-supported solution that will cover certain technological aspects of the trust solution to validate the role of this transformative technology in DE4A.

2 Trust models study

In order to enhance the trust in the internal European market among administrations, public authorities, consumers and small and medium-sized enterprises (SMEs), the eIDAS Regulation proposes concepts that are very relevant to consider as they foster a delegated chain of trust model that can be largely applicable to other cross-border data exchange scenarios, such as those involved in evidence exchange according to the Once-Only principle.

These concepts state requirements and obligations that ensure high-level security and a higher presumption of their legal effect.

2.1 eDelivery trust model

As it is reported in the CEF eDelivery Building Block – Trust Models Guidance [5], the majority of the eDelivery infrastructures that manage messages implement a four-corner model simple messaging approach. This means that the original sender and final recipient delegate into the different components of the CEF eDelivery Building Block the message exchange in a secure and trusted way according to a set of security controls [6] grouped in two types:

- Normative controls: controls required to address the requirements from the eIDAS regulation.
- Non-normative controls: controls not required to address the eIDAS regulation requirements, but necessary to enhance security.

What these security controls have in common is that most of them are based on digital certificates, and its lifecycle is controlled by a trust model.

Another important aspect of the eDelivery approach is that there are three communication layers: transport layer, messaging layer and application layer. While digital certificates need to be used at various levels, the trust model reported here is scoped to the digital certificates' management of the transport layer as it is recommended to follow a common approach to manage trust at a project level for the eDelivery infrastructure e.g. eDelivery Gateways and SMP. Other layers, i.e. messaging and application, use similar rules for trust models but a flexible approach can also be foreseen whereby different certificates from Member States would be used to secure a safe communication channel establishment (TLS handshake) between the backend systems (C1 and C2 in 4-corner model) and corresponding eDelivery Access Points (C3 and C4 in 4-corner model). .

It is important in this context to understand the notion of "Trust Anchor": according to IETF RFC 6024 [7], "a trust anchor represents an authoritative entity via a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information for which the trust anchor is authoritative. A relying party uses trust anchors to determine if a digitally signed object is valid by verifying a digital signature using the trust anchor's public key, and by enforcing the constraints expressed in the associated data for the trust anchor". We could consider this corresponds to the notion of "cryptographic trust anchor" which provides the roots of cryptographic trust and enable cryptographic binding, revocation, authentication, signing, encryption and other trust functions.

However, there are multiple categories of trust anchors including, according to classification by I. Alamillo and P. Curry [8]:

- Legal trust anchors, setting the policy baseline for trust frameworks and which underpin the operating rules

- Data trust anchors, which relate to the entities and attributes to be processed, where very high data quality is vitally important, for example, when using CEF eID we can say that trust is inherited from reliable verification by a MS on the attributes that could be used for record matching in an evidence issuing authority (this does not mean that this fact alone satisfies all local requirements). In this regard, and by being based on a legal trust anchor, such data trust anchor becomes "authoritative",
- Cybersecurity trust anchors, which monitor, detect and respond to policy violations, and enforce policy compliance. This includes assurance, testing and certification regimes

In the case of cryptographic trust anchors used in CEF building blocks like eDelivery (and also in eIDAS), it is relevant to note that a legal trust anchor exists as well (eIDAS Regulation).

According to the above-mentioned authors, "trust anchors are essential to underpin the implementation and operation of trust frameworks at appropriate Levels of Assurance". DE4A will choose appropriate trust anchors, preferring to the extent feasible those which are based on legally recognised trust issuers or even legal trust anchors (in the context of eIDAS, (qualified) trust service providers or eIDs). An example of this is the use of CEF eDelivery PKI Service (see section 4.2.3) which will provide a root PKI for the sub-domain of the project, to be used for SML and also SMP (which could be a central and shared component). Different considerations on trust anchors apply to decentralised environments such as that envisaged for SSI, see Sections 2.2 and 3.1.2.

The eDelivery Building Block proposes four different trust models:

- Dedicated Domain PKI: the digital certificates are associated to single trust anchors, and each trust anchor serves a single domain.
  - Example: in the eProcurement domain, PEPPOL PKI [9] operates a dedicated PKI
- Shared Domain PKI: as in the previous one, digital certificates are associated to a single trust anchor, but each trust anchor serves multiple domains.
  - Example: CEF eDelivery PKI service [10] offering operates a shared PKI model with a single TSP as provider.
- Mutual exchange: the digital certificates are associated to different trust anchors.
  - Example: the Pan-European project in the eJustice domain [11] implements mutual exchange approach.
- Domain trusted lists: in this model there exists a list with the trusted certificates and/or trusted list anchors, grouped by common domain policy.
  - Example: the Noble Project [12] in the Postal Services domain implements this model.

These models will be the base for the proposed DE4A trust model and will be further detailed and analysed in section 4.2.3. This will implement the trust model proposed in section 3.3.1 of D2.4 – Project Start Architecture (PSA) – First iteration [2] making use of the eDelivery Building Blocks components and approach.

2.2 ESSIF trust model

ESSIF final goal is to ensure a European cross-border, trustworthy, privacy-by-design, eco-system, so relying parties can decide which ESSIF features (for example ESSI flows, ESSIF VC, etc.) they want to trust for their business services. This trust approach is defined as "Trusted Issuers", and that information is stored in lists of trust. This makes it unnecessary to have central trust anchors, instead "trust is not created or ensured by a single authority, but by diverse stakeholders who assert things about each other" and which "obtain more than one role, depending on their respective interaction" in order to accomplish more technology related missions (e.g. network participants, infrastructure

vendors, trust anchors, issuers, verifiers, holders, data storage providers, application developers) or less technical ones (legal, business or governance [13]).

In order to ensure trust in the ESSIF ecosystem, the ESSIF trust framework governs its trust policies and all participant parties must adhere to it in order to participate of its services. The trust framework gathers all policies, principles, standards, guidelines and processes that set the rules (in form of “terms and conditions”) for making use and/or membership of the ESSIF services. A key choice underlying the trust model is that to base EBSI on "classic DIDs" whereby the ledgers are used to register DID-documents and VC-meta-data allowing to check Verifiable Credentials and Verifiable Presentations as well as validate if the corresponding DID(-key)s and/or VC have not been suspended or revoked. At a technical level, the DIDs therefore act as trust anchors as they are published on ledgers and can be obtained to establish secure communication among parties (e.g. holders and issuers or holders and verifiers). Nonetheless, at legal and organizational levels requirements still remain to be defined to meet high assurance standards and aspects like liability of issuer or quality and reliability of related identity information influence the trustworthiness of these systems as well.

The ESSIF trust model pursues the goal to unleash multiple benefits [14] for use cases that reach beyond eIDAS into different credentials or verifiable credentials (attestations) involving a rich ecosystem of issuers and relying parties. Indeed, the need arises in multiple business cases to reliably acquire data about citizens but challenges of centralised or even federated trust models in place are equally evident: there is a substantial cost and inefficiency in terms of time and effort needed to establish the veracity of the data and there are issues with semantic meaning especially when crossing organizational and national boundaries, also with the lack of real control by users of their data making it very cumbersome to authorize and even to track when and how it is shared and used.

Thinking from a technical perspective of point-to-point trust models, relying parties (equivalent to data consuming parties in the Once-Only context) spend a lot of effort in establishing and later maintaining system integrations with multiple authoritative sources of information, often having to cater with very heterogeneous technical and legal requirements across the different sources and being subject to lock-in effects when proprietary solutions are involved. Clearly this approach does not scale well in the long run and is also not very privacy-friendly compared to the SSI model depicted below which allows users to obtain and manage their data (obtained from different types of government and non-government issuers) in a standardised manner (which is much better in line with recommendations such as the “Opinion on Personal Information Management Systems” by the European Data Protection Supervisor [15]), presenting such data to different Verifier entities also using standard protocols. It also allows relying parties to trust in the authenticity, origin, and integrity of the respective claims presented to them by the users, lowering above mentioned costs of checks. In turn, claims in the form of VCs act as trust-establishing building blocks in order to enable trustworthy data exchange transactions.

Ultimately, the trust and legal certainty in ESSIF depend on whether VCs can be relied upon or, in other words on trusted issuers’ intrinsic properties (is it recognised as being trustworthy and allowed to issue specific types of VCs) and on well-understood levels of assurance (related to how requesters are identified, to the checks that the trusted issuer will make, and to the trust-levels of the issuer itself).

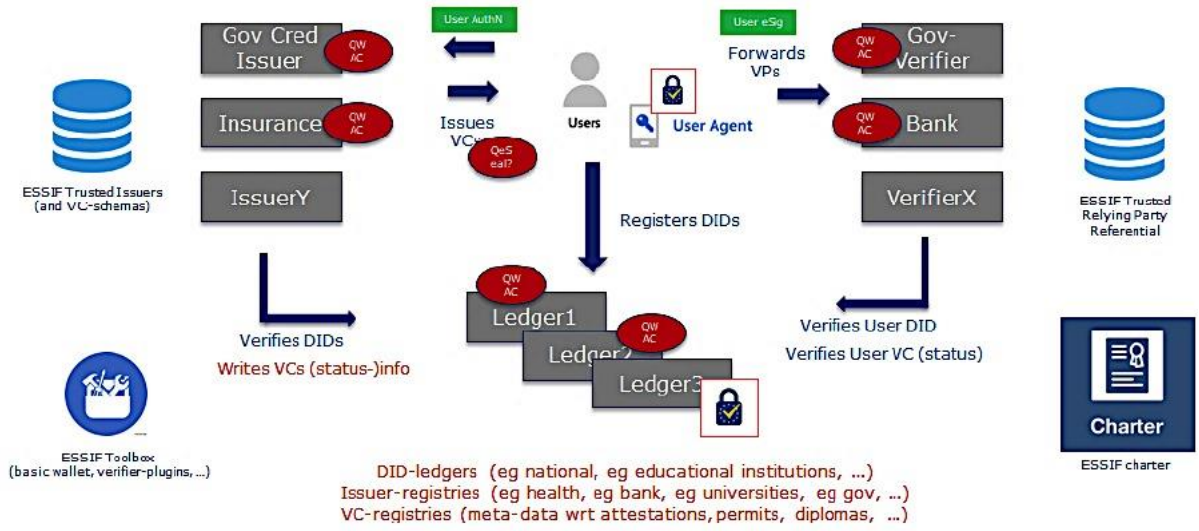


Figure 1: ESSIF EBSIv1 conceptual overview[1]

Starting from the ESSIF EBSIv1 conceptual overview it is possible to detail the main building blocks and how trust is managed with the ESSIF Trust Framework (understood as the collection of "policies, principals, guidelines, standards, processes, … which form the "terms and conditions" of membership and/or usage of ESSIF-services and as such ensure for all parties involved the trust levels parties can count on in the context of ESSIF [16]"):

- ESSIF wallet/agent
  - This building block will be used by different parties to interact with the ESSIF ecosystem. Parties that make use of the wallets/agents can be relying parties, issuers and users, and the functionalities available are:
    - Registration of one or multiple DIDs
    - Interaction with multiple users (and its ledgers) to obtain VCs
    - Interaction with other relying parties, establishing rules for their identifiability/authenticability
- ESSIF plugin
  - Component that supports wallets/agents interfacing with multiple ledgers. Plugins allow wallets/agents interact with:
    - DID resolvers, trusted issuer referentials and VC-schema referentials
    - Different issuers and relying parties that can use different DID and VC schemes
    - Issuers and relying parties that use specific protocols like OIDC
- ESSIF ledgers
  - The interaction with different ledgers is a key concept for ESSIF, and all parties (especially relying parties and users) have to be able to interact with them. This allows a proper establishment of trust in a highly contextual manner, allowing trust anchors to be stored and retrieved from a

[1] Figure source: https://ec.europa.eu/cefdigital/wiki/download/attachments/262505460/image2019-9-23_20-34-0.png?version=1&modificationDate=1594913315613&api=v2

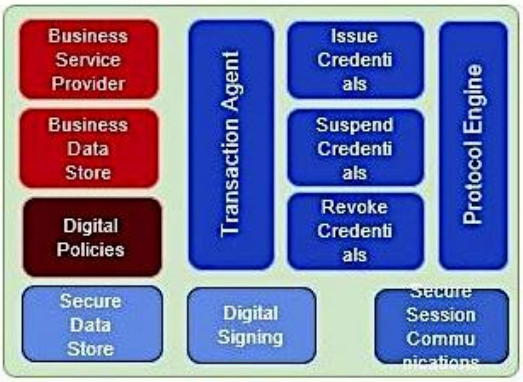
common decentralised infrastructure which is trustworthy and almost impossible to tamper or bring down (e.g. EBSI). Some examples of ledgers to interact:

- DID registrars, for user's registration (they act as trust anchors who facilitate the onboarding of new users into the SSI ecosystem).
- Sector ledgers, for issuers and relying parties registration (sector-specific ledgers are not yet available but are expected for ESSIF v2)
- VC ledgers, for storing metadata related to issued VCs, most notably their level of assurance

- ESSIF Issuer Referential
  - This building block publishes information about the relation of issuers that are allowed to issue which VCs and contributes to ensure legal certainty in ESSIF. This is information can be summarized into:
    - Relation between Trusted Issuers and VCs
    - Relation between VCs and the used schemas
    - Relation between VCs and LoA
- ESSIF Schema Referential
  - Building block responsible of holding all trusted VC schemas, so all parties involved can ensure correct processing.
    - Application of clear schemas and attribute definitions
    - Application of ESSIF guidelines related to VC definitions
    - Provision of a structured catalogue with unique identifiers per VC type and template.

Advanced topics need to be considered in SSI trust models to cater for specific needs or events, for example if the subject loses control over its DID private keys (loss of mobile wallet), mechanism need to exist to be able to recover the DID. For example, ESSIF proposes in this regards to use a DID-card mechanism but indicates that "it is vital that such a recovery process must be very rigid, under control of a trustworthy DID-custodian and should protect the DID(-keys) against compromise or impersonation [17]".

While not part of EBSI core infrastructure of supporting services, ESSIF indicates that the different environments (Relying Party, Issuer, Holder) should not be underestimated and in DE4A these local environments will be thoroughly addressed. In figure below these environments are introduced (Issuer, Holder and Relying Party):



Issuer

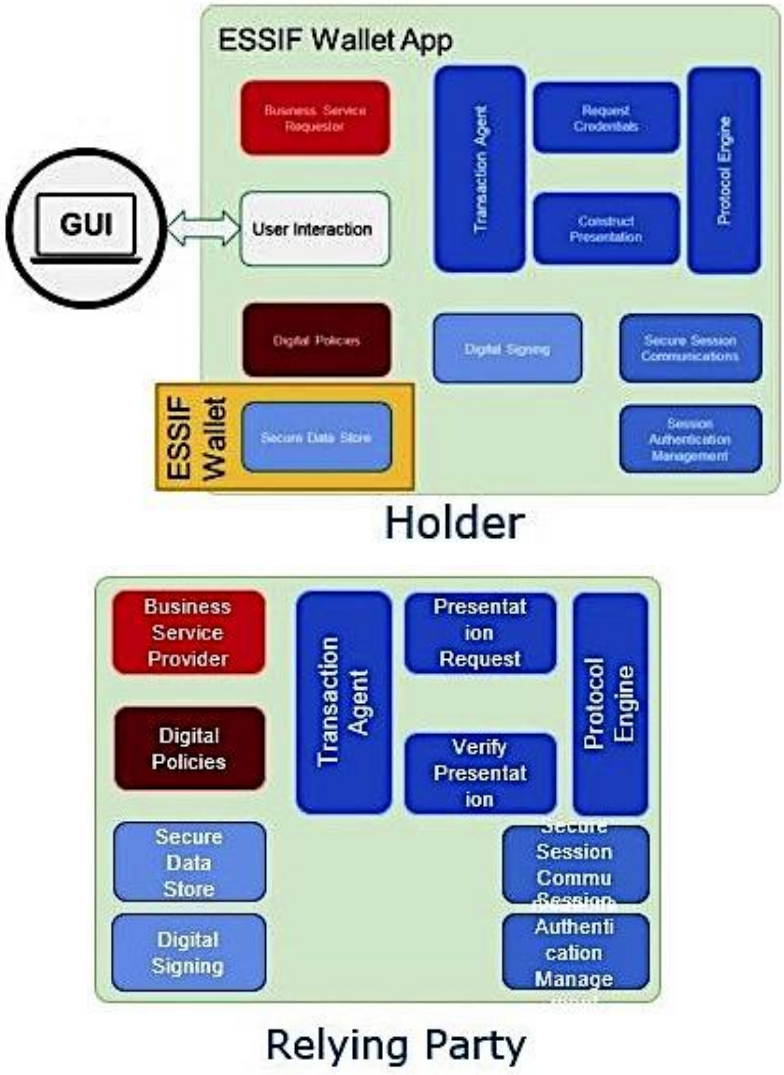


Figure 2: ESSIF EBSIv1 conceptual overview[2]

Relying Party and Issuer environments typically include:

- Services to allow users to Identify/Authenticate themselves (e.g. "classic eID-based authentication)
- A policy engine allowing to configure which DID-methods and VCs will (not) be accepted inbound
- A Verifiable credential generator- supporting issuance policies
- DID-signing- and optional eSealing-services

Holder or subject environment would include:

- An as user-friendly as possible user interface (possibly guiding a user to which VCs could "match" the ongoing request.
- A Verifiable Presentation Generator (based on user decisions made)
- DID-signing- and optionally eSigning-services

[2] Figure source: https://ec.europa.eu/cefdigital/wiki/download/attachments/262505460/local-environmentsJPG.JPG?version=1&modificationDate=1594913315753&api=v2)

ESSIF framework is further supported on EBSI infrastructure (ledgers and smart contracts allowing verification of DID(-keys):

- One or more ledgers to allow for DID-registration (note that different parties might choose in future to "live" in different DID-domains / chose to use different DID-schemas)
- One or more ledgers to support information wrt Verifiable IDs (also here, different parties might choose in future to "live" in different domains / chose to use different VC-schemas)
- One or more ledgers to put information wrt Verifiable Attestations on (also here, different parties might choose in future to "live" in different domains / chose to use different VC-schemas)

Furthermore, EBSI would also provide the following supporting services:

- A DID-registrar allowing authorised DID-schemes to be published (as well as all information needed to interact with those schemes) in a controlled way.
- A trusted Issuer list allowing authorised Issuer to be published (as well as the VCs they are allowed to issue and following which scheme and LoA this will be done, as well as info needed to interact with this issuer).
- A VC-scheme referential which will list the scheme of all VCs that will be supported by ESSIF (note that there are at least two levels: one giving the general formats, second giving the exact format of used high LoA VCs).

This, added to the local environments mentioned above, results in the following consolidated picture of ESSIF components / services and EBSI-infrastructure / EBSI-supporting services:

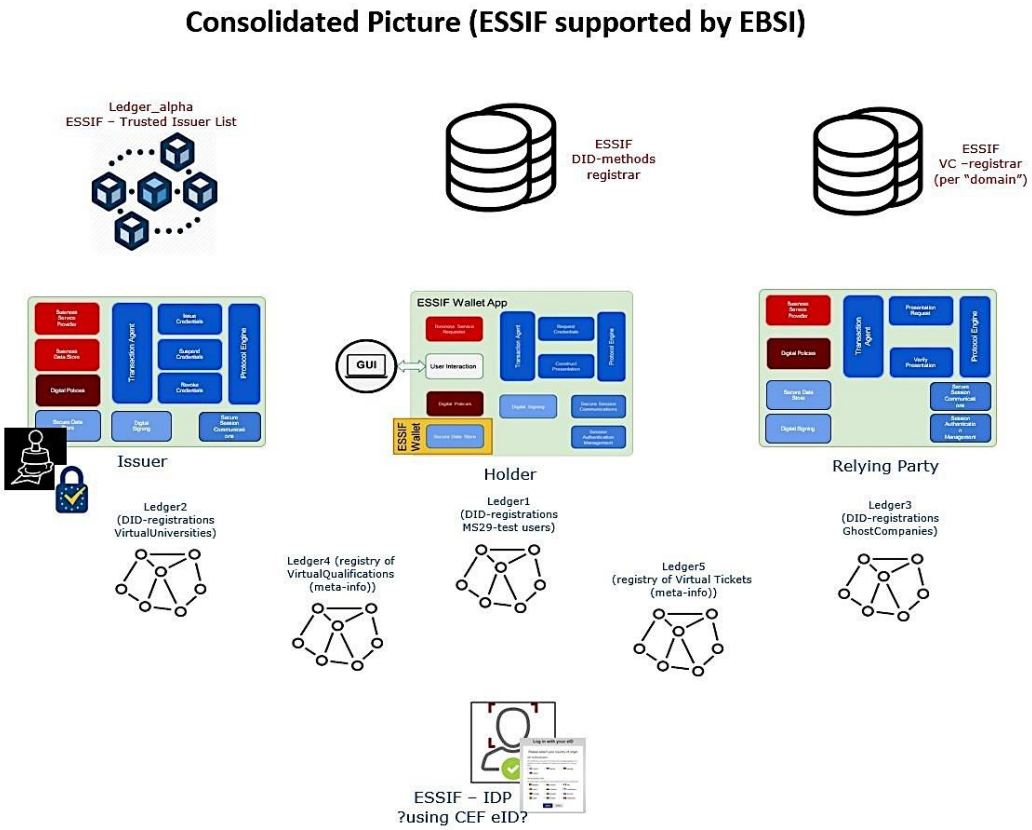


Figure 3: Resulting overall ESSIF-EBSI Framework[3]

[3] Figure source: https://ec.europa.eu/cefdigital/wiki/download/attachments/262505460/cosolidatedJPG.JPG?version=1&modificationDate=1594913315668&api=v2

2.3 eIDAS background

eIDAS Regulation (known simply as eIDAS) refers to Regulation (EU) No 910/2014 [18] on electronic identification (eID) and trust services for electronic transactions in the internal market [18]. It establishes the legal framework and the obligation for the interoperability of state-backed electronic identities across MSs, for the purposes of authentication. It also lays down clear rules for trust services relevant for electronic transactions, including a sound legal framework for electronic signatures and electronic seals (among other types of trust services). Both aspects are relevant in the context of trust models analysis as both the recognition of eID at pan-European level and the use of electronic signatures and/or seals can be considered as major building blocks and artefacts that support electronic evidence about users (natural and legal persons) participating in procedures in the context of the SDGR and that guarantee the origin and integrity of data and other elements of electronic transactions in this context, thereby providing solid foundations for multi-lateral trust between involved stakeholders.

The benefits of procedures to be offered fully online as established in the SDGR [19], in conjunction with the pan-European mutual recognition of notified electronic identification means issued in MS by public or private4 sector organizations (c.f. Arts. 6 and 9 of the eIDAS Regulation [18]), are evident in the context of a common single digital market. This would allow a citizen to perform certain electronic procedures instantly in any other country without the need to obtain an electronic identity on the destination country (a procedure that in most cases requires physical presence), without prejudice of administrative pre-requisites established by respective competent authorities specific to each procedure (but which cannot in any case result in discrimination against cross-border users).

eIDAS is based on **cooperation** and **reciprocity** between states through the **mutual recognition** of eID schemes. A state will formally notify an eID scheme for cross-border use and, once this process is completed, all the other states must recognise it and allow it to be used on their public services. The obligation is only for the eID schemas whose level of assurance (LoA) is “high” or “substantial”; “low” level of assurance schemes is up to each MS to be accepted or not.

It is to be noted that not all services offered by public services are required to support eIDAS notified eIDs. From the above-mentioned mandatory aspect in the regulation, and after discussion with the relevant authorities, it was established that accepting the eIDAS notified eID schemes was mandatory for public services which accept at least substantial or high authentication or signature mechanisms. This leaves out all internal services and services requiring only a low level of credential authentication assurance.

So, under the eIDAS regulation, MSs have the obligation to recognise same or higher grade eID schemes from other states, but have sovereignty over:

To fulfil the requirements of the regulation, an infrastructure is deployed and maintained by the MSs. It involves a set of national entry points (the eIDAS nodes) to allow the federated access to the notified eID schemes. These eIDAS nodes can behave in two roles, eIDAS-Connector when requesting a cross-border authentication, and eIDAS-service, when providing personal identification data in response to a request. These entry points thus act as trusted proxies and as an abstraction element for the trust management: a MS issues a request to the entry point of a country and receives a response, signed not by the identity provider, but by the peer eIDAS node. This creates a delegated trust model, where

[4] From the perspective of the eIDAS Regulation, electronic identification can be seen as a collection of electronic public services, which may also be provided as a private service recognised by the MS (c.f. Art. 7(a)) and always under its liability (c.f. Art. 11).

the entities of a country (both service and identity providers) trust only their national eIDAS node, both as issuers of requests and of responses, following their own national topology and trust model. To interconnect the entities of each state, all the MS eIDAS nodes form a mesh and, effectively, an explicit circle of trust. So, each service provider will trust a response from an identity provider because both the SP and IDP trust their respective nodes, and the nodes trust themselves. To keep this trust chain, all exchanged messages are cryptographically validated and travel through secure channels. It could also be understood, as acknowledged in the ESSIF Vision [14] that "on an infrastructural level, eIDAS works as a harmonisation mechanism that is actively enabling the Once-Only principle by federating member countries' centralised identity systems with each other".

CEF released a set of building blocks to support the deployment of this eIDAS enforcement infrastructure, but each MS has its own mechanism to access the node, and a different internal topology of eIDAS connectors. The trust anchors (certificates) in this mesh used to securely identify each of the participating eIDAS nodes are provided by the MS by means of a number of bodies such as the eIDAS Technical Cooperation Network, the eIDAS Technical Subgroup and the eID Operational Management Board [20]. Furthermore, the eIDAS network is established following common technical specifications and protocols, in particular eIDAS protocol which is commonly specified for cross-border communication between nodes, c.f. eIDAS eID profile which covers the interoperability architecture and message formats among other technical specifications [21]. The technological aspects of this model are presented in sections 3.3 and 4.2.2.

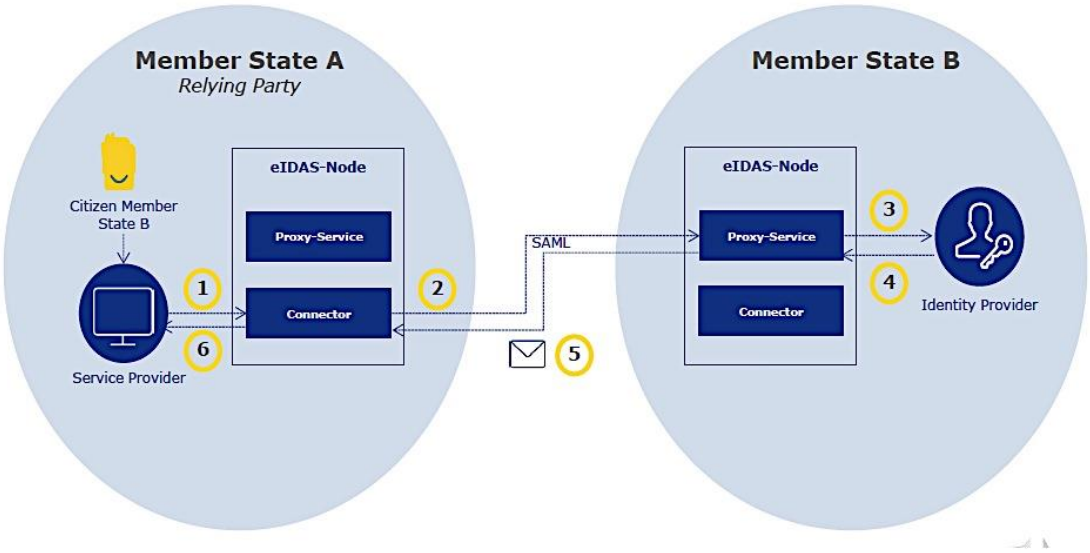


Figure 4: eIDAS eID infrastructure proxy model

Separately, in section 4 within chapter III of the Regulation that addresses Trust Services[5], eIDAS defines the requirements to consider a signature a qualified electronic signature, addressing as well requirements for all the involved elements and actors (qualified certificates, qualified trust service providers, qualified signature creation devices). While following same rules, qualified electronic seals

[5] Understood as electronic services normally provided for remuneration which consists of these functionalities: i) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or ii) the creation, verification and validation of certificates for website authentication; or iii) the preservation of electronic signatures, seals or certificates related to those services.

are intended for legal entities and thus more relevant in the SDGR context where competent authorities need to generate automatically requests for evidence or respond to such requests (electronically sealing and verifying such electronic seals over request and response messages could provide a higher level of trust between competent authorities, coupled with other approaches, e.g. registries that could be queried to verify if a given authority is entitled to make an evidence request for a given type of procedure or provide a certain type of evidence). eIDAS Regulation states in relation to electronic seals that:

"A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States" – Article 35.13

Thus, any electronic document signed with a qualified certificate (of "high" assurance) issued by a MS, must be accepted by any other MS. Similar to the eID case, it does not establish the obligatoriness to accept the non-qualified seals, but neither allows for its automatic dismissal:

"An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals." – Article 35.1

So, MS are encouraged to evaluate on each case grounds the convenience to accept non-qualified seals and electronic evidence.

To conclude, it can be acknowledged that thanks to the eIDAS Regulation, a solid legal foundation and certainty exists for the cross-border use and acceptance of identity which, combined with the closed list of electronic trust services covered by the same regulation, together act as key enablers to build trust in the Digital Single Market. In particular, this is the case for integrated or orchestrated public services offered by competent authorities such as the online procedures linked to key life events contemplated in Annex II of the SDGR.

At the same time, trust remains a very complex and multi-faceted concept that builds upon a complex combination of technical mechanisms and non-technical factors as well, conditioning the success in the adoption of technological change and innovation, in particular in the context of the Digital Transformation of public services. It is in this context that both notified eIDs exchanged over the eIDAS network and the different supervised/accredited trust services -published by the EU as a List of Trusted Lists of all MS- are considered in DE4A project as basic building blocks for trust enablement: they act as mechanisms that ensure secure and protected data exchange in digitally delivered public services.

2.4 Case study: Netherlands

2.4.1 Multi means eID system Netherlands

There are many ongoing programmes/projects and there is also law making in progress. This is the current status (March 2020), but things could very well change in the nearby future.

A distinction can be made between public and private means:

2.4.1.1 Public eID means (Ministry of the Interior and Kingdom Relations)

- DigID
  - Mainly for citizens
  - ETD also public (Ministry of Economic Affairs and Climate Policy)
- eHerkenning
  - Mainly for companies
  - Private eID means (banking world)
- iDIN

Four domains (two dimensions) are distinguished: citizens and companies with private services and public services. For example, the BSN-domain is regulated by law.

The means can cover one or more domains. Another important aspect is that some companies are persons or vice versa (e.g. one person companies).

2.4.2 DigID

It can be used for services from government organisations or private organisations which perform government tasks (regulated by law).

Table 1: DigID Trust levels

DigID		eIDAS
Basic	User/password	Basic
Middle	User/password + SMS Smartphone DigID app	
Substantial	Smartphone DigiD app + upgrade (RDA) e.g. with chip on driver's license	Substantial
High	Not (yet) available	High

2.4.2.1 Legal authorization

It is possible to authorise a natural person or legal person to act on your behalf. There are various systems in place and there are also ongoing developments. Big opportunities can be expected here.

2.4.3 eHerkenning

eHerkenning is like DigID. Just like citizens can use DigiD to login with the government agencies, companies, entrepreneurs and professionals can do that with eHerkenning.

An eHerkenning tool is person-bound. It cannot be transferred to someone else, such as a colleague. As user of eHerkenning, you can be authorised by your supervisor to act on behalf of your company with your service providers. One or more authorisations are registered when applying for a tool.

Currently, eHerkenning is the only eIDAS notified means. I expect more in the future, both public and private.

Table 2: eHerkenning Trust levels

eHerkenning		eIDAS
EH1 (low)	Will be discontinued	-
EH2 (low)	User/(strong) password	Basic
EH2+ (low)	Idem + SMS-code or a pin code (via token)	Basic
EH3 (substantial)	As EH2+ but verification process for obtaining EH3 is stricter	Substantial
EH4 (high)	PKI certificate or 2FA	High

2.4.3.1 Legal authorization

Organisations often need to deal with the government, local authorities or other bodies. They may need an environmental permit, for instance, or want to apply for a government subsidy. With the use of an eHerkenning token, an employee can manage these affairs online on behalf of an organisation. But first the employee needs to be legally authorised.

With legal authorisations, organisations can be sure that only authorised employees can manage particular affairs online. And they can be sure that the affairs are being handled safely and reliably. An eHerkenning token and the corresponding legal authorisations are personal and cannot be shared or transferred to other employees. That means that legal authorisations must be registered per person and per service with a certified supplier of eHerkenning.

The legal representative of the organisation can appoint an authorisation manager to handle this. The authorisation manager will then arrange who will be legally authorised for which online service.

2.4.4 iDIN

The identification of the user is done via his/her bank and is used by citizens and companies.

