D1.2

Specification of Reference Architecture

Project number:	959072
Project acronym:	mGov4EU
Project title:	Mobile Cross-Border Government Services for Europe
Start date of the project:	1st January, 2021
Duration:	36 months
Programme / Topic:	H2020-SC6-GOVERNANCE-2020, Governance for the future

Deliverable type:	Report
Deliverable reference number:	DT-GOVERNANCE-05-959072 / D1.2 / V1.1
Work package contributing to the deliverable:	WP1
Due date:	June 2021 – M06
Actual submission date:	23rd May 2022

Responsible organisation:	ECS
Editor:	Detlef Hühnlein
Dissemination level:	PU
Revision:	V1.1

Abstract:	This deliverable covers a reference architecture, which identifies the main building blocks and their interfaces.
Keywords:	eID, eSignature, eDelivery, eIDAS, TOOP, SDG

The project mGov4EU has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 959072.

Editor

Detlef Hühnlein (ECS)

Contributors

Christian Kollmann (A-SIT)

Thomas Zefferer (A-SIT)

Steffen Hammer (ECS)

Tobias Wich (ECS)

Andreea-Ancuta Corici (FHG)

Blaž Podgorelec (TUG)

Executive Summary

This document defines and describes the technical reference architecture of the mGov4EU project and has been created based on pertinent standards and specifications, as far as possible. The document first recalls relevant previous work, suitable CEF building blocks, and requirements, before it identifies fundamental modules and interfaces to provide a solid basis for further technical work within the mGov4EU project.

The reference architecture discusses components of the mobile user device and backend services as its two main layers. The components address electronic signature, electronic identity, single digital gateway, platform functionalities, as well as wallet-related components and components related to the mGov4EU pilots.

The mGov4EU architecture relies to a large extent on standards and existing modules like CEF building blocks. The main contribution of and what will be developed by mGov4EU are the eIDAS App and the Digital Wallet that enhance the mobile use.

The following table shows the relation between D1.2 and other tasks, work packages and deliverables:

Contributing tasks of this WP	T1.2
Input from other tasks/WPs	T1.1
Output to other tasks/WPs	T1.3, T2.1, T2.2, T2.3, T2.4, T2.5, T2.6 (WP3, WP4)
Output to other deliverables	D1.3, D2.1, D2.2, D2.3, D2.4, D2.5, D2.7, (WP3)

Table of Content

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Meaning
AdES	Advanced Electronic Signature
AS4	Applicability Statement 4 (Electronic Delivery Interface)
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CAdES	CMS Advanced Electronic Signature
CEF	Connecting Europe Facility
CIR	Commission Implementing Regulation
DataX	Data Exchange
DC	Data Consumer
DP	Data Provider
DSD	Data Service Directory
EBSI	European Blockchain Services Infrastructure
ETSI	European Telecommunications Standards Institute
ESSIF	European Self Sovereign Identity Framework
ESSP	European Social Security Pass
eID	Electronic identification
eIDAS	Electronic identification and trust services
HW	(Cryptographic) Hardware
IdP	Identity Provider
JAdES	JSON Advanced Electronic Signature
MS	Member State
OOP	Once Only Principle
PAdES	PDF Advanced Electronic Signature
SAML	Security Assertion Markup Language
SCA	Signature Creation Application
SDG(R)	Single Digital Gateway (Regulation)

SIC	Signer Interaction Component
SMP	Service Metadata Publishing
SME	Small or medium size enterprise
SP	Service Provider
SSA	Server Signing Application
TOOP	The One Only Principle
TS	Technical Specification
UA	User Agent
XAdES	XML Advanced Electronic Signature

Chapter 1 Introduction

The mGov4EU reference architecture identifies modules and interfaces to provide a solid basis for further technical work within the mGov4EU project. It consists of two main layers: the mobile user device and the backend services. These components address electronic identity, electronic signature, single digital gateway, and platform functionalities.

The present document is organized as follows: it first recalls the necessary background (Chapter 2) and provides an overview of the reference architecture (0). Later on it describes details with respect to components related to eID (Chapter 5), signature (Chapter 4), SDG (Chapter 6) and wallet (Chapter 7). The document closes with a short summary and conclusions (Chapter 8).

Chapter 2 Background

The mGov4EU project intends to build upon the knowledge and results of previous work of research projects and as much as possible and aims to reuse existing building blocks provided by the programs (e.g., Connecting Europe Facility - CEF) funded by the European Commission. Therefore, this Chapter identifies relevant previous research projects and suitable building blocks that show the potential to be re-used within the mGov4EU project and to be considered during the design of the mGov4EU reference architecture. The present Chapter also augments the system requirements elicited in Deliverable D1.3 [1] and specifies requirements for the Reference Architecture itself in Section 2.3.

2.1 Relevant Previous Work

One of the main goals of the mGov4EU project is to facilitate the usage of cross-border services backed by the Single Digital Gateway Regulation (SDGR) and by the eIDAS Regulation using mobile devices. mGov4EU will build upon previous work in pertinent research projects. One of these fundamental projects that are highly relevant for mGov4EU is TOOP. Based on the example of the TOOP architecture, we show the interplay of foreseen concepts (i.e., SDG and eID) from the regulations mentioned above (i.e., SDGR and eIDAS Regulation).

2.1.1 TOOP Project

During the TOOP project, an implementation of a subset of SDGR requirements has been developed. The solution architecture has focused on the evidence-retrieval procedures and has integrated the eDelivery and Once Only Principle Building Blocks (see Figure 1). Although the building block (i.e., eID Building Block) from the eIDAS infrastructure has been included in the solution architecture, its integration has only been addressed at a theoretical level, i.e., without integrating its implementation into the developed solution.

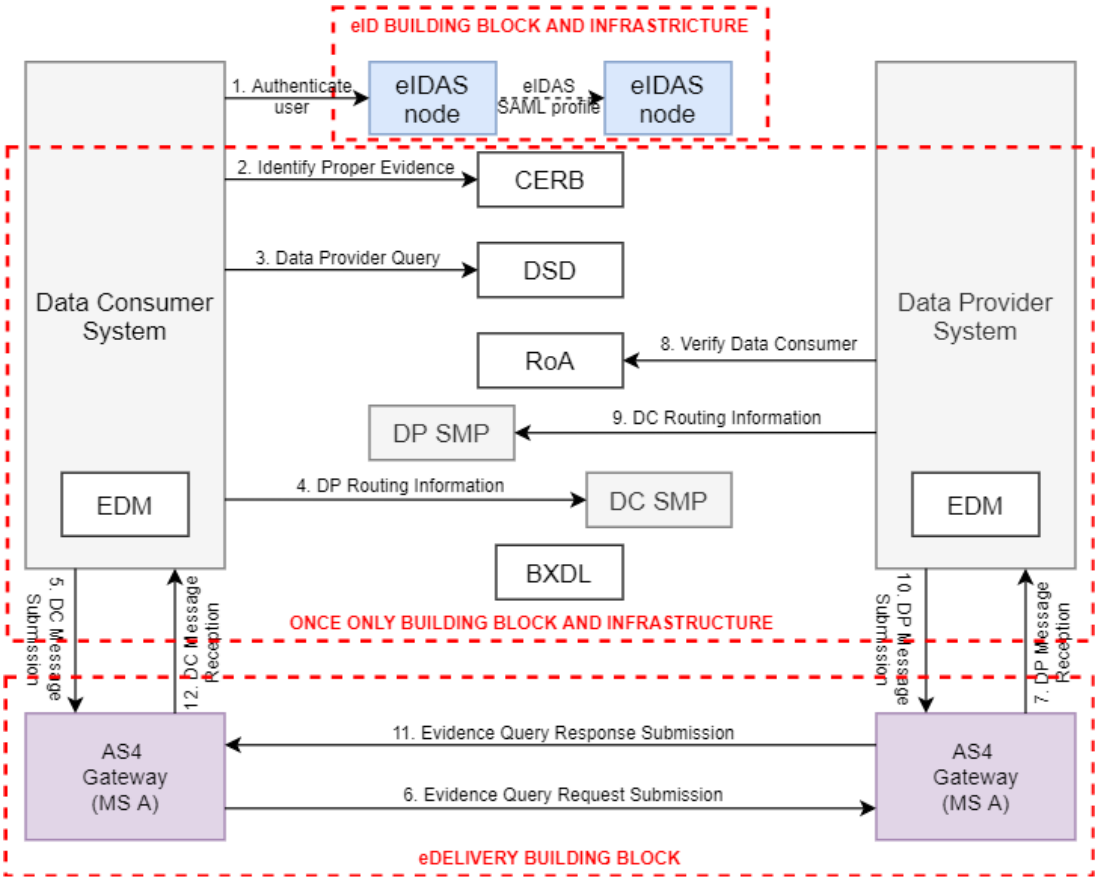

Figure 1: TOOP project Solution Architecture with eID and SDG related building blocks

Moreover, during the project, the implementation was based on a desktop platform with little effort on how the end-user applications can interact to exchange information via mobile devices.

The mGov4EU project will build on available TOOP results and will provide a new component for the Explicit Request Management interacting with the eIDAS infrastructure components to engage the user to grant access to the evidence for retrieval purposes. It will also include in the mobile set of applications the SDG App as a necessary component for this operation and preview the retrieved evidence (see Section 3.3 for more information). Furthermore, the user authentication and electronic-signature features (see Section 3.5 for more information) will also be made available to the end-users by means of a mobile device. To enable the aforementioned features, an eIDAS App (see 0 for more details) with the additional ability to interact with a Digital Wallet component will be introduced (see Section 3.5 for more information).

