European Digital Identity

Architecture and Reference Framework

– Outline –

1 TABLE OF CONTENTS

1 INTRODUCTION

1.1 CONTEXT

On 3 June 2021, the Commission adopted a Recommendation[1] calling on Member States to work towards the development of a Toolbox including a technical Architecture and Reference Framework (ARF), a set of common standards and technical specifications and a set of common guidelines and best practice.

The Recommendation specifies that these outcomes will serve as a basis for the implementation of the European Digital Identity Framework Regulation[2] once adopted, without the process of developing the Toolbox interfering or prejudging the legislative process.

The Recommendation foresees that the Toolbox is developed by Member States' experts regrouped in the eIDAS expert group[3] in close coordination with the Commission and, where relevant, other concerned public and private sector parties.

Following the indicative timeline set by the Recommendation, the eIDAS expert group agreed on process and working procedures at its first meeting on 30 September 2021 and discussed a non-paper on a high-level description of the European Digital Identity Wallet ecosystem (hereinafter "EUDI Wallet") proposed by the Commission[4].

On this basis, the expert group decided to focus first on a more detailed description of the EUDI Wallet concept, its functionalities and security aspects and on a number of core use cases between October and December 2021.

1.2 PURPOSE OF THE DOCUMENT

The present outline provides a summary description of the eIDAS expert group's understanding of the EUDI Wallet concept including:

- objectives of the EUDI Wallet,
- roles of the actors of the ecosystem,
- wallet's functional and non-functional requirements and

[1] COMMISSION RECOMMENDATION (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework, OJ L 210/51, 14.6.2021

[2] 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, COM(2021) 281 final, 3.6.2021

[3] https://ec.europa.eu/transparency/expert-groups-register/screen/expert groups/consult?do=groupDetail.groupDetail&groupID=3032

[4] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2021.210.01.0051.01.ENG

- potential building blocks.

The outline is non-mandatory and presents the state of play of the ongoing work of the eIDAS expert group and does not imply any formal agreement regarding its content or the regulation proposal. It will be complemented and updated in the process of establishing the toolbox. It is intended to develop this outline to a full Architecture and Reference Framework of the European Digital Identity Framework (ARF) as set out in the Recommendation. The ARF will be aligned to the outcome of the legislative negotiations of the proposal for a European Digital Identity Framework and the present document will be updated.

The present document uses the terms "**shall**"[5] and "**may**"[6] to express requirements currently foreseen in the legislative proposal or possibilities not necessarily proposed as mandatory, but should not in this document be understood as formally prescriptive or legally binding.

Only the finally adopted European Digital Identity Framework Regulation, and the implementing and delegated acts adopted under that legal basis, will be mandatory.

The eIDAS expert group adopted the present document on 22 February 2022 and decided to publish it for stakeholder feedback.

[5] "shall": is used to express mandatory requirements (provisions that have to be followed). The negative form is "shall not".

[6] "may" is used to express permissible actions (provisions that an implementation is able to follow or not follow). The negative form is "need not".

2 OBJECTIVES OF THE EUDI WALLET

The primary objective of the proposed European Digital Identity Wallet is to promote trusted digital identities for all Europeans allowing users to be in control of their own online interactions and presence. It can be seen as a combination of several products and trust services that enables users to securely request, obtain and store their information allowing them to access online services, share data about them and electronically sign/seal documents.

A number of use cases will underpin the development of the EUDI Wallet to deliver effectively and seamlessly on its functionalities in all Member States. The eIDAS expert group has worked on a number of first use-case areas which include:

- *Secure and trusted identification to access online services*

While secure authentication is a functionality of the EUDI Wallet, relying parties identifying users with a defined set of person identification data for the purposes of allowing access to online public and private services is a specific use case. For instance, private relying parties shall accept the use of EUDI Wallets where they are required to use strong user authentication for online identification.

- *Mobility and digital driving licence*

The EUDI Wallet may enable a fully digital European Driving Licence for online and offline scenarios. It could link to a series of further attestations offered by public or private providers covering legal requirements (e.g Certificate of Professional Capacity) or business requirements and standards (e.g. for road tolling) in the road transport area.

- *Health*

Easy access to health data is crucial in both national and cross-border contexts. Based on the experience from the EU Digital COVID Certificate[7], the EUDI Wallet would enable access to patient summary, ePrescriptions, etc.

- *Education / Diploma*

Providing documents for qualification recognition procedures can be costly and time-consuming for end users, companies and employers, education and training providers, and other academic institutions. For example, digital diploma attestations could be shared cross-border in a verifiable, trusted, and consumable format to another education or training institution or a prospective employer. The EUDI Wallet can be a repository for educational digital credentials as electronic attestations of attributes and a means for exchanging them by a learner.