Table 3: iDIN Trust levels

iDIN		eIDAS
Only one level	Substantial	Substantial

2.5 Case study: Spain

2.5.1 Data Intermediation Platform (DIP)

2.5.1.1 Description of the procedure

This procedure is based on a process (asking for any data or evidence of a person or enterprise) in which a public authority (for example, the Ministry of Education, the Region of Madrid or Madrid City Council) can require a data service (or an evidence service) and previously must provide a set of "access evidence or proof of claims" to be online approved by the data provider.

If a data service request arrives without having the required proof of claims, the data provider should ignore or reject the message. A proper and standardised code and message error should be provided.

A data transmission (containing the evidence, individual data or a document) can be identified as a 4-stage process.

- Authorization Request
- Data Exchange (proper)
- Audit and control of the exchanged data
- Business Control: data usage audit and administrative processing (internal on Data Requestor only)

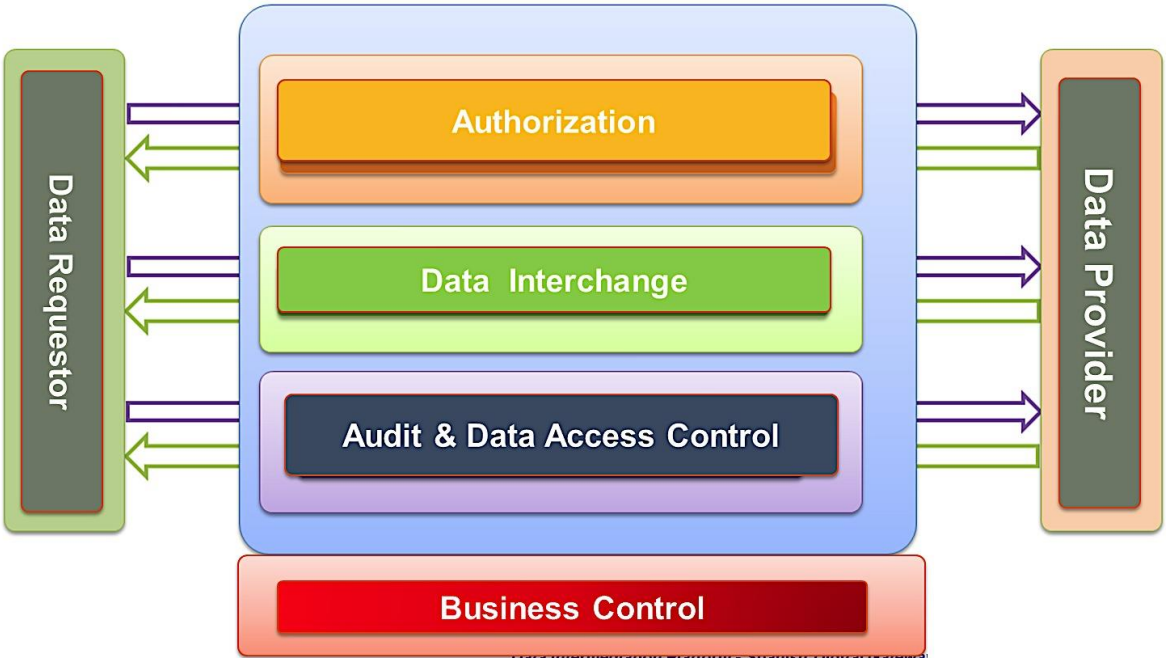


Figure 5: Data Intermediation Platform information flow

The last "Business Control" activity would not be of relevance to this project, as it is an internal issue of the final service provider.

Each service or procedure managed by the agency providing the final service to the citizen must have a unique code or identifier. This eases the authentication and authorisation process: "Unique IDs for procedures".

In Spain, there is a System/Registry to collect all procedure information. The preferred option is to use the Unique IDs generated by this system although DIP accepts any Unique ID per Data consumer.

Any "Data Service" provided by DIP is identified by a "unique service identifier".

This unique service identifier will be used in the authorisation request process and later on in the data transmission process.

2.5.1.2 Roles involved

The following roles are identified in data transmission

- **Data Owner**: any organization owning information about citizens that might be necessary for another organization to exercise their competencies. It is responsible of authorisation approval and data transmission audit
- **Data Transferor:** technical responsible of data transmission. Typically, Data Owner and Data Provider are the same, but in some cases, they may be different organisms
- **Data Evaluator:** any organization authorised to search for citizens' data in information owned by a Data Owner.
- **Data Requestor:** the actor making search possible in terms of technology. Data Evaluators who make their own searches shall be considered as both Evaluators and Requestors.

Every Data Transferor controls the access (authentication and authorisation process) to each service.

The control of authorisations to access the different data services must establish a mechanism based on who requests the data, the requested service and the previously authorised procedure, so it should be based on the following elements:

- **Data Requestor Identifier**. It is identified from the electronic signature of the requests made by the applications. A component certificate that identifies the agency is required.
- **Data Evaluator Unique Identifier** (fiscal Id. number of the organism) usually identified at the level of the Ministry or the Secretary of State.
- **Procedure or Service Code:** that requires access to data. As set out in the data protection regulations should be clear that the procedure needs the data and therefore must be individualized by procedure.
- **Evidence Data Service Identifier**, according to the catalogue of Evidence Data services published in the technical system.

On top of every single data transmission control **[Data Requestor, Data Evaluator Unique Identifier, Procedure Code/ID, and Data Service Id]** the data transmission contains:

- Organizational Unit ID & Name.
- Civil Servant ID.
- Consent Indicator [Yes, No opposition, Law (when neither "consent" nor "No opposition" are needed, like in Inspection procedures)].
- Expiry date in case the law that enables the data consultation is known. Usually calls for scholarships and grants.

2.5.1.3 Technical information regarding data flow

Data messages are digitally signed by Data Requestor using WS Security. Internal evidence could also be signed (for example "Address certificate sent by Local entities", a PDF certificate, etc.)

The Data Intermediation Platform behaves like a broker, a Single Point of Service for "all" base registries information. For this purpose —that also entailed the interconnection of public Administrations—, an interchange format was defined in order to achieve total interoperability of services.

For that reason, the current Platform of Data Intermediation is defined as a Service Oriented Architecture (SOA) based on the following elements:

- Web Services specifications based on WSDLOpen national standard for data interchange "SCSPv3". Supporting synchronous and asynchronous.
- Use of XML documents to exchange data among the different services involved in the system. XSD compliant with SCSPv3 Protocol.
- **Web Services plus electronic signature through XMLDsig, WS-Security or XADEs-B.**
- **Establishment of secure communication channels through SSL protocol.**
- **Use of electronic and recognised certificates.**
- **Use of Time Stamping Services (TSA).**
- Orchestration of services when legally possible, simplifying data consumption.

Furthermore, this process is compliant with eIDAS regulation with the adoption of:

- Advanced electronic signatures.
- Qualified digital certificates

Synchronous behaviour is composed by:

- A request & response message

Asynchronous behaviour is composed by:

- A request & confirmation (ACK) message
- A "request for response" message & response message

2.5.1.4 Trust management flow

Authorisation management flow

Data consumer claims for authorisation providing the law information that must be evaluated by data provider, including article and regulation. The authorisation request includes an Official Form signed by data consumer, containing internal roles requested by DIP, like Audit Responsible, Technical Responsible and so on.

Once the Authorisation request is approved, Data consumer could send the request messages.

Data management flow

The following image shows the flow:

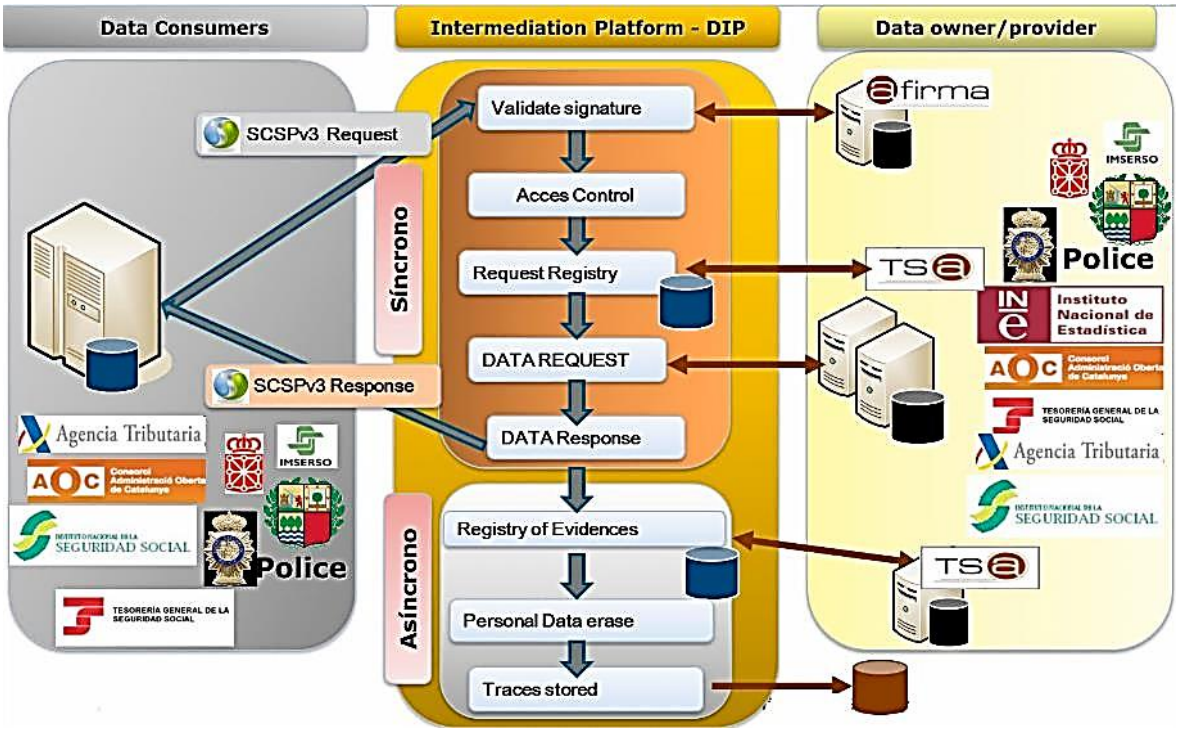


Figure 6: DIP message processing flow

1. Organisms will send their XML request message that will be managed by a TOMCAT server. (*Synchronous*) DIP stands for Data Intermediation Platform:
    a. DIP checks the validity of the signature of the received request.
    b. DIP checks if the author of the request has the rights to access this data.
    c. To show evidence of the moment when the public organization makes the request, DIP uses the TSA system for stamping the time when the request was received. It can be internally computed like a "time mark".
    d. The system leaves a signed register of the received request, the origin of the latter, and the moment of the consultation (stamp of time).
    e. DIP makes the request of the personal data to the corresponding administration department according to the case (i.e. personal identity to the General Directorate of Police, residence place to the National Statistical Institute, and so on). This request is signed by the system.
    f. DIP receives the answer generated by corresponding department and checks its signature and the validity of this certificate.
    g. DIP leaves register of the request and the answer received.
    h. The final signed answer is given to the public organization by DIP.
    i. The public organization receives the answer and continues with its procedure.

2. At a later moment, thanks to an architecture based on message queuing following activities are also performed. *(Asynchronous)*:
    a. DIP registers, signs and stamps the time the answer is returned to the public organization.
    b. Personal Information is deleted in order not to store personal information from Data Providers.
    c. Messages older than one week are extracted from the system and are stored.

2.5.2 Cl@ve

Cl@ve is a system aimed at unifying and simplifying citizens' electronic access to public services. Its main objective is that citizens can identify themselves to any Public Authority by means of concerted key passwords (a username and a password), without having to remember different key passwords to access the different services provided by each organism.

Cl@ve complements the current access systems through e-NID (electronic National ID) and electronic certificate, and even includes the possibility of cloud signing with personal certificates stored on remote servers.

It is a common platform for electronic identification, authentication and signature, an interoperable and horizontal system that avoids Public Administrations having to implement and manage their own identification and signature systems, as well as citizens having to use different identification methods to interact electronically with the Administration.

Cl@ve allows e-government applications to define the Quality Authentication Assurance (QAA) level they need, based on the data they treat and the security classification following the recommendations of the Spanish National Security Framework. Thereby, public service providers “activate” only the identification methods that meet the security requirements that each service demands among those available in Cl@ve. Finally, citizens using those services can then choose by which means they wish to be identified from those allowed for the QAA level required by the application.

2.5.2.1 Identification systems allowed

Cl@ve contemplates the use of identification systems based on **concerted key passwords** and **electronic certificates** (including the e-NID).

As regards the concerted key passwords, Cl@ve supports two possibilities of use:

- **PIN Cl@ve.** It is aimed at users who sporadically access public services. This electronic identification system is based on the use of a code chosen by the user during the authentication process and a PIN (a One-Time Password) sent to the user’s mobile phone via PIN Cl@ve app or an SMS message. It is a very simple system, since it does not require the user to remember a password permanently, and it is very secure, since the validity of the password is limited in time.
- **Permanent Cl@ve.** It is aimed at regular users of public services. Users access using a username (the National ID) and a password, reinforced with OTP sent by SMS. The password is valid for a long time, although not unlimited. This system also allows citizens access to the cloud signature.

To be able to use these concerted key passwords and the cloud signature services, citizens must previously register in the system. There are two types of registration:

- **Basic.** Telematic registration by postal mail and using a Secure Verification Code (an alphanumeric code with which to check the integrity and authenticity of the data). For the accreditation of identity, certain information known to both parties is provided (for example, the date of issue and expiration of the National Identity Card).
- **Advanced.** Through two possibilities:
  - On-site registration at a Registration Office. Citizens must prove their identity through their physical presence and by providing the corresponding supporting documentation of their identity (National Identity Card, Alien’s Identity Number, Passport, travel documents, etc.).
  - Telematic registration using a qualified certificate (including the e-NID, which is considered as a qualified certificate).

2.5.2.2 Architecture

Cl@ve's design is based on a federated identity model, which integrates different elements:

- **E-government Service Providers (SP).** Entities that provide electronic services to citizens and use the platform to identify and authenticate them.
- **Identification and Authentication Service Providers (IdP).** Entities that provide citizen identification and authentication mechanisms to be used as common means by other entities (SP). Initially, the existence of two identification service providers is contemplated: the Official Tax Administration Authority (AEAT) that offers the identification and authentication services corresponding to the *PIN Cl@ve* system, and the Social Security Information Technology Management (GISS) that offers the *permanent Cl@ve* services. The design of the solution contemplates the extension to other potential identity providers, if deemed appropriate.
- **Gateway / Identification Manager.** Intermediary system that gives service providers access to the different identification mechanisms. It also allows users the selection of the identification mechanisms available.

According to this design, service providers only have to integrate with the Identification Manager. It is in charge of establishing trust relationships between the different actors through electronic certificates and the exchange of signed messages. This guarantees the secure transmission of information throughout the identification and authentication process.

Additionally, Cl@ve is integrated with two other identification intermediary systems:

- **@firma.** Suite of products available to Public Administrations that allows e-government services to manage identification and signature through electronic certificates, including e-NID.
- **STORK-eIDAS.** Interoperability platform that allows cross-border recognition of electronic identities.

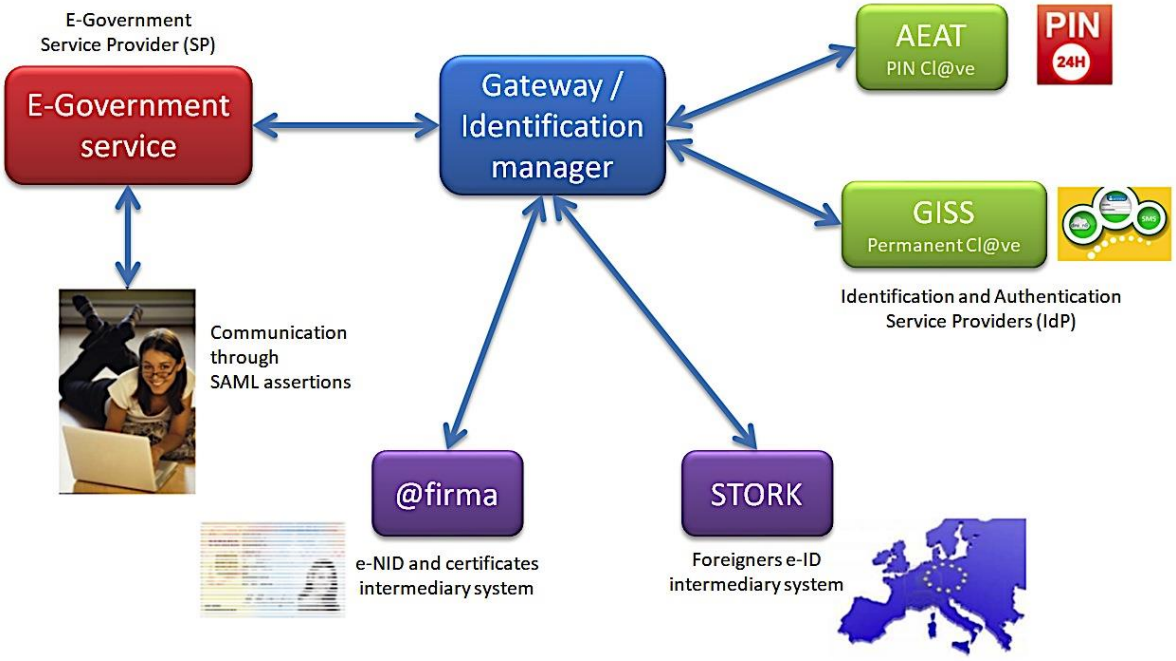


Figure 7: Components of the architecture of Cl@ve

2.5.2.3 Interaction flow

For citizen identification, the identity federated model of Cl@ve is based on the SAML standard. Therefore, the way to connect to the Cl@ve service is not through Web services, but through browser **SAML assertions**.

Specifically, Cl@ve is based on the **SAML 2.0 profile defined by STORK and updated by eIDAS**. This profile will be used both for integration between Cl@ve and the service provider, and for integration between Cl@ve and the identity provider.

The flow of user interaction is depicted in the following diagram:

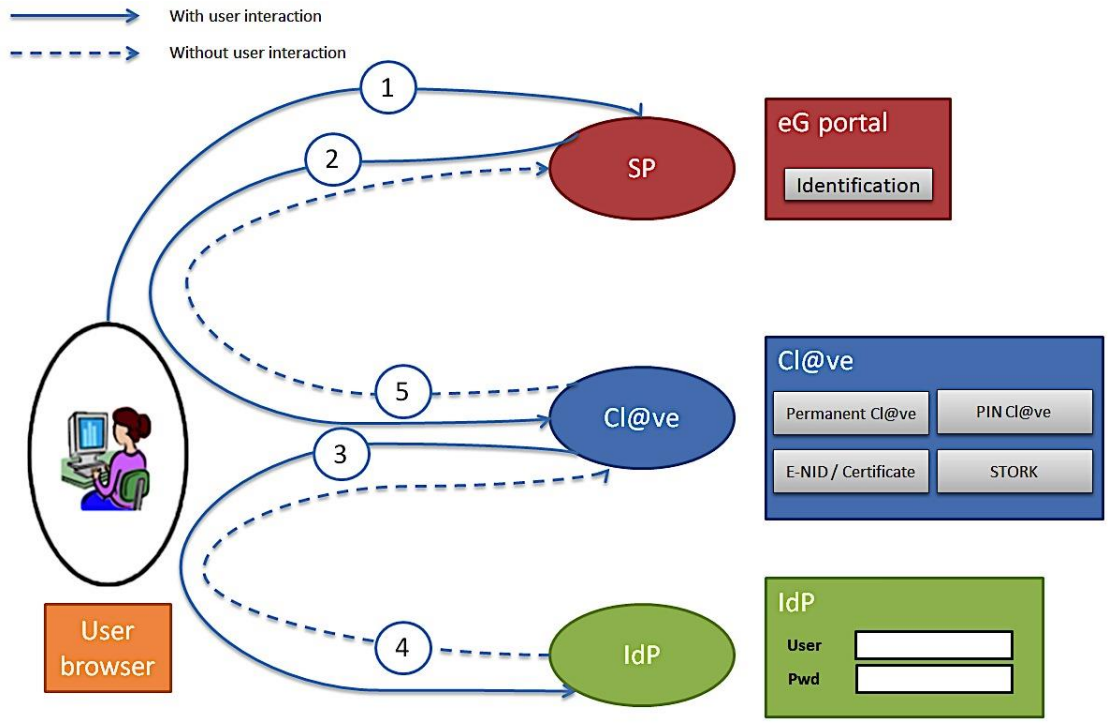


Figure 8: User flow interaction diagram in Cl@ve

Communication between components is realised through the exchange of tokens that previously pass through the citizen's browser. Consequently, each identification service provider only responds to the citizen from whom it has received an authentication request.

In the generic use case shown in the figure, it is seen that the SP does not interact directly with any IdP, but exclusively through the citizen's browser.

The steps of the interaction are as follows:

1. Citizens access a digital service integrated with Cl@ve that requires identification.
2. The citizen is redirected to Cl@ve, which displays a screen in which they must select the identification method they want to use. The active options on the screen depend on the parameters the SP has indicated in the message sent to Cl@ve regarding the IdP and QAA levels allowed.
3. The citizen selects the method of identification and is redirected to the corresponding IdP, where they can carry out the authentication process.

4. In a transparent way for the citizen, they are redirected back to Cl@ve with the result of the electronic identification.
5. Again, in a transparent way, and without need for interaction, the citizen is redirected back to the SP, which at the same time receives the information about the identity of the citizen.

All exchanged tokens are signed by the issuing entity. Indirect communication of the different components of the system occurs due to the creation and validation of those tokens. Thereby, regardless of the chosen mechanism and in the event that everything has gone well, the citizen ends up obtaining the same result, a signed SAML with their identifying data.

This mode of operation is modular, that is, each validation system is independent of the others, and can be enabled or disabled depending on the needs of the client application. This modularisation allows the system to be easily scalable if new authentication methods permitted by Public Administration appear in the future.

For this purpose, each identification system shall have an assigned quality indicator that uniquely identifies the strength of each of the authentication methods supported by it (the QAA level). Thus, the client application may choose the set of identification systems it allows based on the QAA it requires.

2.5.2.4 Assurance levels in Cl@ve

Table 4: Assurance levels correlation between STORK QAA, ISO 29115, eIDAS and Cl@ve depicts the correlation between the assurance levels defined in the STORK QAA model, the ISO 29115 Standard, the eIDAS Regulation and the Cl@ve platform. It is based on the type of registration (basic or advanced) and the authentication method used.

Table 4: Assurance levels correlation between STORK QAA, ISO 29115, eIDAS and Cl@ve

STORK QAA level	ISO 29115 level	eIDAS level	Cl@ve level	Type of registration	Authentication method
1	1-low	-	-	-	-
2	2-medium	Low	2 (low)	Basic	PIN Cl@ve Permanent Cl@ve without OTP
				Advanced	Permanent Cl@ve without OTP
3	3-high	Substantial	3 (medium)	Advanced	PIN Cl@ve Permanent Cl@ve with OTP Certificate in SW support
4	4-very high	High	4 (high)	Advanced	Qualified certificate in HW support e-NID

2.6 Case study: Portugal

2.6.1 Overview on eID and trust services

In Portugal, qualified digital certificates have been used for authentication and electronic signature. On top of that an authentication platform ensures different authentication methods with different trust levels. Portugal has its own eIDAS node, ensuring authentication of valid citizens in Portugal and allowing authentication of citizens from other European States.

Designed to ensure citizens can act on behalf of a company, there is in place a system to allow citizens to have professional attributes aggregated to their identity.

2.6.2 Authentication and eSignature services

Authentication and eSignature services rely on Autenticação.gov platform to provide a secure access to identity and digital certificates. No information is provided without user consent, and the information is gathered from different providers using an interoperability platform. European authentication, eIDAS, follows the same path to provide authentication and request citizen's data.

Currently this platform is used by both, Public and Private sector entities and services.

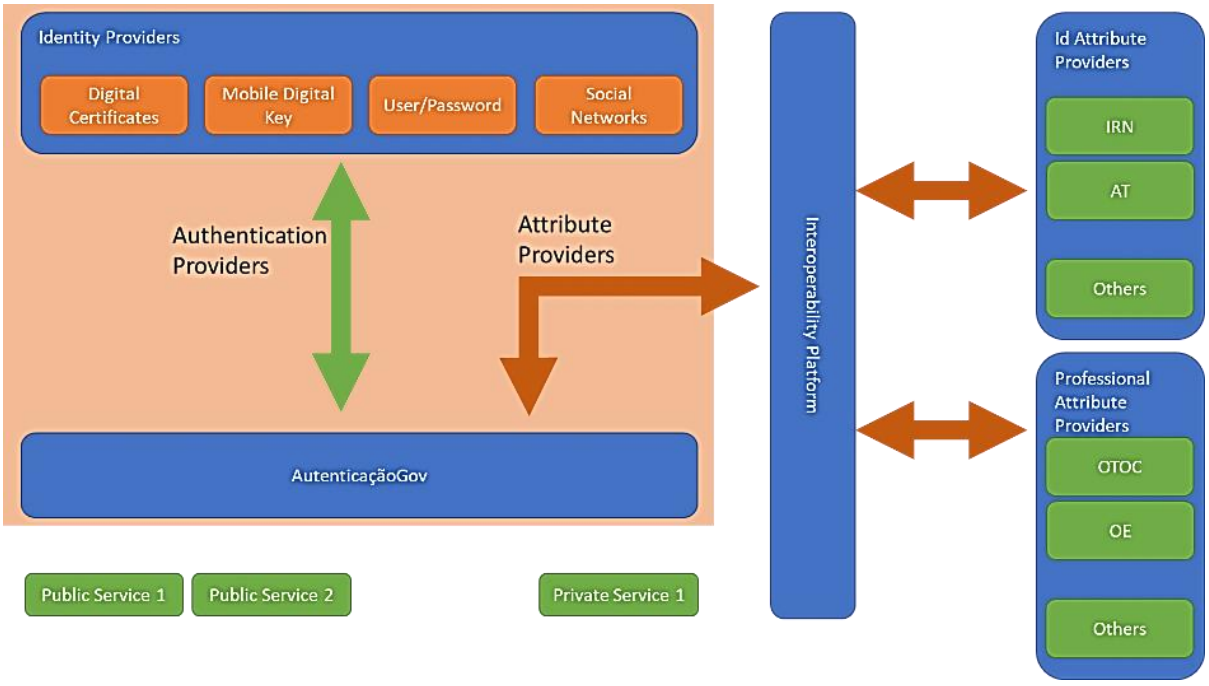


Figure 9: Authentication and attribute providers

2.6.2.1 Autenticação.Gov

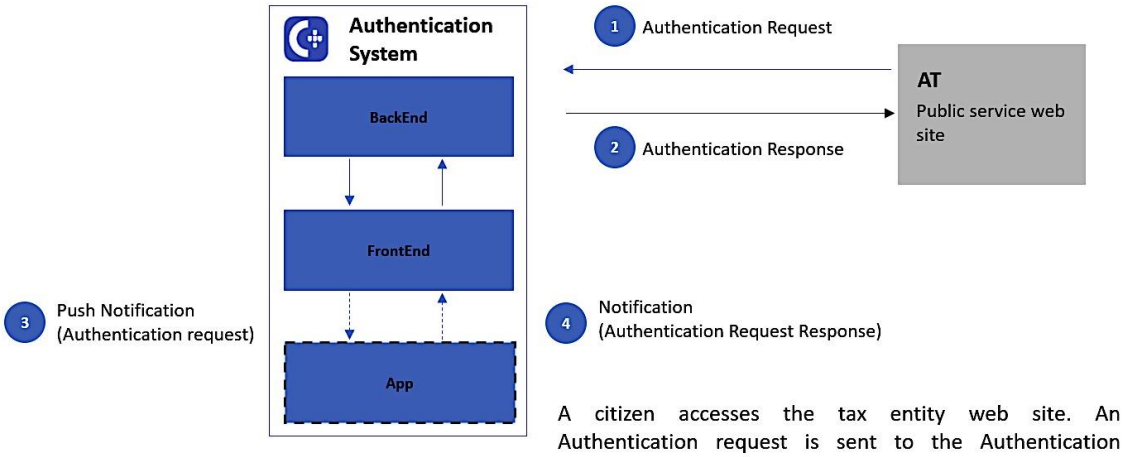
Autenticação.Gov is the main authentication provider for Portuguese citizens and people living in Portugal. Additionally, citizens can authenticate as a professional role using an authentication method provided by external entities.

Apart from authenticating the citizen, identity attributes are provided by the Autenticação.Gov platform. Many of the identity attributes that can be provided are owned by external entities or

governmental agencies. Depending on the trust level of the means/method the citizen chooses, some attributes may be restricted. A higher level of trust enables access to more identity attributes.

Table 10: Status and eIDAS readiness of authentication mechanisms

Autenticação.Gov	Status	eIDAS level
Professional Certificates	-	-
Username/Password	-	-
Social Networks	-	-
Professional Attributes Certification System (SCAP)	Pre-notified	High
Digital Mobile Key (CMD)	Notified	High
Portuguese national identity Card (eID card)	Notified	High



A citizen accesses the tax entity web site. An Authentication request is sent to the Authentication System backend which is then forwarded to its Frontend. The citizen chooses which way to authentify him/herself. Either he uses a card reader to read his/her eID card (citizen card) or he prompts the frontend to send a push notification to his/her mobile app. After reading the eID card or acknowledging the notification, the frontend returns the Authentication response to the backend and then from the Authentication System to the tax entity web site.

Figure 11: Authentication request example

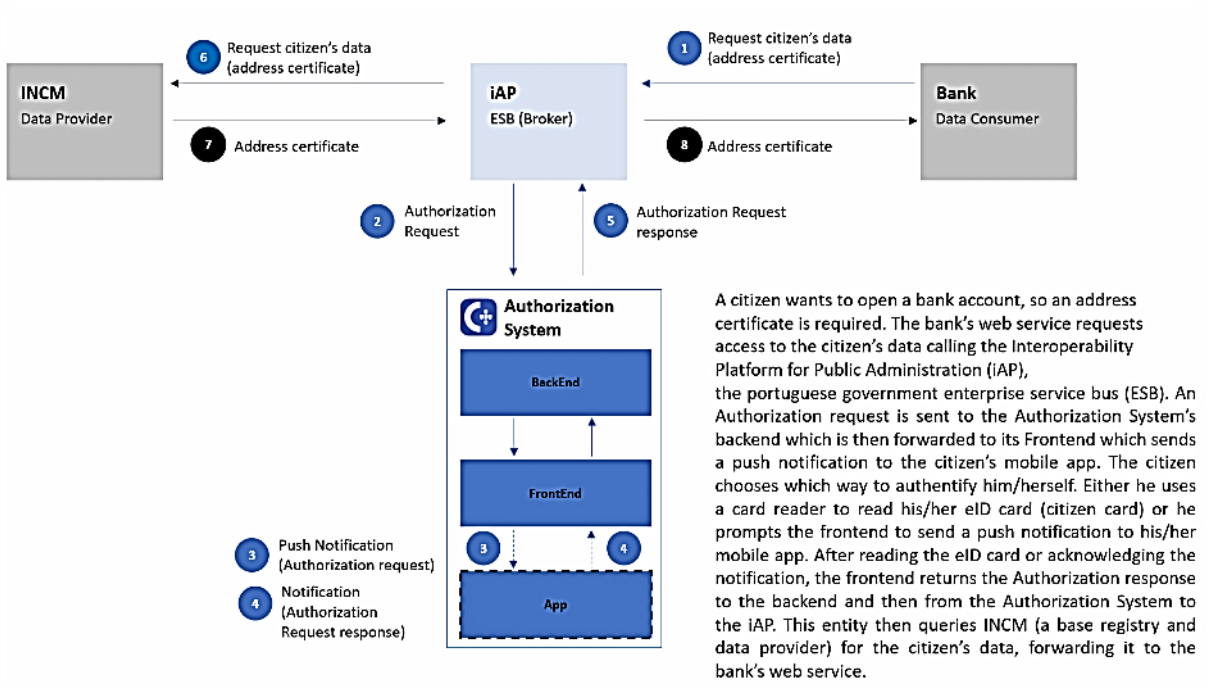


Figure 12: Attributes and authorization request example

2.6.2.1.1 Portuguese national identity card (eID card)

The Portuguese national identity card (Cartão de Cidadão) contains qualified digital certificates unique to each citizen. These certificates can be used as an authentication method by means of a software for reading the cards digital certificates that are protected by a PIN code.

This is considered the most trusted authentication method.

2.6.2.1.2 Digital Mobile Key

Autenticação.Gov allows a card less authentication method, Digital Mobile Key (Chave Móvel Digital, or CMD), that relies on a second authentication factor. The user can associate a mobile phone number and additionally an email address or a twitter account. The user must provide an identifier (phone number, email, twitter account), a PIN code (not the same as the ID card PIN), and a temporary security code the system generates. This is sent to the user's email, twitter account or mobile as an SMS or as a push notification.

Using the phone number with the Digital Mobile Key is the second most trusted authentication method. Using email or twitter is a level below.

2.6.2.1.3 Professional Attributes Certification System

In addition to the identity attributes, the system can provide attributes related to the professional activity of a citizen. These attributes are retrieved when the user authenticates him/herself. Depending on the trusted level of the authentication method used some of the attributes may or may not be available.