2.1.2 Other Projects

The present work builds upon the knowledge of previous work in the following pertinent research projects, for example:

- STORK – EU large scale pilot where a European **eID interoperability** platform has been established. The interoperability has been achieved between existing national **eID infrastructures** and thus enabled the **identification and authentication of citizens** in the pan-European context.
- STORK 2 – EU large-scale pilot – the successor of the aforementioned STORK project – built on an already established STORK platform for cross-border electronic **identification and authentication (eID)** of citizens and businesses in the European context. STORK 2.0 enabled citizens to identify themselves in a cross-border context by using identity-related data from authentic and reliable sources (attribute providers) or to represent other natural or legal persons in the context of different business domains.
- CREDENTIAL – A **cloud-based digital wallet** for storing, managing, and sharing personal data has been developed.
- SkIDentity – **Electronic identification (eID)** was redesigned and thus offered to citizens for straightforward use of eID on the Internet and in mobile environments. The SkIDentity Service offers "**Mobile eID as a Service**" and, if necessary, derives cryptographically protected "Cloud Identities" from eIDs, which can be transferred to any smartphone and securely used there.
- FutureID – Secure **electronic identity (eID)** infrastructure (that supports any **eID card, token and mobile identity technology**) that provides many services and boosts competitiveness and could be used on a wide scale across the EU has been built.
- FutureTrust - The results of the project concerned many aspects of the eIDAS ecosystem, including 1.) the existing **European Trusted List (TL)** has been extended, 2.) Open Source Validation Service and a Preservation Service for **electronic signatures and seals** have been developed, and 3.) components for the **eID-based application** for qualified certificates across borders and the trustworthy creation of **remote signatures and seals in a mobile environment** have been provided.

2.2 Suitable CEF Building Blocks

Where suitable, the present work builds upon and integrates CEF Building Blocks, such as the

- eID Building Block,
- eSignature Building Block,
- eDelivery Building Block,
- Once Only Principle Building Block, and
- Blockchain (EBSI) Building Block.

A brief description of suitable CEF Building Blocks and an expected domain of integration in the scope of the mGov4EU project are provided in the following subsections.

2.2.1 eID

The eID Building Block offers a set of services supported by the Member States capable of electronically identifying users (i.e., citizens) in the cross-border context across Europe. Primarily, it allows integration and connection with a technical infrastructure that connects national electronic identification (eID) schemes via the eIDAS Network. The Building Block serves the Member States to run and operate their own eIDAS Node in the eIDAS Network. Furthermore, the eID Building Block supports Service Providers to connect their services to the eIDAS Network and thus enrich their services with features of cross-border electronic identification, which are fully aligned with the eIDAS Regulation. As described in deliverable D1.3 [1], the eID Building Block functionalities and related proxy services are envisioned to be used in mGov4EU pilots, namely, eVoting Pilot and the Smart Mobility Pilot.

2.2.2 eSignature

The eSignature Building Block is a set of standards, tools, and services that supports the creation and verification of electronic signatures in line with the standards acknowledged by the European Commission. The integration of eSignature Building Block in Service Providers solutions (Government and Businesses) improves trust and facilitates the mutual recognition and cross-border interoperability of electronic signatures and seals according to the eIDAS Regulation. As described in D1.3, the eSignatures Building Block features are envisioned to be used in the Mobile Signature Pilot of the mGov4EU project.

2.2.3 eDelivery

The eDelivery Building Block offers a set of technical specifications, standards, software, and ancillary services that supports the exchange of electronic data and documents in an interoperable and secure way. The eDelivery Building Block allows to create and connect to a private network (via AS4 Access Point - each access point becomes an independent node within distributed messaging infrastructure) consisting of any types of beneficiaries (i.e., public or private organisations) from different sectors to establish a secure and interoperable channel for secure digital data exchange. As described in D1.3, the eDelivery Building Block functionalities are envisioned to be used together with the Once Only Principle in mGov4EU pilots, namely, eVoting Pilot and the Smart Mobility Pilot.

2.2.4 Once Only Principle

The Once Only Principle (OOP) Building Block is still under preparatory action within CEF. The decision, whether OOP should be considered a Building Block or service of any existing Building Block is still pending. However, the Once Only Principle goal is to reduce the administrative burden for individuals and businesses. This can be achieved by making data sharable between different EU public administrations in a transparent and secure manner. Furthermore, users are always asked for approval, and only information relevant to the current procedure is shared by obeying data protection and privacy rules. As described in D1.3, the Once Only Principle is envisioned to be used together with the eDelivery Building Block in mGov4EU pilots, namely, eVoting Pilot and the Smart Mobility Pilot.

2.2.5 Blockchain (EBSI)

The Blockchain (European Blockchain Services Infrastructure - EBSI) Building Block offers a set of reusable software, specifications, and services that employ blockchain technology and thus support the creation of cross-border services for public administrations and their ecosystems, to make those services more trustworthy with the help of features offered by distributed ledger technology (" blockchain"). The EBSI provides a peer-to-peer network of nodes distributed among the European Union. The nodes on the European level are operated by European Commission, while Member States can mandate the operation of EBSI nodes at the national level. For third parties (e.g., software providers, service provides, etc.), these nodes are reachable via standardized APIs, through which

transactions are created and broadcasted to the shared distributed ledger. Currently, EBSI supports different cross-border services, i.e., use-cases (Self-Sovereign Identity - ESSIF, Diploma Management, Document Traceability, Trust Data Sharing, SME Financing, European Social Security Pass - ESSP, and Asylum Process Management) that could help citizens and businesses manage identities, educational credentials, and registration of documents. Since mGov4EU envisions implementing and integrating a Digital Wallet (implemented locally (Mobile Wallet) or in a cloud environment (Cloud Wallet)) into eID, e-signature, and SDG-related procedures, the Blockchain (EBSI) Building Block could be used in mGov4EU pilots and other mGov4EU building blocks wherever distributed ledger features are required or recommended.

2.3 Requirements for the Reference Architecture

Deliverable D1.3 [1] captures requirements in various categories, such as general system requirements, software requirements, economic and policy requirements, usability requirements, legal requirements and last but not least security and accountability requirements. These requirements entered the design of the present Reference Architecture. In addition, the following requirements have been specified for the Reference Architecture, upon suggestion of the reviewers:

Name	Requirement
R-RA-01	**Reference Architecture considers system requirements** The Reference Architecture SHALL consider all requirements specified in Deliverable D1.3 [1].
R-RA-02	**Reference Architecture has adequate level of abstraction** The Reference Architecture is sufficiently abstract to provide a manageable overview of the complex overall mGov4EU system and specific enough to allow a suitable refinement in the forthcoming design work package WP 2.
R-RA-03	**Reference Architecture contains relevant building blocks** The Reference Architecture SHALL cover the main building blocks for mGov4EU including eSignature, eID, SDG and the EU Digital Identity wallet.
R-RA-04	**Reference Architecture integrates input from stakeholders** The Reference Architecture SHALL integrate input provided by all relevant stakeholders[1].

Table 1: Requirements for the Reference Architecture

[1] See deliverable D2.1 [2] for an overview on potentially relevant stakeholders.

Chapter 3 Overview of mGov4EU Reference Architecture

A compact overview of the mGov4EU Reference Architecture is provided in the following Figure 2.

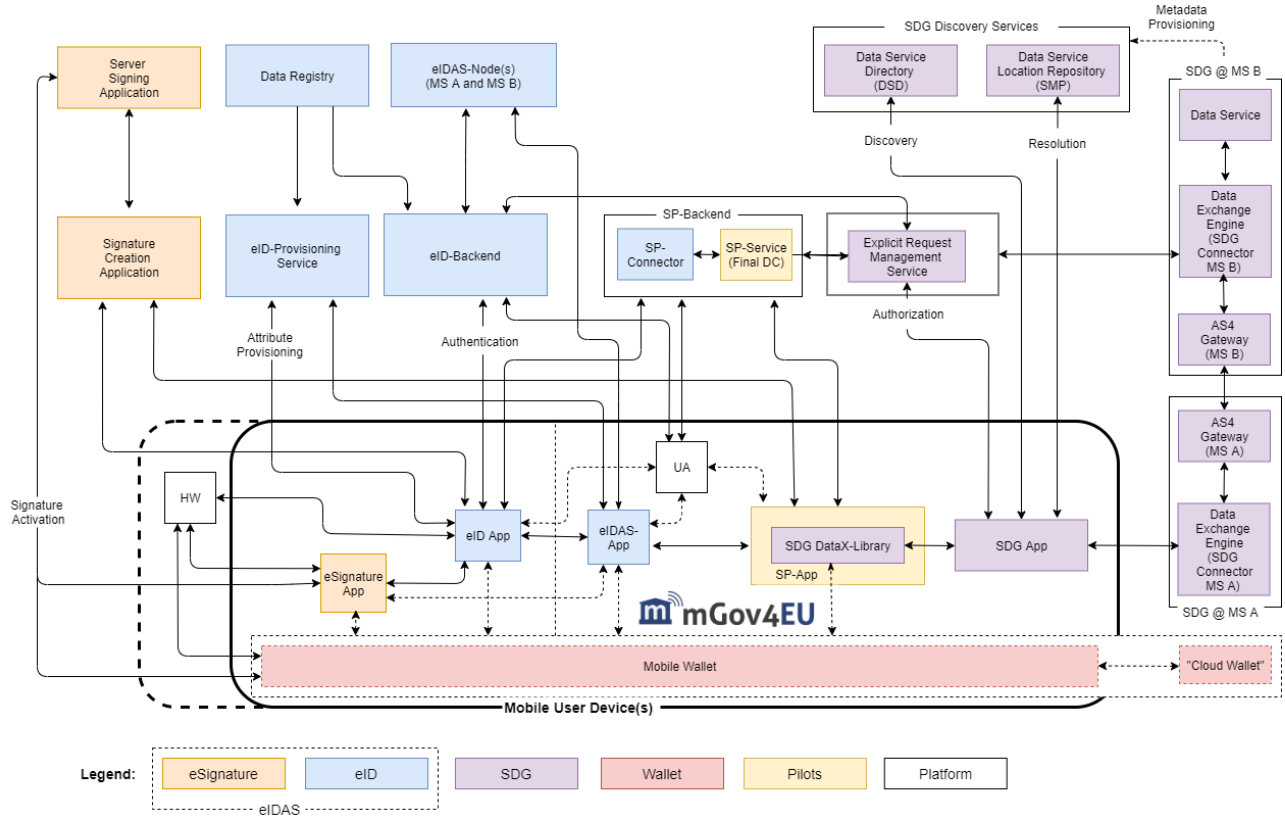

Figure 2: mGov4EU – Reference Architecture at a glance

It consists of different mobile apps on the Mobile User Device and certain background services, which may be grouped to mainly belong to

- eSignature (orange),
- eID (blue),
- SDG (purple),
- Digital Wallet (red),
- Platform (white) or
- are specifically built within mGov4EU pilots (yellow).