2.6.2.1.4 Social Networks

One of the lower levels of trust allow the citizen to authenticate him/herself using a social network as an Identity Provider.

2.6.2.1.5 Username/Password

Another low trust method is the use of a username and password.

2.6.2.1.6 Professional Certificates

Besides Autenticação.Gov main target being the authentication of citizens it also supports the authentication of professionals using digital certificates from trusted organizations. Presently this can be used to authenticate lawyers, notaries and solicitors.

With this method, only specific professional identity attributes can be provided. There is no relationship between the professional role authenticated and a citizen.

2.6.2.2 Portuguese eIDAS Node

The Portuguese eIDAS node is configured to delegate authentication into Autenticação.Gov. The rules for authentication are similar but there are no additional attributes provided for now. Portugal follows the centralized model, therefore only one eIDAS Connector is available, at least as it concerns the public sector.

2.6.2.3 eSignature

Electronic signature service for documents provides eSignature providing high trust authentication mechanisms, currently citizen card certificates and Digital Mobile Key certificates, to identify the citizen signing the documents. Additionally, professional attributes can be used to identify that the citizen is signing the document in a professional role or mandated.

To electronically sign the documents, the user must use a desktop software to ensure that the document is signed with the citizen's personal digital certificates. The software can use the citizen's eID card or the Digital Mobile Key.

2.7 Case study: Austria

2.7.1 General considerations on eID in Austria (eGovernment Act)

The e-government law is the centrepiece of Austrian e-government legislation and the basis for digital Austria. The law entered into force on March 1, 2004 and was last amended in 2018. In the meantime, there have been adjustments to the regulation for electronic identification and trust services for electronic transactions in the internal market (eIDAS regulation). The core elements of e-government in Austria are digital projects such as the Citizen Card, which functions as an electronic ID on the Internet. Electronic official services, such as electronic delivery, were only possible thanks to the possibility of identification on the Internet using a citizen card. This clear identification and authentication by the Citizen Card enable the generation of a qualified electronic signature. This enables applications or contracts to be signed that would otherwise require a handwritten signature6 [22]. It includes the definition and the involved organisational dependences and responsibilities how the trust systems “Bürgerkarte” and “Handy Signatur” (Citizen Card and Mobile Signature) are built up.

One specific instrument for Trust in Austria represents the sourcePIN Register (Stammzahlregister): The Federal Ministry for Digital and Economic Affairs as the sourcePIN Register keeps the sourcePIN as well as corresponding registers for the clear identification of persons and their powers of representation. By the Federal Ministries Act 2017, BGBI. No. 164/2017, which entered into force on January 8, 2018, there have been some changes in the responsibilities of the respective federal ministries. Due to the BMG amendment 2017, the tasks of the sourcePIN Register also fall within the scope of the BMDW with the "E-government affairs" [23].

In order to fulfil data protection, Austrian individuals do not use uniform personal identifiers in procedures in natural e-government, but "field-specific" personal identifiers, which are derived from the number of the natural person concerned and the respective procedural area. Cryptographic procedures are used that are irreversible. This means that the Field Specific Pin can no longer be calculated back to the master number (hash operation). For reasons of data protection law, authorities may under no circumstances save the number of natural persons as an identity feature. If the Citizen Card is used to sign an electronic application, after checking the signature the master number is read from the Citizen Card and transferred to a secure Citizen Card Environment, in which a Field Specific Pin (bPK)7 is automatically derived. The bPK generated is calculated from the master number for the specific procedural area of the authority. After affixing with the Citizen Card, the authority only has the bPK - relevant for their area of activity - of the person concerned [24].

2.7.2 Citizen Card / Handy Signatur / etc. (Citizen related)

The Austrian eID system is a technology neutral, voluntary system. There is no particular issuer of eID credentials. The system is based on three high-level requirements that are:

- the eID means has to be capable of creating qualified electronic signatures
- the eID means has to store the identity link
- the eID means has to be capable of storing mandate and representation data for “authentication on behalf” scenarios.

[7] In German: Bereichsspezifisches Personenkennzeichen

The third requirement, however, is meanwhile obsolete, as the authority to authenticate on behalf of another (natural or legal) person is queried on the fly from online authoritative sources (e.g. a mandate register or the company register).

Austrian eID is based on different eID means: smartcards or mobile ID. It has been introduced in 2003 and the first rollouts were in 2005. The Citizen Card is a smartcard QSCD (qualified signature creation device) for some professional representatives (lawyers, notaries, civil engineers, officials authorized to represent citizens). It specifies object identifiers in the qualified signature certificate indicate the holder's professional capacity. In Austria each citizen obtains a health insurance card which is a smartcard QSCD issued to replaced previously paper-based health insurance certificates. From 2005 onwards it can be activated as eID. The number of active eIDs raised to about 80 thousand in 2014, but with the success of the mobile eID "Handy-Signatur" the number decreased to about 40 thousand active eIDs (April 2017). The activation of the health insurance card as eID is free of charge for the citizen.

Mobile ID Handy-Signatur [25] is based on remote qualified electronic signatures, i.e. the signature creation is managed with a QSCD in a hardware security module (HSM) by a qualified trust service provider on behalf of the signatory. It is a two-factor authentication system with username/password as "knowledge" and the citizen's mobile phone as "possession" (an app cryptographically linked to the HSM for smartphones, or SMS onetime passwords). The mobile ID is free of charge for citizens. In May 2020 more than 1.400.00 active users could be measured.

All Austrian eID means have in common that it is a QSCD, which fulfil the requirements of the above mentioned (1) and (2).

The identity link is a SAML record electronically signed by the source PIN register authority (the Austrian Data Protection Authority which is the authority in charge of the eID system). It is created upon eID issuance and links the qualified certificate to a source personal identifier (source-PIN) which is a citizen's unique identifier that is cryptographically derived from a Central Population Register [23] identifier. Identification is based on sector-specific identifiers – during the authentication process a different person identifier is cryptographically derived for each sector of state activity (like health, tax, education), for each private sector organization, respectively (see previous chapter).

The Austrian eID system is browser-based. The integration of any eID mean is supported with an open source module "MOA-ID" (Module for Online Application – Identification) [26] that is operated by the service provider. MOA-ID represents an identity provider which offers two interfaces, one controlling the eID tokens and one interfacing to the services:

- The interface to the citizen's eID token is working via HTTP that either is provided by the mobile ID service provider or, for smartcard eIDs, through a software running at the citizen's PC.
- The interface to the service provider is either SAML (SAML 2.0 for the majority of services, SAML 1 for a few older legacy application), OAuth is offered as well.

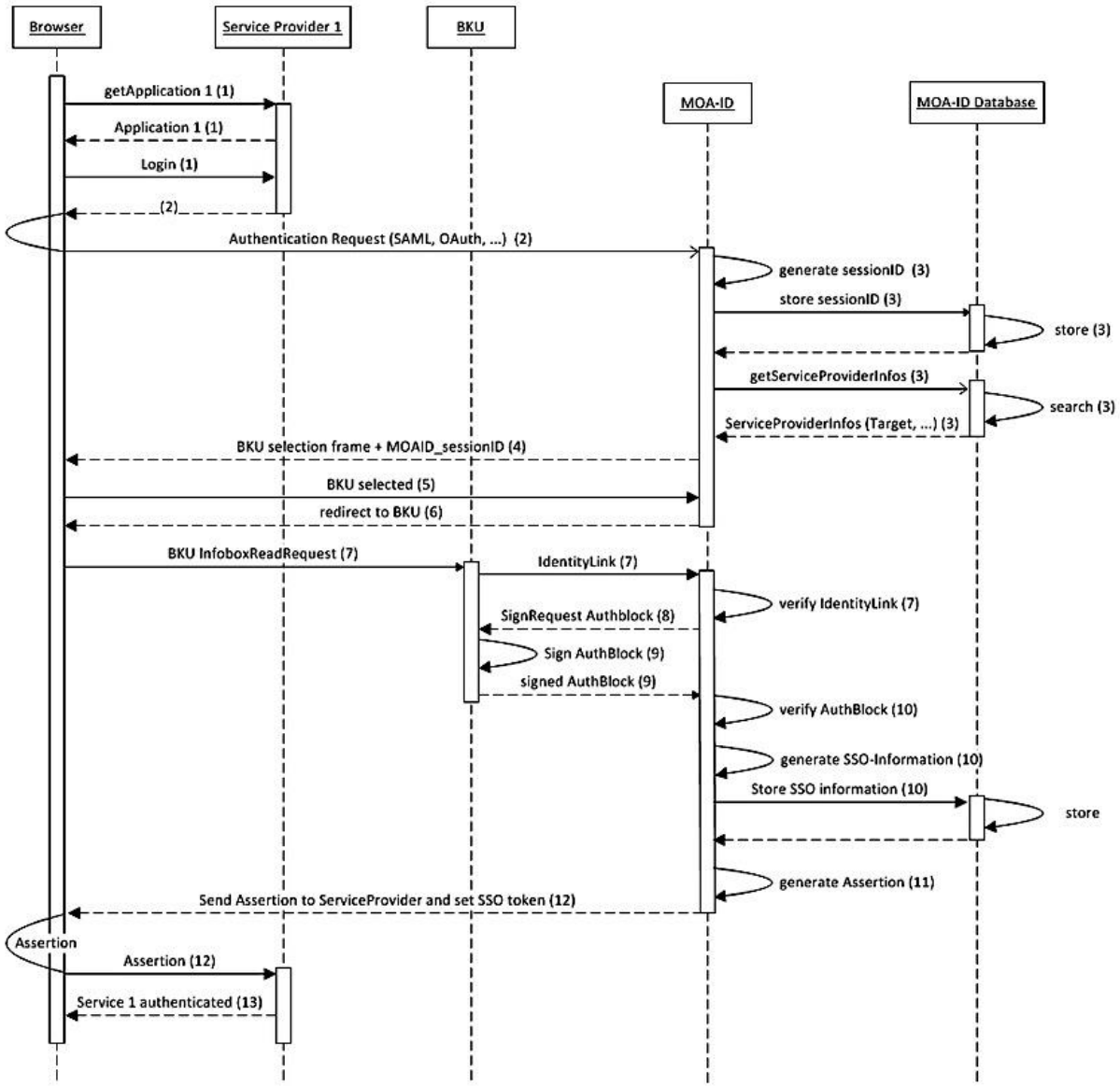


Figure 13: Depiction of an eID application and authentication process[8]

The Austrian eID can be used in about 300 public sector and private sector services. The main ones are tax online, social security services, or the electronic health records. Private sector services include Internet banking or electronic delivery. Services of the public sector (e.g., Tax Authority, Citizen Portal) are also managing username/password solutions as fallback mechanisms in case the user does not use one of the mentioned eID means.

2.7.3 SEMPER - business representatives' login (business oriented)

The business use case must be distinguished from the citizen use case because in this case citizens act as representatives for businesses. There is an ongoing EU-project called SEMPER to evaluate the

[8] Source: https://apps.egiz.gv.at/handbooks/moa-id/handbook/intro/intro.html

necessary extensions of the EIDAS login in the context of business use cases. EGIZ (technical university Graz) is taking part in the SEMPER project for AT.

The results of the SEMPER project must be incorporated in the DE4A architecture.

2.7.4 Finance Online eID

Finance Online, the central platform for citizens and business for tax declarations (and other online services) exhibits another eID widely used in Austria. It offers an eID with three different credential parts:

- Participant identification (TID)
- User identification (BENID)
- Personal identification number (PIN)

These access codes are transmitted by postal delivery with a return receipt. It is possible to apply personally, via eForm or in form of an allowed representative of a person. [27]

2.7.5 Inner Government Trust on Applications

The Portal Network (PV) represents a uniform framework for access to cross-agency web applications and the administration of the associated rights. It acts as a single point of administration and enables users and their rights to be managed in one place - regardless of the number of applications used - where the user is a member of staff. PVP represents a single sign on functionality, means that all applications in the portal network can be addressed with a single registration process. To ensure a uniform security policy and to determine the organizational responsibilities, the participants in the portal network have undertaken to comply with the regulations of the portal network agreement [28].

The aim of the Austrian Portal Network system is secure and efficient communication within and between authorities at different administrative levels. The Portal Network enables the participants to use their local user administration for external applications. Providers of authority applications therefore do not have to worry about user administration and single sign-on (SSO) for all Portal Network applications is made possible. Participation in the Portal Network is regulated in the Portal Network Contract (PVV). This contains rights and obligations which the participating organizations undertake to adhere to when they join. The technical basis for the Portal Network is the Portal Network Protocol (PVP) [29].

Portals are defined as entry points into a system that can be reached via electronic communication. Master portals (Identity Providers) are the portals on which the users with their access rights are administered. Application portals are those systems that are upstream of applications and allow access to the applications from the Portal Network. In the new SAML 2 standard integrated in the Portal Network, an application portal roughly corresponds to a service provider. Users log on to their main portal and can call up the desired target applications (e.g. GDB, ZMR) from the application list if they have the appropriate authorization. Due to the trust relationship within the Portal Network, the application portal accepts the user rights reported by the main portal for a user. On the application portal, maximum rights per application can be set for the organizations involved (access-authorized bodies) [29].

The Austrian SAML Profile “PVP 2” is a national SAML 2.0 profile that is pretty close to the Kantara eGov 2.0 profile, as well as close to eIDAS. The Austrian integration middleware “MOA-ID” has an eIDAS interface, it has undergone and passed the CEF eIDAS conformance test in March 2017.

2.7.6 eIDAS in Austria (Node)

For the governmental connection to the eIDAS node a specific online application is necessary: the MOA-ID. For services in the public sector, the current version of MOA-ID supports user authentication via mobile signature (or citizen card) and this infrastructure allows the authentication via eIDAS-compliant European eIDs. The aim is to make the user authentication method actually used (mobile signature or eIDAS-compliant eID) as transparent as possible for the service provider [30].

However, due to technical restrictions, there are occasional differences in authentication via an eIDAS-compliant eID, which may be relevant for service providers.

To illustrate this, a typical authentication process using an eIDAS-compliant electronic ID (e.g. German eID card) as outlined below. The basic assumption behind the sketched example is accordingly that a (German) user would like to register with an Austrian service provider with his or her eID [30].

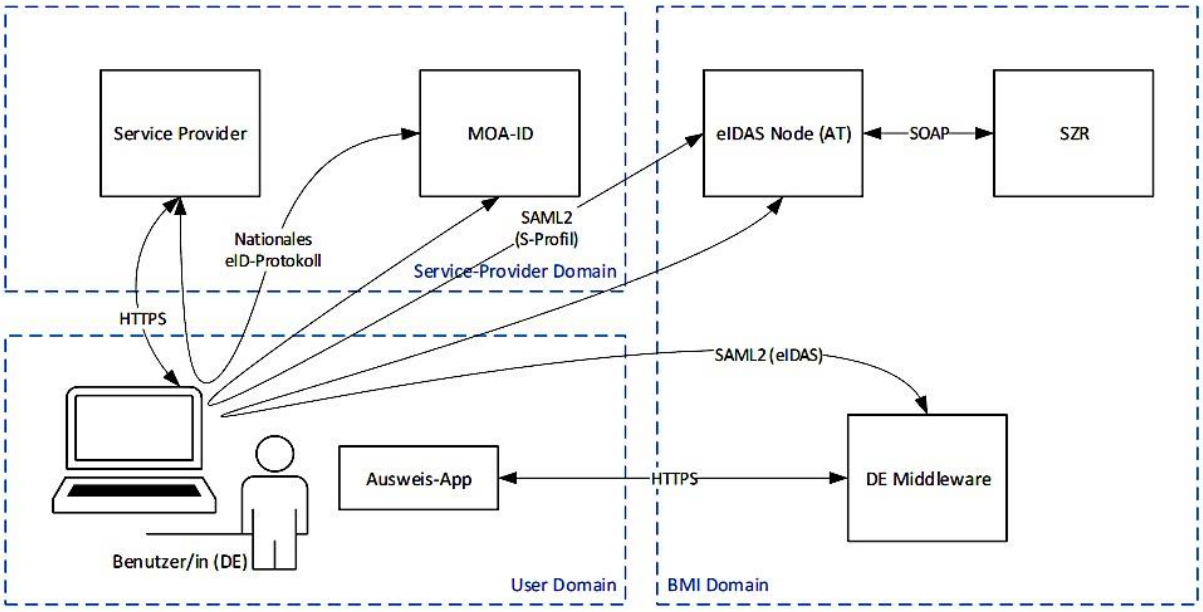


Figure 14: eIDAS based user authentication depiction (AT model)[9]

2.7.7 Notarisation via Blockchain

Austria has developed a pilot project to evaluate the use of Blockchain-technology in the context of notarization. The pilot project was completed successfully but is not yet deployed in production.

[9] Source: https://intranet.e-gov.ooe.gv.at/?selectedTab=help

2.8 Case study: Sweden

2.8.1 Background

Since September 29, 2018, it has been possible to log in with some foreign e-credentials in public Swedish e-services and in some private services that require e-identification.

Sweden Connect provides access to Sweden's eIDAS node and secure login and e-signatures for users with Swedish and foreign e-credentials.

The principal responsible for Sweden Connect is DIGG - the digital administration authority, which is a government agency with the task of supporting and coordinating the public sector in matters relating to e-identification and e-signature, nationally and internationally.

Sweden Connect contains functions for electronic identification and is the point of connection for eIDAS in Sweden.

Sweden Connect consists of:

- A technical framework that describes how connecting services and e-credentials must behave in order to function
- An actor registry where services and e-credentials register contact information and SAML metadata.
- The Swedish eIDAS country node that connects services and e-identification providers and handles e-identification traffic across the national border according to eIDAS.

2.8.2 Trust Levels

eIDAS's confidence levels and the Swedish Confidence Framework are based on the same international standard. The higher the level of trust, the safer the e-identification, both in terms of degree of security in technology and identification.

Within eIDAS, the three levels of trust are “low”, “substantial” and “high”. In Sweden, according to the Trust Framework for Swedish e-identification, confidence levels 1-4 are part of the national scheme of levels of assurance. The level of confidence "substantial" according to eIDAS corresponds fully to level of confidence 3 according to Swedish e-identification. The confidence level "high" corresponds to the Swedish level of confidence 4 except that personal visits are not required when renewal of the e-identification. The Swedish confidence levels 2-4 are described in the Swedish Confidentiality Framework for Swedish e-identification.

According to the eIDAS Regulation, it is mandatory for public authorities to recognize notified, foreign e - credentials at the level of trust “substantial” and “high”. That is, the legal requirement covers those e-services that require in-country e-identification with confidence level 3 or 4 for login. It is optional to rely on registered e - credentials with a “low” level of trust.

The basis for the level of security that is applied when a user identifies is the level of confidence in the e-identification that the e-service requires. All issuers of identity certificates must show that the entire process that forms the basis for issuing identity certificates meets the requirements of the requested level of trust.

- Requirements for the creation of the identity card.
- Electronic identification requirements (authentication).
- Requirements for the issuing process.
- Requirements for e-identification itself and its use.

- Requirements for the issuer of the e-identification.
- Requirements for establishing the identity of the e-identification applicant.

The level of trust required by an e-service credential depends on how sensitive the information is and, on the consequences, if it goes into wrong hands. For example, logging in to book time in the laundry room does not justify as high a level of trust as financial transactions. Therefore, the person responsible for the e-service needs to assess the level of trust in relation to information security requirements.

2.8.3 Technical Framework

Sweden Connect Technical Framework is adapted for identity federations based on SAML 2.0. Reliable parties receive identity certificates in a standardized format from a credentialing service.

E-services that require signatures do not need to be adapted to different users' e-credentials to create electronic signatures. Instead, the e-service transfers this to a signature service where users with the support of credentials through a credentialing service are given the opportunity to sign electronic documents.

Within the federation, e-services and similarly trusted parties assume the role of Service Provider (SP), while identification services that issue identity certificates assume the role of Identity Provider (IdP) and thus the person who authenticates the user, regardless of which e-service the user legitimizes.

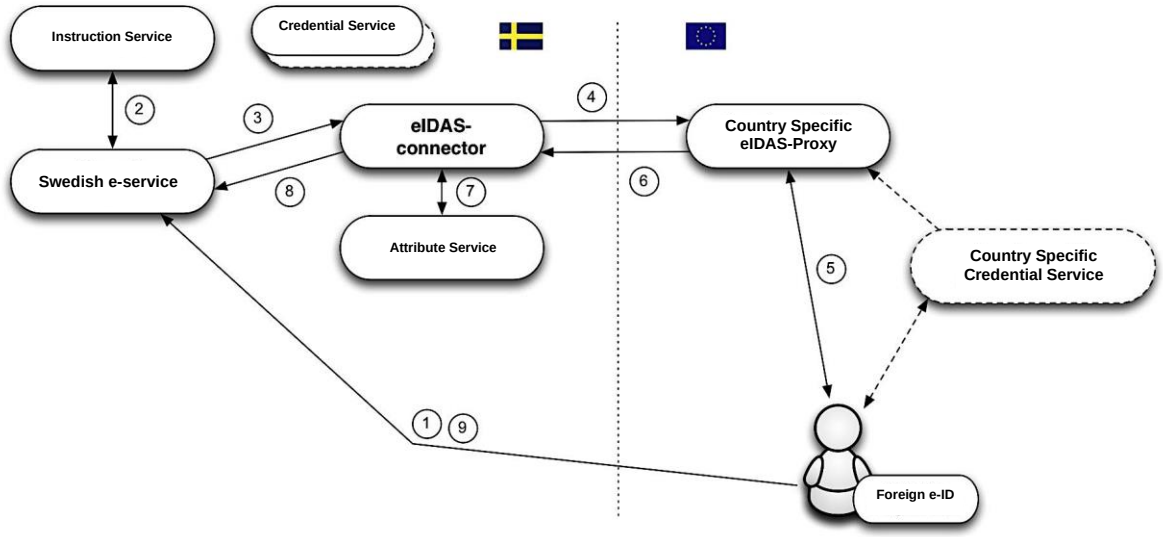
For those cases where the e-service needs more information about the user e.g. For information on legal jurisdiction, a question can be asked to an Attribute Authority (AA) within the federation, if such a relevant attribute service exists. Through an attribute request, the e-service can obtain the necessary additional information in order to be able to authorize the user and give access to the e-service or the equivalent.

Since both personal identity information and other attributes associated with users are provided through identity certificates and attribute certificates, all types of e-credentials, that the trusting party has an agreement with and which are part of the federation, can be used for identification with an e-service that requires both social security numbers and additional information, including if the e-identification does not contain any specific personal information (egg code boxes for generating one-time passwords).

The technical specifications for eIDAS, such as the technical framework, are based on SAML standards, and although there are many similarities, there are differences in these specifications. However, a Swedish e-service should not relate directly to eIDAS's technical specifications.

2.8.4 Process Description

The picture below illustrates how the Swedish eIDAS node (eIDAS connector) acts as a bridge between other countries and the Swedish federation when a person is authenticated with a foreign e-identification against a Swedish e-service. The Swedish eIDAS node is part of a technical framework.



The process is as follows:

1. A user with a foreign e-ID requests access to a Swedish e-service (i.e., log in).
2. The e-service allows the user to choose a login method with the help of an instructions service. A selection "Foreign eID" is displayed, which the user chooses in the eIDAS case.
3. The e-service creates a credentialing request in accordance with this technical framework and directs the user to the Swedish eIDAS node (connector) for which DIGG is responsible. The eIDAS node acts as an Identity Provider (Identity Provider) in the Federation towards Swedish trusting parties, which means that communication with this service is carried out in the same way as other legitimation services within federations that follow a technical framework.
4. The received request is processed and the eIDAS node displays a selection page where the user selects "their country" 1. The Swedish eIDAS node now converts the received credential request into a credential request according to eIDAS and the user is directed to the selected country's "eIDAS Proxy service".
5. When the credential request is received by the eIDAS-Proxy service for the selected country, this country's technology for authentication takes over. Not all eIDAS countries use SAML for authentication, but if that were the case in our example, the user would be redirected to an Identity Provider, and before that, perhaps even a credential service selection service.
6. When an authentication is performed, a certificate (Assertion) is created according to eIDAS specifications. This certificate includes: eIDAS-specific attributes that identify the user.
7. This certificate is now passed on to the Swedish eIDAS node. The node receives the certificate and validates its accuracy. When the certificate is transformed from eIDAS format to a certificate designed according to a technical framework, the node also invokes an attribute service to obtain, if possible, given eIDAS attributes supported by the Swedish e-service (e.g. look up a Swedish social security number given an eIDAS PersonIdentifier attribute).
8. Finally, a certificate, in a format that meets the technical framework, is posted to the e-service.
9. Any trusting party may supplement additional information and decide whether the user should be granted access to the service.

Swedish e-services thus only need to support the technical framework in order to handle an authentication performed with a European e-identification. However, the e-service must be able to handle the identity presented, which is not necessarily a social security number. Thus, it may happen

that an e-service authenticates a user via the eIDAS framework, but that the user's presented identity cannot be used with the e-service.

2.8.5 Status

In Sweden, some authorities have made it possible to log in with foreign (eIDAS) eID. In most cases, the user then comes to a "waiting room" and is not given access to the various services provided by the authorities as it is often required to have a Swedish personal identity number. However, the Swedish Tax Agency has developed the service "Rot and rut for companies", which is a service where a person hiring another person to do ROT (Repairs, Conversion, Extension) or RUT (Cleaning, Maintenance and Laundry) work may get a tax reduction. In the service it is possible to log in and also sign with a foreign (eIDAS) eID. The Swedish Tax Agency also plans to open additional services for those with foreign eIDs.

When it comes to the question of notifying a Swedish eID-solution in accordance with the eIDAS regulation, Sweden has not done so yet and there is no decision as to which Swedish e-identification will be notified, but it is likely to occur within a not too distant future.

It may also be mentioned that work has been initiated at national level to identify and analyse the public administration's need for measures to increase and standardize the use of trusted services and to propose such measures, in particular when clarifying when advanced and qualified electronic signatures should be used in public administration.

Connected countries with permissible e-credentials in Swedish public e-services are currently:

- Belgium
- Estonia
- Italy
- Croatia
- Luxembourg
- Spain
- Germany

2.9 Case study: Slovenia

2.9.1 General considerations on eID and trust services in Slovenia

In Slovenia, qualified digital certificates have been used for user authentication and electronic signature since 2000, when the eSignature EU directive was implemented. Despite the fact that qualified certificates are being issued by the public and private certification authorities for more than 19 years, the adoption and use of e-identities still remains relatively complex and insufficiently widespread to allow for a wider implementation of eCommerce in both the private and the public sector. If such situation pertains, and the uptake of e-services does not improve substantially at a national level, no significant success can be expected in the digital single market as well. Therefore, promotion and acceleration of the employment of eID and eSignature digital service infrastructure amongst both public and private entities is an important step not to meet only the requirements of the eIDAS and SDGR regulation with "once only" principle implementation, but to reach the digital transformation of the society in general.

In Slovenia the new legislation for eID and trust services is under preparation. It is expected that it will be adopted in 2020. The new act will introduce the national e-identities that will be based on the national identity card and mobile based solution. Such approach is supported also by Slovenian private sector. The new national identity card is planned for mid-2021, mobile based solution will be further developed to meet the technological development.

The Ministry of Public Administration Republic of Slovenia, as the main coordinating body for e-Government service development and implementation in Slovenia, has been managing various building blocks for trust services and e-identification. Their usage is widely promoted for the Slovenian public administration.

2.9.2 Authentication and eSignature service in Slovenia

The Authentication and e-Signature Service SI-PASS is composed of the following components:

- Slovenian Central Authentication System (SI-CAS)
- Slovenian Central Server-based eSignature system (SI-CeS)
- Slovenian eIDAS Node (SI-PEPS)

2.9.2.1 Slovenian Central Authentication System (SI-CAS)

SI-CAS is an existing Slovenian central service for identity verification, which is operated by the Ministry of Public Administration. It is part of the national trust enabling infrastructure and is available to the e-services of the public sector. It provides a central identity to all users and supports different authentication methods that can be used by the Slovenian e-services. Furthermore, SI-CAS is coupled with the Slovenian business and citizen registries and provides trusted attributes to the services integrated within SI-CAS. The integration with SI-PEPS enables citizens and businesses from the EU MS to access the Slovenian public and private e-services. On the other hand, Slovenian citizens will be able to use e-services in other MS, when Slovenia notifies their national e-identities, expected to take place toward the end of 2021.

Users can authenticate using different eIDs, having different trust assurance levels, from the lowest (usernames and passwords, Facebook profile, etc.) to the highest level (e-identity on a secure token, e.g. on a smart card, notified eIDs with assurance level High), issued by different identity providers. The only user data stored in SI-CAS are their e-mail address and appropriately protected (encrypted or

protected by a hash function) basic identifiers. Information about the registered identity providers and the available attributes providers is also stored in the system.

A service provider that opts for SI-CAS is not required to engage with each identity provider and attribute provider separately. Instead, its interaction is only with the SI-CAS directly. In the process of authentication, SI-CAS acts as a trusted intermediary. Thus, on the service provider's request, SI-CAS verifies the user's identity at the relevant identity provider and, when necessary, obtains further identification attributes from the identity or attribute providers. For this purpose, SI-CAS has established direct trust with the service providers, identity providers and attributes providers. Trust is established both on the technical and formal level. High level architecture is given below.

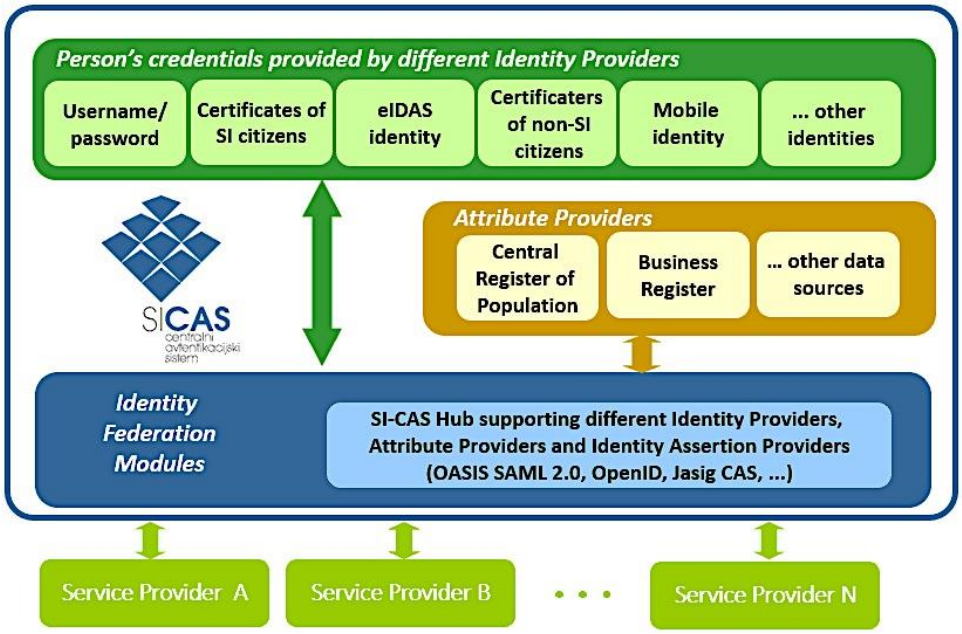


Figure 15: SI-CAS high level architecture

SI-CAS went live in November 2015 together with the new Slovenian state portal eUprava for citizens.

2.9.2.2 Slovenian eIDAS Node (SI-PEPS)

Slovenian eIDAS node was established in 2018 at the Ministry of Public Administration as part of the CEF Telecom SI-PASS (Slovenian eIDAS node and integrated services) project activities and was validated by DIGIT in June 2018. The node in production is based on the version 2.3.1 of the eIDAS sample implementation for Member States, and is currently connected to eight countries: Belgium, Croatia, Estonia, Germany, Italy, Luxemburg, Portugal and Spain. Connection with the remaining EU MSs that have already notified their identification schemes will follow in Q2 2020. The preproduction eIDAS node used for testing is currently connected to 12 MSs.

According to the eIDAS Interoperability Architecture SI-PEPS comprises eIDAS Connector (an eIDAS-Node requesting a cross-border authentication) and proxy-based eIDAS Service (an eIDAS-Node providing cross-border authentication). Slovenia is following the centralized model, therefore only one eIDAS Connector is available, at least as it concerns the public sector.

2.9.2.3 Slovenian Central Server-based eSignature system (SI-CeS)

The remote eSignature service SI-CeS was built with the aim to be modular, comprised of open-standards solutions, as well as various EU solutions developed by other initiatives, like the DSI building blocks. SI-CeS is tightly coupled with an Identity provider service, as strong authentication is a key

component in creating a remote signature. SI-CeS offers digital signatures with different levels of trust, including qualified digital signatures compliant with the EU legislation. SI-CeS currently supports different levels of advanced electronic signatures based on initial set of authentication mechanisms - SMS OTP two factor authentications and other authentication mechanisms (software based digital certificate, digital certificates with smart cards, eIDAS-based notified identification means).