The mGov4EU project builts upon various CEF building blocks (see Section 2.2) and other existing components from previous projects (see Section 2.1). The innovations of mGov4EU are mostly related to the practical combination of eID and SDG related aspects and the mobile use of the partly existing components. The completely new components are all located on the mobile device of the user and comprise

- the eIDAS App,
- the Digital Wallet, which may consist of a Mobile Wallet and a Cloud Wallet,
- the SDG DataX-Library and
- the SDG App.

3.1 eSignature-related components

The eSignature-related components (orange) are aligned with ETSI TS 119 432 [3] given as follows:

- **eSignature App** (Signer Interaction Component, SIC in [3]) – allows the user to authorize the creation of the digital signature via the SCA and SSA,
- **Signature Creation Application (SCA)** – takes care about the creation of the advanced electronic signature format according to EN 319 142 PAdES [4], EN 319 122 (CAdES) [5], EN 319 122 (XAdES) [6] or TS 119 182 (JAdES) [7] and
- **Server Signing Application (SSA)** – creates the digital signature upon authorization of the signatory based on a hash of the data to be signed.

The eSignature-related components are planned to be used in the Mobile Signature pilot. Please refer to Chapter 4 for more information about and the interplay of these components and to D1.3 for more information on the pilot.

3.2 eID-related components

The eID-related components (blue) comprise

- **eID-App** – which is the local component of the user performing the eID protocol, such as an eID-Client according to BSI TR-03124 [8] for example,
- **eID-Backend** – is the server-side component performing the eID protocol, such as an eID-Server according to BSI TR-03130 [9] for example,
- **eIDAS App** – is a smartphone app or a library[2], which aims at integrating the existing eID Apps and eSignature Apps of the Member States,
- **eIDAS-Node(s)** – are server-side components according to Article 5 of CIR (EU) 2015/1501 [10], which are involved in cross-border identification processes,
- **SP-Connector** – is a server-side component, which may act as SAML [11] Service Provider for example and takes care about the integration with the application-specific SP-Service,
- **eID-Provisioning Service** – is a server-side component, which communicates with the eID App in order to issue credentials or provide additional attributes for the user,
- **Data Registry** – is the authoritative source for the additional attributes, which are provisioned by the eID-Provisioning Service.

The eID-related components are used in the Smart Mobility and eVoting pilots. Please refer to Chapter 5 for more information and the interplay of these components and to D1.3 for more information on the pilots.

3.3 SDG-related components

The SDG-related components (purple) comprise

- **SDG DataX-Library** – which can be integrated into an application-specific SP-App3 for triggering the usage of the SDG App in order to perform SDG-related procedures.
- **Data Service Directory (DSD)** – which allows to look up the address of the Data Service which needs to be contacted in the SDG procedure. Similar to the TOOP Technical Solution Architecture (see Figure 1), the DSD can be contacted via an interface according to OASIS ebXML RegRep Version 4.0 [10] for search queries involving the MS Name and type of evidence.

[2] The technical details of the eIDAS App will be defined in WP 2.

[3] The SDG DataX-Library can also be integrated into a standalone SDG App. The technical details of the SDG DataX-Library, the SDG App and the SP App will be defined in WP 2.

- **Data Service Location Repository (DS Location Repository)** – allows to look up the location of the Data Service in term of communication parameters (IP and port) and exposes an SMP interface.
- **SDG App** – is the central component in an SDG procedure, which takes care of the different sub-procedures: interaction with the Data Service Directory, the Data Service Location Repository, the eDelivery components as well as allowing the user to preview the data and accept or cancel the usage of the evidence. Specific to the mGov4EU project, after accepting the usage of the evidence, it allows the user to save to the Digital Wallet the information of the type of evidence and the queried Data Service during the SDG procedure. It has the role of the SDG Connector on the Data Consumer side in the 4 Corner Architecture of the eDelivery Architecture (see Figure 1).
- **Access Point(s)** – embody one AS4 Gateway from the CEF eDelivery Building Block in the case of an SDG procedure inside a single MS, and two AS4 Gateways in case the request is part of a cross-border procedure between MS A and MS B respectively.
- **Data Service** – is the recipient of a SDG request in an SDG procedure, which is operated by or on behalf of a Data Provider. After validating the SDG request in terms of user eID and Explicit Request provided Token, it will attempt to retrieve the evidence and reply to the SDG request by including the evidence in the SDG reply body.
- **Data Exchange Engine** – is located in Member State B and is, from the Data Provider side, capable of registering the Data Service to the DS Directory and the DS Location Repository. It is acting as the SDG Connector MS B from the eDelivery architecture (see deliverable D1.1 [13] and Figure 1). In the Member State A, the Data Exchange Engine acts as an anchor for the requests and responses related to SDG evidence retrieval procedure, handling sanity checks.
- **Explicit Request Management Service** – is a specific Authorization Server that can be used to retrieve an access token regarding the tuple: (user, evidence type and Data Service) to be included in an evidence request sent by the user through the SDG App and checked by the Data Service while validating the evidence request.

The SDG-related components are used in the Smart Mobility and eVoting pilots. Please refer to Chapter 6 for more information and the interplay of these components and to D1.3 for more information on the pilots.

3.4 Platform-related components

The platform-related components (white) comprise

- **UA** – is a plain browser (“User Agent”), which is provided by the Mobile User Device and
- **HW** – is a piece of cryptographic hardware (“HW”), which may be embedded in the Mobile User Device or provided externally in form of a FIDO U2F [14] token for example.

3.5 Wallet-related components

The Digital Wallet (red) may comprise:

- **Mobile Wallet**[4] – is a user-controlled storage for verifiable “credentials”5 and “evidences” on the Mobile User Device, which allows to be called from different smartphone apps in order to store credentials and evidences in a secure manner. The difference between “credential” and “evidence” is that an “evidence” is only a “bearer token”, whereas a “credential” would also allow to support a “holder of key” transaction. An “evidence” is defined to be “any document

[4] The recently published draft of the eIDAS Amendment [15] introduces in Art. 3 (42) the *“European Digital Identity Wallet”*, which *“is a product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals”*.

[5] The recently published draft of the eIDAS Amendment [15] defines *“Credential”* in Art. 3 (52) as *“a proof of a person’s abilities, experience, right or permission”*.

or data, including text or sound, visual or audiovisual recording, irrespective of the medium used, required by a competent authority to prove facts or compliance with procedural requirements" under the SDGR. A "credential" is a special type of "evidence".

- **Cloud Wallet** – is a server-side component, which allows to store verifiable credentials and evidences in a secure and user-controlled manner.

The Digital Wallet is of central importance for the mGov4EU project and the forthcoming eIDAS-related Ecosystem[6]. Please refer to Chapter 7 for more information about these components.

3.6 Components related to mGov4EU pilots

Last but not least, the following pilot-specific components exist (yellow):

- **SP-Service** – is an application-specific service, which implements some application logic and serves as Data Consumer in the SDG perspective. The pilots outlined in D1.3 are examples of SP-Services.
- **SP-App** – is an application-specific mobile app, which implements some application logic.

Please refer to D1.3 "Specification of System Requirements" for more information on the mGov4EU pilots.

[6] See [15] and https://blog.eid.as/eidas-ecosystem/.

Chapter 4 eSignature-related Architecture

This Chapter focuses on those parts of the reference architecture that are relevant for eSignature-related use cases and process flows. The interplay of the different eSignature-related components is depicted in the following Figure 3.

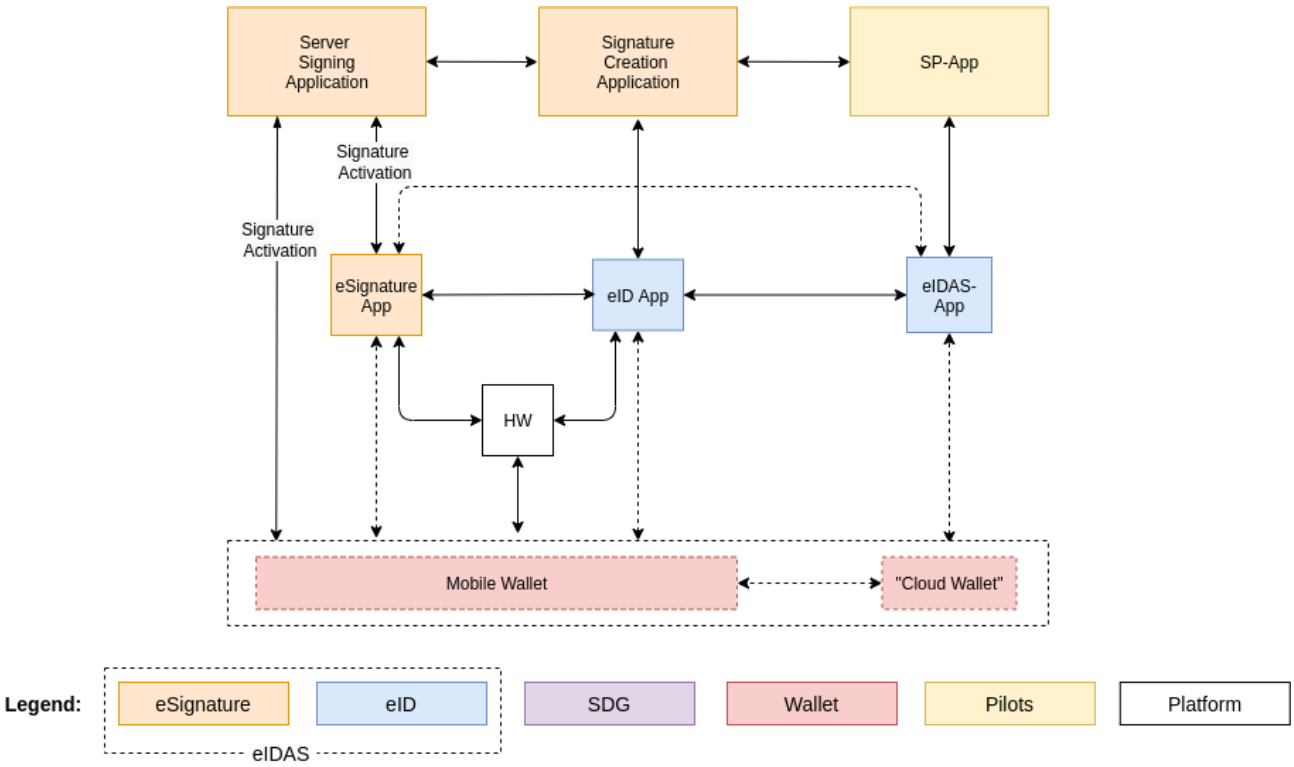

Figure 3: Interplay of eSignature-related components

The SP App shown in Figure 3 implements business logic to provide a service to the user. During service provision, the SP App requires the user to create an electronic signature. Basically, the SP App can start the signature-creation process (1) via the file-sharing feature of the mobile device platform (“Share Document”), i.e., by sharing the document to be signed, or (2) via invocation of the SCA interface.

The eIDAS App offers functionality for “Signature System Selection” and a variety of signature handlers, which either allow to (a) invoke an external signature app or (b) compute a signature using the “Embedded Handler”, which is able to support a “Remote Signature System” (Server Signing Application; cf. Figure 14).

The sequence diagrams depicted in the following figures illustrate different signature-creation processes. These processes mainly differ in the way the preferred signature-creation solution is selected. In all processes, a user of Member State (MS) B wants to create an electronic signature using a specific Signature System (potentially of MS A). Therefore, several steps need to be performed to redirect the user to the desired Signature System in a secure and reliable way. These steps are coordinated by the eIDAS App introduced by mGov4EU. The following paragraphs give an overview of the authentication flows depicted in the respective figures.

In the process flow shown in Figure 4, the signature-creation process is initiated via an SCA-Request. The SP App requiring the signature sets the correct signature parameters. It then invokes the eIDAS App and transmits the document to be signed together with the required signature parameters. In the eIDAS App, the user then selects the preferred Signature System. Next, the eIDAS App identifies an appropriate way to contact the SCA App (eSignature App) and securely forwards the signing request by taking into account the specific characteristics of the selected SCA App.

Depending on the type of the SCA and its concrete implementation, a Remote Signature System can be employed to handle the signature-creation process. The Signature Solution, making use of the SCA App and/or a Remote Signature System, then authenticates the user to authorize the use of the user's private signing key and the creation of the electronic signature using this key. After successfully obtaining the user's approval to sign the document, the signature is created on the provided document. The signed document is then returned to the initially requesting SP App passing through the eIDAS App.

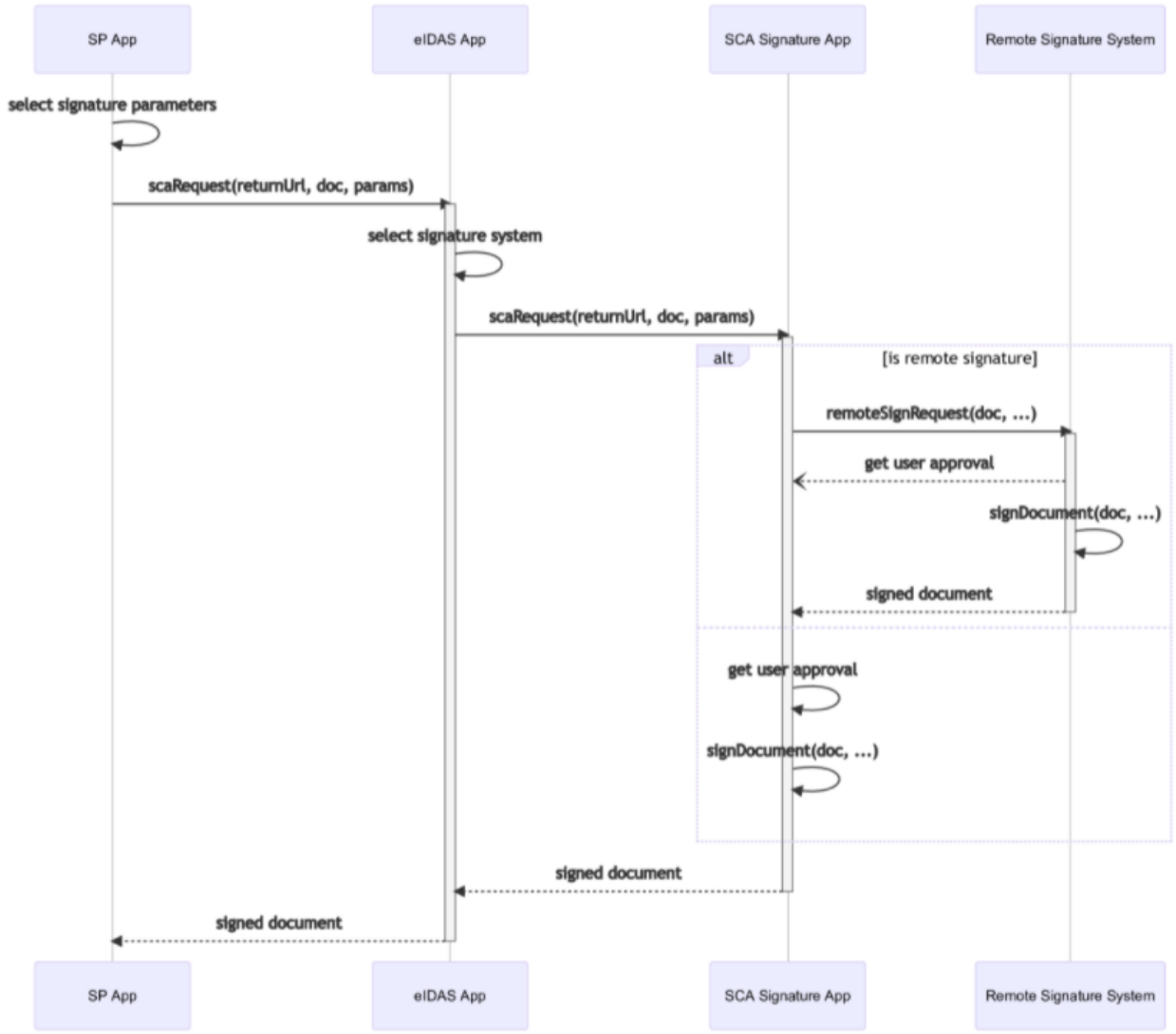

Figure 4: Signature system selection using mGov4EU's eIDAS App

Figure 5 depicts a slightly different process flow, which, however, in large parts resembles the flow shown above in Figure 4. Again, the SP App requires the user to sign a document. However, in this case, the SP App simply shares the document to be signed with the eIDAS App using built-in features of the respective mobile operating platform. In the eIDAS App, the user then selects the preferred Signature System, while the eIDAS App determines the appropriate signature parameters.

The next steps resemble those described above for the first scenario. The eIDAS App identifies an appropriate way to contact the selected SCA App (eSignature App) and securely forwards the signing request by taking into account the specific characteristics of the SCA App. Depending on the type of the selected SCA, a "Remote Signature System" can be employed to handle the signature-creation process and to create the electronic signature. After the device has verified the user's approval to sign (by authenticating the user), it creates the signature on the provided document. The signed document is finally returned to the eIDAS App, which then saves the document for the user.

Note that in this scenario there is no re-invocation of the SP App, which initiated the signature-creation process.

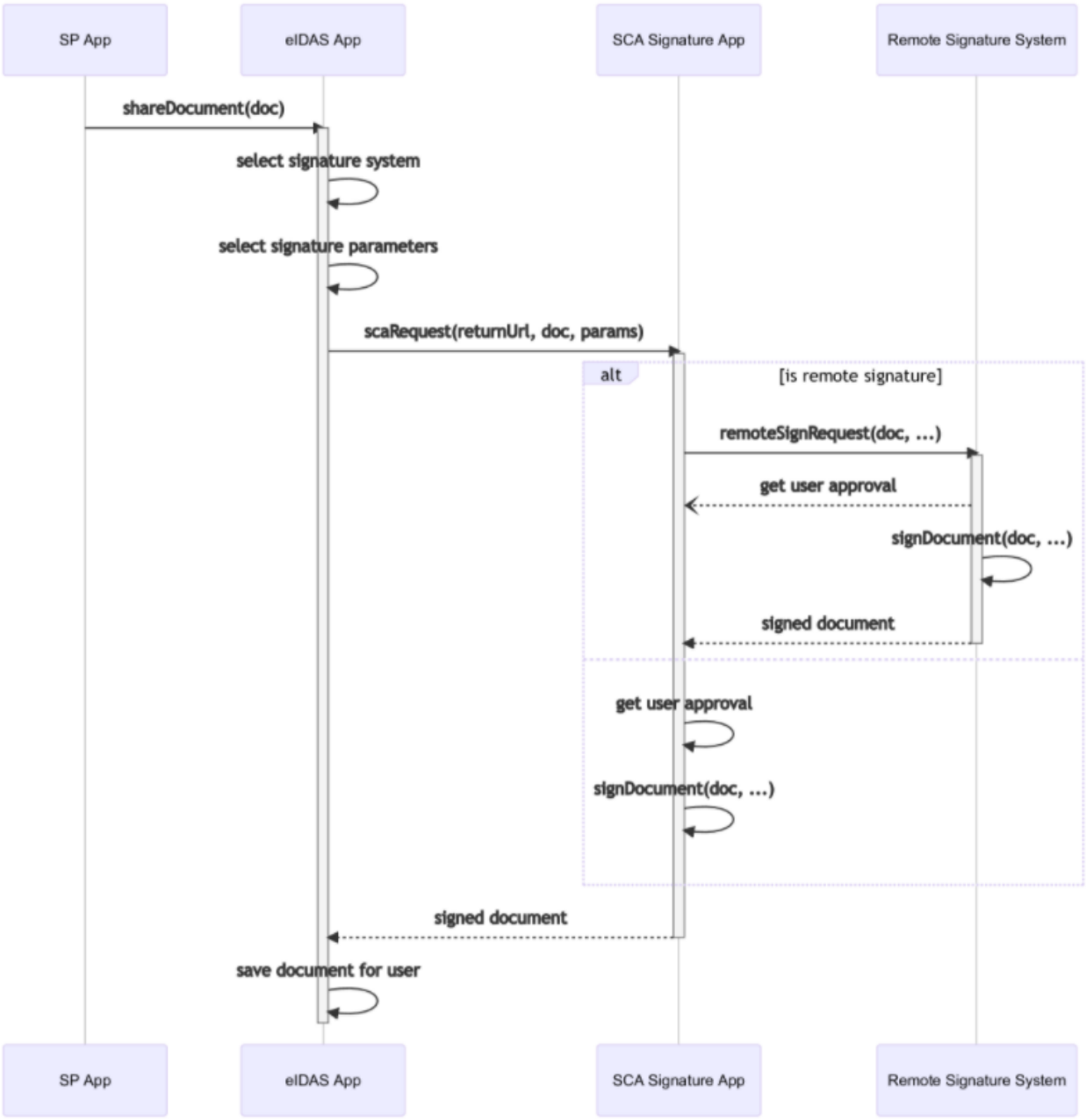

Figure 5: Signature system selection and creation via a shared document

Finally, Figure 6 depicts a scenario, in which a user wants to sign a document using a Legacy Signature App. In the eIDAS App, the user selects the document and the Legacy Signature System for the signature-creation process. Similar to the previous scenarios, the eIDAS App identifies an appropriate way to contact the Legacy Signature App and shares the document to be signed by taking into account the specific characteristics of the Legacy Signature App, which is to be called.