The core module is the signing server, which provides the functionality of preparing a request for signing and creating a digital envelope of the documents' signature. Several standards of digital signatures are supported by SI-CeS: XML/XAdES, PDF/PAdES and PKCS7/CMS/CAdES. An additional module that is part of the platform is a module for safe management of the holder's keys and for creation of a remote signature.

SI-CeS went live in May 2017.

2.9.2.4 SI-PASS service

All three described building blocks (SI-CAS, SI-CeS and SI-PEPS) are combined in the SI-PASS service as depicted in the figure below.

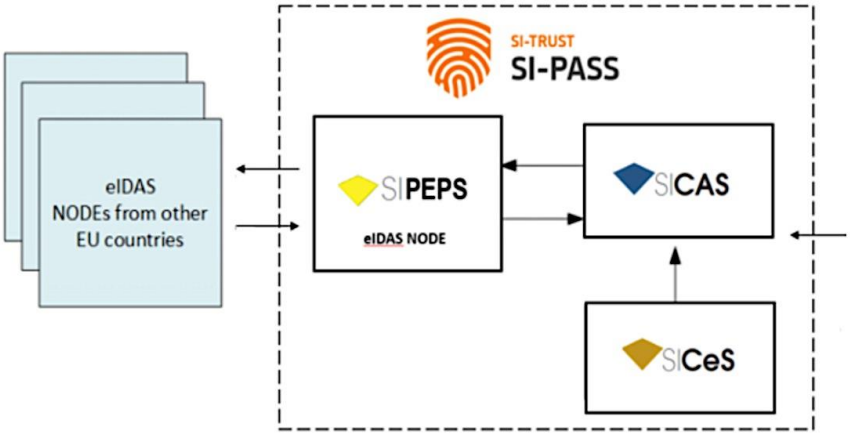


Figure 16: SI-PASS service high level architecture

2.9.2.5 Identity matching

Most of the Slovenian e-services request by the practical implementation or by the national law Slovenian national identifiers. The authentication of the cross-border users should be available fully online, also for retrieving the necessary national identifiers, like personal registration number (in Slov. EMŠO) or tax code.

In Slovenia, identity matching is performed centrally at the SI-PASS service (SI-CAS component), through queries in the Central Population Register (CRP) and/or Tax Register (RDZ). User-acquired attributes, namely personal registration number or tax code, are forwarded to the CRP and/or RDZ together with the attributes obtained through eIDAS to check if the data matches. In this case all these attributes are provided to the service provider as verified and therefore trusted.

3 Technological study

A study of different technologies that will support the integration of trusted services in the architecture is presented below. This study, in combination with the trust model assessment and elicitation will provide the technical baseline for the architecture that will be implemented and deployed in a joint effort in WP4 (Cross-border Pilots for Citizens and Business and Evaluation) and WP5 (Common Component Design & Development).

3.1 Self-Sovereign Identity (SSI) approach

3.1.1 Motivation and Policy Background

The technological advances (e.g. personal mobile devices, developments in cryptography and emergence of blockchain) are opening the prospect to build new identity frameworks that are based on the concept of decentralised identities. These decentralised identities are required to be self – sovereign. The SSI's ideation is to set up a system in which the user controls both the identity and the data associated with it. As noted by "The European Union blockchain observatory and forum" [31], the idea of SSI is that the individual identity holders can fully create and control their credentials, without being forced to request permission of an intermediary or centralised authority and gives control over how their personal data is shared and used. The user has a means of generating and controlling unique identifiers (called Decentralized Identity (DID)) as well as some facility to store identity data [31]. The users are not restricted on use of specific identity data (these could be verifiable credentials, data from a social media account, a history of transactions on an e-commerce site, or even attestations from other users).

Essentially, SSI is addressing the lack of existing partial or integrative approaches related to the existing notion of identity: data acquisition and maintenance, data processing, data silos, lack of data control, privacy issues, lack of universality and interoperability, limitations of eIDAS and lack of certification. The general observation of the forum is, that the "digital identity experience today is fragmented, with few standards or interoperability, and it is insecure, as the almost daily reports of hacks and data breaches reminds us" [31].

While other implementations would be possible for SSI, having its support on blockchain, including for trust management, is particularly well-suited considering the decentralised philosophy of this approach, given that as part of the inherent defining characteristics of blockchain technology, is the fact that it is able to confer a shared state of trust by means of its distributed replication of factual information across multiple nodes under a common consensus mechanism. In this way, the recorded information (e.g. claims as verifiable credentials, the role as issuers of such claims of accredited organizations or the existence of decentralised identifiers of stakeholders) can be truly considered tamper-proof and its notarization over this infrastructure also becomes highly trustworthy in terms of enabling verification of integrity and veracity of multiple different assertions. Blockchain infrastructure such as EBSI [32], particularly aimed on supporting public services, helps to realize principles and verify properties that strongly relate to multi-lateral trust, such as existence and persistence of information, transparency, non-repudiation, full control, access or consent.

Of particular relevance in the context of DE4A, and as acknowledged in its Thematic Report - Blockchain for Government and Public Services [33] "…agencies could share citizen identity data, saving them – and the citizen – the time and expense of continuously having to collect this information anew. By extension, blockchain should make it easier for governments to share data and services securely across borders, something of great import in a supra-national body like the EU. This could aid in implementing

the “once-only principle” as enshrined in the European e-Government Action Plan 2016-2020, which aims to reduce the administrative burden for citizens, institutions and companies in the EU by allowing them to provide certain kinds of standard information to authorities once, which the authorities can then re-use”. Similarly, the European Parliament Resolution on DLT and Blockchain [34] acknowledged the “potential for DLT for public sector services and management as regards reducing bureaucracy, especially with a view to enforcement of the eGov Action Plan with particular reference to the EU-wide adoption of the digital Once-Only Principle”.

It is precisely in the context of eGovernment, as also acknowledged by ESSIF Orientation Vision Text [14], where electronic procedures of public administrations (and other organisations) shall benefit from the possibility to acquire in digital data about citizens that can be immediately and reliably verified leading to clear efficiency gains. Indeed, much effort and time is currently wasted in manual checks to establish the veracity and validity of identity and of other data linked to it, clarifying semantic meaning (as an example, TNO has estimated that in the Netherlands, the annual cost of validating information supplied by citizens in electronic forms, exceeds 1 billion Euros). This is in addition to the savings in time for citizens and administrative staff of avoiding the former to have to visit physically places to collect and/or present the data, which also leads to better social inclusion (as in-person procedures can be a barrier for persons with disabilities for example) and a more green economy considering paper-less procedures. Considering the combination of these factors, they will lead to a better perception of public services by citizens and businesses as their users, leading to higher usage and increased trust in them (also related to users being in stronger control of the data related to them).

The current eIDAS framework, inasmuch it federates MS centralized identity systems, acts already as a powerful catalyst to enable the Once-Only principle and is in that sense acknowledged as a relevant building block already by the SDGR (Art.13). Designing SSI solutions aligned with and supporting the EU regulation on electronic identification, authentication and trust services (eIDAS), pertaining to government-issued/recognised identity credentials and currently under a review process, is a necessary goal currently [35] being addressed in the context of identity services in EBSI -European Self-Sovereign Identity Framework (ESSIF) [36] - both from a technical [37] and legal perspective [38], e.g. the legal report produced by ESSIF outlines a number of short and mid to long-term scenarios that would allow a gradual convergence of SSI with eIDAS and the potential evolution of the latter.

In this context, SSI is also perfectly positioned to complement the solid legal framework for identity (and trust services) of the eIDAS regulation with a more flexible yet secure approach towards managing, under the full control of the user, domain-specific attributes (including more complex standardised data structures) without requiring changes to the currently supported Minimum Data Set for natural and legal persons in eIDAS, while also enabling powerful features related to minimum disclosure (e.g. “proofs”) and materialising the data minimisation principle of the GDPR and bringing into the picture a more easy integration with a wider ecosystem of stakeholder, including the private sector.

The further development of the idea of SSI and its potential influencing the future development of regulatory frameworks is part as well of the context in DE4A for the assessment of innovative technologies with transformative impact such as blockchain, with a positive role to substantiate the vision to reinforce trust in public institutions’ transparency and protection of users’ information. In fact, longer-term time horizons beyond the implementation of the SDGR, e.g. towards a European Government Interoperability Platform (c.f. DE4A D2.1 [25]), would largely benefit from the transformative technologies presented in this section.

3.1.2 Trust Model of SSI and Conceptual Building Blocks

Blockchain-based eGovernment solutions need to consider an emergent trust model which presents a number of distinctive and original features. In DLT and blockchain-based systems, a centralised registration system is not needed but these are rather based on Decentralised Public Key Infrastructure (DPKI) which combines Decentralised Identifiers (DIDs) with a Decentralised Key Management System (DKMS) for cryptographic key management and where the root of trust is in a distributed ledger (as decentralised key-value datastores) that supports the anchoring of such DIDs (in this model cryptographic trust anchor stores are replaced by the DLT implementing the DPKI). DIDs act as a standardised type of unique identifier (https://w3c.github.io/did-core/) under the control of subjects (users being natural or legal persons) and which serves as basis for self-sovereign identity, relating through a uniform resource locator a subject with a "DID Document" that describes how the DID should be used e.g. for authentication [39]. DID documents are discovered or read by means of a lookup function (in a step known as resolving the DID), which in EBSI is offered by a "DID API" [40]. DE4A will use similar DID-resolver functionality too.

While this trust model (being decentralised), features key differences with e.g. PKI-based federated models, some similarities can also be found with highly successful trust frameworks such as eIDAS, for example, service providers (i.e. online procedure portals acting as Data Evaluators in DE4A), in the role of Verifiers can check the DID of the Issuer (e.g. a University or Ministry of Education) and of the Subject (Holder e.g. a student) presenting a VC and could check the structure of data corresponds to a standardized data model (registered schema) but they will still need to trust that the actuality and veracity of the content of the VC is guaranteed by its Issuer (e.g. that a student was indeed awarded a Diploma), without knowing further details about the underlying process behind. This is similar to eIDAS trust framework where a MS requesting authentication of a user relies on the truthfulness of the result of such authentication to a given LoA and the attributes provided in the response by the issuer of the eID.

The constituent elements of the model are subsequently described in more detail.

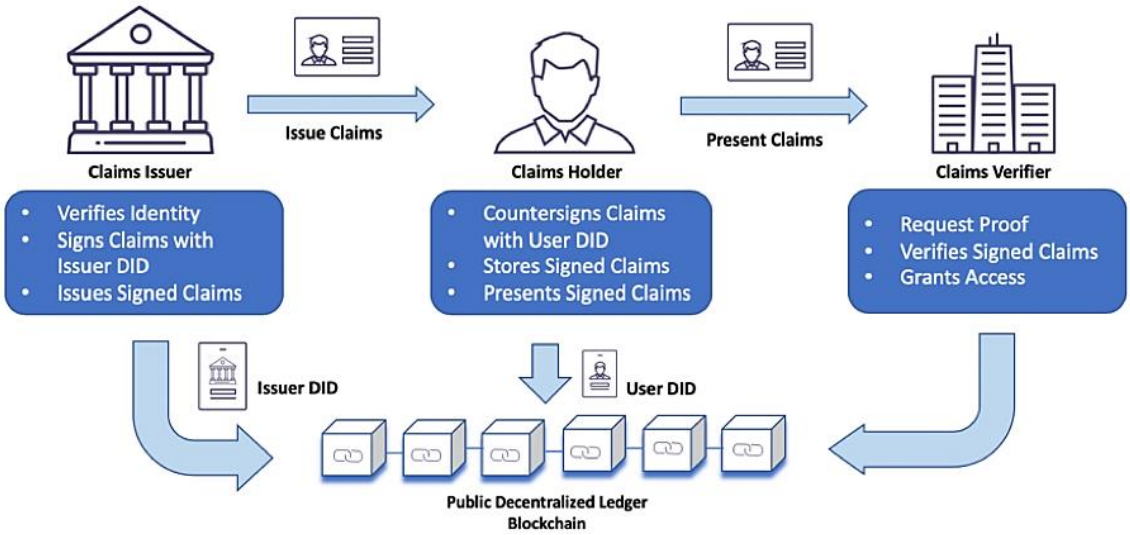


Figure 17: Conceptual representation of the SSI approach [41].

As presented in Figure 17, the VC's Subject, i.e., Claims Holder, also referred as User, can use a secure wallet on his edge device to generate public/private key pairs and thus create his decentralized identifier. The private key with which the DID is managed is stored within the wallet (also known as User Agent). Usually (but not necessary) the DIDs of Claims Issuer and Claims Holder are published, i.e., registered on a decentralized ledger (DLT). In the case of peer-to-peer DID connection between entities, typically only the Claims Issuer registers his DID. Later, DID can be resolved to DID document, which contains all the necessary pieces of information (authentication methods, endpoints where entities can be reached, etc.) about the entity, i.e., Issuer or Holder.

As can be seen in the figure, the User plays a central role in the above model and can request a trusted authority (e.g., University) for validated claims, normally in the form of a Verifiable Credential, including attributes about the User (claims), which are digitally signed with the Issuer DID. A third party service provider (i.e., Claims Verifier), to which the User presents claims (VCs), can validate the authenticity by verifying the public key signatures related to the Holder DID and Issuer DID registered on the decentralized ledger and provide the requested service based on the presented claims. With this approach, citizens (and also non-residents) will be able to provide such VCs (attestations) issued to them by both governmental and non-governmental organisations enabling the Claims Verifier (e.g. a governmental agency, a university admissions department, etc.) to obtain with high assurance that the subject is eligible to the requested service (e.g. social benefits, academic grant, etc.) or can be authorized to access given IT systems or act under a given role or position.

Subjects (Claims Holder in the above figure) are enabled and requested to demonstrate DID ownership linked to their control of cryptographic material that was generated when the DID was created: by using the DID private key they possess, they can construct (sign) a response to a challenge sent by the relying party (c.f. EBSI DID Auth Service [42] based on DID auth project, https://github.com/decentralized-identity) who can verify it based on the public key of the DID available through its ledger record. Issuers' DIDs would also be registered in a specific ledger, equivalent to the concept of Trusted Issuer Ledger (storing information about trusted issuers without the need for a chain of trust) present in EBSI [43].

In this model, owners of DIDs will communicate with issuers of verifiable credentials (e.g. data providers issuing certain attestations like a diploma) and with verifiers of such data (relying parties such as online procedure portals) by means of Agents [44]: for example, the client or edge agent of a subject implemented as a mobile app or wallet and the server-based agents of data issuing and consuming authorities, running as back-office services. The secure connection establishment between parties is thus mediated by their Agents and can be bootstrapped by means of popular mechanisms, e.g. scanning of a QR barcode presented from one agent to another. It is expected ESSIF only provides implementation-neutral guidelines in relation to these Agents, whereas it is expected that the industry will offer different production-grade implementations and projects like DE4A will support pilot-level implementations. Currently ESSIF offers for demo purposes a simple front-end example of web-based user agent (Wallet Web Client [45]) which features access control through ECAS login authentication (https://app.ebsi.xyz/wallet/login) and is based on the Wallet core service specification [46].

As VCs include attestations (digital claims) about certain attributes which cannot be tampered with, it becomes, together with the DID concept, crucial to creating trust in an SSI ecosystem in order to enable transactions. However, as attestations have a broader scope compared to eID and, as the consequences of both involuntary errors and malicious attacks on exchanged data can be largely variable depending on the specific use of the information and the domain(s) involved, more careful consideration is needed of multiple aspects with an impact on trust, including but not limited to quality of information assurance, liability of involved parties (including infrastructure providers/operators), SLAs, governance, etc. Nonetheless, most of these aspects are not specific to the use of blockchain as

underlying technology and those that are specific, like functional components with a role in trust management (consensus protocol, peer-to-peer communication) are based either on international standards or community-based open source efforts which allow to detect and correct more quickly any design or implementation flaws.

3.1.3 Instantiating the SSI Approach in DE4A

Taking this to the context of DE4A's Diplomas Verification use case of the "Studying Abroad pilot", the DID cryptographic properties will be re-used to secure direct bilateral exchanges, that is, confidential communications between natural persons (students) and certain issuing authorities of academic information (e.g. universities or Education Ministries) as well as in communications where such data are presented as to the authorities consuming and verifying such information which is required for certain online procedures. DIDs of communicating parties will be verified against ledgers where they were registered when such DIDs were created and where public keys can be fetched in order to determine DID ownership as previously described.

In particular, given the fact that SSI scope can be understood as broader than only user-centric management of identity attributes (e.g. Verifiable IDs), in DE4A the focus will be on validating its benefits for managing other more complex types of information (e.g. diplomas in Studying Abroad pilot) which are verifiable attestations, which can be presented as Verifiable Credentials and become notarised in a privacy-preserving manner on blockchain ledgers as immutable proof system, in the form of automatically verifiable pieces of information that can be consulted by third parties. Thus, the SSI trust model will also be used in DE4A to allow data issuing authorities to also act as "trust providers" inasmuch as they will be issuing attestations (Verifiable Credentials or VCs) to the DID of a subject that they can verify [47]. Such Verifiable Credentials will also be notarized in a ledger and represent properties about the subject he or she can use at their own will (independently from the issuer) towards different third parties (Verifiers). By relying on the Issuer and the cryptography inherent to the blockchain infrastructure these thirds parties (Data Consumers in DE4A) are able to trust or rely in the provided information (through the citizen in the case of DE4A Verifiable Credentials pattern [2]) These in turn can verify the DID-signature of the VC against data in different ledgers that the VC was issued by an authoritative source (the VC contains the Issuer's DID) and that the VC has not been later suspended or revoked. They can also verify the formal correctness of the data structure against the corresponding schema also notarized in a specific ledger [48]. The SSI trust model thus enables decoupling the anchoring DIDs to the ledger from the issuance of VCs and their presentation to other parties, giving full control to users through their edge clients or agents ("wallets") of this lifecycle and enabling actors to accept the underlying shared trust framework.

DE4A Agent components will interact with different ledgers (and where applicable "registrars") to register DIDs of authorities and users in ledger-based registries accessible by counterparts in an electronic data exchange. For example, EBSI provides a public Trusted Issuers Registry service and API [49] that allows to verify whether a legal entity is authorised to issue specific W3C Verifiable Credentials. Such approach plays a major role in the context of establishing mutual trust in a decentralised system by providing a register of trusted public entities with their respective self-sovereign identities and their authorised list of VCs they are allowed to issue. Such registry can be considered to be similar to the "Registry of Authorities" of the SDG OOP Technical System. More specifically in the context of EBSI's Diploma's Use Case it is envisaged that entities like universities or other competent education authorities in a MS can only be registered by entities responsible to accredit them e.g. asserting the types of higher education diplomas a University can issue. Such approaches will be further explored by DE4A. Furthermore, it will be further investigated how the concept of Level of Assurance can be managed in relation to these "registrars" (i.e. based on their meeting of certain security requirements, etc.), which is important as it can be used to determine the

amount of trust that relying parties (Verifiers) can have in the DIDs. Specific VCs could also have a LoA associated to them in the Trusted Issuers Registry.

A Verifiable Credentials API and service exists in EBSI which provides "the capability of creating W3C credentials ready for signing" by the user wallet service and later validating the VC format and signature by receiving entities (Verifiers). It effectively enables "a flexible integration of verifiable credentials flows into any use case [49]". The metadata of VCs will also be registered on a ledger, allowing issuers to support suspension/revocation of issued verifiable attestations (e.g. case of fraud detection after issuing of a diploma [50]). Furthermore, used data models or recognised schemes for evidences exchanged in the VC pattern by DE4A would also be available in a catalogue supported on a specific ledger as proposed by ESSIF, allowing to check the VC conformance to harmonized standards (e.g. DE4A is considering Europass-EDCI data models along with pilot-specific requirements for its ontology of diplomas). In this regard and given that all entities will be known by their DIDs (strongly related to different supporting ledgers and DPKI's), "registrars" of DIDs and the related ledgers act as the true anchors of the whole trust ecosystem [51].

It is to be noted that, as enforced by ESSIF, data protection is built into the core of SSI approach, avoiding to store "on ledger" any information that would disclose real identity of DID owners, any such information will be stored "off chain" by means of Trusted Storage Providers [52]; DE4A will follow all available guidelines in this regard in a privacy-by-design manner ensuring GDPR compliance (c.f. SSI eIDAS legal report [53] and EBSI GDPR Assessment report). Also, ESSIF foresees in the future domain-specific ledgers, although this is not so relevant for DE4A pilots as VC pattern would focus only on the education domain.

While DIDs will serve to identify the stakeholders in the context of these communications [54], DE4A will not use SSI credentials for the purpose of authenticating e.g. students to service providers, as the ESSIF concept of Verifiable Identities still lacks the needed legal certainty compared to e.g. notified eIDs under eIDAS regulation. Rather, students will be first authenticated using standard eIDAS means and will later be able to obtain any missing data in the form of VCs from the corresponding Issuer(s) [55]. Such VCs will be used to represent Verifiable Attestations (e.g. Diplomas) and a DID-signing method will be used to support the needed guarantees of authenticity and integrity of the information; in regards to the legal value of attestations in the form of Verifiable Presentations, the eIDAS-bridge [56] concept related to the use of eIDAS eSeals over VCs when issued by authorities is also being closely monitored but its exact functional scope in EBSI-ESSIF v2.0 is not yet clear at this stage, see section [57] (at least for the first iteration of piloting it is unlikely that and additional eIDAS eSeal would be used on the issued VCs).

A specific consideration in the context of eGovernment services, and an advantage in this case, is that trust in our case does not need to rely on reputational trust models (as is the case in other blockchain approaches) because both the infrastructure and APIs (EBSI-ESSIF) and the stakeholders (public service owners) are already backed/operated by EU MS and it can be expected as well that a future legal framework (complementary to eIDAS or part of its evolution after its revision) will legally enable requirements related to proofs, minimum disclosure or full control to protect the subject and other participating parties. Both from technical and legal perspectives, it can be expected that approaches based on transformative technologies, which are researched in DE4A in conjunction with the current EBSI and ESSIF work, and the future update of legal framework will, just like eIDAS, serve to continue to remove obstacles to the functioning of the internal market; strengthen trust and, finally, increase legal certainty.

In the following section open source technologies are presented that DE4A could consider in the context of realizing Blockchain and SSI support.

3.2 Open source technological solutions study

3.2.1 Hyperledger Indy

Hyperledger Indy provides tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other silo. Indy is interoperable with other blockchains or can be used standalone powering the decentralization of identity [58].

Key Characteristics [59]:

- Distributed ledger purpose-built for decentralized identity
- Correlation-resistant by design
- DIDs (Decentralized Identifiers) that are globally unique and resolvable (via a ledger) without requiring any centralized resolution authority
- Pairwise Identifiers create secure, 1:1 relationship between any two entities
- Verifiable Claims are interoperable format for exchange of digital identity attributes and relationships currently in the standardization pipeline at the W3C
- Zero Knowledge Proofs which prove that some or all of the data in a set of Claims is true without revealing any additional information, including the identity of the Prover

Indy provides a software ecosystem for private, secure, and powerful identity, and libindy enables clients for it. Indy puts people — not the organizations that traditionally centralize identity — in charge of decisions about their own privacy and disclosure. This enables all kinds of rich innovation: connection contracts, revocation, novel payment workflows, asset and document management features, creative forms of escrow, curated reputation, integrations with other cool technologies, and so on [60].

Indy uses open-source, distributed ledger technology. These ledgers are a form of database that is provided cooperatively by a pool of participants, instead of by a giant database with a central admin. Data lives redundantly in many places, and it accrues in transactions orchestrated by many machines. Strong, industry-standard cryptography protects it. Best practices in key management and cybersecurity pervade its design. The result is a reliable, public source of truth under no single entity's control, robust to system failure, resilient to hacking, and highly immune to subversion by hostile entities [60].

- License: Licensed under a Creative Commons Attribution 4.0 International License
- Web: https://www.hyperledger.org/use/hyperledger-indy

3.2.2 uPort

A self-sovereign identity and user-centric data platform.

Built on interoperable standards, it offers a collection of tools and protocols allowing users to establish identities, send and request credentials, sign transactions, and securely manage keys & data. Portable

and reusable verifiable credentials give organizations and individuals the power to easily and fluidly control their data transactions with security, privacy and trust.

uPort is backed by ConsenSys, a global incubator of blockchain applications [61]. For more information:

- **Web**: www.uport.me
- **License**: Apache 2.0 / GNU GPL 3.0 (UPort Mobile)

3.2.3 Sovrin

'Sovrin' most commonly refers to the Sovrin Network, a public service utility enabling self-sovereign identity on the Internet. The Sovrin Network is decentralized, meaning individuals can collect, hold, and choose which identity credentials —such as a driver's license or employment credential—without relying on individual siloed databases that manage the access to those credentials.

Sovrin is an open source project that offers the tools and libraries to create private and secure data management solutions that then run on Sovrin's identity network [62].

The Sovrin Network consists of server nodes located around the world hosted and administered by a diverse group of trusted entities called Stewards. Each node contains a copy of the ledger, a record of publicly accessed information needed to verify the validity of credentials issued within the network.

In Sovrin, Stewards cross reference each transaction to assure consistency about what information is written on the ledger and in what order. This is done with a combination of cryptography and a Redundant Byzantine Fault Tolerant algorithm.

Identity holders, credential issuers, and verifying entities access these services on the Sovrin Network using Agents. Agents can be as simple as a mobile app and have the important job to hold and process claims on the Sovrin Network. Agents can perform identity transactions on the identity owner's behalf and exchange information directly with other agents with secure encrypted connections to each other. This way, only public identifiers of an issuer are anchored on the ledger, but an identity holder's actual proof of their credential is privately transmitted to a validator. Sovrin has specific instructions and developed code for the creation of these agents, so different agents from a variety of developers may all work together within the Network. This allows every person, organization, and thing to interoperate.

Sovrin allows the sharing of trustable digital credentials. The Sovrin Network is designed to be private by design on a global scale by using pairwise pseudonymous identifiers, peer-to-peer interactions, and allow selective disclosure of personal data using zero-knowledge proofs.

Simply put, when an identity holder decides to share a verifiable credential with a relying entity using the Sovrin Network, they create a proof containing only the specific information that was requested using a combination of elements from any of their verifiable credentials in their digital wallet. The verifier only learns the information that was shared and nothing else. The verifier cannot take the learned information and prove who it came from.

Using the Sovrin Network, each person, organization, or IOT device that validates the identity holder's proof can be completely confident that the proof or information being relayed is accurate and timely. Businesses can also avoid the regulatory burdens associated from storing mass amounts of customer data which could be stolen or misused [63].

- **License**: Apache 2.0
- **Web**: https://sovrin.org/

3.2.4 Hyperledger Besu

Hyperledger Besu is an open-source Ethereum client developed under the Apache 2.0 license and written in Java. It runs on the Ethereum public network, private networks, and test networks such as Rinkeby, Ropsten, and Görli. Besu implements Proof of Work (Ethash) and Proof of Authority (IBFT 2.0 and Clique) consensus mechanisms.

You can use Besu to develop enterprise applications requiring secure, high-performance transaction processing in a private network.

Besu supports enterprise features including privacy and permissioning.

Besu includes a command line interface and JSON-RPC API for running, maintaining, debugging, and monitoring nodes in an Ethereum network. You can use the API via RPC over HTTP or via WebSockets. Besu also supports Pub/Sub. The API supports typical Ethereum functionalities such as:

- Ether mining
- Smart contract development
- Decentralized application (Dapp) development.
- Besu does not support key management inside the client. You can use EthSigner with Besu to access your key store and sign transactions [64].

- **License**: Apache 2.0 license
- **Web**: https://besu.hyperledger.org/en/stable/

3.2.5 Hyperledger Fabric

Hyperledger Fabric is an enterprise-grade, distributed ledger platform that offers modularity and versatility for a broad set of industry use cases. The modular architecture for Hyperledger Fabric accommodates the diversity of enterprise use cases through plug and play components, such as consensus, privacy and membership services.

Hyperledger Fabric is intended as a foundation for developing applications or solutions with a modular architecture. It offers a unique approach to consensus that enables performance at scale while preserving privacy.

One of the many compelling Fabric features is the enablement of a network of networks. Members of a network work together, but because businesses need some of their data to remain private, they often maintain separate relationships within their networks. For example, a purchaser may work with different sellers, selling the same product. The transactional relationship between the purchaser and each of the sellers should remain private and not visible across all sellers.

This is made possible via the “channels” feature in Hyperledger Fabric if you need total transaction isolation, and the “private data” feature if you’d like to keep data private while sharing hashes as transaction evidence on the ledger (private data can be shared among “collection” members, or with a specific organization on a need-to-know basis. Rather than an open, permission-less system, Fabric offers a scalable and secure platform that sup-ports private transactions and confidential contracts.

This architecture allows for solutions developed with Fabric to be adapted for any industry, thus ushering in a new era trust, transparency, and accountability for businesses. From the very beginning, Hyperledger Fabric was designed for enterprise use. It is intended as a foundation for developing applications or solutions with a modular architecture. Its modular and versatile design satisfies a broad range of industry use cases. It offers a unique approach to consensus that enables performance at scale while preserving privacy.

Unlike some other distributed ledger technologies that were originally designed for ad hoc, public use (where there is no privacy and no governance) which had to be significantly redesigned to add in support for permissions and privacy; Hyperledger Fabric was designed with these features as foundational. In this regard, Hyperledger Fabric has had a head start over many of the competing frameworks. For example, while there may be promise in some of the Ethereum 2.0 implementations, these are still mostly oriented to public network use, and in the Ethereum public network, the new architecture has still yet to be rolled out while Hyperledger Fabric has reached its version 2.0 milestone.

Below are some of the key features of Hyperledger Fabric and what differentiates it from other distributed ledger technologies.

- Permissioned architecture
- Highly modular
- Pluggable consensus
- Open smart contract model — flexibility to implement any desired solution model (account model, UTXO model, structured data, unstructured data, etc)
- Low latency of finality/confirmation
- Flexible approach to data privacy: data isolation using ‘channels’, or share private data on a need-to-know basis using private data ‘collections’
- Multi-language smart contract support: Go, Java, Javascript
- Support for EVM and Solidity
- Designed for continuous operations, including rolling upgrades and asymmetric version support
- Governance and versioning of smart contracts
- Flexible endorsement model for achieving consensus across required organizations
- Queryable data (key-based queries and JSON queries)

- **License**: Apache 2.0
- **Web**: https://www.hyperledger.org/use/fabric

3.3 Integration of trusted services

Qualified trust services are recognized independently of the MS where the Qualified Trust Service provider is established. Qualified trust service providers must issue, since July 1st 2016, qualified certificates for trust services already ensuring a high level of trust as they will "verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued [...] remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high' (eIDAS Regulation Art. 24 (1) (b)).

This new approach, which enables "a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions" (Recital 2 of eIDAS Regulation [18]), compared to the former eSignature Directive [65], some changes in the integration of trusted services are depicted:

- An electronic signature can only be used by a natural person to sign (express consent on the data where the signature is put). In the eSignature Directive, the electronic signature could be used also by legal persons, as a mean for authentication. However, legal persons can use electronic seals to sign different types of documents and data.
- The "signatory" is a natural person who creates an electronic signature. This implies that the certificates for electronic signatures can't be issued for legal persons anymore, and those type of entities have available other instruments like certificates for electronic seals, as means to ensure the authenticity and integrity of the data.

The trusted services emerged in different MSs since the adoption of the eSignature Directive in 1999 that are integrated under the eIDAS umbrella can be grouped in [66]:

1. Electronic signatures and electronic seals: data attached to electronic documents, guaranteeing its origin and integrity. A relevant difference of electronic seals with electronic signatures, is that in the case of electronic seals, they can only be issued to and used by legal persons to ensure origin (authenticity) and integrity of data / documents. As organizational trust measure, when using electronic seals, it is recommended that an internal mechanism is used to control that only the natural persons entitled to act on behalf of the legal entity are allowed to make use of them. Furthermore, signature/seal creation data must be under the (exclusive in the case of signature) control of the signatory (compatible with the fact that the Regulation enables –Art. 30- the possibility to provide and use remote sealing/signing services provided by qualified trust service providers). Qualified seals/signatures, which must be recognised among MS, make use of qualified certificates for this purpose issued by qualified trust service providers and the seal or signature is created using a qualified creation device (hardware or software). Qualified electronic seals, as expressly indicated in eIDAS Art. 35 (2) will "enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked". Therefore, they could be particularly well suited for the purpose of having public sector bodies guarantee and verify the authenticity and integrity of electronic documents they issue. In addition to signature/seal creation services (following different ETSI standards depending on the format of the data to be signed or sealed), ancillary validation services exist to confirm the validity of a (qualified) eSignature or eSeal. Such a process entails the verification that the requirements of the Regulation are met by a (qualified) eSignature or eSeal in order to confirm its validity.
2. Time Stamping: in the article 3 of the regulation [18], an electronic timestamp is defined as the data in electronic format that links other data in electronic format with a specific time,

providing proof that the latter data existed at that time. It thus can be used to ensure the correctness of the time linked to data / documents.