Depending on the type and concrete technical implementation of the Legacy Signature App, a “Remote Signature System” can be employed to handle the actual signature creation. After the device has obtained and verified the user’s approval to sign, it creates the signature on the provided document. The signed document is then saved for the user directly by the Legacy Signature App, i.e., it is not transferred back to the eIDAS App.

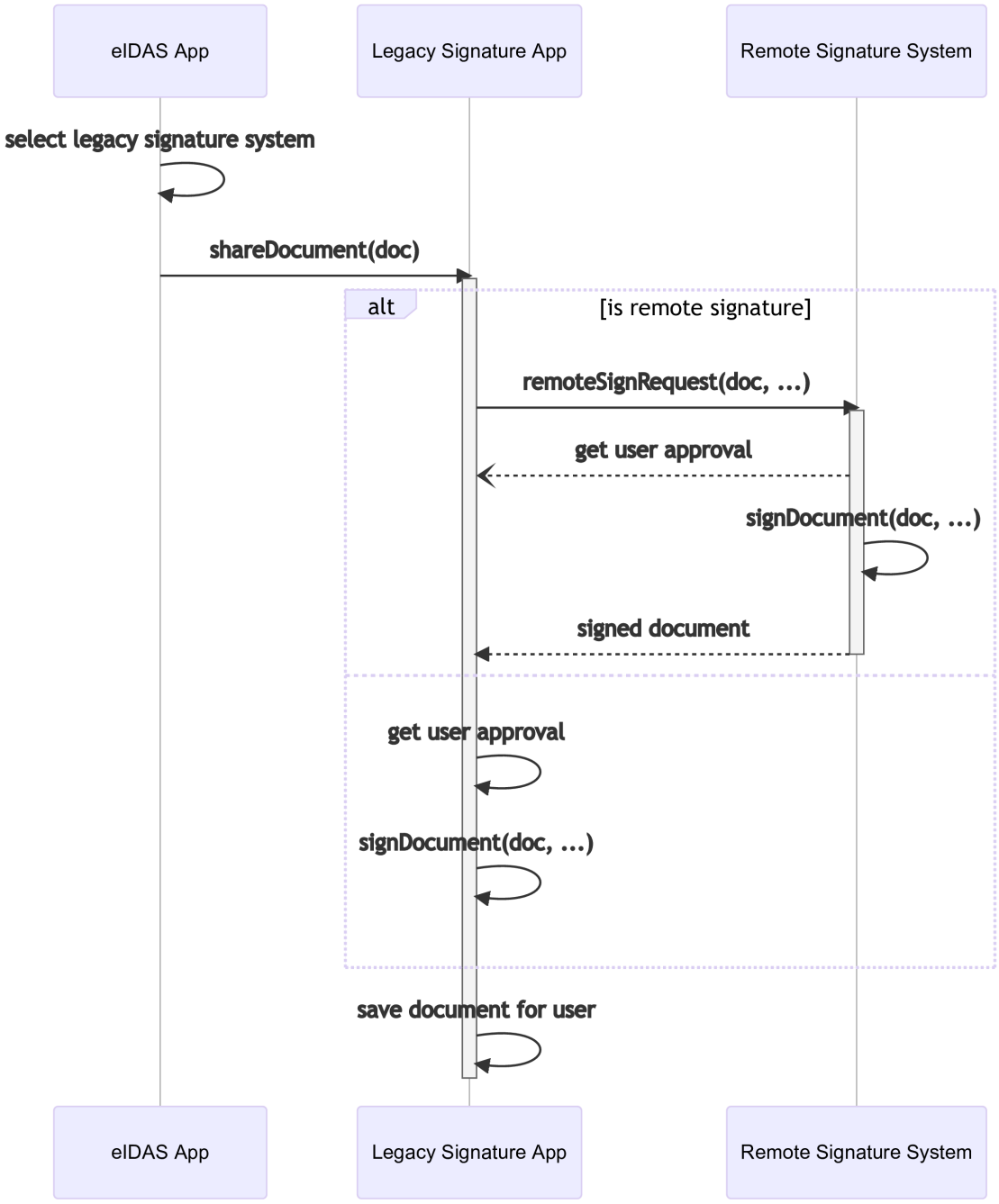

Figure 6: Legacy signature system selection

The three process variants depicted above must not be regarded as exhaustive. They merely serve as examples and a means to illustrate that the reference architecture shown in Figure 2 allows for the realization of various different scenarios and process flows related to the creation of electronic signatures.

Also, the process flows described above have intentionally been kept on a rather abstract level. This way, the level of abstraction resembles the one of the reference architecture itself. When further developing the process flows towards concrete technical implementations, several additional details will be considered and exposed. This is supposed to be carried out in WP2, which will take the rather abstract architectures and process-flow descriptions in this deliverable as a starting point for further refinement.

Chapter 5 eID-related Architecture

The interplay of the different eID-related components is depicted in Figure 7.

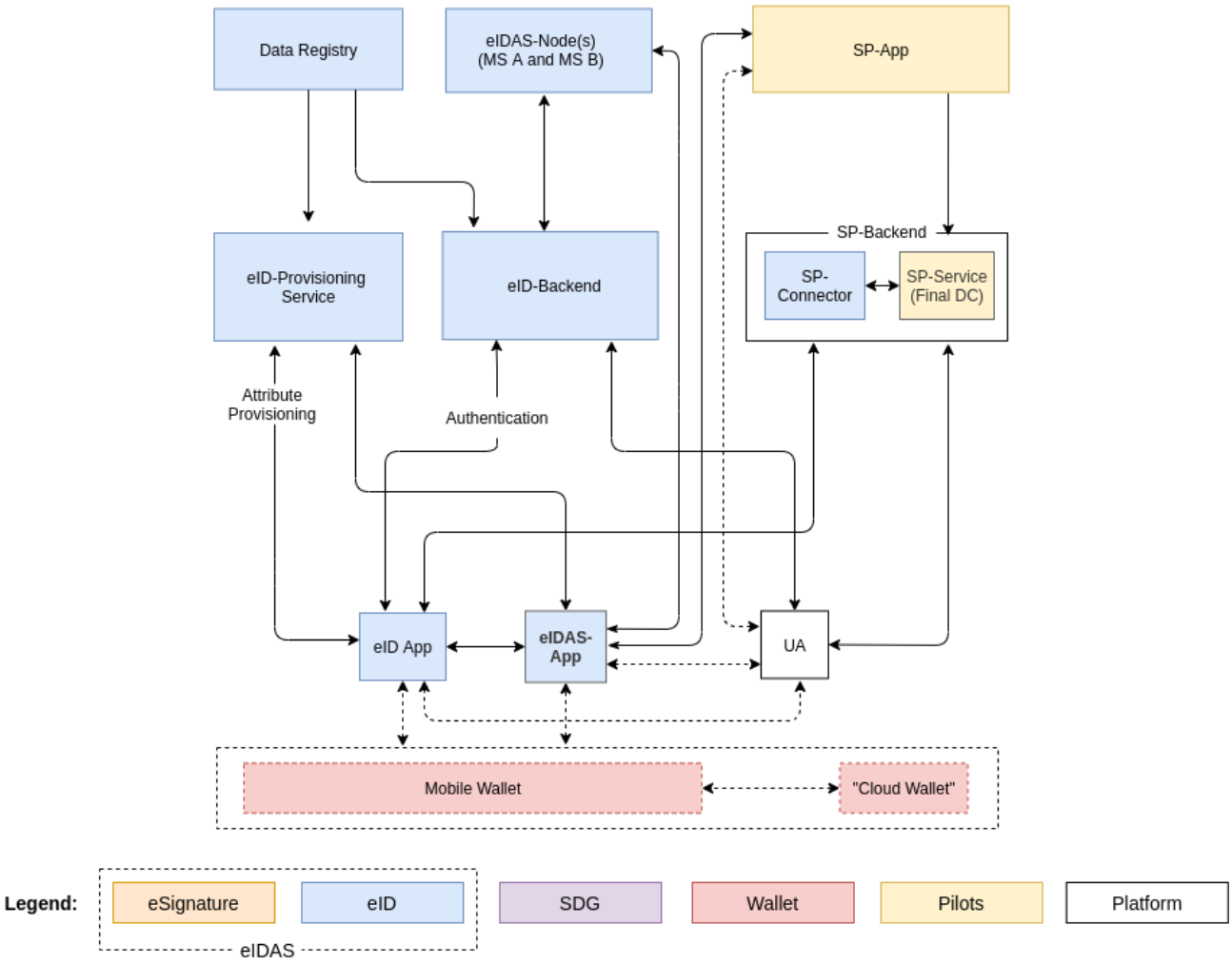

Figure 7 Interplay of eID related components

The sequence diagrams depicted in the following figures (Figure 8, Figure 9, Figure 10) illustrate a cross-border identification and authentication flow. A user of Member State (MS) B wants to access a restricted resource using an SP App of MS A and authentication means of MS B. Therefore, several steps are performed which can loosely be categorized in cross-border and non-cross-border (national) actions, where the cross-border actions are coordinated by a special eIDAS App. The following paragraphs describe the authentication flow on a more abstract level.