3. Preservation of electronic signatures, electronic seals or certificates related to trust services: this service deals with the maintenance of the integrity and authenticity of signed data for long periods of time which can be undetermined in duration. It thus guarantees the trustworthiness of a qualified electronic signature or qualified electronic seal through time.
4. Electronic registered delivery service: it makes possible the transmission of data between third parties by electronic means and the provision of evidences related to the handling of the transmitted data, with the proofs of sending and receiving of that data. The CEF eDelivery Building Block [67] can be considered the most representative embodiment of this trust service.
5. Website authentication: eIDAS regulation [18] describes the requirements for website authentication certificates to be considered trustworthy. These are issued to ensure the users (in particular citizens and SMEs) that behind the website there is a legal person identifiable by trustworthy information. For example, the regulation ensures transparency regarding the quality of the service offered to users, accountability of providers with regard to security of their services, trustworthiness of the data associated to authenticated websites and technological neutrality of services and solutions. The Regulation also covers the verification and validation of certificates for website authentication.

This set of trusted services are integrated making extensive use of different initiatives and projects, such as the eIDAS bridge, in combination with initiatives addressing the needs of legal persons and their representatives like SEMPER and can also be combined in complete electronic procedures transactions flows with eIDAS ID. In the context of CEF eDelivery, electronic seals will be used to verify integrity and source of messages and receipts exchanged between Access Points (C2 and C3), ensuring non-repudiation. Furthermore the eDelivery Access Points (C2 and C3) use a time stamp to testify the time of sending and a time stamp for the time of receipt.

3.3.1 eIDAS bridge

The strategic benefits the eIDAS regulation projects over the electronic service scenario in Europe are a game-changer. Many pre-existing technologies, with extended use within the public sector, for example in universities, were deployed in a limited sectorial trust scenario. The trust was established bona fide between the participants, without any overlying liability or trust framework. eIDAS opens the door to using MS backed electronic identities, with a high level of trust on the enrolment and the authentication. It also establishes the legal obligations and guarantees of all the participants. This leap forward enables the possibility of using them to reinforce the trust models in existing service infrastructures, thus generating the concept of eIDAS bridging.

There are at least two eIDAS bridging infrastructures worth analysing: the EduGAIN bridge, and the SSI bridge.

3.3.1.1 EduGAIN – eIDAS bridge

EduGAIN is an academic identity federation established two decades ago. It allows members of the academic community belonging to a university to authenticate using their local credentials, on any federated service offered by any other university belonging to this network. According to the eduGAIN eIDAS cross-sector interoperability documentation [68], it is similar to the eIDAS eID infrastructure in mission, but the topology and the trust management are a bit different. All connections between SPs and IDPs are direct, so the trust is direct between the SP and the IDP. The trust material exchange (the metadata exchange) has a more hierarchical approach, as every SP or IDP belongs to a national

federation, and each national federation can establish different acceptance policies, but in the end, the last decision to trust is on each SP or IDP.

Thus, identity federation has been successfully in use for decades in the academic sector, with millions of yearly authentications, but the lack of a legal framework has affected its growth in some respects. Being this a cross-border trust exchange, and lacking this common legal cover, in case of an unlawful authentication, the chances for a SP organisation to obtain a repair for the liability of the IDP organisation in a potential unlawful user validation are close to none. Also, given the nature of the design of the SAML2 protocol and the need to provide a seamless experience for the untrained user (for example, avoiding consent forms), the personal data transfers between the IDP and the SP might not fit different data protection legislations. All these legal pitfalls have caused some endemic issues in EduGAIN, including:

- The reserve to export own's metadata beyond the national federation to eduGAIN
- The reserve to import external SPs and IDPs metadata beyond the national federation to eduGAIN
- The fear to export attributes on the responses, minimising the attribute set to minimal levels, to cover only the authentication needs.

In more recent times, some initiatives inside EduGAIN have appeared to create advanced trust frameworks to enhance this metadata and attributes flow, but all of them are internal initiatives, not enforced by any higher authority.

All the above, and the fact that the identities in EduGAIN are enrolled at the universities (and thus, they cannot ensure the same level of trust as government-enrolled identities), limits the variety and sensitiveness of the services that can be federated.

The apparition of eIDAS in the federation scene opens a whole new horizon of opportunities. Member-state backed identities provide a better authentication mechanism, to enable federated access to official and administrative university procedures.

In parallel, some initiatives have also materialised in the last years in the GÉANT/eduGAIN sphere with relevance for aspects related to academic attribute management:

- InAcademia service [69] reliably validates the fact that a natural person is affiliated with an academic institution, providing a light-weight, cost-effective and easy-to-use solution towards service providers outside the eduGAIN federation, where minimum disclosure of data is guaranteed: just a Boolean assertion confirming affiliation is returned under user consent and the service provider does not necessarily need to manage any personal data (the request for validation triggers an eduGAIN authentication process managed by the users themselves).
- The AARC project (https://aarc-project.eu/) includes multiple pilots focused on identity interfederation and attribute management demonstrating how membership attributes or other attributes from multiple sources can be used in a federated environment to regulate access to services. A good example is the AttributeManagementPilot [70].

In this sense, different projects have tackled the task of building a solution to functionally bridge eIDAS eID and EduGAIN, establishing mechanisms to address the functional differences among both environments, like pairing the attribute profiles, the levels of assurance, and handling the eIDAS extensions to the SAML 2 protocol. Three use cases were initially analysed (including interactions between eduGAIN and eIDAS experts in 2016) bridging eduGAIN and eIDAS [68]:

- Use case 1: authenticate to an eduGAIN servicewith eIDAS eID

- Use case 2: authentication to an eduGAIN service where a higher Level of Assurance is required
- Use case 3: registering at a university online with cross-border attribute provision

MyAcademicID project (see below) has continued the initial work in the context of CEF, materialising an eIDAS-eduGAIN bridge.

ESMO project10 seeks a double goal: enabling EduGAIN SPs to easily consume eIDAS identities and enabling the exchange over eIDAS of academic sectorial attributes, obtained from different sources like EduGAIN IDPs. This is achieved through the development of a reusable and versatile piece of proxy software, the ESMO Hub, which has extended proxying and data aggregating capabilities. It can support eIDAS IDPs and SPs through performing protocol translation, and the hub to hub proxy capacity, it could allow the deployment of a parallel service network to eIDAS, offering additional sectorial data to be served, with zero impact on the eIDAS infrastructure.

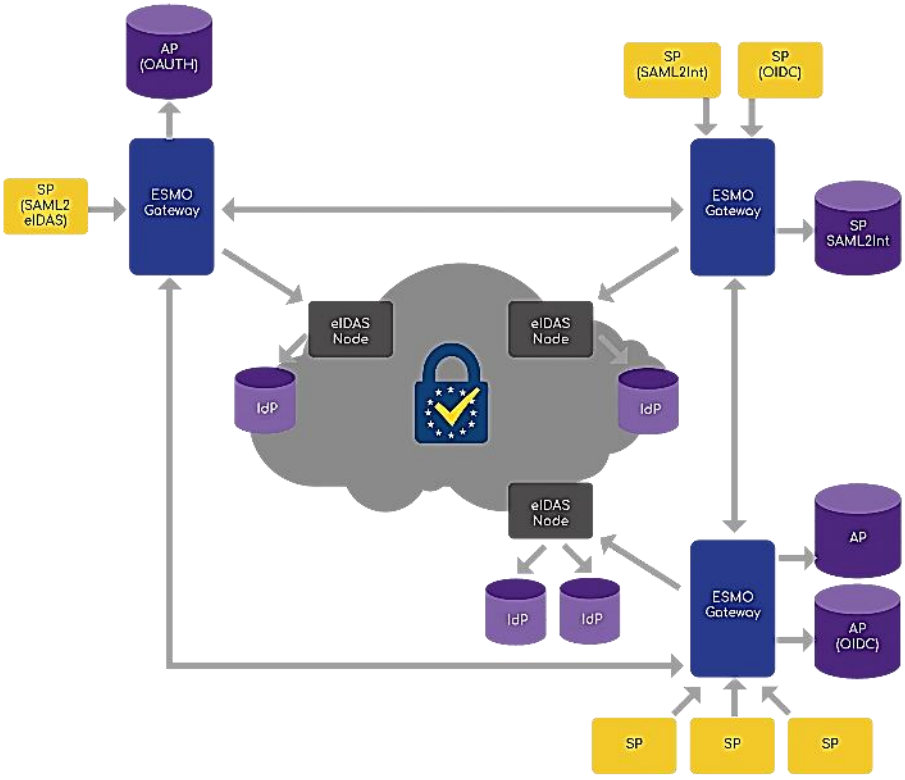


Figure 18: Example infrastructure of an ESMO supported network

MyAcademicID project[11] takes a different approach: besides the goal of deploying a unified student identifier, it focuses on deploying an actual service infrastructure to provide eIDAS identities to EduGAIN services.

[10] http://www.esmo-project.eu/
[11] https://www.myacademic-id.eu/

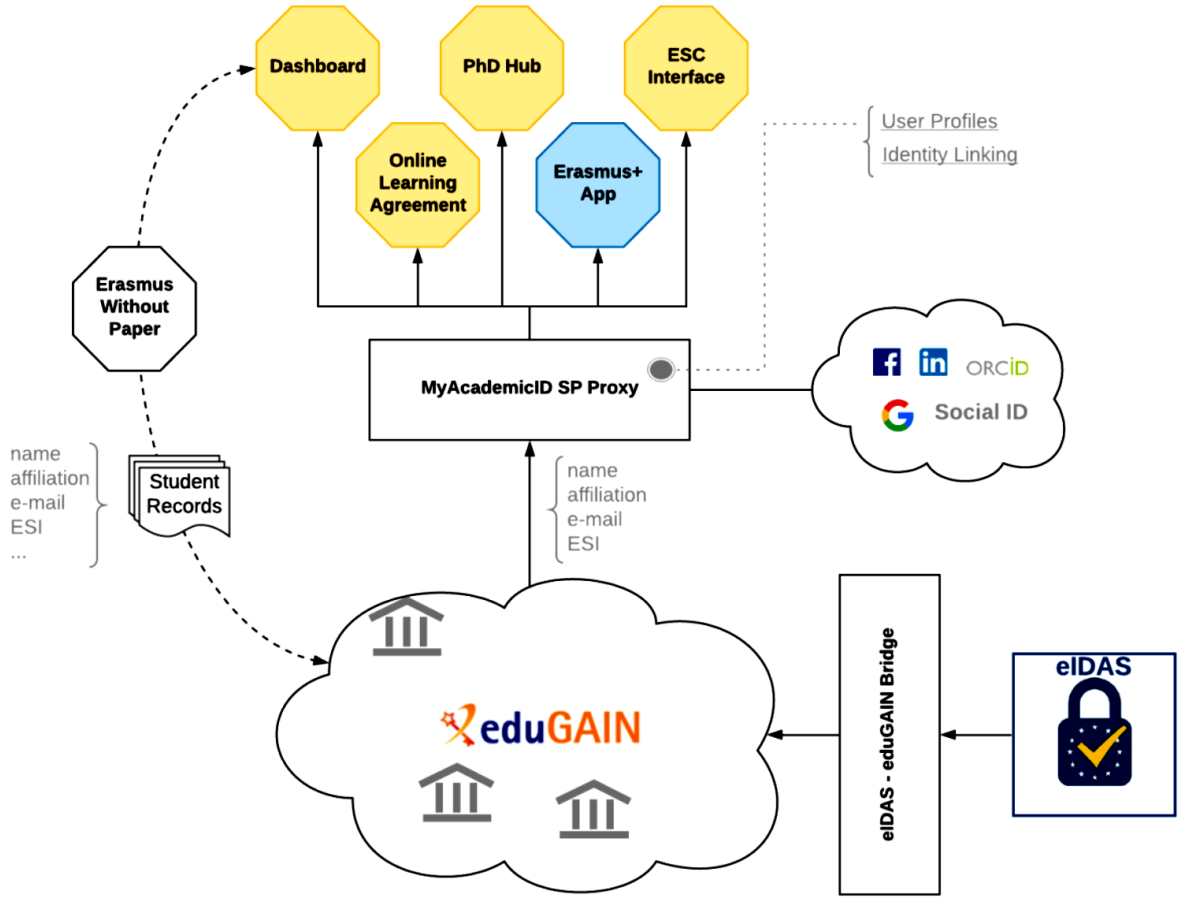


Figure 19: MyAcademicID service infrastructure

3.3.1.2 SSI – eIDAS bridge

The emerging interest in distributed ledger technologies and self-sovereign identity opens a door to the combination of user-based distributed information management with the trust of government on issued data. The final goal of this is to allow a user to lawfully hold and carry Verifiable Claims including personal information. Despite being in an SSI environment, those would not be self-asserted claims, but claims produced from a trusted government source and signed by an issuer entity, whose certificate is valid under eIDAS provisions, and thus, strongly linked to a trusted government entity. This way, the consumer of said entity will be able to trust its contents to some legally binding extent.

The SSI- eIDAS bridge [71] is a building block, adopted by the ESSIF project and compatible with the EBSI technology, to facilitate this task of providing eIDAS level trust to the SSI processes based on the issuing and validation of VCs based on qualified electronic signatures. As ESSIF evolves to its next version, it is expected that eIDAS bridge (which was more a proof of concept in ESSIFv1) will experience changes i.e. some functions may be kept but implemented differently to ensure alignment with GDPR. For example, instead of a central remote eSealing creation or validation services, Issuers would likely have to integrate services from eIDAS-compliant (Qualified) Trust Service Providers. For this reason, details below only reflect what was available in public documentation at the time of writing the deliverable. This caveat applies as well to some considerations given below, inasmuch the bridge specifications would also be upgraded, likely solving some of the identified issues.

The bridge is composed of two modules: an electronic sealing module and a verifier. Both abstract the complexities of producing a qualified signature (access to the configured Trust Signature Provider to sign the hash of the VC) and of validating a qualified signature (validating the trust chain of the certificate used to sign the VC, validate the revocation state of the certificate, and validate that the trust services provider for that signature is actually on a Trust Services List).

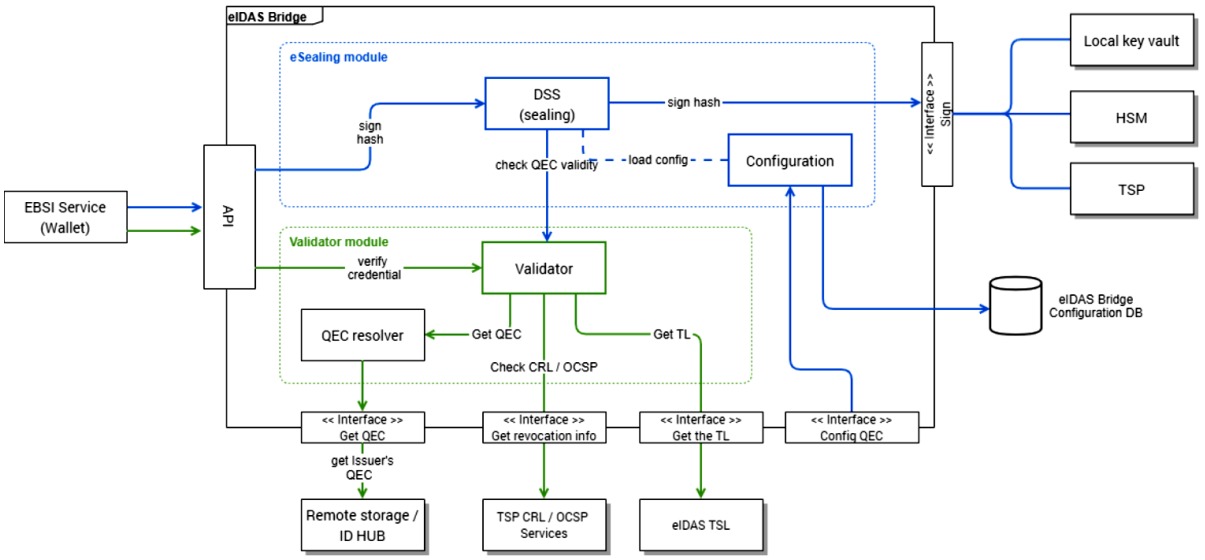


Figure 20: Logical architecture of the SSI - EIDAS Bridge [72]

The bridge is intended to be deployed to support the key actors in a public procedure involving evidence exchange (Data Providers and Data Consumers). Different instances could be deployed in a MS, depending on the requirements. Given the sensitive operations it performs (load of cryptographic material, perform signature or validation under request of objects containing personal information), it is extremely important that the access to these services is properly secured and restricted. It is also extremely important that any data sent for signature is obtained from a trusted source and can be ensured not tampered in the process, because on a flawed deployment, the bridge could be misused to issue unlawful signatures.

The available documentation is not clear enough in this point, so it does not allow to determine the exact nature of the data flow prior to the arrival at the bridge. On deployment on a real data exchange procedure, it must be closely analysed, as it could suppose a data integrity breach. In the use case documentation, the element that interacts with the eIDAS bridge is a wallet. In an SSI environment, a wallet is under the control of an entity that owns it and holds its own data there. So, a wallet is the final destination of a VC, issued for the specific DID that owns the wallet (which implies a cryptographic proof that the holder is legitimate because it owns the associated private key for which the VC was issued), not its source for a potential signature by a government entity. It is the issuer who has the trust on the validity of the data. In this eIDAS-backed environment, the issuers of the data are the lawful MS entities that hold the data, so for them to issue a VC signed with their own qualified certificate, they must be the legitimate source or handlers of this data, and their integrity must be guaranteed. It is not acceptable for a legal government entity to issue a signature over citizen self-stated data (or that might have been tampered by them). And neither citizen-signed data (even if with a qualified certificate) should be accepted if the data is not a self-asserted declaration. Any data issued by a government entity should be signed by the same or an equivalent-trusted entity.

This is the excerpt from the documentation that causes the uncertainty:

eIDAS Bridge will receive eSeal requests from eIDAS Wallet containing:

- *Authenticated request.*
- *VC to be eSealed or, optionally, only the hash of the VC to be signed.*

eIDAS Bridge will verify the request comes from an authenticated source (a wallet) and will route the request to the Digital Signature Service module

So, as explained, the "eIDAS Wallet" should be the issuer of the VC content, not the end wallet of the holder, as the diagram below displays. And the verifier will trust the issuer not the IDI of the holder. The DID proof of the holder will only be used to ensure that a claim has not been reused by any unlawful entity, only by the rightful owner that VC was issued at (so, becoming just a sort of transport security, not part of the trust framework).

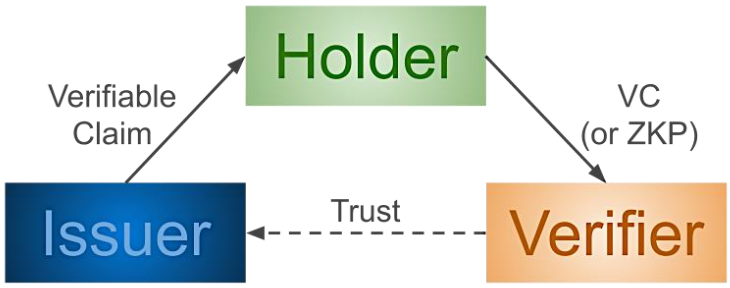


Figure 21: SSI VC exchange model

As the same documentation exposes, there are two different types of keys, *"DID keys" and "(Q)eSeal keys"*. But then it goes to explain that there are two approaches to the sealing of the VCs:

- Seal the VC once with a qualified certificate (what is used in the proof of concept of the bridge).
- Seal the VC twice. Once with a qualified certificate and once with the DID keys, *creating thus 2 proof objects (one for "transport/authenticity-reasons" and one for "giving legal effect"), a possibility also described in the W3C Verifiable Credentials Data Model*.

The proper approach would be the second one, but it seems to clash in many aspects with existing implementations and accepted proceedings. The first solution would allow for a disclosed VC to be taken and reused by an unlawful holder if it is not cryptographically linked to the lawful holder.

This brings to another recurring issue. Most (if not all) of eIDAS signature and eID schemes are based on RSA public cryptography, but SSI environments tend to favour Elliptic Curve Cryptography, as the size of keys is smaller, and operations require less computational effort. But RSA and Elliptic Curve are not compatible, so any eIDAS signatures must be parallel to the SSI environment cryptographic proofs (DID signatures, etc.). This would suppose a challenge for validators, as they would need to integrate the eIDAs bridge in their environment. It can be expected that such technical challenges will be addressed in the coming months in the ESSIF Community.

3.3.2 SEMPER

The main goal of SEMPER, an Action funded within CEF Digital, is to provide technical solutions for cross-border powers of representation and electronic mandates building on eIDAS and considering previous ISA2 Action on semantic interoperability of representation of powers and mandates (RPaM) [73]. The technical solutions are based on the semantic definitions of the mandate attributes that have been released in the scope of SEMPER, and the enhancement of eIDAS Interoperability Framework by providing appropriate elements on protocol-level and modules for the integration of national mandate management infrastructures.

As seen in DE4A Doing Business Abroad Pilot [74], in many transactions the subject is not a natural person but a legal person, for example a company that wants to open an account with a bank or interact with government through eDelivery. Usually a natural person acts on behalf of the company (e.g. an employee) and service providers need to figure out if this person is allowed to act in name of the company (represent it). Currently they rely for doing this on additional infrastructure that exists in some MS on a national level (Mandate Management Systems) but to address this on a cross-border level other solutions are needed which are also beyond the current eIDAS specifications, which is the challenge addressed by SEMPER.

The SEMPER context, shown in Figure 22: SEMPER context(extracted from [75]), details how SEMPER approach fills the gap of eIDAS when dealing with powers of representation. eIDAS solves the authentication and cross-border communication with server providers in another MS, whilst SEMPER specifies the information flow between mandate attribute providers and service providers through the eIDAS network in order to provide access to electronic services in another MS. It extends eIDAS protocol to also support representation (semantic definition of representation requirements and mandate attributes), also taking the reference code of eIDAS nodes and extending it to support the new protocol extensions. Validation is done in pilots connecting both national mandate management systems to the extended nodes and some service providers in Austria, Spain, Slovenia and The Netherlands.

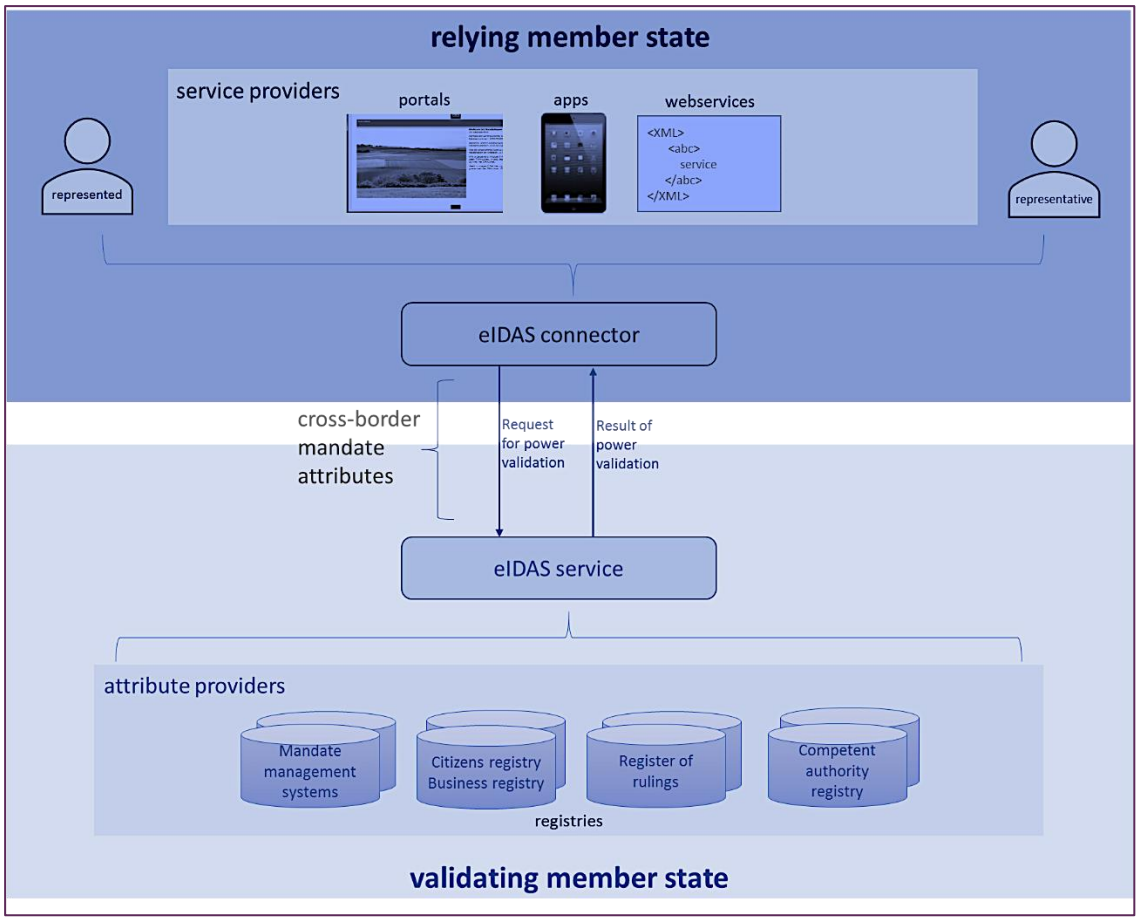


Figure 22: SEMPER context

Trust in the SEMPER models is connected with the validation and access policies. In the validation process, the validating MS set the rules for the validation, these are the specifications in which cases powers are valid. This is aligned with the goal to keep the model as simple as possible, hiding national complexities (furthermore, legislation is not harmonised on powers of representations definitions and their sources). Furthermore, national regulations and laws, and policy of the validating MS apply to the process. For example, for expressing the scope of powers of representation this can done according to a "harmonized" approach, referring to types of procedures contemplated in regulations (e.g. procedures in Annex II of the SDGR). However, to cater for specific services, service providers may also express this scope referring to non-harmonized services.

Different scenarios are contemplated by SEMPER:

1. Natural person is represented by another natural person.

2. Natural person can act on behalf of (represents a) legal person.

3. An employee of a company works on behalf of a customer of the company (customer can be a natural person)

4. An employee of a company works on behalf of a customer of the company (customer can be a legal person) e.g. employee of an accounting firm representing a customer in all kinds of financial affairs towards public authority.

SEMPER considers four sources for electronic mandates:

1. Wilful act (a mandate as per ISA2, can be person to person e.g. a mother granting powers to a son),
2. Grounded in legislation (e.g. a parent representing under-aged child),
3. Court ruling (e.g. judge has a saying in powers of representation in case of bankrupt company)
4. Regulated professions (e.g. notaries, doctors, etc.; a standardised list of regulated professions which can impact way service providers deal with powers the professional has).

The powers validation request reaches a validating MS and basically answers with an « ok » or « not ok » response (valid for a few minutes as powers may change over time and the focus is on result of whether person has sufficient powers to represent for a given purpose at this moment). It is important to note that SEMPER does not establish standards on mandates management (e.g. how attributes are registered in a Mandate Management System) as these, fall under the responsibility of the MS. This process matches the validation request against the national validation rules. The relying MS will trust the validating MS and will accept the response as provided. Eventually, the validating member state should be legally liable for the validation of powers. And, just like in eIDAS, the relying member state should always accept a powers validation result from 'notified' MS.

In SEMPER powers validation declaration includes information on representative, represented (optionally intermediary) and results of powers validation (yes/no), on the source of the power and optionally on the regulated profession of the representative. The model also gives the possibility to return optional information on power use constraints (limitations in time for use of powers, power to authorize costs up to a given monetary amount, etc.).

The trust model relies on the eIDAS acceptance of a result. The relying MS, which launches the request, is in charge of granting access according to its own rules (eAuthorisation). Given the need that the rules and legislation of each relying MS apply, each one of them have to determine the required level of assurance, sources of power allowed, need to receive information on the intermediary person, etc.

SEMPER pilots cover a limited scope of the overall conceptual scope: only public services are involved and only the scenario of natural persons representing legal persons (without other intermediaries) is considered and no piloting of power use constraints or use of regulated professions as source is expected either.

Re-use of SEMPER results is being considered in the context of Doing Business Abroad pilot where currently two different scenarios are seen as relevant depending on where powers of representation are managed: in the Member State responsible for the service (online procedure) or in the Member State of the representative (natural) and represented (legal person):

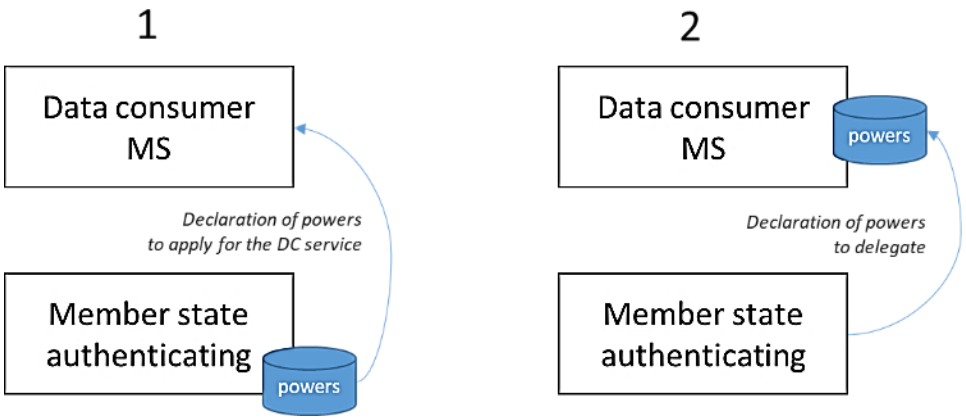


Figure 23: Multiple-Scenario Support based on SEMPER

3.3.3 eIDAS eID

As introduced in section 3.3.1, the eIDAS regulation introduced a legal and trust framework for the cross-border use of MS issued eIDs on authentication and signature purposes on public service procedures. To enforce this regulation, a support infrastructure maintained by the same MSs in close collaboration was required. This is the eIDAS eID network.

As described above, the central infrastructure is organized as a full-mesh network of state contact points, the eIDAS nodes: all of them trust among themselves through the direct exchange (through trusted and identified channels) of the cryptographic public keys the rest of nodes will use to issue requests or responses. So, all eIDAS nodes trust all eIDAS nodes.

The communication between nodes happens through front-channel redirections. This way, on each step, the user agent (the browser) is accessing the domains of that entity (and can be displayed specific UI). To secure these redirections, SAML2 tokens are exchanged; specifically, SAML2 AuthnRequests and SAML2 Responses. All tokens are digitally signed using asymmetric RSA keys (specifically the sender's private key), and exchanged through secure channels (HTTPS, which is HTTP requests exchanged over a TLS secured socket). This guarantees both the privacy and integrity of the tokens, as well as the fact that the issuer is the expected trusted entity (the recipient will validate the signature using the trustfully owned issuer's public key). To provide additional security, the Assertion, containing personal data, is encrypted using the public key of the recipient. This way, only the holder of the associated private key (the recipient), can decrypt its content.

This is the common network and specification, which allows the interoperability of entities in one MS with entities on any other MS. But the communication, protocols, trust models and topology inside a MS are established purely under that state's sovereignty.

A common reference implementation exists under open source license (EUPL) for eIDAS node [76] , developed and released by the EC DG-DIGIT services (CEF eID sample implementation software) as well as a set of common specifications for MS to follow e.g. in case of own implementations of the node [77]. Each country will have at least one eIDAS connector to allow the national entities to interact with the node (some countries may choose to have different connectors for the public and private sector SPs). Since one of the latest versions of the software, and to better separate the specific and the common communication part with the node, the connectors can communicate with the node through a simple relay protocol developed internally by the node implementers. This is an example request token (decoded from base64):

```
specificCommunicationDefinitionConnectorRequest|d65b5e13-6fa9-4795-
9b21-f56847128701|2020-06-05                                  01:46:47
350|W1TQXGbC9sb6RsCSpCrHijHy1/MPfYg4D4/y+tGrucQ=
```

This request will be used by the node part of the connector to retrieve through a direct back-channel connection the data to build the node SAML2 request.

So, in a typical case, a Service Provider in MS1 will contact its assigned connector (usually through a SAML2 request, but each MS can decide). The user will be prompted (at the SP or at the connector) to choose the country of origin.

The connector would contact the node and issue a SAML2 request to the node of the country of origin (usually, the SP will issue the request with a list of the attributes to be requested to the IDP). There, depending on the topology of the country and the available eIDs, the user will be asked to select the

IDP, authenticate, and the authentication assertion will be relayed back to the SP through both eIDAS nodes.

On every step, and as different protocols may apply, the authentication assertion is destroyed and reissued by each entity in the path. This implies that each involved entity between the IDP and the SP (at least the SP country eIDAS node and the IDP country eIDAS node) has the potential to tamper the content of the security assertion issued by the IDP, thus the importance of the trust framework established among all the involved elements to ensure the legitimate data is transported from end to end.

Currently, only Germany, due to legal restrictions on the export of data, require using an alternative mechanism; what is known as the middleware model. In this use case, the destination country is not requested any data. All available data access and authentication is performed locally within the origin eIDAS node, by directly accessing the eID (e.g. For smartcard based eIDs). Each deployed eIDAS node has a specific module to handle the interaction with the notified middleware eID schemes, and this module issues a SAML2 response to the node, to resume the expected flow. But, again, the destination country is never contacted.

As stated above, SAML2 is used for the request/response exchange between nodes, but not standard SAML2: eIDAS specifies an extended profile of SAML2, to support a series of additional capabilities [78]:

- Possibility to specify a list of attributes to request on the same AuthnRequest [79]
- Definition of a Level of Assurance schema, where a minimum level can be requested.
- Definition of an eIDAS specific attribute profile, covering the personal identification attributes of a natural or legal person, and the same in the context of representation of another person.

The eIDAS profile defines an extended metadata exchange profile, based on the standard SAML 2 metadata, but the exchange publication model is not automatized. MS node operators maintain a collaboration network between them, that allows for a trusted communication for the exchange and update of entity trust data. As stated in the “eIDAS Interoperability Architecture” documentation, trust anchors in the form of “certificates for SAML signing and encryption of messages between nodes are exchanged directly between the entities via SAML metadata » , allowing Nodes to be also securely identified « to provide an uninterrupted chain of trust for authentications, as well as an uninterrupted chain of responsibility for integrity/authenticity and confidentiality for personal identification data [80]». The SAML metadata objects describing the node contain the following information:

- The MS operating the eIDAS-Node;
- The URL under which the eIDAS-Node is operated;
- A communication address (preferably email);
- The certificates corresponding to the SAML signature and decryption keys;
- An indication if the eIDAS-Node serves public and/or private parties.

These SAML metadata objects are available under an https URL (referenced in the SAML requests and responses) and are signed by a certificate the chain of which must start at the trust anchor (root designated by the MS) or by another entity (e.g. the operator of the Node). Therefore, it is possible « to separate the trust anchor from the actual SAML end points (Nodes), implying « that the entity providing the trust (and holding the “root key”) is not necessarily the same providing the SAML metadata, i.e. the Node operator. Since the trust anchors are exchanged bilaterally, and all trust (including Node certificates) is derived from these anchors, it is not necessary to use certificates from public CAs for these certificates [80]. » According to this, different deployment scenarios are possible (arrows denote signatures):

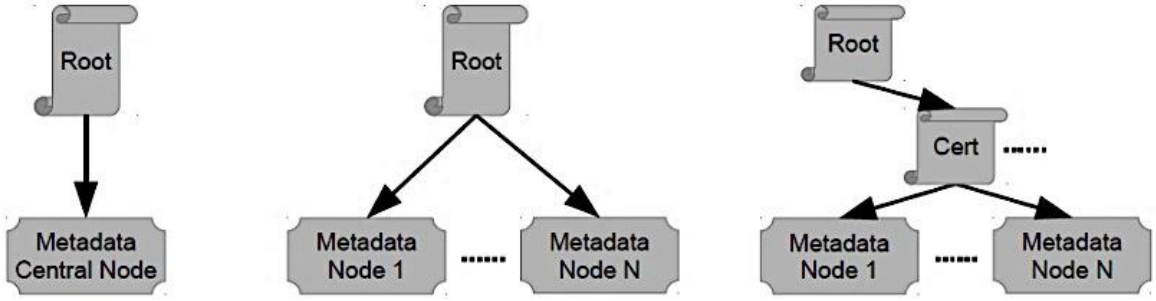


Figure 24: Metadata Trust Management in eIDAS [80]

Matching the trust model with the eIDAS architecture [80] is one of the key challenges. The trust model requirements based on the CEF eDelivery Building Blocks from its assessment in D2.4 – Project Start Architecture (PSA) [2] are matched in two ways, with the ERDS [81] and with the eIDAS regulation:

Requirement	Description	eIDAS reference [65]
Message integrity	Messages should be secured against any modification during its transmission	▸ Article 3 (36) ▸ Article 19 ▸ Article 24 ▸ Article 44 ▸ (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
Message confidentiality	Messages should be encrypted during its transmission	▸ Article 5 ▸ Article 19 ▸ Article 24
Sender identification	Identity of the sender should be verified	▸ Article 24 ▸ Article 44 ▸ (b) they ensure with a high level of confidence the identification of the sender
Recipient identification	Recipient identity should be verified before the delivery of the message	▸ Article 24 ▸ Article 44 ▸ (c) they ensure the identification of the addressee before the delivery of the data;
Time reference	Date and time of sending and receiving a message should be	▸ Article 44 ▸ (f) the date and time of sending, receiving and any

Requirement	Description	eIDAS reference [65]
	indicated via a qualified electronic timestamp	change of data are indicated by a qualified electronic time stamp
Proof of send/receive	Sender and receiver of the message should be provided with evidence of message recipient and deliver	▸ Article 3 ▸ (36) *"... provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data..."*

As result of this matching exercise, and when addressing the set of requirements from the architecture approach, the trust model provided will be compliant with the eIDAS principles, and the trust scope defined in DE4A pilots that will deploy and implement this model (the implementation is foreseen to be done under the scope of WP4 Cross-border Pilots for Citizens and Business and Evaluation and the deployment will be performed in a joint effort under the umbrellas of WP4 and WP5) will be a subset of the trust management approach described in the eIDAS regulatory framework.

4 Architectural Trust and Blockchain Support Framework

This chapter is divided into three different (but complementary) parts. The first of them addresses the different initiatives and projects supported and fostered by European and international authorities and bodies aimed to support, develop and deploy different infrastructures, platforms and solutions with relation to blockchain/DLTs technologies that are an important input for the technological basis of DE4A.

The second block of the chapter describes at high level the conceptual ideas of the inception of the Architectural Trust Framework. This trust architecture will be based on mature technologies such as PKI infrastructure and certificates (necessary to support the message and transport layers related to evidence exchange supported on the eDelivery building block) and extended to include the capabilities of cutting edge blockchain technologies, which are scoped to be implemented and validated for Diplomas Recognition scenario of "Studying Abroad" pilot within DE4A.

The third and final part of this chapter depicts the Blockchain Support Architecture, the interoperable blockchain-supported solution that will cover certain technological aspects of the trust solution to validate the role of this transformative technology in DE4A.

4.1 European and international initiatives

4.1.1 European Blockchain Services Infrastructure

The European Blockchain Services Infrastructure (EBSI) is an initiative of the European Commission and the European Blockchain Partnership that aims to provide cross-border public services by using blockchain technology [32]. Also, starting 2020, EBSI became an official CEF building block. The EBSI goal is to "enhance efficiency, security, transparency and engagement, providing an interoperable framework for data and services that from one side enables the key EU visions (Once Only, Single Digital Gateway,...) and at the same time allows each participating entity to run cross-border or internal services with secure access to needed information while maintaining autonomy running its own processes with its own technology stacks, regardless of the processes and technologies of any other entity" [82]. This will be realized through an EU-level network of peer-to-peer EBSI nodes in MSs that deliver the infrastructure to third parties (e.g. academic institutions). Each node creates and broadcasts transactions to the entire ledger, whilst synchronously keeping an up-to-date ledger and off chain storage for each node in the network.

In 2019, four pilots use cases were defined for EBSI12, where for each use case, there is a dedicated team developing required components and specifications using blockchain technology:

- Notarisation – enables the creation of trusted digital trails,
- Diplomas – enables the management of education credentials in a verifiable manner,
- European Self-Sovereign Identity Framework – enables users to create and manage their digital identities in a decentralized manner (this is achieved by implementing the Self-Sovereign Identity concept), and
- Trusted Data Sharing – enables secure cross-border data sharing.

On a lower level, the architecture of an EBSI node includes three functional areas:

[12] New use cases were added in 2020

1. Main services – include components common to all EBSI use cases (e.g. core services, connection to blockchain networks, etc.),
2. Use cases – includes sample applications for each EBSI use case to demonstrate the usage and technical implementation requirements, and
3. Business applications – enables third party organizations to develop their custom applications and connect them to an EBSI node to maximize code re-usage (this last level is the one more interesting for DE4A in terms of potential usage of EBSI functionality for the pilot use case based on Verifiable Credentials).

4.1.2 European Self-Sovereign Identity Framework

The European Self-Sovereign Identity (SSI) Framework's (ESSIF) was started as an initiative of European Blockchain Partnership by certain Member States and it is part of EBSI. The initiative was designed to address the following key questions/issues [83]:

- How to facilitate cross-border interaction with SSI?
- How to make/keep national SSI projects interoperable?
- How to integrate/align existing building blocks such as eIDAS, e-delivery, once-only with SSI?
- How to conceptualize and build an identity layer in the new European Blockchain Services Infrastructure?
- How to preserve European/democratic values in the implementation of Self Sovereign identity?

The idea of SSI is to decentralize digital identities (which can be perceived as a total sum of all the attributes that exist about us in the digital realm), as opposed to the centralized single sign-on (SSO) solutions. The goal of ESSIF is to implement a generic SSI capability, which allows users to manage their own digital identities (understood to also comprise as well claims or attestations about other related personal attributes) across borders without the need for a centralized authority. In this way, the use of such identities is not linked nor controlled by the issuing entities [14]. In addition to EU citizens, ESSIF brings benefits also to EU institutions and national administrations. It facilitates cross-border business activity and institution collaboration by enabling different scenarios, for example, that a given entity can obtain verifiable credentials (VC) and VC claims and register verifiable consents. Overall, ESSIF represents a "once-only" approach and includes CEF components to be implemented in MSs on large scale in 2021-2022. Please see more details on how trust is addressed in the SSI model supported by ESSIF in Section 3.1.2.

4.1.3 INATBA

The International Association for Trusted Blockchain Applications (INATBA) [84] is a not for profit consortium of more than 170 public and private organisations from 34 countries that offers developers and users of distributed ledger technologies a forum for interaction with regulators and policy makers.

INATBA aims to bringing blockchain and Distributed Ledger Technology (DLT) to the mainstream and to be scaled-up across multiple sectors. The goal of INATBA is to develop a framework that facilitates public and private sector collaboration and legal convergence, while ensuring transparency and integrity [85]. A large focus is on enabling standards-based interoperability, and INATBA acts as an "interdisciplinary vehicle" with Standards Bodies (ISO, IEEE, W3C, CEN-CENELEC, ETSI, ITU, …) to provide exchange, recommendations, papers and to identify other areas of standardization for consistent future frameworks [86]. This is to be achieved by:

- bringing together industry, start-ups, small and medium sized enterprises (SMEs), policy makers, international organisations, regulators, civil society, and standard setting bodies,

- developing a framework that promotes public and private sector collaboration, regulatory convergence, legal predictability and ensures the system's integrity and transparency. Convergence of standards and policies through cooperation is a major aspect addressed in this regard.

With the successful completion of the goals the vision of transparent governance, interoperability, legal certainty and trust in services should be enabled.

INATBA has three committees:

1. standardization committee: for governance and interoperability (a Help Center supports INATBA Members with "De Facto" standards),
2. legal committee: for legal issues and is currently engaged in smart contracts,
3. membership committee: for reviewing membership applications.

INATBA has 14 working groups: climate action, education, energy, finance, governance, healthcare, identity, interoperability, mobility, privacy, public sector, real estate, social impact and supply chain.

INATBA is organizing the work in several working groups, one of them being Identity Working Group [87] that supports and fosters the creation of an identity ecosystem for interoperable, trusted blockchain services. INATBA also plans to support the development and adoption of interoperability guidelines, specifications and global standards, to enhance trusted, traceable, user-centric digital services. No architectural frameworks seem to be available from INATBA at the time of writing this document but its Interoperability, Governance [88], Privacy [89], and Public Sector [90] Working Groups can be of relevance for DE4A in the coming stages of the project which are producing relevant outputs such as:

- Code of conduct for blockchain ecosystems
- Governance Best Practices, Guidance & Toolkit
- Governance Standards for global codes and best practices
- Broad survey conducted to substantiate the efforts and understand in more detail how blockchain projects perceive privacy regulations, in particular the GDPR, and how it impacts them.
- Identify digital identity sandboxes in the EU
- Extend the support to external organizations and stakeholders (eg. EBSI-ESSIF stakeholder meetings)

4.1.4 EIRA

The European Interoperability Reference Architecture (EIRA) is an architecture metamodel released by the ISA Programme. This metamodel is based on the European Interoperability Framework, and contains four layers of interoperability:

- Legal interoperability
- Organisational interoperability
- Semantic interoperability
- Technical interoperability

This metamodel, and all the recommendations that are given as outputs, are a very useful tool for defining and shaping the functionalities of the building blocks needed to build interoperable eGovernment systems and applications. Furthermore, it provides a common and general terminology adopted as standard that can be used by different partners involved in architecture and system development tasks in public administrations. DE4A already established alignment with EIRA (at the level of architecture metamodel) and the European Interoperability Framework (EIF), as explained in D2.1 [91].

Of special relevance to our trust considerations in this deliverable is the fact that EIRA, in its Technical – Infrastructure View [92], states that "trust between systems is established with [Trust Service Provisioning Components] realised using Signature validation and verification such as [e-Signing Creation Service], [e-Signature Verification and Validation Service], [e-Signature Preservation Service], and through e-Seal services such as [e-Seal Creation Service], [e-Seal Verification and Validation Service], [e-Seal Preservation Service], and e-timestamping services such as [e-Timestamp Creation Service], [e- timestamp Verification and Validation Service]." The mutual and close relationship between trust and security is further affirmed by the fact that in EIRA, trust service provisioning components are modelled as Infrastructure Security Enablers.

4.1.4.1 EIRA characteristics

EIRA is a reference architecture divided in four different views. Its main purpose is delivering interoperable cross-border and multi-sector digital services. The main pillars of EIRA are:

1. Common terminology to achieve coordination
   Common understanding of the most relevant architectural building blocks to be used in building interoperable public services.
2. Reference architecture for delivering digital public services
   Categorisation of reusable Solution Building Blocks (SBBs) of an eGovernment solution using its own framework. Tools, methods and practices that allow portfolio managers to rationalize, manage and document different solutions portfolios.
3. Technology and product neutral and a service-oriented architecture (SOA) style
   ArchiMate is promoted as modelling notation, so Architecture Building Blocks (ABBs) are considered as extensions of the different model concepts in ArchiMate.
4. Alignment with EIF and TOGAF
   EIRA is aligned with the European Interoperability Framework and complies with the context and recommendations given in the Implementation Strategy of the European Interoperability Framework.
   This alignment is addressed by the correspondence of the four EIRA views to the interoperability levels in the EIF: legal, organizational, semantic and technical interoperability. Within TOGAF and the Enterprise Architecture Continuum, EIRA is focused on the architecture continuum. It reuses terminology and paradigms from TOGAF such as architecture patterns, building blocks and views.

4.1.5 CEF Building Blocks

The Connecting Europe Facility (CEF) in Telecom is a key EU funding instrument (facilitating cross-border interaction between public administrations, businesses, and citizens), to promote growth, jobs and competitiveness through targeted infrastructure investment at European level. The Building Blocks (BBs) for Digital Government have been funded by the CEF Telecom programme, and can take the shape of a framework, a standard, a software, or a software as a service (SaaS), or any combination thereof that can be used by governments or other parties to integrate with their digital solutions to ensure the compatibility with other cross-border solutions.

The BBs are endorsed by the European Commission and they ensure that the digital service is fully compatible with other on the market. Current list of available BBs is as follows [93]:

- Big Data Test Infrastructure: free online sandbox for analysing big data sets and test data-driven decision making
- Blockchain (EBSI): building the next generation of European blockchain services,
- Context Broker: gathering data in real-time from all smart applications and sensors,

- eArchiving: preserving, migrating, and reusing data securely, accordingly to European standards,
- eDelivery: exchanging electronic data and documents in an interoperable and secure way,
- eID: offering services capable of electronically identifying users across Europe,
- eInvoicing: sending and receiving electronic invoices with automated processing, in line with the European standard,
- eSignature: creating and verifying electronic, paperless signature
- eTranslation: free and secure machine translation tool for documents,
- Once Only Principle: for reducing administrative burden on individuals and businesses (currently, the Once Only Principle (OOP) is undergoing a preparatory action within CEF and the various work packages involved will define if this should be considered as a Building Block per se). Even if OOP is presented as a building block in CEF, it is difficult to consider it as a building block. As no implementation has really been done in a production environment and as there is no mature or final solution that can be reused for OOP. If it would be really a building block, then DE4A and also the activities in the context of SDG OOP would be essentially or at least to a very large extent superfluous.

In the rest of this subsection, some of the building blocks that are considered for use in DE4A are briefly described. EBSI, which is planned to be used in the Studying Abroad pilot, has already been described in more detail above in Section 4.1.1. For the Once only principle, which is currently undergoing a preparatory action within CEF, it still needs to be defined whether it is going to be delivered as a building block. The presented building blocks have already been assessed in detail within WP2 as potential DE4A solution building blocks.

Furthermore, in D2.4 – Project Start Architecture, an assessment of the CEF Building Blocks has been performed. This assessment of the suitability of the BBs identified and catalogued has been very useful for its use within DE4A project.

4.1.5.1 eID

CEF eID is a set of services (including software, documentation, training and support) which helps public administrations and private service providers to extend the use of their online services to citizens from other MSs. To facilitate the integration of electronic identification into existing services, a reference implementation is available, which includes the implementation of an eIDAS node and a testing tool (test identity provider and test service provider). The latest versions of the reference implementation are 1.4.5, published in April 2019, and 2.4 from December 2019 [76]. Both versions are based on the eIDAS v1.1 technical specification. As explained in the previous section, one MS (Germany) is using a different, middleware model, which requires implementation of the German Middleware software (the latest version is 1.2.1). At the end of 2020, the next version is expected that will also enable support of non-notified identification schemes.

4.1.5.2 eSignature

To facilitate the integration of electronic signatures into existing services, an open source DSS (Digital Signature Services) library is available within CEF to create and verify electronic signatures in accordance with European legislation. The Java library can be used in several different ways: in an applet, in a standalone application, or for server signing. In accordance with ETSI standards, the DSS supports various forms of documents and signatures, including PAdES, XAdES, CAdES and AsiC, and is in line with Implementing Decision 2015/1506 / EU. The current version of DSS, released in August 2020, is 5.7 [94].

4.1.5.3 eDelivery

The CEF eDelivery building block helps public administrations to exchange electronic data and documents with other public administrations, businesses and citizens, in an interoperable, secure,

reliable and trusted way. The solution, as depicted on the following figure, is based on a distributed model called the "4-corner model", where the back-end systems exchange data with each other through access points.

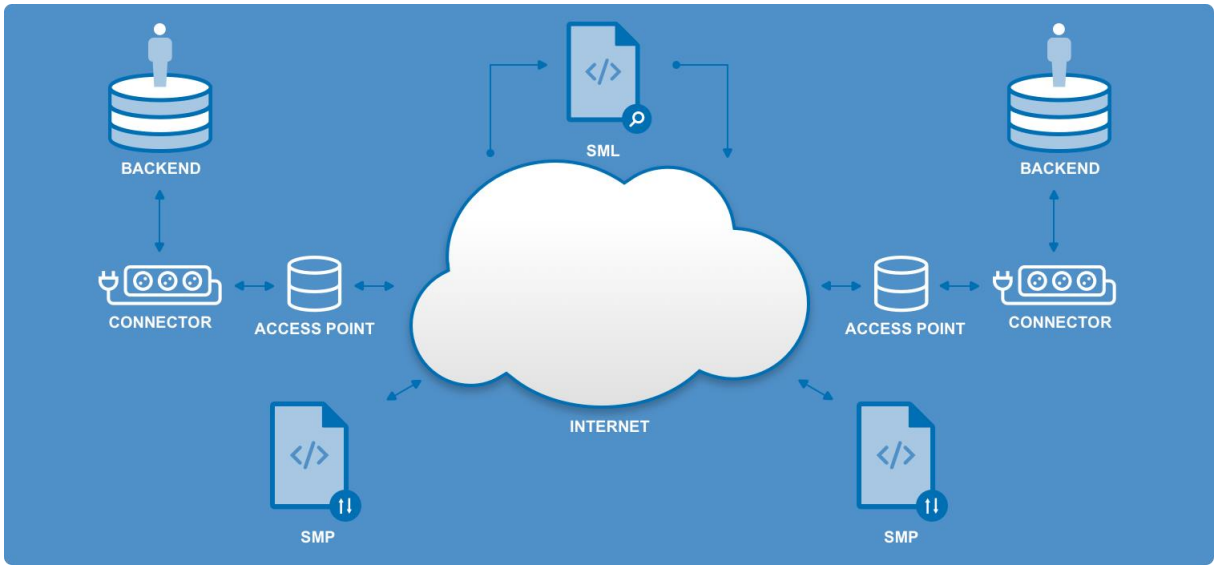


Figure 25: eDelivery model [67]

From its security model as is detailed in [67], the final goal is the fostering of trust among all participants in the message exchange network. This objective is addressed by four points:

- Integrity: Assure that data and documents are secured against any modification (electronic seals can be used for addressing this).
- Confidentiality: Documents are encrypted during its transmission.
- Trust: The origin and destination of the documents are trustworthy (electronic seals can be used for addressing this).
- Auditability: Provide access to advanced and configurable logging of venets related to the exchange of data and documents.

More detailed assessment of eDelivery from trust perspective that will be considered for further work in WP5 (Common Component Design & Development) is provided in Section 2.1 and Section 4.2.3.

4.1.5.4 eTranslation

The CEF eTranslation building block provides machine translation capabilities that enable services to be multilingual. It enables translation of formatted documents and plain text between any pair of EU official languages, as well as Norwegian and Icelandic, while preserving to the greatest extent possible the structure and format of those documents. For the DE4A project, an integrated machine translation functionality is potentially interesting for the machine-to-machine use of translation capabilities through an API but this building block is in principle not apt for generating translations with legal value (e.g. for evidences) and its use is not considered initially for implementation of DE4A platform.

4.2 Trust support framework

This definition of a consistent framework will be essential as an input for the development in further work packages a solution for providing trust services across the complete Only-Once Technical System. The integration of different systems managing different PKIs in parallel and a lot of encryption and security systems, would result into an unmanageable solution, so the Trust Support Framework will keep the complexity level under reasonable levels when managing keys and certificates.

4.2.1 Requirements and specifications

In addition to other more specific requirements and considerations on trust applicable to identity, eDelivery and SSI addressed in other sections of this deliverable, we have also considered for the trust management models functional requirements covered by the Architectural Trust Framework the following more generic requirements, based on previous cloud computing trust models, i.e. mentioned in [95] . These models share the following common set of requirements:

- Certificate/keys/tickets verification
- The trustworthiness of trust service providers (responsible for the issuing and generation of the certificates) shall rely on the supervision (conformity assessment) of such providers by accredited conformity assessment bodies, c.f. Art. 20 of eIDAS regulation [18]. That verification and validation should be a key feature of the Architectural Trust Framework.
- Robust binding
- The underlying platform and implementation details shall be invisible to the consumers, so the certificates should pass through a binding process with the entire provisioning stack. This can be achieved by issuing a certificate for each single module/component that requires it known as robust binding for certificates. This one can also be considered as an essential functionality.
- Dynamic trust update
- The calculation of different trust levels (inter-domain and/or within-domain) shall be done on the basis of successful transactions between users and service providers respectively. The evaluated trust value should be updated considering the time of the last transaction between two nodes. This is an option that is considered mainly in reputation-based trust models but may not be of relevance for DE4A.
- Transaction history logging
- The Architectural Trust Framework shall maintain complete logs of the historical of the transactions among the actors in the same or different nodes and domains, depending on the interaction model that has been implemented in each particular case. Further analysis of logging and audit needs will be addressed in the detailed technical specification phase of the project.
- Recommended trust collection
- This requirement comes directly from the eIDAS regulation, where trust tables (trusted lists) should be available in the scope of the trust model. This trust collection would classify trustworthy services according to a pre-defined scheme. This is already the case in eIDAS and regulated by a specific Implementing Decision [96].

4.2.2 eIDAS record/identity matching

In DE4A, both the authorities having the role of Data Evaluator (in MS requesting evidence data for specific administrative procedures) and the authorities with the role of Data Owners (in MS issuing evidence across borders for a given previous request of data) have the need to reliably establish the identity of users (natural persons, legal persons and their representatives) in order to satisfy different needs: this results in multiple identity matchings in scenarios of cross-border Once-Only data

exchanges. We hereby explore some of the complexities involved in such procedures as they bear an impact on cross-border trust enablement.

Specifically, Data Evaluators need to provide their services (procedures) to previously identified and authenticated users and to potentially launch requests for evidence exchange across borders when those users have expressed an explicit request to use a platform like DE4A to facilitate the obtention of evidence(s) needed for the procedure from different Member State(s); Data Owners, on the other hand, need to ensure that the evidence to be exchanged corresponds to the correct identity, that is, to match the identity of persons to whom the requested evidence refers, with existing records in their local systems. In both cases, the person may be registered or have records under a (local) identifier different from presented identity (e.g. eIDAS UniquenessID). There are similarities, but differences as well for matching on both sides, so it is advisable to separate consideration of both cases.

This means that a matching process needs to be done based on available identity attributes uniquely representing a person (sectorial requirements may also apply in some cases e.g. social security identifiers). When identity credentials refer to a notified eID under eIDAS, these will be at least mandatory attributes contained in the eIDAS Minimum Data Sets for natural or legal persons [97] and this comparison is primarily the responsibility of Member States, given that different semantic rules and procedural steps apply to this matching (e.g. language specific constraints, strategies to manage false positives and negatives, etc.). At national level there could be authorization rules to be observed to access the data or even legal impediments to release evidence directly to a foreign requesting entity without interaction with the user or a sufficient assurance about the identity of the user to which the evidence refers to. Thus, the authorization to disclose evidence referring to a particular citizen can critically depend currently on this record matching process (among other conditions), that is, on the degree of certainty that can be obtained in relation to the identity of the person for whom the evidence is requested (depending on the interaction pattern used in the cross-border exchange, the person may have authenticated only in the evidence requesting country / not be available for further interaction such as obtaining more attributes or information to validate in cases where doubts about the actual identity exist). For these reasons, the record matching process also plays a relevant role when we consider the challenges of cross-border online procedures and the trust aspects involved between competent authorities engaging in an exchange of data referring to a person. Complex cases involving more than two MS (e.g. a 3-MS scenario, where a Data Evaluator requests evidence to a foreign Data Owner about a user from a different MS than that of the requesting or issuing country and the user has no residency status) may also happen in reality.

While statistically the number of cases where automated matching based on eIDAS Minimum Data Set results in failure (e.g. due to collisions) is not large13, the liabilities and negative consequences derived from wrongly disclosing an evidence understandably justify that MS want to ensure, to the extent feasible, that such errors are minimized as much as possible, resulting in longer response times for the administrative procedure in question when such cases arise due to additional interactions or checks.

In cases when eIDAS attributes include an identifier and attributes that are already known to the Data Owner then it may be an easy match. Problems are more likely to arise when it is the first time evidence about a given person is being requested at the Data Owner and the user is not known by their eIDAS Uniqueness ID. When eID is issued from a country different from that of the Data Owner a match can be difficult as e.g. matching rules may be less efficient on foreign names.

Online procedures of the public sector will often require that the eIDAS eID is matched to a national registration number / identifier via a specific online procedure once a first time and then automatically

[13] For example, in one MS participating in DE4A it has been observed to be around 3%.

for subsequent accesses. In this regard, a major finding is that it has been observed that the percentage of failure can be minimized when a previous identity linking process is in place to link a foreign eID with identity used in the MS issuing the evidence (e.g. population register identity), given that during that process a high quality enrolment or onboarding of the person is performed.

In these cases, matching procedures at national level usually are designed in a way that they (manually/with intervention of specialized personnel) check the probability of the right person asking for the matching. They can for example, request additional attributes like the place of birth (which is optional in eIDAS Minimum Data Set and often not provided for this reason) or a national identification number. However, the possibility to ask the user about additional attributes, for example remembering a national identifier is not exempt either from problems as it may not be always the case that the user knows/is able to remember these other identifiers leading to the need for further interactions / additional checks like requesting an email address and use this to send a confirmation email. It is to be noted that these interactions where users provide information themselves can be subject to issues with data quality (e.g. errors typing information) or be less trustworthy when compared to obtaining the data from other trusted sources.

While the general case in cross-border transactions could be based on eIDAS authentication, there may be cases where the identification could need to relate to e.g. national identifier of the evidence issuing country14. As this identifier is only used normally in that MS and even there could be legal impediments to use it from another MS15 (e.g. asking the user to provide it at the evidence requesting competent authority) this introduces yet more complexity in these scenarios. Another issue relates to the persistence of identifiers as while in many MS the same identifier is used during the lifetime of the person in some MS the eID identifier changes upon renewal of the document and for other MS the outbound identifier changes for each country (or even service provider but remains persistent.

It can be concluded that it is important to acknowledge the key role of MS competent authorities (Data Evaluators and Data Owners) in the record matching processes, and that a principles-based approach that recognises the problem is to be addressed nationally as applicable rules are very much MS-specific, coupled with a continued exchange of best practices on practical solutions for matching and their efficiency, seems the preferable way forward. Based on above discussed aspects, principles fostering trust could include:

- For public sector services -like SDGR Annex II fully online procedures- having a solid knowledge of the real identity of the user is a major requirement. For self-provided attributes it should be possible to verify to a sufficient level of assurance that they are correct or else they may not have a role in record matching: self-provided attributes cannot generally replace a safe and (to the extent possible) automatic matching.
- Similarity algorithms and transliteration should be considered by competent authorities for evidence / identity matching, as user data could be registered with slight differences in the involved countries. Given that population registers are developed, managed and governed under national law and using national formats to register first-names, pre-fixes and last-names these algorithms should be developed by each MS. Sharing of knowledge about the algorithms and practices involved will benefit all MS.

[14] According to Survey to the Cooperation Network, eIDAS expert group and eID technical subgroup representatives from EU-28 and EEA countries, between 20 April 2018 and 14 May 2018, 14 countries have a national identifier assigned to foreign citizens and 3 countries do not have a national identifier assigned to foreign citizens.

[15] National citizen numbers are not permitted under some national laws to be used across-borders (advanced encryption schemes could potentially be devised in relation to safe use of such data).

- Perceptions are varied on record matching issues: some MS are confident on evidence matching processes in place e.g. residual risk of false positives or disclosing evidences to a wrong person is small, while others are more worried with such risks. More experience needs to be accumulated and studied to be confident on security and reliability of identity matching and eIDAS as its deployment and uptake still can be largely improved, and experience is still to be accumulated for large scale operation scenarios.
- Encouraging MS in eIDAS (that have notified eID) to provide optional attributes defined in the MDS (especially place of birth but also gender, address…) whenever available could have a very positive impact.
- It should be further investigated the possibilities and consequence for once-only evidence exchange solutions the possibility of allowing Data Owners to interact with users for additional assurance about their identity, if required and possible to do at the Data Owner side16 and with due consideration to all applicable legal and technical aspects.

4.2.3 Trust model management in Once Only interaction patterns

The starting point for the design of a trust management strategy in the scope of DE4A are the four trust models used for the implementation of the CEF eDelivery Building Block. According to [5], a trust model is « a collection of rules that ensure the legitimacy of the digital certificates used by the CEF eDelivery components. Digital certificates enable the identification of the organisations using eDelivery and are instrumental for the authenticity, confidentiality, integrity and non-repudiation of the information. Different trust models are available based on different trust anchor models and different rules to create, manage, distribute, store and revoke the digital certificates». These digital certificates, at the level of eDelivery transport and message layers and in particular associated to the Access Points (C3 and C4 in the 4-corner model), play a crucial role, acting as trust anchors to ensure confidentiality, integrity and non-repudiation of the data moving across systems.

DE4A would assume a default Delegation scenario for communications in the context of the 4-corner model of eDelivery: an organisation operating the original sender C1 (for example a Data Requestor in DE4A which is a national OOP system in the Member State requesting evidence to other Member States) connects to the C2 system, but explicitly delegates the message security (e.g. sealing and encryption) to C2. The sealing is performed using the credentials from the C2's certificate, while C1 is still identified as the original sender in the metadata. From a data security point of view, every MS will be expected to operate their own Access Point or AS4 Gateway (at least one) corresponding either to C2 or C3.

[16] In some cases when OOP TS requests data from base registries, user interaction is not possible because many of them are built for doing real time record matching without user interaction.