A User wants to access a restricted resource at the SP Connector of MS A via the SP-App of MS A. To make an authorization decision the SP Connector initiates an authentication request at the eID-Backend of MS A, which is forwarded to the UA by the SP app. (see Figure 8, steps 1-4)

The User Agent (e.g. a web-browser) handles the communication with the eID-Backend of MS A. It forwards the authentication request to the eID-Backend, which in turn offers different login means the user can chose from. In this example, the option eIDAS login is selected. To initiate the eIDAS authentication, the eID-Backend of MS A creates an authentication request for the eIDAS node of MS A, which is forwarded to the eIDAS App by the UA. (see Figure 8, steps 5-10)

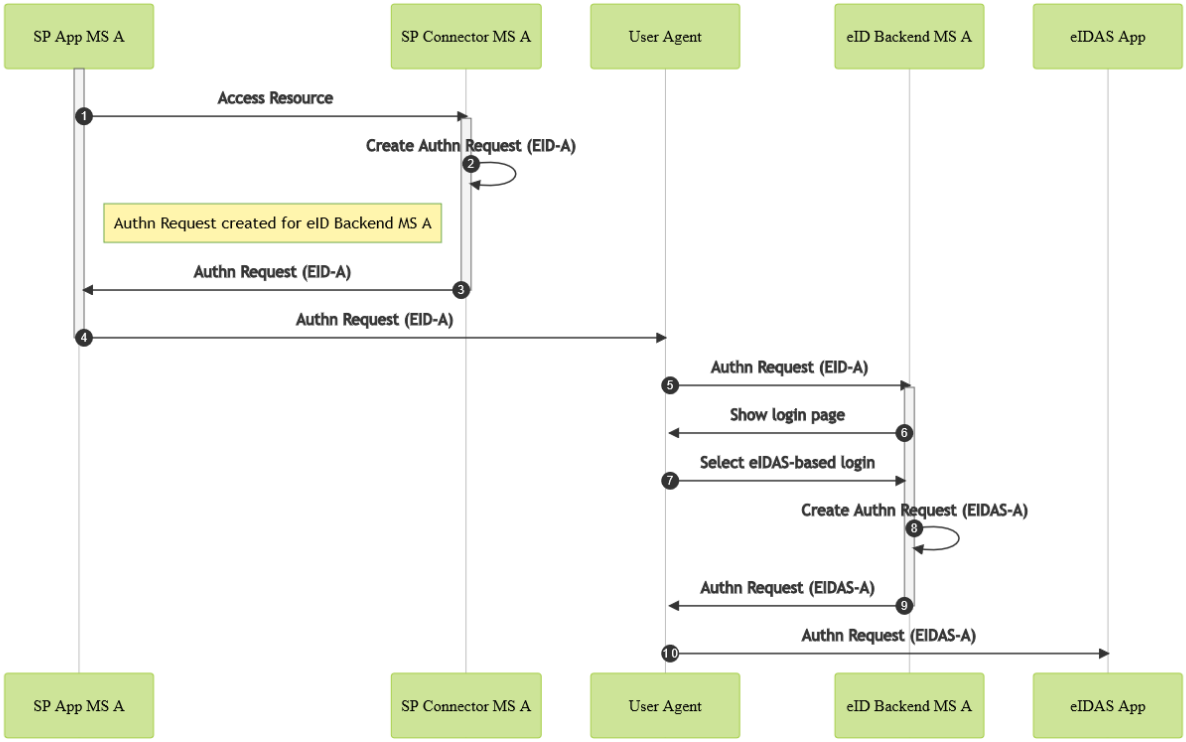

Figure 8: Cross-border identification and authentication flow (part 1)

The eIDAS App has two main tasks. One is to coordinate the communication between the eIDAS-Nodes of different MS. The other is to retrieve the requested credentials from targeted MS from either the eID-App of that MS or from the Digital Wallet.

In the depicted example (see Figure 9) the eIDAS App forwards the authentication request to the eIDAS-Node of MS A. In return the eIDAS-Node offers login choices for all available MS. Based on the user choice an authentication request for the selected MS eIDAS-Node is generated. In this example MS B is selected and an authentication request to eIDAS-Node of MS B is created. The eIDAS App forwards the authentication request to the eIDAS node of MS B, which creates and returns an authentication request targeting the eID-Backend of MS B (see Figure 9: Cross-border identification and authentication flow (part 2), steps 1-8).

If an eID-App of MS B is available and installed on the mobile device, then the eIDAS App forwards the authentication request generated by the eIDAS-Node of MS B to the eID-App. The eID-App handles the authentication of the user at the eID backend of MS B. The authentication means available to the user can differ between the MSs. After the successful authentication, the eID-Backend replies with an authentication response, which is forwarded to the eIDAS App (see Figure 9, step 9-16).

As an alternative to the eID-App based approach, a Digital Wallet can be used to retrieve user credentials, which have been created before using the eID-Provisioning Service. Therefore, the eIDAS App requests the necessary attributes – specified by the authentication request of the eIDAS backend of MS B – from the Digital Wallet. After the successful authentication of the user, the Digital Wallet releases the requested attributes. The eIDAS App then wraps these attributes into an authentication response aligning with the authentication response structure of the eID-Backend of MS B (see Figure 9, steps 17-20).

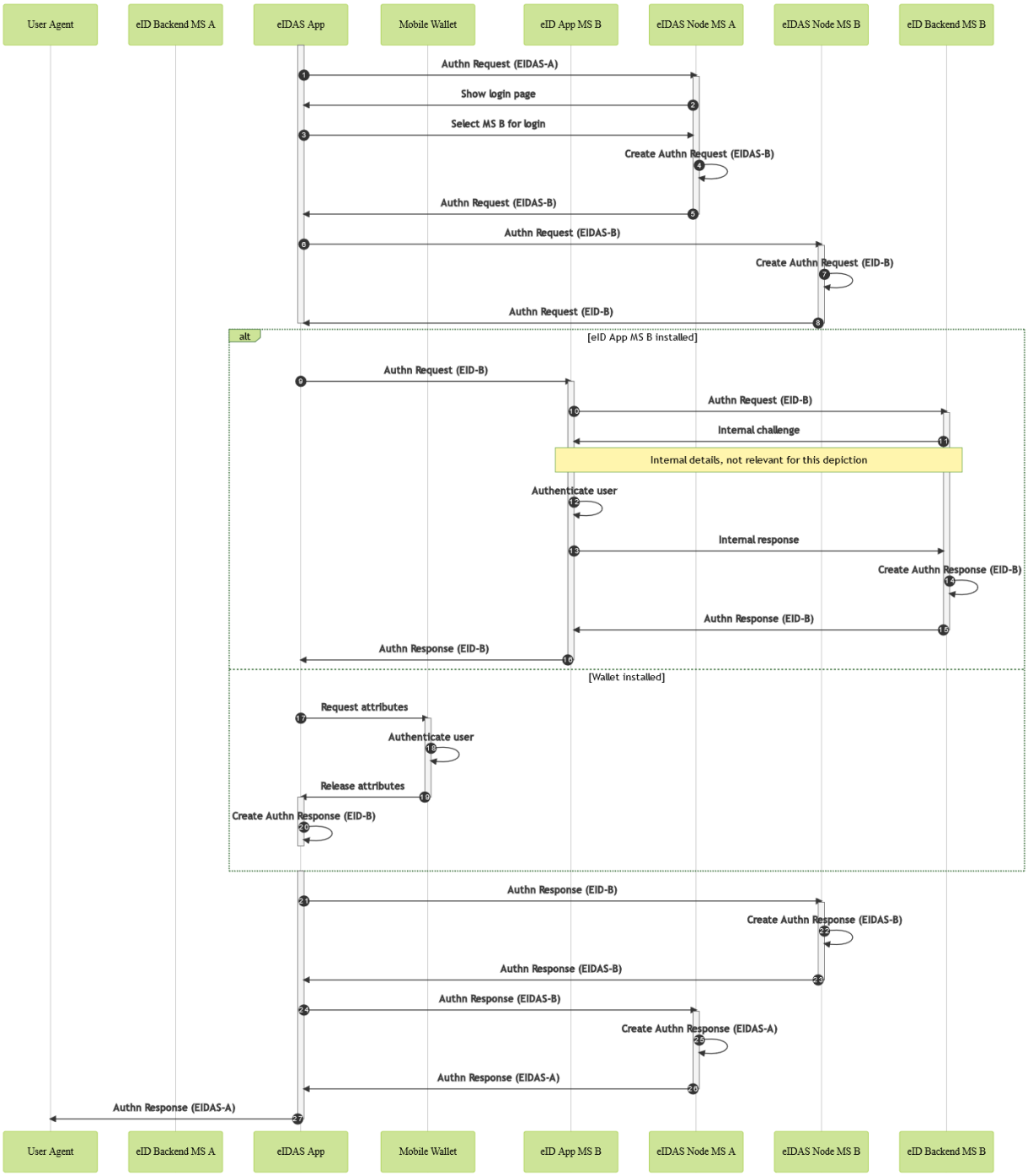

Figure 9: Cross-border identification and authentication flow (part 2)

The eIDAS App coordinates the response for the cross-border flow by sending the authentication response of the eID-Backend of MS B to the eIDAS-Node of MS B. The resulting response is then sent to the eIDAS-Node of MS A, whose response is forwarded to the UA. The UA communicates with the eID-Backend of MS A to retrieve the authentication response, which is used by the SP-App to access the restricted resource (see Figure 9, steps 21-27 and Figure 10).