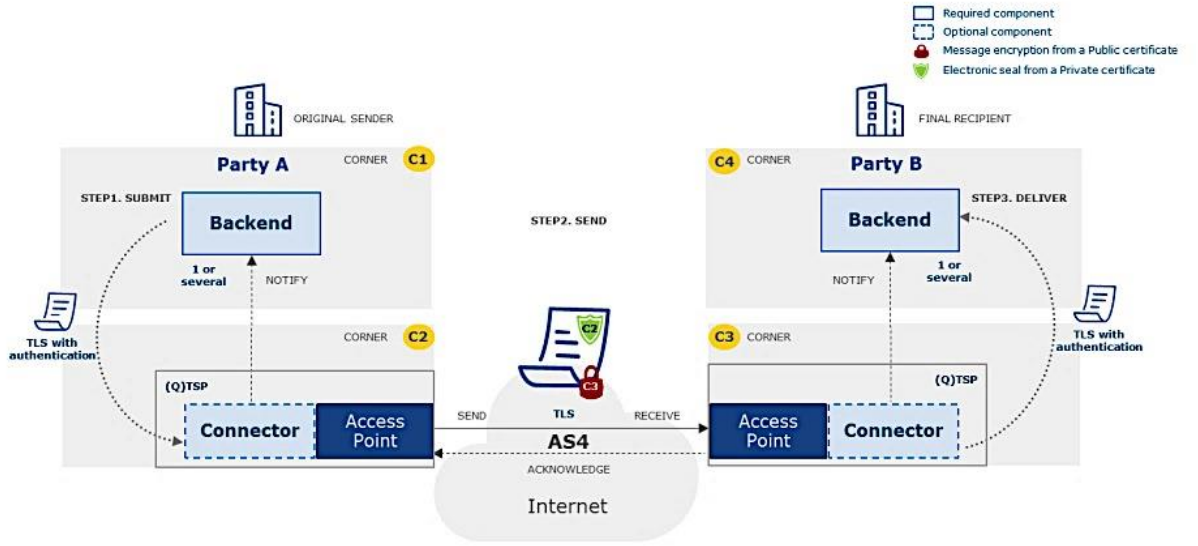


Figure 26: eDelivery delegation scenario (i.e. default scenario) on a four-corner model[17]

On the recipient side, C4 can verify that the original sender of the message is C1 through the metadata and C3 can verify that C2 digitally sealed the message using its certificate. To implement this scenario, C2 needs to authenticate C1 before sealing the message. In addition to the existing security controls provided by the eDelivery building block, the TLS protocol needs to be implemented between C1-C2 and C3-C4 (most likely Member States will choose to use and manage their own existing digital certificates for TLS secure channel communications). The C1 to C4 authentication is performed by the trusted service provided by C2 – C3: this same assumption is made in TOOP and in the CEF OOP High Level architecture, as it has been considered that an end-to-end encryption approach is not desirable to implement given the high level trust and security guarantees of the eDelivery infrastructure and the challenges such end-to-end encryption would create considering the complexity of managing certificates among a large number of competent authorities and the impact on other components that may need to have access to unencryopted evidence details e.g. the Preview function (see considerations on “Encryption Gap” in section 2.3.10 of deliverable D2.1). As the message is sealed by C2, the legal implications related to electronic sealing are related to a legal person that operates C2.

In figure below, normative security controls that are implemented by default in the Cross-party Security domain (by the eDelivery Access Points) are depicted in yellow colour.

[17] Figure source: p.27 of CEF eDelivery Building Block Security Controls, https://ec.europa.eu/cefdigital/wiki/download/attachments/82773295/%28CEFeDelivery%29.%28SecurityControls%29.%28v1.00%29.pdf?version=2&modificationDate=1510311998644&api=v2

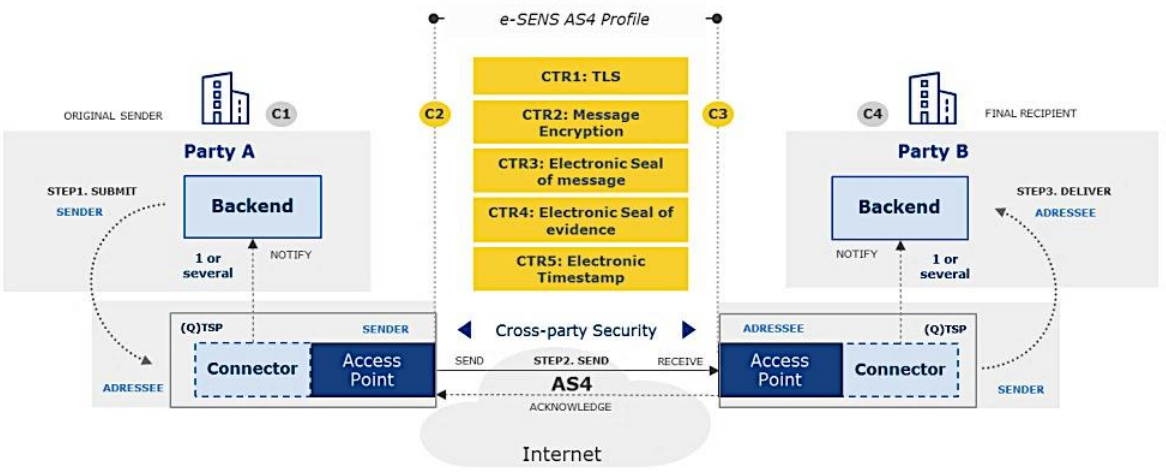


Figure 27: Security Controls at Cross-party (C2-C3) Security Domain[18]

The Delegation scenario is depicted below:

Note: In the same Security Controls documentation, the detailed 4 steps for message exchange between C2 and C3 Access Points and the technical and legal implications of the security controls at Cross-party Security domain are described in Annex I.1. These will be considered as the baseline scenario for DE4A message exchange (except for the VC pattern) and will be subject to further analysis in the context of activities of DE4A WP5 (Common Component Design & Development).

- **Dedicated domain PKI**

In this trust model, the digital certificates are associated to a single trust anchor (dedicated anchor), so it serves to a single domain -or rather sub-domain within the overall eDelivery domain-. CEF eDelivery considers different EU initiatives or projects as different (dedicated) (sub-)domains within the overall CEF domain. This is the recommended model for eDelivery AS4 Gateways (also SMPs) and is also used in TOOP [98] (although from internal perspective of the project, i.e. from exclusive scope of the eDelivery AS4 Gateways invoved in the project and being considered as its own domain, it could also be seen as "Shared domain PKI"). Considering the DE4A project will constitute its own dedicated domain separate from other projects, a more in-depth analysis is provided here, together with trust (PKI certificates-based) considerations for the relevant CEF eDelivery components involved.

In this model, a dedicated PKI (root -that in reality is issued for the specific sub-domains of projects or initiatives within eDelivery-) exists for the policy domain (e.g. DE4A domain where entities such as Data Requestors and Data Transferors use eDelivery to securely exchange information through AS4 Gateways / eDelivery Access points). It enables the eDelivery components (APs, SMPs and SML) to trust each other by sharing the common root CA (Certification Authority) certificate as a trust anchor [99]. Policy Domain Owners may use the CEF eDelivery PKI service (a managed service offered from CEF Support, as SML service) to create secure networks for information exchange and facilitate the dynamic registration and discovery of participants.

[18] Ibidem, p.17

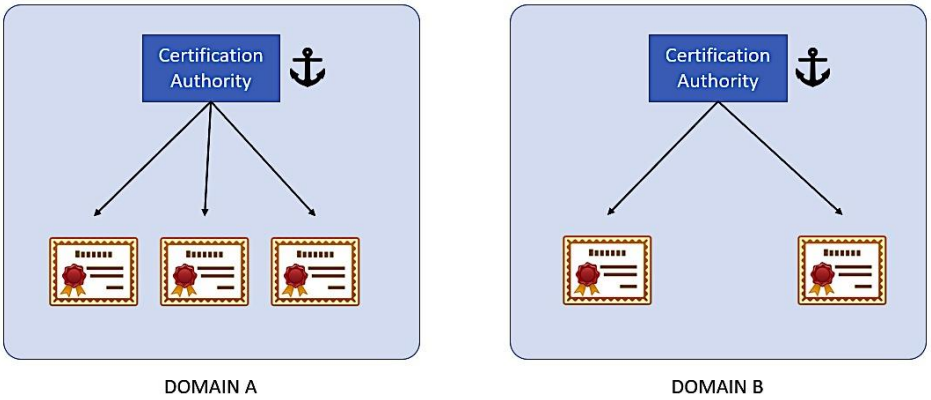


Figure 28: Dedicated domain PKI high level concept

To facilitate building of such a trust model, in particular for communications with the SML service and also for a central/shared SMP, DG DIGIT provides support for the PKI services by establishing so-called eDelivery CA. The CEF eDelivery Service Offering Document [100] describes the scope of the service: 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. It is offered to EU/EEA public administrations that wish to be established as sub-domain owners in the PKI service and which are interested in creating a trust circle for information exchange using the technical specifications and mentioned components of CEF eDelivery. Legal entities (organisations) operating eDelivery components can request to make use of this service in order to be issued with certificates that serve two purposes:

1. Signing a message: When an CEF eDelivery component, i.e. AP or SMP, needs to send a signed message, the signing operation is performed using the private key associated to the certificate. The CEF eDelivery component receiving the signed message uses information included in the certificate of the sender to check the signature of the message.
2. Encrypting a message: When an CEF eDelivery component (AP, SMP) needs to encrypt a message, the encryption is performed using the public key included in the certificate of the receiving component. The receiving component is the only one able to decrypt the message, as it is the only one to know the private key corresponding to its certificate.

Further to these certificates, SMPs as consumers of SML service need to consider that this service only authorizes an SMP to send requests by means of mutual HTTPS authentication (two-way SSL / TLS connection). Therefore, an SMP client TLS certificate with private key has to be configured on SMP side (one certificate if it only serves one domain). The PKI service of CEF eDelivery can be used to issue SMP certificate(s). SML will sign its response using WS-Security response to SMPs.

X509 authentication is optionally allowed for client authentications at SMPs with SpringSecurity.

SMPs automatically create a single keystore to manage certificates for standard SMP operations and interactions with SML and a truststore for user certificate verification. Users can manage them through SMP GUI. More details can be found in [101].

APs comply with AS4 security guidelines: certificates of recipient participants need to be present in the AP truststore, which are then used to encrypt the messages. Conversely, recipients will decrypt messages using recipient's private key located in the recipient's Keystore. In a production environment, each participant would need a certificate delivered by a certification authority and remote exchanges

between business partners would be managed by each partner's PMode configuration file (that should be uploaded on each Access Point). For the digital certificates of APs, which are necessary to enable real data exchanges, DE4A could consider to set up a domain specific PKI, sharing a common root certificate (taking care that certificates of APs are not be self-signed) and experience in this regard from TOOP will be considered (e.g. trust verifying components produce more satisfactory results with a single shared PKI compared with a trust list). It is also recommended to follow the same environment of PKI implementation from development to production levels in order to have the same technical setup from the beginning, ensuring an adequate level of security results from the final choices made to establish this setup.

Further details on AS4 security will be addressed using latest available version of eDelivery specification (currently v1.14 available from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.14). In particular, aspects of Transport Layer Security (TLS), when handled by the Access Points, are covered in order to ensure the right configurations for server authentication19, using a server certificate, allowing the client to make sure the HTTPS connection is set up with the right server (when a message is pushed, the Sending AP authenticates the HTTPS server of the Receiving AP). For instance, it is prescribed as part of this security profile that conformant implementations of APs MUST support TLS 1.2 [RFC5246], using cypher suites that ENISA [102] considers future-proof. At the level of message layer, it is required to use the following WS-Security v1.1.1 OASIS specifications (profiled in ebMS3.0 and AS4):

- Web Services Security SOAP Message Security [WSSSMS]
- Web Services Security X.509 Certificate Token Profile [WSSX509] which supports the signing[20] and encryption of AS4 messages (this profile REQUIRES the use of X.509 tokens for message signing and encryption, for all AS4 exchanges).
- Web Services Security SOAP Message with Attachments (SwA) Profile [WSSSWA]

AS4 message signing is based on the W3C XML Signature recommendation used by WS-Security and SHA2 is to be used in line with ENISA recommendations.

The use of XML Signature in AS4 provides Non-Repudiation of Origin (NRO) at Message Exchange level. Relevant for trust considerations is the fact that the use of non-repudiation information to resolve any disputes requires the communication partners to store data such as the exchanged AS4 messages, AS4 receipts corresponding to these messages, and possibly other verification data such as OCSP responses, for the period during which any such disputes may arise (minimum retention period to be applied SHOULD be specified in a formal policy and be consistent with legal-regulatory requirements, business needs, and available storage/processing capacities).

For encryption, WS-Security leverages the W3C XML Encryption recommendation used by WS-Security, AES128 algorithm is used (with AES GCM strongly recommended over any CBC block encryption algorithms). Also, when XML Encryption is used, all and only payload MIME parts MUST be encrypted (The eb:Messaging header and any of its sub-elements MUST NOT be encrypted). Finally, other details are specified for Key Transport algorithms that are used for encrypting and decrypting keys.

Validation of certificates issued for these two purposes by CEF eDelivery PKI Service is implemented by each CEF eDelivery component and is part of the CEF eDelivery source code. It includes the verification of the expiration date, revocation status, and sub-CA signature on the certificate. APs and SMP list certificates they trust in their local trust stores. CEF eDelivery certificate validation verifies if

[19] Use of client authentication at the Transport Layer is considered redundant due to the use of WS-Security, but is allowed to be used depending on the deployment environment.
[20] The AS4 message MUST be signed prior to being encrypted.

the certificate is listed in local trust store of the verifying component and if the certificate itself is valid, e.g. authentic, not revoked and not expired.

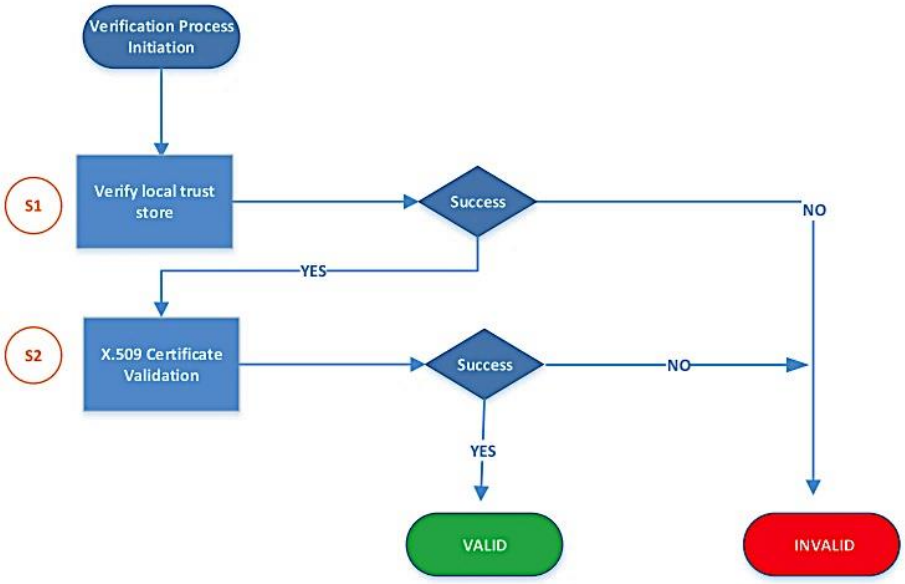


Figure 29: Certificate Validation Process in CEF eDelivery PKI[21]

A Registration Authority (RA) registers and approves the requests of issuance, revocation and renewal of certificates for operators of SMPs and APs (actually sub-divided into sub-RAs attending requests from different eDelivery sub-domains22). In fact, to support separate domains or "areas of responsibility", a dedicated sub-domain-specific sub-CAs are used that issue end-entity certificates to all the components/participants in each CEF eDelivery sub-domain. By setting the sub-domain specific sub-CAs as trust anchors for the CEF eDelivery components, it is ensured that only the components within the sub-domain are trusted. In order to achieve separation per area of responsibility, the CEF eDelivery PKI service uses a specific naming convention in the certificate metadata [102]. The certificate policy is the same for all the sub-domains (algorithms and key lengths are fixed, keys are 2048 bits long and the signature algorithm is SHA256RSA).

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 the PKI service.

The service offers the following benefits:

- A user-friendly interface to request and manage digital certificates (issuance, revocation, renewal);
- Well-established processes and procedures supported by the CEF Support Team;

[21] Figure source: p.28 of CEF eDelivery PKI Service. Service Offering Document v2.1, https://ec.europa.eu/cefdigital/wiki/download/attachments/82773287/%28CEF%20eDelivery%29.%28PKI%29.%28SOD%29.%28v2.10%29.pdf?version=1&modificationDate=1538388819391&api=v2

[22] One of the security requirements for the CEF eDelivery DSI is to create separated areas of responsibilities that correspond to different CEF eDelivery sub-domains, e.g. eHealth, eJustice, etc. This means that all the CEF eDelivery components (APs and SMPs) that belong to the same sub-domain trust each other.

- Digital certificates issued by a renowned PKI service provider;
- Published certificate validation information (CRL (Certificate Revocation List), ARL (Authority Revocation List) and OCSP (Online Certificate Status Protocol);
- Free-of-charge PKI service for a limited number of certificates;
- Support by CEF eDelivery Service Desk on questions related to certificates when these have been issued by CEF PKI.

In the case of DE4A it can be foreseen that the project will act as a CEF eDelivery Sub-domain owner, initiating the process of creating the area of responsibility for its sub-domain under the CEF eDelivery PKI domain and later approving certificate issuance requests submitted by the AP/SMP Operators in its sub-domain (dedicated domain PKI). The CEF support team (DIGIT) registers the sub-domain for the project and handle new certificate issuance, renewal and revocation requests for each specific operator of APs and SMPs.

Shared domain PKI

This trust model relies on the concept of the trust anchor serving multiple domains (shared anchor). As example of application of this interaction pattern, CEF has a certification authority that is providing certificates as part of the SML operations to different domains.

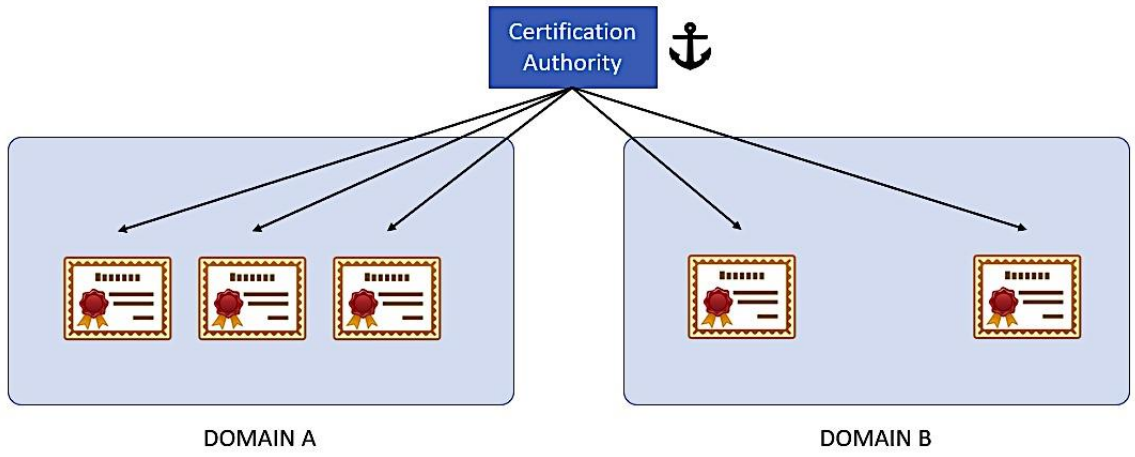


Figure 30 Shared domain PKI high level concept

Mutual exchange

The main characteristic of this trust model is the management of certificates from different trust anchors.

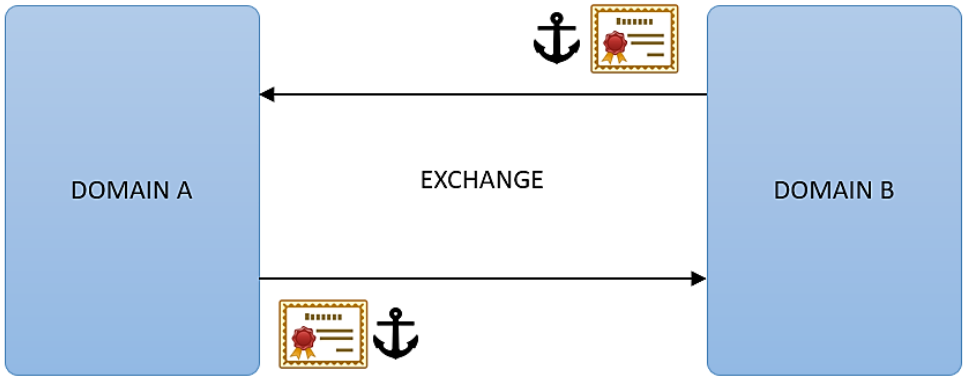


Figure 31: Mutual exchange high level concept

- **Domain trusted lists**

This approach, described in the eIDAS regulation, is based on the issuing Certification Authorities available on a domain trusted list.

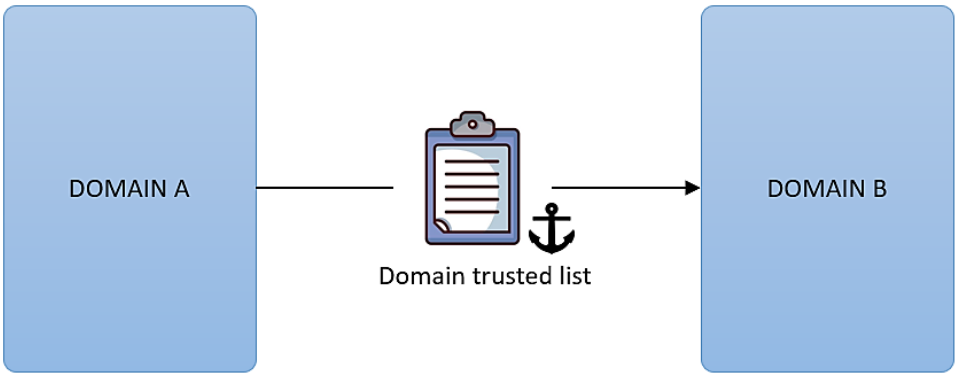


Figure 32: Domain trusted lists high level concept

In order to make a comparative among all the trust models described, CEF describes [5] six requirement areas that are provided to organizations to choose the specific trust model that fit into its business and technical requirements. These requirement areas are:

Table 5: CEF eDelivery requirement areas

Area	Requirement
Setup	The following elements are contained in this area: ▸ Policies: policies specify the operational, issuing and security level requirements of the certificates. These policies follow industry standards and may also specify technical provisions. Qualified auditing procedures may be used to enforce the policy requirements and rules.

Area	Requirement
	▸ TSP: represents the (legal) entity that generates and issues certificates. It can therefore play the role of a Certification Authority. A TSP also manages a certificate revocation list. The TSPs receive certificate requests for issuance, revocation and renewal of the digital certificates from a Registration Authority (RA). According to [5], the TSP is often externalised. ▸ PKI factory: the infrastructure required for the creation, renewal and revocation of digital certificates. Typically, the factory of the (external) TSP is used by organisations. ▸ RA: legal entity performing the identification, authentication and subscription of applicants. It guarantees that the information that the TSP is receiving is valid. The RA must be fulfilled by an organization that understands the project using the CEF eDelivery Building Block, unlike de TSP.
Operational effort	The Operational effort includes the effort of maintenance and operation of the trust model: the policies, infrastructure and local trust stores initiated during setup. This includes the day-to-day operations of: ▸ Certificate and key storage: the configurations required to store digital certificates and associated public and private keys. For instance, the additional security provisions required to keep the embedded private key secure. ▸ Certificate and key management: configurations that ensure the key validity, security and lifecycle management. Updating expired/revoked certificates or reissuing certificates are part of this effort.
Scalability	Deals with the ability and projections of the trust model to efficiently extend it to support different messaging topologies, number of users, configurations and security levels (including strong and semi-strong models support).
Flexibility and interoperability	When organisation participate in different policy domains, flexibility is the ability to integrate with other trust models.
Readiness	Current state of the organisations to support a trust model. This includes their technological maturity and technical skills to implement, support and maintain the trust model
Trustworthiness	Trust level defined by the security and certificate policies. The trust level reflects the quality and security assurance for electronic transactions. This must be respected by the TSP according to the requirements put forth by the eIDAS Regulation [21] either according to the qualified or non-qualified level. Both levels benefit from non-discrimination clause as a legal evidence. However, due to the stringent requirements for the TSP to obtain qualified status, qualified status provides a stronger legal binding at European level.
Cost	Setup cost and associated recurrent costs of running, maintenance and support the trust model, for example: ▸ Price of digital certificates acquisition

Area	Requirement
	▸ Price of maintenance and operation of the infrastructure supporting the trust model In [5] is indicated that the cost is directly dependant of the sourcing model of the organisations.

With the requirement areas defined, the exercise is made of identifying the strengths and weaknesses of each one of the proposed trust models [5]. This can give us a clear view of the aspects that will hay specific weight when taking a decision for proposing one of them for the DE4A Trust Model.

Table 6: eDelivery trust models strengths and weaknesses

Trust model	Requirement	Strengths	Weaknesses
Dedicated domain PKI	Setup	Simple configuration as all components share the same CA	Domain owners are responsible of the creation and establishment of the specific policy and publishing the certificate policy documents to be used by the organisations in the dedicated domain. This requires establishing and request a domain specific CA from TSPs, which increases the technical and administrative workload to setup this model.
	Operational effort	This model is restricted to single domain and closed group environments, and it provides: · Transparent and single certificate policy used by all organisations in the same domain, allowing for better control of the security and configurations. · No need to setup a local trusted store as trust is directly attained CA provided and managed by DIGIT	
	Scalability	Domain topology can be changed as the model allows for issuing digital certificates directly under the same dedicated CA	

Trust model	Requirement	Strengths	Weaknesses
		for new organisations and components joining the same specific domain. The issuing of new digital certificates is managed by a domain specific RA. Easy to add/remove APs/SMPs as they have the same trust root.	
	Flexibility & Interoperability		Full reliance on the root CA certificate: it is a single domain solution that does not allow other domains to use their own CAs. The interoperability with other domains and models relying on different CAs requires cross-certification and setting up a local trust store which increases the operational effort for organisations.
	Trustworthiness	Trust is limited to the domain and the dedicated CA used to generate digital certificates. Obtaining qualified status requires extra effort. Transparent certificate policy and accurate certificate status info.	
	Cost	Low maintenance cost as all components share the same CA. PKI architecture provided by DIGIT.	Tailored certificate policies and dedicated CA may imply extra costs.
Shared domain PKI	Setup	This model simplifies the process of acquiring digital certificates by relying on already available and existing CAs under well-established policies and the possible use of multiple RAs.	Additional technical and administrative workload to setup a RA.
	Operational effort	Low setup and operational effort, much	

Trust model	Requirement	Strengths	Weaknesses
		lower than the dedicated domain PKI. Organisations can use any shared issuing CA or RA, improving the readiness.	
	Scalability	This model allows to issue certificates directly for new components and organisations under the same shared CA.	
	Flexibility & Interoperability	The shared domain CA provides digital certificates that are cross-domain, reusable and interoperable with other domains with the same CA.	
	Trustworthiness	Trust is dependent on the used TSP and shared CA.	
	Cost		Costs can increase with the number digital certificates and levels of assurance required (i.e. qualified vs. non-qualified).
Mutual exchange	Setup	The creation, operation and maintenance of local trust stores provide a simplified way for establishing common trust anchors among different parties without the need for additional cross certification.	Technical and administrative workload to setup a local trust store. The PKI factories could be reused from the TSPs. However, a party can chose to setup its own PKI factory, which implies technical and administrative workload.
	Operational effort		Increased operational effort and cost with the increase of communication parties, as trust stores need to be updated accordingly.
	Scalability		Requires extra operational processes and mechanisms for exchanging certificates whenever the topology and the number of users' changes.

Trust model	Requirement	Strengths	Weaknesses
	Flexibility & Interoperability	Digital certificates are re-usable between different models, allowing organisations to freely choose the issuing CAs. Trust is attained via the exchanged certificate and its availability on the local trust store. This model is ideal for topologies with a low number of users.	
	Trustworthiness	Direct trust on the digital certificate exchanged after exchange process.	
	Cost		Costs for setting up the infrastructure to support the certificate exchange, storage and management.
Domain trusted list	Setup		Trusted lists must be integrity protected with an electronic seal by the policy domain owner reflecting each content change, such as addition and deletion of digital certificates. The CA of the digital certificate of the domain owner is required to be available to the domain participants for verification and validation of the list integrity. The domain owner is responsible for the integrity protection and distribution of the domain trusted list upon each update.
	Operational effort	Organisations do not need to maintain a local trust store as trust is directly attained via the CAs available in the trusted list.	
	Scalability	The decentralised issuance of certificates allows organisations to freely choose their own	

Trust model	Requirement	Strengths	Weaknesses
		TSP from the list of represented TSPs in the domain trusted list. This model can also be extended to a multiple trusted lists model, by using a master trusted list that concentrates the multiple trusted lists trust anchors in a single place.	
	Flexibility & Interoperability		
	Trustworthiness		Managing the different levels of assurance and levels of trust from the issuing CAs in the domain trusted list is complex. Trust is dependent on the levels of assurance defined by the domain owner responsible
	Cost		This model is currently not widely supported by solutions available in the market, which may lead to higher costs.

To conclude this section, it relevant to indicate that a number of additional aspects are being addressed in the design of DE4A, which contribute to the establishment and management of trust from specific perspectives of the interaction between stakeholders in once-only interaction patterns. Only to mention two such aspects we can mention:

- the design of a mechanism which would allow to uniquely identify each request instance for cross-border evidence exchanges given that evidence requestion authorities will need to simultaneously manage multiple flows for different users of the same or different procedures and will therefore also receive multiple evidence response messages: a UUID can be generated that can be guaranteed to be unique (based on a unique MAC address, a timestamp and a random seed) and which will be later included in by evidence issuing authorities in an evidence response message. This will ensure that at the requesting competent authority responses are interpreted correctly i.e. paired to the right evidence requests. Given the serious implications that an error could have i.e. attributing wrong data to a data subject in a procedure, the availability and reliability of such a mechanism is clear and becomes another contributing factor for the trust that competent authorities need to have in the overall scenario of exchanging lawfully issued evidences across borders.

- for data issuing competent authorities who need to authorize the transfer of evidence to a requesting competent authority of another MS, it is necessary to have some proof of the fact that a system user has actually indicated through an explicit (freely given, specific, informed and unambiguous) request their will to use the once-only system to automatically retrieve evidence across borders (when this constitutes a necessary requirement for the automated transfer of evidence i.e. where it is not the case that a relevant Union or national law allows for automated cross-border data exchange without an explicit user request). The specific mechanism by which this should be achieved in order to satisfy relevant legal and organisational requirements is subject to discussion in the context of the technical design of the SDG Once-Only Technical System, but DE4A is exploring through collaboration of its technical work packages some practical options which include some form of "token" that would be provided as a complex object that could contain relevant information about the explicit request given by a user to a competent authority indicating their will to use the system (or alternatively what other legal basis exists for the exchange), but which could also be used to transport other relevant data for determining e.g. if Preview functionality is also to be provided or an exemption for such a Preview applies. For the initial Minimum Viable Product (first iteration of DE4A pilots), the implementation of this token may be quite simplified while more sophisticated options are further investigated.

4.3 Blockchain Support Framework

4.3.1 Requirements and specifications

This section provides an overview of the identified various business and technical functional and non-functional requirements that must be addressed by the Architecture and Solution Building Blocks included in the blockchain support framework architecture in order to build an interoperable blockchain-supported solution. While this can be used as a basis for specific application in DE4A, e.g. in combination with the PSA specification of Verifiable Credentials pattern described in Section 4.6 of D2.1 [1], the proposed Blockchain Support Framework is generic in its nature and versatile enough to be used for other purposes where Blockchain can be of use in eGovernment interoperability platforms.

Business requirements:

- The solution must be developed by using a technology that is mature enough (i.e. not in an experimental stage) nor at the end of its lifecycle and (about to be) made obsolete by newer technology (e.g. by using the CEF blockchain building block, EBSI).
- It is recommended that the solution supports user authentication through identification tools/mechanisms established on the European level (e.g. eID).
- A robust, scalable, secure and reliable protocol should be established across all MSs for exchanging Business Information in a chosen standardized (machine-readable) format.
- A secure message delivery between different participants must be guaranteed via the authentication, authorization, integrity, confidentiality, signature and other security mechanisms.
- The solution must be able to achieve interoperability with other national-level solutions for easier exchange of information.
- The solution must follow agreed public policies (national- and European-level).
- It is recommended that the solution is built by using open-source independent of private interests.

- The developed solution must ensure compliance with the GDPR regulation to protect users' data privacy.

Technical Functional requirements:

- A blockchain network must be established with clear specifications of nodes and their roles (validator, signer, proxy etc.).
- A distributed ledger platform must be selected based on the consensus of participating MSs (e.g. Hyperledger Fabric, Indy, Besu or other), but it is recommended that the platform is aligned with the CEF blockchain building block.
- Each user owns/controls his/her digital identity that is based on the PKI infrastructure.
- Each blockchain transaction should be signed or sealed by the user either by using his digital identities' private key through a dedicated software or by using a dedicated sealing server (e.g. when the user is an authority).
- Secure transfer of application data between different services must be ensured and guaranteed.
- The solution must be able to authenticate all participants of the exchanges.
- A robust, scalable, secure, reliable and interoperable protocol and format must be agreed for blockchain transactions.
- The immutability of the stored records in the blockchain ledger must be ensured.
- A clear Solution Interface specification must be defined in order to achieve interoperability with other building blocks.