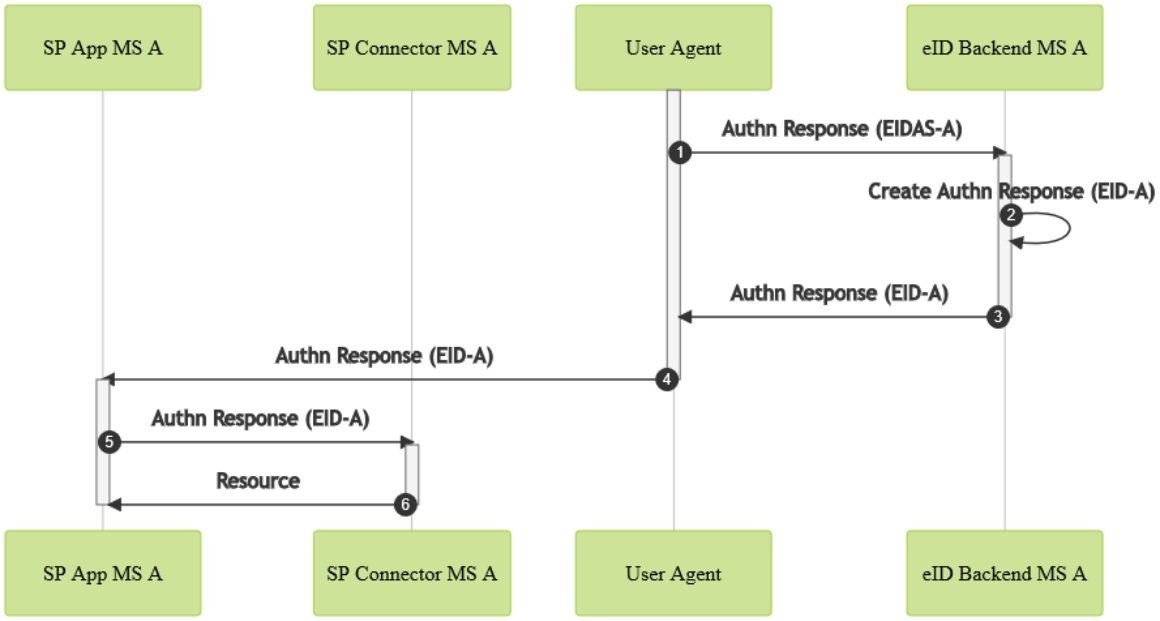

Figure 10: Cross-border identification and authentication flow (part 3)

Chapter 6 SDG-related Architecture

The interplay of the different SDG-related components is depicted in Figure 11.

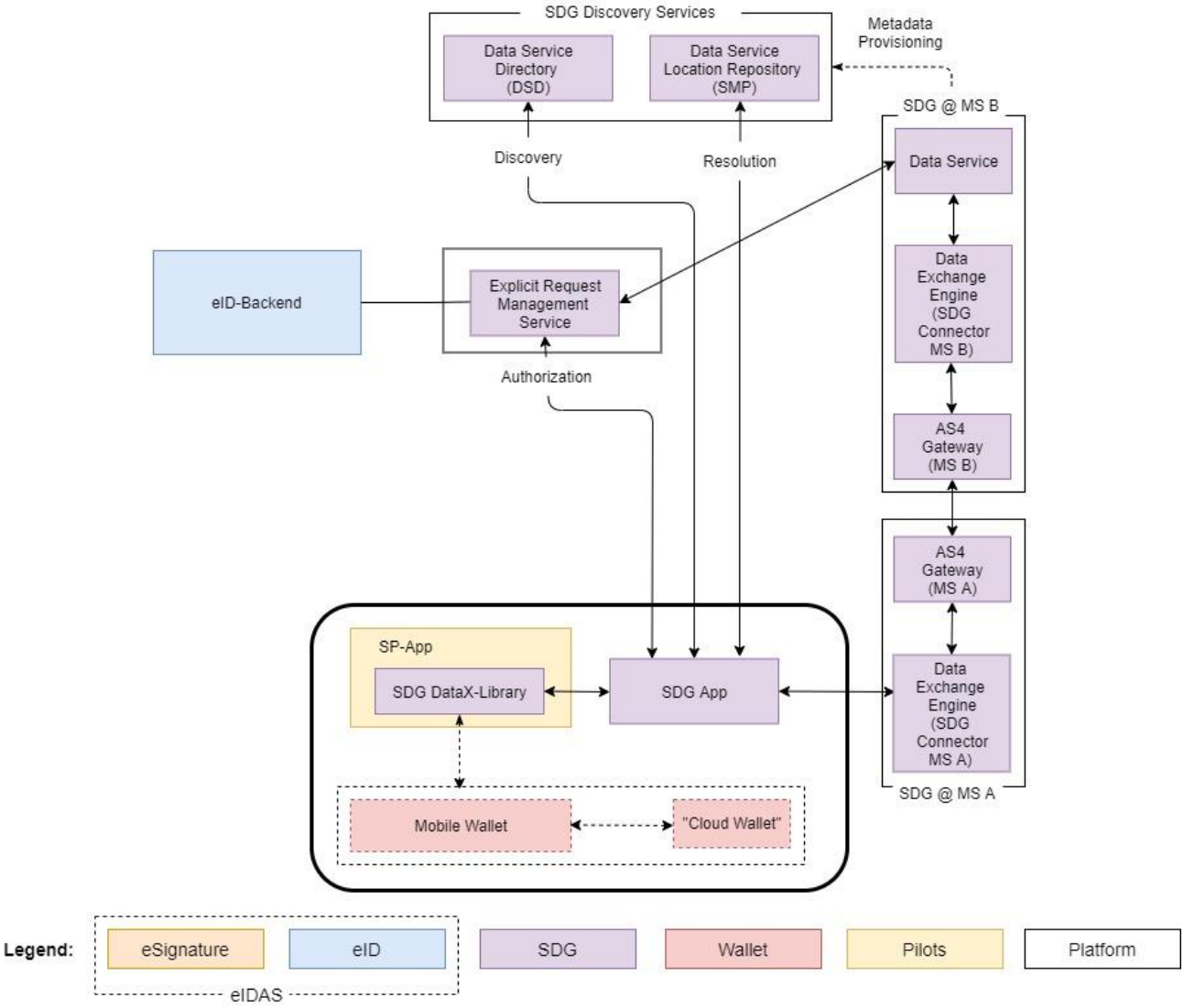

Figure 11: Interplay of SDG-related components

The sequence diagram for searching the Data Service for a specific evidence type and country can be seen in Figure 12. Evidence type and country are provided as parameters and the query is encoded using OASIS RegRep protocol and targeted to the Data Service Directory. The returned information is first processed in the SDG App. If the Data Service is found, the user has to select the desired Data Service to be used and afterwards the SDG App will receive the Data Service identifier (DS Id), otherwise an error will be returned.

The sequence diagram for retrieving an evidence with a specific evidence type from the selected Data Service is depicted in Figure 13. After retrieving the token using the Authorization interface from the Explicit Request Management Service, the SDG App will then resolve the Data Service by communicating with the Data Service Location Repository. After a successful resolution, the eDelivery request is encoded by including the requested evidence type, the user identity information, the authorization token and the Data Service Id. The request is then forwarded to the well-known (configured) Member State A national eDelivery AS4 Gateway, which will then forward it to the Member State B national eDelivery AS4 Gateway, in case the request will be a cross-border request. After the Data Service connector or the Data Service itself has checked the user identity and the provided authorization token, it will retrieve the required evidence. The evidence will then be encoded

in an eDeliery response and sent back towards the user. After being forwarded by the AS 4 Gateway(s), the response will be decapsulated by the SDG App. In case the evidence is present, it will be displayed to the user for preview and the user will be asked, whether the evidence should be accepted. In case of an affirmative answer, the evidence will be sent to the SDG Data-X-Lib through a callback.