Technical cross-cutting requirements (non-functional):

- The blockchain network must be able to handle higher volume exchanges between nodes.
- The addition of new participants with different Business Roles to the infrastructure must be done with minimum difficulties.
- The Application Services included in the solution must have compatible interfaces to establish collaboration.
- Each node/user can be uniquely identified by other nodes/users based on its digital identity.

4.3.2 Functional blocks and components

This section contains a description of the high-level architecture and solution blocks, which compose the interoperable blockchain support framework. The high-level architecture diagram depicted in Figure 33 is created by using the ArchiMate modelling language. The diagram presents a general overview of the functional and logical blocks and their relations. Based on the EIRA reference architecture [103], the functional and logical blocks are divided among the following three layers:

1. Business layer,
2. Application layer and
3. Technology layer.

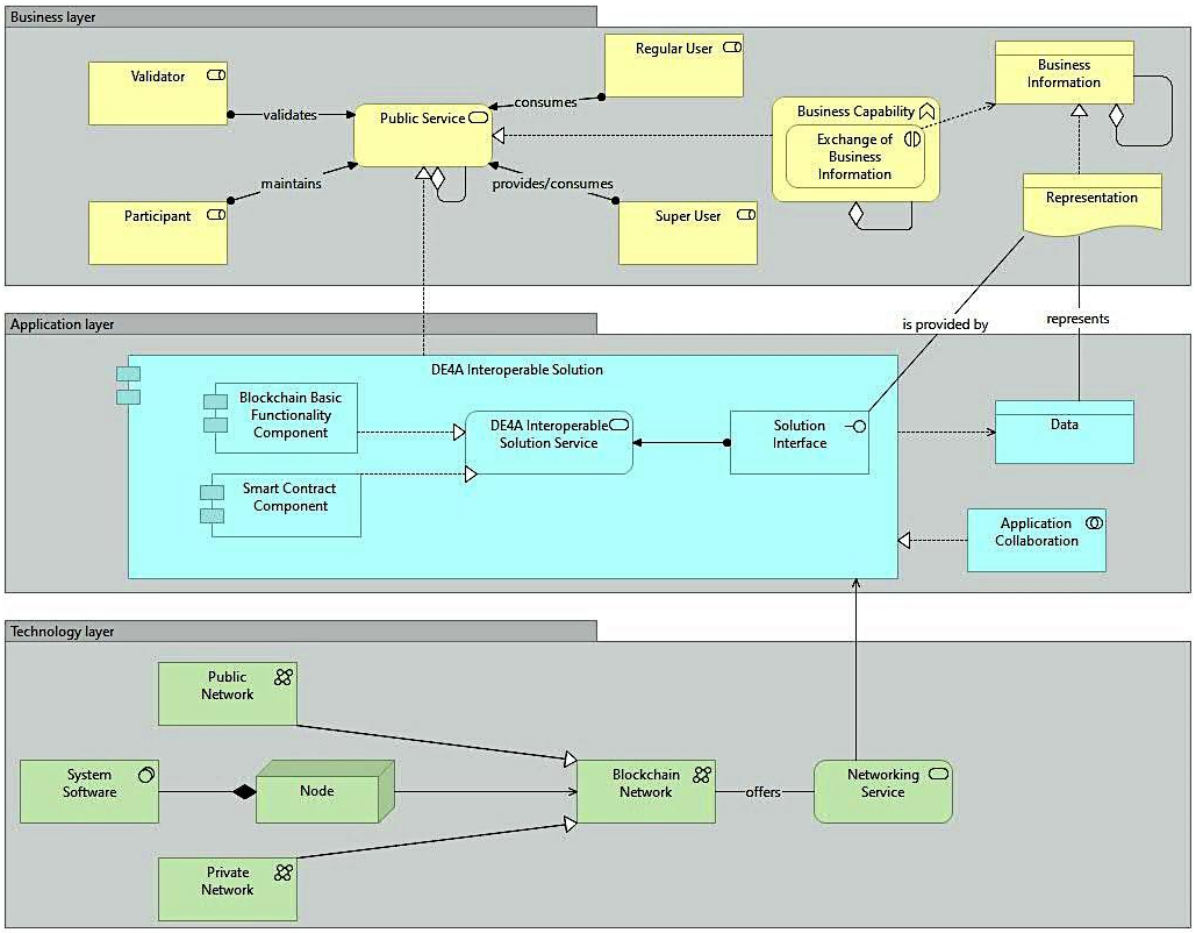


Figure 33: Blockchain support framework architecture

Narrative:

In the Business Layer, the [Public Service] is the basic unit of business functionality, which may be an aggregation of other [Public Service] blocks. The [Validator] role serves to validate blockchain transactions used by the service, whereas the [Participant] role helps to maintain the collection of blocks used by the [Public Service]. The [Regular User] consumes data stored in blocks, whereas the [Super User] can both consume and/or provide data. A given business role can be fulfilled by either natural persons or public institutions. The [Public Service] is realized by a [Business Capability], which can be an aggregation of other [Business Capabilities]. Within a given [Business Capability], the [Exchange of Business Information] takes place, which accesses the [Business Information]. The [Exchange of Business Information] is realized by a [Representation] of [Data], which describes interactions between different participants.

In the Application Layer, the [DE4A Interoperable Solution] realizes one or more [Public Services] and exposes the functionality of its [DE4A Interoperable Solution Services] to external building blocks through the [Solution Interface]. The [DE4A Interoperable Solution Services] is realized through an [Application Collaboration] between the [Blockchain Basic Functionality Component] and (optional) [Smart Contract Component]. The [DE4A Interoperable Solution] uses the [Networking Service].

In the Technology Layer, the [Networking Service] offers the functionality of the [Blockchain Network] to the [DE4A Interoperable Solution] and other external sources. The [Blockchain Network] can be

implemented as either a [Public Network] or [Private Network]. The [Nodes] serve the [Blockchain Network] by implementing their functionality through the [System Software].

4.3.3 Business layer

- **Business service** enables that, if there is a need, the business processes of public services used by citizens, public institutions and businesses are supported with blockchain technology features (i.e. immutability, traceability, integrity and transparency).
- **Business process** is performed by a blockchain transaction, which results in an immutable record stored within all for this action authorized business roles.
- **Event** is any activity where any of blockchain technology innovations are needed. For example, the need that some information related to a to business process (e.g. evidence) is immutably written, or a business process requires a secure, transparent audit trail.
- **Business roles** are classified in the following four roles:
  - Validator - validates blockchain transactions collected in blocks,
  - Participant - maintains the collection of blocks and does not participate in the transaction validation process (but makes an important contribution to transparency),
  - Regular-user - has permissions only to read from a ledger, and
  - Super-user - has permissions to both read and write from/to a ledger.
- **Business Collaboration** is established between Validator and Participant roles, as well as between Participant and User roles (i.e. Regular-user, Super-user).
- **Business Actor** is a natural or legal person within blockchain technology represented with public-key infrastructure.
- **Business Object** is data (e.g. evidence) representing an input piece of information to a blockchain transaction.
- **Representation** is a blockchain transaction whose form is dependent on the type of the underlying blockchain technology infrastructure.

4.3.4 Application layer

- **Application services** consist of a set of functionalities that are available to Business roles to perform with blockchain technology-related Business processes. Typically, these functionalities are accessible via communication protocols (e.g., HTTP, RPC) through Application Programming Interfaces exposed by Technology layer services running on the system software of nodes.
- There are two types **of application components**:
  - The ones that offer basic functionalities of blockchain technology, and
  - The ones that offer self-programmable functionalities, usually through smart contracts.
- **Application collaboration** between the components mentioned above, i.e. the basic blockchain functionality component and the smart contract component, is crucial to support the whole stack blockchain features, including a self-programmable plug-in to business domain-related functionalities. Not all application instances of blockchain support, however, would requires smart contracts or self-programmable plug-in.
- The **application interfaces** are a point of access to the blockchain technology functionalities that are running on the bottom technology layer.
- **Data objects** within blockchain technology are indirectly presented as a blockchain transaction, which as input takes a business object and execute a business process.

4.3.5 Technology layer

- **Technology services** expose the functionalities of those nodes whose purpose is to provide functionalities to external sources.

- **Node** is a vital component of a blockchain network and is a virtual or physical server that is in the peer-to-peer manner connected to all nodes that form a blockchain network. All the nodes store all historical data related to performed blockchain transactions, but not all nodes are of the same type. Some nodes participate in the blockchain consensus protocol where validation of the transactions packed in blocks is performed. Other nodes store all historical data and add the transparency feature, as they also serve as an access point in which a connection to a blockchain network from external sources is established.
- **System Software** in blockchain technology depends on the chosen blockchain platform (e.g. Hyperledger Fabric, Hyperledger Besu, Hyperledger Indy, etc) and its implementation.

4.3.6 Interoperability

Blockchain building block functionalities are available to third-party entities (i.e. other building blocks) through its machine-to-machine interface (i.e. Solution Interface) located in the Application layer of Blockchain support framework. Within the interface mentioned above, the blockchain framework interoperability with other potential building blocks services (e.g. eDelivery, eID, eSignature, OOP, etc.) is achieved. Services that need to integrate blockchain technology features (i.e. immutability, traceability, integrity and transparency) into their process can achieve this through the interface that supports various types of communication protocols (e.g. HTTP, RPC), broadcast their business-related data in the form of a blockchain transaction.

5 Conclusions

Citizens and businesses demand secure cross-border digital transactions: trust plays a crucial role to satisfy confidence of the users that services built around such transactions are indeed reliable and safe for them to use, also in terms of a perception of a certain absence of vulnerabilities for the processes to which they are incorporated; it is worth mentioning here that recent eGovernment Benchmark Reports have highlighted how trust in government is increasingly important for people in Europe. Similarly, the proposed trust mechanisms will also serve the crucial purpose of realizing trustworthy interactions between competent authorities, such as the exchange of evidence requests and provision of evidence in the context of SDGR procedures. This requires as a basis the existence of comparable trust models and use of high standards, that have been explored in this deliverable, in order to support global interoperability and seamless trustworthy data exchange, covering from the well-established registered electronic delivery (CEF eDelivery) and delegated authentication model in the eIDAS federated identity network (CEF eID) to the more innovative European Self-Sovereign Identity Framework (ESSIF).

The work of task 2.2 has been focused on setting up the technological basis in terms of trust management and disruptive technologies adoption (such as blockchain). In this deliverable, the implementation of different regulatory frameworks (eIDAS, SDG, national…), DSI, and interoperability status in a representative sample of MS (those involved in the Trust Management Models task) has also been addressed, covering the technological objective of identification and analysis of the current situation of eGovernment digital transformation landscape in such MS. The provided analysis in chapter 2 of this deliverable, shows a highly heterogeneous landscape in terms of trust models across the MS, with many initiatives aimed at the digital transformation of public services in line with strategic national and EU-level policy instruments (such as the Tallinn Ministerial Declaration on eGovernment [3]) and some major common trends which offer best practices and experiences valuable on the wider level of pan-European interactions between public administrations, including:

- the relevance of electronic identification and authentication schemes -mainly for citizens but in some cases also for companies and with mechanisms such as mandate management systems to register powers/legal authorizations of representatives to represent legal persons- which are also mapped to eIDAS trust assurance levels and notified for the effect of mutual cross-border recognition under the provisions of the eIDAS regulation [18]. Often such schemes are further integrated into federated identity models and platforms comprising gateways that interconnect multiple national identity providers and identity registers with service providers (and which also establish trust relationships between such actors through electronic certificates and the exchange of signed messages) or with advanced services such as signature creation or validation services.
- the establishment of trust models within national Once-Only data exchange platforms (acting as single points of administration / federated networks of eGovernment portals or broker systems for base registries information towards other public competent authorities). They are supported on technical mechanisms (e.g. central authentication or single-sign on, use of certificates to sign information requests, etc.) and organisational measures that effectively serve to underpin not only the interoperability that is necessary to interconnect public administrations at different administrative levels, but also materializing the specific national trust model among the involved actors and which enables such data exchanges to take place in a reliable manner.

This deliverable provides a high-level picture of a valid trust solutions framework considering the cases studied, but these guidelines can be adapted to any other technical, functional or business particularities of the systems to be implemented and deployed. In this regard, the trust management proposal includes different alternatives taken from the CEF Building Blocks and Digital Services Infrastructure trust management approaches, able to be adapted to different scenarios and technical situations. In particular, we have considered the CEF eID and eDelivery building blocks offer a delegated trust model which is relevant for DE4A, as they both feature “nodes” that act as trusted proxies in each MS and serve as abstraction elements for the trust management, allowing endpoints that request or provide data to interact just with their national nodes to which they are connected and trust but where an effective trust chain is also established across borders by virtue of this trust delegation and common standards and specifications in place at European level. To keep this trust chain, all exchanged messages are cryptographically validated and travel through secure channels. In practice, the use of eID and eDelivery (or EBSI-ESSIF) works as a harmonisation mechanism on the larger cross-border infrastructure integration between MS, as it federates the different identity and Once-Only platforms with each other in the context of a common trust framework. Further details of the underlying federated and decentralised trust models/frameworks and their related trust anchors and trust-enabling components have been covered in chapter 2 for eDelivery, ESSIF and eIDAS eID. Furthermore, benefits in terms of efficiency, scalability and cost reduction of innovative decentralised trust models have also been addressed in this chapter.

As analysed in section 3.1 the SSI approach complements eIDAS and generates advantages for public administrations and citizens in terms of the setting up of systems in which the user controls both the identity and the data associated with it and where the use of blockhain decentralised infrastructure is considered highly trustworthy given its guarantees of tamper-proof and non-repudiable factual information that can be notarized in a distributed manner (e.g. claims as verifiable credentials, registration as issuers of such claims of accredited organizations and also of verifiers as consumers of such claims), enabling as well the instantaneous verification of veracity and integrity of the information. Furthermore, other advantages of this SSI approach e.g. more privacy by keeping personal data out of centralized systems and more security by the decentralized nature of blockchain networks, help to address a number of DE4A challenges. In the horizon, it can be foreseen that this new paradigm will enable European public administrations to share data in a more efficient (eliminating much of current bureaucracy and manual checks to validate information), inclusive and secure manner across borders, opening new avenues for implementing the Once-Only and digital-by-default principles across the EU. The higher degree of automation that can be achieved through the use of such transformative and innovative approaches will further ensure the adoption of paper-less and fully online procedures, contributing substantiate to the vision of reinforcing trust in public institutions’ transparency and protection of users’ information as well as to other strategic objectives (e.g. Green Deal). This will lead to a much more positive perception of public services by citizens and businesses. It is also to be noted that while Self-Sovereign Identity frameworks can be perceived as disruptive with respect to previous trust frameworks and models, in reality efforts supported from the EC and the MS like EBSI and ESSIF serve to support an evolutionary approach, inasmuch as its adoption is envisaged to be gradual and would accompany the revision of eIDAS regulation and can thus be seen as a complementing and re-inforcing factor to the benefits already made possible by such solid legal foundations for eID and trust services across the EU. The offered analysis is exemplified in the context of DE4A in the context of its Diplomas Verification use case, introducing the necessary components and their role in the trust model as well as relevant open source technologies that are being considered to realize blockchain and SSI support in DE4A.

Further to this, the key role of trust services such as eSeals has been assessed in section 3.3, as well as mechanisms that allow to bridge trust across infrastructures (e.g. on eID between eIDAS and eduGAIN

in the Higher Education sector or to facilitate the application of trust services to ensure the trustworthiness of Verifiable Credentials in SSI scenarios). Furthermore, SEMPER Action is also introduced, which is relevant for DE4A for scenarios where solutions beyond the current eIDAS implementation are necessary to manage across-borders powers of representation and electronic mandates. Technical details substantiating how the trust model of eIDAS works among its nodes and further matching of DE4A architectural requirements to the proposed trust model (related as well to principles in the eIDAS regulation) have also been provided in this section.

In the last chapter of this deliverable we have introduced several public and industry wide-initiatives supporting blockchain/DLT technologies and public services interoperability. Consolidating analyses in previous chapters, an architectural trust framework is presented based on mature technologies, also extended to include benefits enabled by more transformative blockachain technologies. In particular different overall requirements for this framework have been considered, as well as a detailed analysis in section 4.2.2 of aspects related to eIDAS identity/record matching establishing some common principles and recommendations to reinforce in this important area between competent authorities (acknowledging that such record matching processes are implemented under specific MS rules). Regarding the intermediation and user-supported intermediation patterns described in D2.4 [2], it has been analysed in section 4.2.3 how the implementation can be done making use of functionalities and components of the CEF eDelivery Building Block, considering the default delegation scenario on a four-corner model and providing extensive details on the security model and the proposed approach to address PKI aspects necessary to manage needed digital certificates as trust anchors of this infrastructure, enabling the necessary confidentiality, integrity and non-repudiation of the data exchanged across systems. This is why after the assessment done in section 4.2, including proposed requirement areas and studying the weaknesses and strengths of the four different trust models, the adoption of the Dedicated Domain PKI trust model is proposed for its implementation in DE4A eDelivery infrastructure. This approach also is aligned with the TOOP project [98], where the trust model is being implemented from a dual approach, with the Dedicated Domain PKI model with a single trust anchor for the AS4 gateways (Access Points). Finally, in section 4.3, Blockchain Support Architecture has been described, as the proposed interoperable blockchain-supported solution that will cover certain technological aspects of the trust solution to validate the role of this transformative technology in DE4A e.g. for implementing the Verifiable Credentials interaction pattern needed in the Diplomas Verification use case. Such Blockchain Support Framework is generic in its nature and designed to be versatile in order for it to be used for further purposes where Blockchain provide an added value in eGovernment interoperability platforms.

While trust has been identified in this deliverable to be a very complex and multi-faceted concept building on a complex combination of technical mechanisms and non-technical factors as well, that conditions the success in the adoption of technological change and innovation in the context of the Digital Transformation of public services, a comprehensive analysis of its constituent elements has been undertaken, related to the relevant experience of MS and the trust models in pan-European Digital Service Infrastructures (eIDAS eID, eDelivery, EBSI-ESSIF). It is by building upon such solid trust mechanisms, that Once-Only stakeholders will be able to establish multi-lateral chains of trust allowing, among others:

- to be able to rely on the identity of subjects authenticated to a sufficient level of assurance by corresponding authorities in charge of online procedure portals and the matching of such identity to local records enabling use of e-services or extraction of evidence about such subjects,
- to verify the authenticity, confidentiality and integrity of exchanged information through a common secure transport layer and its origin from authoritative sources,

- to use so-called Information Desk components and registries in order to discover which competent data issuing authorities can (as authoritative sources) 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,
- to assess legitimacy of requests for evidence coming from foreign requesting competent authorities for given procedures as a relevant element to authorize cross-border evidence exchange,
- to foster secure communications between eDelivery access points or between "agents" in the context of SSI (enabling Issuer-Holder-Verifier relations) or, in that same context, to automatically verify in distributed ledgers notarized information about registered actors in data exchange and about issued data itself,
- foster a participatory culture of trust around co-creation, co-responsibility for a more cooperative delivery of services to citizens and businesses
- the technological reference framework proposed in section 4 includes the disruptive technological adoption of blockchain for supporting technical interoperability and an open self-sovereign identity approach that also will provide support to current and future trust models.

6 References

[1] «DE4A - D2.1 Architectural Framework,» [Online]. Available: https://www.de4a.eu/project-deliverables.

[2] «DE4A - D2.4 Project Start Architecture (PSA) - First iteration,» 2020.

[3] «Ministerial Declaration on eGovernment - the Tallinn Declaration,» [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration .

[4] «EIRA v3.0, Section 4.11, p.57,» [Online]. Available: https://joinup.ec.europa.eu/sites/default/files/distribution/access_url/2019-03/76cb237b-0de8-464c-84ca-1327945eac3e/EIRA_v3_0_0_Overview.pdf.

[5] «CEF eDelivery Building Block Trust Models,» 2018. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/82773598/%28CEF_eDelivery%29.%28Trust_Models%29.%28v1.2%29.pdf?version=1&modificationDate=1536676833138&api=v2.

[6] «eDelivery Security Controls Guidance,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Security+Controls+guidance.

[7] «Trust Anchor Management Requirements,» 22 June 2020. [Online]. Available: https://tools.ietf.org/html/rfc6024.

[8] «TADIM SP - Report Overview Trust Anchors for decentralised identity management at "Joining Forces for Blockchain Stardardization" event organised by European Commission on june 17th 2020,» 22 June 2020. [Online]. Available: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68430.

[9] «Peppol PKI explained,» [Online]. Available: https://peppol.helger.com/public/menuitem-docs-peppol-pki.

[10] «eDelivery PKI service,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service.

[11] «The European e-Justice Portal,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2017/06/07/European+e-Justice+Portal.

[12] «The Noble project,» [Online]. Available: http://www.mju.gov.si/si/delovna_podrocja/informatika/mednarodni_projekti/noble/.

[13] ıw we use SSI,» 20 June 2020. [Online]. Available: ıs://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+How+we+use+SSI.

[14] «ESSIF Orientation Vision Text,» 1 October 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+Orientation+Vision+Text,.

[15] «EDPS Opinion on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data,» 12 June 2020. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf.

[16] «Ecosystem vs. Trust Framework,» 2 September 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+Conceptual+Reference+for

+Architecture+Definition#ESSIFConceptualReferenceforArchitectureDefinition-ESSIFEcosystem%E2%80%93TrustFramework%E2%80%93EBSI.

[17] «ESSIF Concepts and relationships,» 2 September 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+Conceptual+Reference+for+Architecture+Definition#ESSIFConceptualReferenceforArchitectureDefinition-ESSIFConceptsandrelationships.

[18] «eIDAS regulation,» [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

[19] «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),» 15 March 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0001.01.ENG&toc=OJ:L:2018:295:TOC.

[20] «eID Support and Community,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Support+eID.

[21] «eIDAS eID Profile,» 15 June 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile.

[22] «BMDW - Digitales Österreich,» [Online]. Available: https://www.bmdw.gv.at/Themen/Digitalisierung/Digitales-Oesterreich.html .

[23] «Stammzahlenregisterbehörde,» [Online]. Available: https://www.bmdw.gv.at/Ministerium/DasBMDW/Stammzahlenregisterbehoerde.html.

[24] «Beschreibung von bereichsspezifischen Personenkennzeichen,» [Online]. Available: https://www.bmdw.gv.at/Ministerium/DasBMDW/Stammzahlenregisterbehoerde/Bereichsspezifische_Personenkennzeichen/Beschreibung-von-bereichsspezifischen-Personenkennzeichen.html.

[25] «Handy-Signatur,» [Online]. Available: https://www.handy-signatur.at/.

[26] «MOA-ID,» [Online]. Available: https://apps.egiz.gv.at/handbooks/moa-id/handbook/intro/intro.html.

[27] «Anmeldung, Rücksetzen und Abmeldung für Bürger,» [Online]. Available: https://www.bmf.gv.at/services/finanzonline/informationen-fuer-buerger/anmeldung-buerger.html.

[28] «Portal Network Agreement,» [Online]. Available: https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund.

[29] «Portal Network Protocol,» [Online]. Available: https://intranet.e-gov.ooe.gv.at/?selectedTab=help.

[30] «Benutzerauthentifizierung über MOA-ID und eIDAS-Infrastruktur,» [Online]. Available: https://joinup.ec.europa.eu/sites/default/files/news/2018-08/Information%20f%C3%BCr%20Service%20Provider%20zur%20eIDAS-Integration%20v1.1.pdf.

[31] E. U. B. O. a. Forum, «Thematic Report on Blockchain and Identity,» [Online]. Available: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf .

[32] «European Blockchain Services Infrastructure,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI .

[33] E. U. B. O. a. Forum, «Thematic report on Government and Public Services,» [Online]. Available: https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf.

[34] «European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust,» [Online]. Available: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_EN.html.

[35] «European Self-Sovereign Identity Framework,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505360.

[36] «European Self-Sovereign Identity Framework,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505360,.

[37] «EBSI Architecture. Core Services Layer. Identity,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Identity.

[38] «SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market,» [Online]. Available: https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf.

[39] «Technical Specification (2) - DID Modelling,» 12 june 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Technical+Specification+%282%29+-+DID+Modelling.

[40] «What is the DID API Service,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/DID+API.

[41] «Self-Sovereign Identity: A Distant Dream or an Immediate Possibility?,» [Online]. Available: https://securityboulevard.com/2019/11/self-sovereign-identity-a-distant-dream-or-an-immediate-possibility/.

[42] «What is the EBSI DID Auth service,» 12 june 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/EBSI+DID+Auth.

[43] «Technical specifications - Description of Trusted Issuer Referential/Ledger,» 12 June 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505886.

[44] «Technical specification - View/decomposition of the user environment,» 12 june 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505858.

[45] «What is the Wallet Web Client service,» 12 june 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Wallet+Web+Client.

[46] «What is the Wallet services category,» 12 june 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Wallet.

[47] «Technical Specifications - View/Decomposition of the Issuer Environment,» 12 September 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505856.

[48] «Technical specification - View/Decomposition of the Relying Party Environment,» 12 september 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505852.

[49] «What is the Trusted Issuers Registry API service,» 12 September 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Trusted+Issuers+Registry+API.

[50] «Technical Specification (5) - DID-registration / updating / suspension / revocation /renewal for end users (incl. listing needed services),» 12 September 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505761.

[51] «Technical Specification (16) - Description of DID Registrar / Resolver,» 12 september 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505873.

[52] «What is the External Storage service,» 12 June 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/External+Storage.

[53] «SSI eIDAS Legal Report,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Legal+Assessment+Reports.

[54] «Technical Specification (5) - DID-registration / updating / suspension / revocation /renewal for end users (incl. listing needed services),» 21 September 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505761.

[55] «Technical Specification (7) - Obtaining VC using eIDAS-AuthN,» 12 June 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Technical+Specification+%287%29+-+Obtaining+VC+using+eIDAS-AuthN.

[56] «Technical Specification (15) - eIDAS bridge for VC-eSealing,» 11 September 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Technical+Specification+%2815%29+-+eIDAS+bridge+for+VC-eSealing.

[57] «What is the eIDAS Bridge API service,» 12 September 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/eIDAS+Bridge+API.

[58] «Hyperledger Indy,» [Online]. Available: https://www.hyperledger.org/use/hyperledger-indy.

[59] «Hyperledger Indy Documentation,» [Online]. Available: https://hyperledger-indy.readthedocs.io/en/latest/.

[60] «Indy Walkthrough. A Developer Guide for Building Indy Clients Using Libindy,» [Online]. Available: https://hyperledger-indy.readthedocs.io/projects/sdk/en/latest/docs/getting-started/indy-walkthrough.html.

[61] «uPort - LinkedIn,» [Online]. Available: https://www.linkedin.com/company/uport.

[62] «What is Sovrin?,» [Online]. Available: https://sovrin.org/faq/what-is-sovrin-2.

[63] «How does Sovrin work?,» [Online]. Available: https://sovrin.org/faq/how-does-sovrin-work-2.

[64] «Hyperledger Besu,» [Online]. Available: https://besu.hyperledger.org/en/stable/.

[65] «Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,» [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093.

[66] «Questions and Answers on Trust Services under eIDAS,» [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas.

[67] «Introduction to the CEF eDelivery Building Block,» [Online]. Available: https://ec.europa.eu/inea/sites/inea/files/building_block_dsi-introdocument_edelivery_v1_00.pdf.

[68] e. SG, «eIDAS cross-sector interoperability,» [Online]. Available: https://wiki.geant.org/download/attachments/121348242/20161013-eIDAS-Update-wiki.pdf?version=1&modificationDate=1504211431502&api=v2 .

[69] «InAcademia Online student validation,» 5 October 2020. [Online]. Available: http://inacademia.org.

[70] «AttributeManagementPilot,» 5 October 2020. [Online]. Available: https://wiki.geant.org/display/AARC/AttributeManagementPilot.

[71] C. Digital, «SSI eIDAS Bridge Technical Deliverables,» [Online]. Available: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/technical-deliverables .

[72] E. -. D. D3, «eIDAS Bridge: WP2 Use cases and technical specifications,» [Online]. Available: https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI%20eIDAS%20Bridge%20-%20Use%20cases%20and%20Technical%20Specifications%20v1.pdf.

[73] «ISA² - Interoperability solutions for public administrations, businesses and citizens,» 9 october 2020. [Online]. Available: https://ec.europa.eu/isa2/actions/sharing-information-powers-and-mandates-legal-entities_en.

[74] «DE4A D4.5 Doing Business Abroad - Use case definition and requirements,» 9 october 2020. [Online]. Available: https://www.de4a.eu/project-deliverables.

[75] B. V. B. E. F. Ivar Vennekens, «SEMPER - Report on mandate attributes and solutions for cross-border mandate attributes».

[76] «package, eIDAS-Node integration,» 1 June 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+Integration+Package.

[77] «eIDAS eID profile,» 1 June 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile.

[78] «eIDAS SAML Message Format,» 1 June 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Message%20Format%20v.1.2%20Final.pdf?version=3&modificationDate=1571068651727&api=v2.

[79] «eIDAS SAML Attribute Profile,» 1 June 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf?version=2&modificationDate=1571068651772&api=v2.

[80] «eIDAS Interoperability Architecture v1.2, section 6 "Metadata Exchange",» 1 june 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile?preview=/82773108/148898845/eIDAS%20Interoperability%20Architecture%20v.1.2%20Final.pdf.

[81] «Electronic Registered Delivery Service and eIDAS regulation,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/32052812/CEF%20eDelivery%20Live%20Webinar%20-%20ERDS%20and%20the%20eIDAS%20Regulation.pdf?version=1&modificationDate=1473689858106&api=v2.

[82] «Mapping of Vision, Mission and Goals,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Mapping+of+Vision%2C+Mission%2C+and+Goals .

[83] «SSI Ambassador: ESSIF,» [Online]. Available: https://medium.com/@SSI_Ambassador/essif-the-european-self-sovereign-identity-framework-4572f6875e12 .

[84] «International Association for trusted Blockchain Application,» [Online]. Available: https://inatba.org.

[85] «Launch of the International Association of Trusted Blockchain Applications - INATBA,» [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/launch-international-association-trusted-blockchain-applications-inatba .

[86] «INATBA Convenes Global Conversation on Standards, Governance and Interoperability,» 2 October 2020. [Online]. Available: https://inatba.org/news/inatba-convenes-global-conversation-on-standards-governance-and-interoperability/.

[87] «Identity Working Group,» 5 October 2020. [Online]. Available: https://inatba.org/working-groups/identity-working-group/.

[88] «Governance Working Group,» 5 October 2020. [Online]. Available: https://inatba.org/working-groups/identity-working-group/.

[89] «Privacy Working Group,» 5 October 2020. [Online]. Available: https://inatba.org/working-groups/identity-working-group/.

[90] «Public Sector Working Group,» 5 October 2020. [Online]. Available: https://inatba.org/working-groups/public-sector-working-group/.

[91] «DE4A D2.1 Architecture Framework, chapter 5, « Architecture Time Horizons »,» [Online]. Available: https://www.de4a.eu/project-deliverables.

[92] «EIRA v3.0. section 4.6, p.49,» [Online]. Available: https://joinup.ec.europa.eu/sites/default/files/distribution/access_url/2019-03/76cb237b-0de8-464c-84ca-1327945eac3e/EIRA_v3_0_0_Overview.pdf.

[93] «CEF Digital,» 15 June 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home.

[94] «DSS v5.7,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS+v5.7.

[95] R. M. M. A. S. R. M. Ayesha Kanwal, «Taxonomy for Trust Models in Cloud,» *The Computer Journal Advance Access,* 2014.

[96] «Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists,» 9 October 2020. [Online]. Available: https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1505_en_txt.pdf.

[97] «COMMISSION IMPLEMENTING REGULATION (EU) 2015/1505 of 8 September 2015,» 2 october 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1501&from=EN.

[98] «The TOOP project,» [Online]. Available: www.toop.eu.

[99] «How can CEF help you set-up your eDelivery infrastructure?,» 20 September 2020. [Online]. Available:

https://ec.europa.eu/cefdigital/wiki/download/attachments/82773419/eDelivery%20tutorial%20v1.2.pptx?version=2&modificationDate=1505837144204&api=v2.

[100] «CEF eDelivery PKI Service. Service Offering Document v2.1,» [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/82773287/%28CEF%20eDelivery%29.%28PKI%29.%28SOD%29.%28v2.10%29.pdf?version=1&modificationDate=1538388819391&api=v2.

[101] «Service Metadata Publisher Administration Guide SMP 4.X,» [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi32uPny-TsAhWRi1wKHdcTD5IQFjABegQIBBAC&url=https%3A%2F%2Fec.europa.eu%2Fcefdigital%2Fwiki%2Fdownload%2Fattachments%2F82773286%2F%2528eDelivery%2529%2528SMP%2529%2528A.

[102] «Algorithms, Key Sizes and Parameters Report - 2013,» [Online]. Available: https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report.

[103] «EIRA Reference Architecture,» [Online]. Available: https://joinup.ec.europa.eu/solution/eira.

[104] «eIDAS Bridge WP2 - Use cases and technical specifications,» [Online]. Available: https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI%20eIDAS%20Bridge%20-%20Use%20cases%20and%20Technical%20Specifications%20v1.pdf.

[105] «What is the Verifiable Credential API service?,» 12 September 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Verifiable+Credential+API.