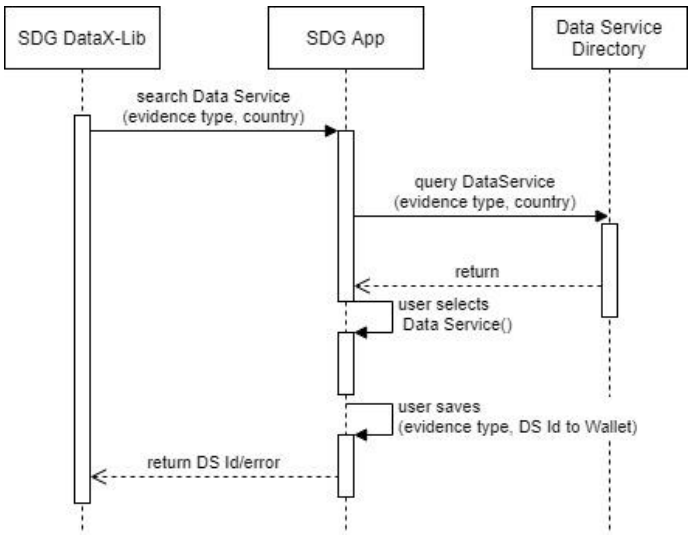

Figure 12: Message flow for the discovery of the Data Service

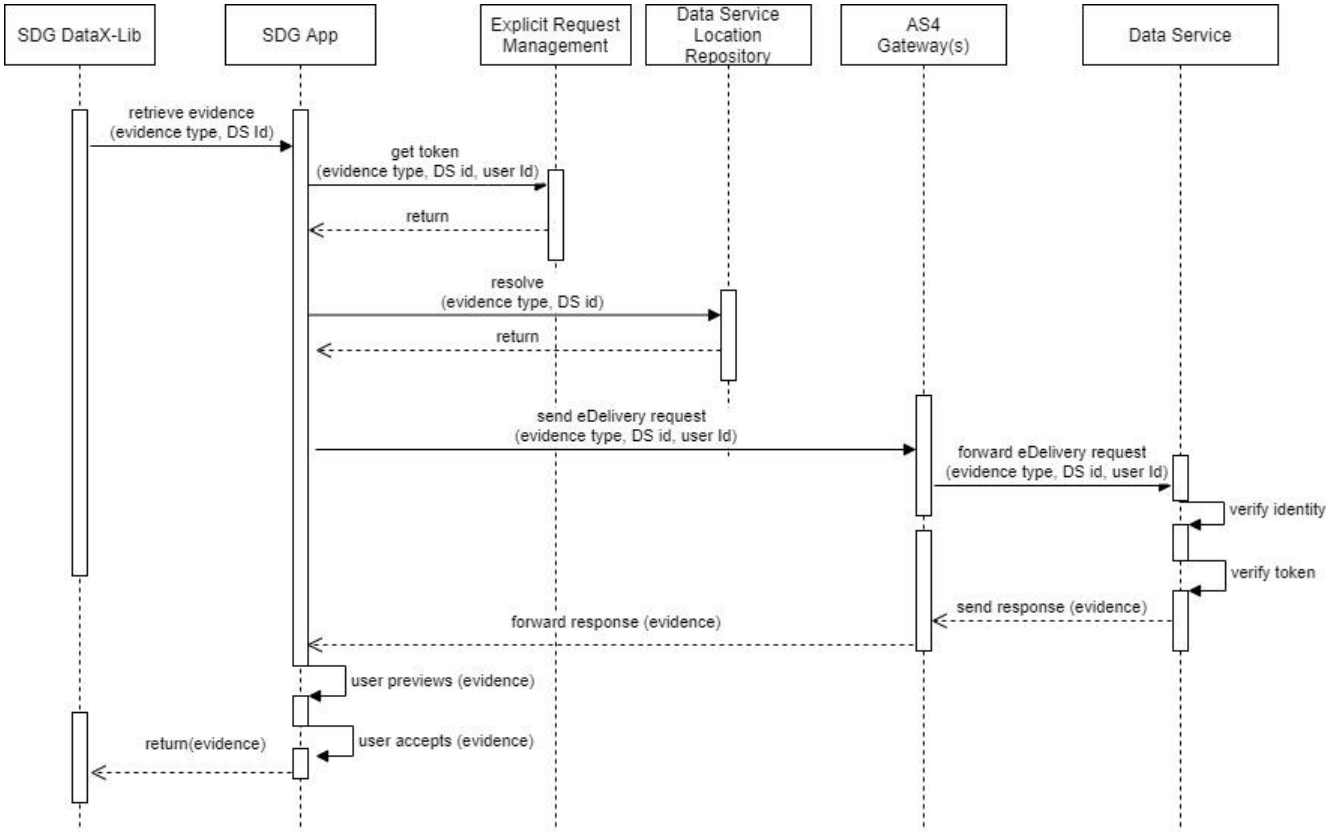

Figure 13: Message flow for retrieving an evidence

Chapter 7 Wallet-related Components

Art. 3 (42) of the recently provided draft for the eIDAS-Amendment [15] defines the *"European Digital Identity Wallet"* to be *"a product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals"*.

Such a Digital Wallet, which may consist of a Mobile Wallet and a Cloud Wallet, and its interfaces to related components is outlined in the following Figure 14. More technical details with respect to the components and its interfaces will be elaborated in WP2.

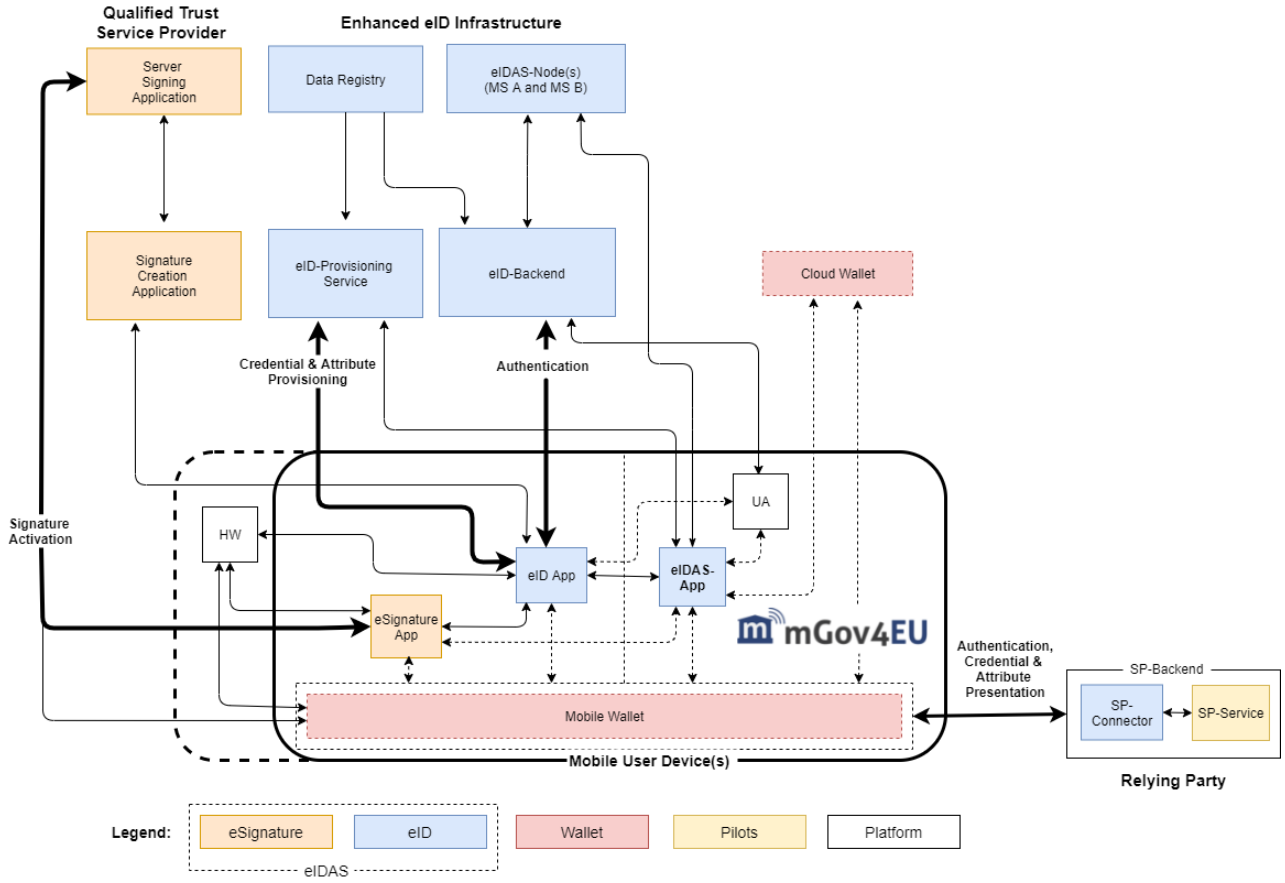

Figure 14: Wallet-related components

Given the definition it becomes immediately clear, that the Digital Wallet, which may consist of a Mobile Wallet and/or Cloud Wallet, will need to be capable to **store** identity data, credentials and attributes linked to her/his identity and have interfaces to different external components including

- the **Relying Party** for the authentication (online and offline) and for the presentation of credentials and attributes upon request,
- the **eID-Backend** for authentication (online) and identification,
- the **eID-Provisioning Service** for the provisioning of credentials and attributes and
- the **Qualified Trust Service Provider** to create qualified electronic signatures and seals.

Chapter 8 Summary and Conclusion

This document has first recalled the main existing building blocks and requirements relevant to the mGov4EU project (Chapter 2) and developed a corresponding technical Reference Architecture based on these building blocks and requirements in 0. This Reference Architecture has identified the main modules and outlines interfaces between the modules. It comprises components related to eSignature, eID, SDG, as well as platform- and wallet-related components and, components specific to the pilots to be developed and executed within the mGov4EU project.

The Reference Architecture describes the main components, interfaces, and - if necessary - processes with respect to eSignature (Chapter 4), eID (Chapter 5), the Single Digital Gateway (Chapter 6), and the Digital Wallet (Chapter 7) in order to provide a solid foundation for the upcoming work in mGov4EU. In particular, it serves as foundation for the specification of requirements in task 1.3 and will serve as input for the upcoming design (WP 2) and implementation work (WP 3). For this purpose, WP 2 will develop a detailed design for the Digital Wallet, the eIDAS App and the SDG DataX-library, as well as related components.

Considering the fact that the Reference Architecture contains different apps (eSignature App, eID-App, eIDAS-App, SP-App, SDG-App, Mobile Wallet), which often need to communicate with each other, we conclude that the App-to-App-communication will play an important role within the forthcoming design and implementation of the mGov4EU building blocks in WP2 and WP3 respectively.

Chapter 9 Bibliography

[1] mGov4EU, 'Specification of System Requirements', Deliverable 1.3, 2021.

[2] mGov4EU, 'Business Model and Stakeholder Ecosystem Development', Deliverable D2.1, 2021.

[3] European Telecommunications Standards Institute (ETSI), *Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation, ETSI TS 119 432, Version 1.1.1*. 2019.

[4] European Telecommunications Standards Institute (ETSI), *Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures; Part 1: Building Blocks and PAdES Baseline Signatures, ETSI EN 319 142-1, Version 1.1.1*. 2016.

[5] European Telecommunications Standards Institute (ETSI), *Electronic Signatures and Infrastructures (ESI); CAdES Digital Signatures; Part 1: Building Blocks and CAdES Baseline Signatures, ETSI EN 319 122-1, Version 1.1.1*. 2016.

[6] European Telecommunications Standards Institute (ETSI), *Electronic Signatures and Infrastructures (ESI); XAdES Digital Signatures; Part 1: Building Blocks and XAdES Baseline Signatures, ETSI EN 319 132-1, Version 1.1.1*. 2016.

[7] European Telecommunications Standards Institute (ETSI), *Electronic Signatures and Infrastructures (ESI); JAdES digital signatures built on JSON Web Signatures; Part 1: Building blocks and JAdES baseline signatures, Draft ETSI TS 119 182-1*. 2020.

[8] Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik), 'BSI TR-03124 - eID-Client', Technical Guideline, 2017. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03124/TR-03124_node.html

[9] Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik), *BSI TR-03130 - eID-Server*. 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_Part1.pdf

[10] European Commission, *COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*. 2015. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1501&from=EN

[11] S. Cantor, J. Moreh, R. Philpott, and E. Maler, 'OASIS Standard', OASIS, Mar. 2005. Accessed: Mar. 05, 2021. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/

[12] 'OASIS ebXML RegRep Version 4.0', OASIS Standard, 2012. [Online]. Available: http://docs.oasis-open.org/regrep/regrep-core/v4.0/regrep-core-overview-v4.0.html

[13] mGov4EU, 'Survey of related work', Deliverable D1.1. [Online]. Available: https://www.mgov4.eu/fileadmin/mgov-files/pub/mGov4EU-D1.1-PU-M03-website.pdf

[14] FIDO Alliance, 'Universal 2nd Factor (U2F) Overview'. https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.pdf (accessed Mar. 05, 2021).

[15] European Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity', SEC(2021) 228 final.