- *Digital Finance*

The EUDI Wallet could facilitate payment authentication with a high degree of security and enable a frictionless experience in payments. In line with the Commission's Retail Payments Strategy[8], the use case

[7] Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic

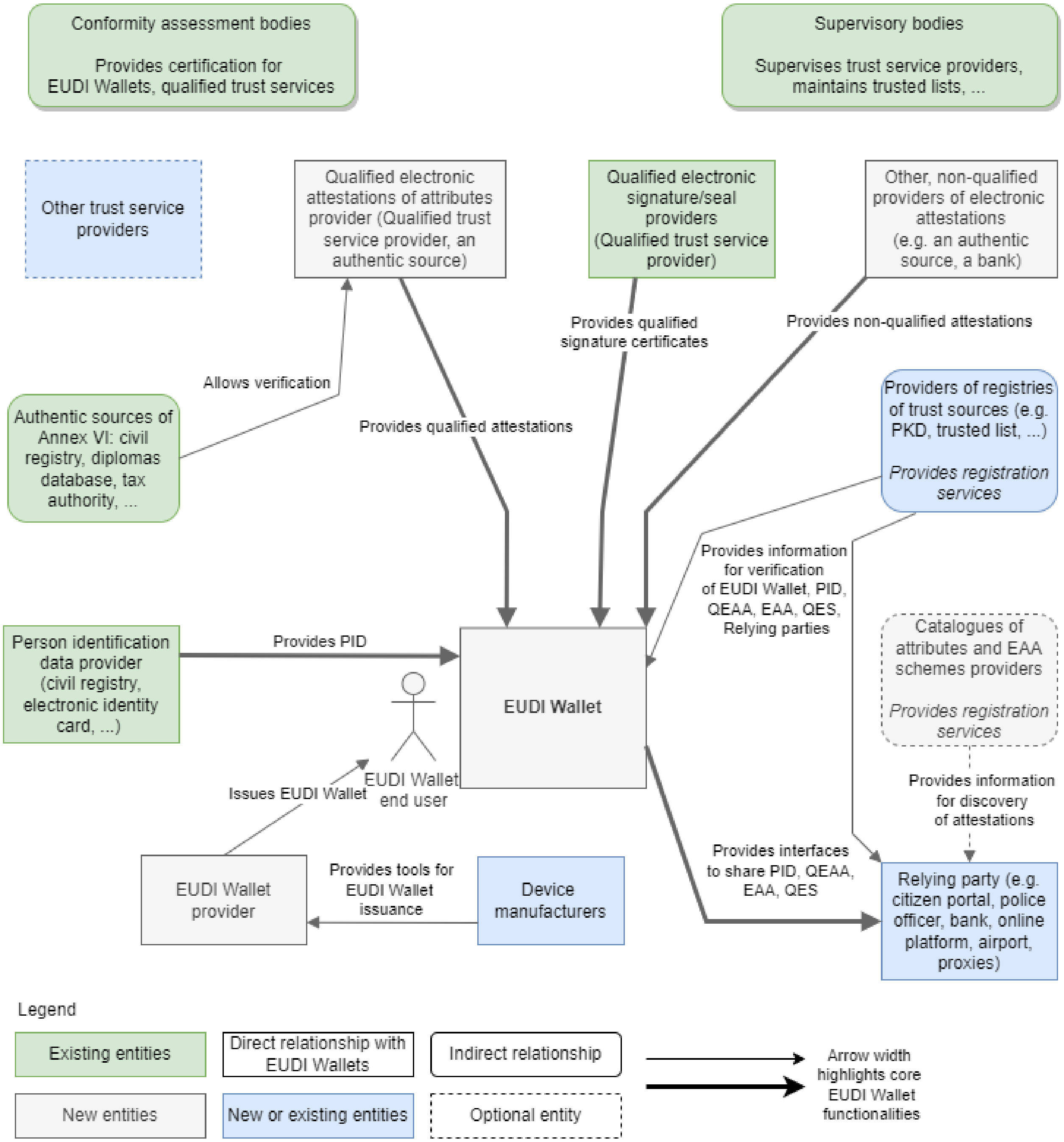
[8] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on a Retail Payments Strategy for the EU COM/2020/592 final

would be developed in close coordination with Member States' advisory groups on retail payments and the finance industry.

This work may in future be extended to additional use cases.

3 ROLES IN THE ECOSYSTEM

This chapter sets out a possible architecture of the future EUDI Wallet ecosystem. It provides a basis for discussion to be updated and completed in the course of the toolbox process. The draft architecture sets out the different roles and the relevant process flows. The potential roles of the EUDI Wallet ecosystem are described in Figure 1.



Conformity assessment bodies
Provides certification for EUDI Wallets, qualified trust services
Supervisory bodies
Supervises trust service providers, maintains trusted lists, ...
Other trust service providers
Qualified electronic attestations of attributes provider (Qualified trust service provider, an authentic source)
Qualified electronic signature/seal providers (Qualified trust service provider)
Other, non-qualified providers of electronic attestations (e.g. an authentic source, a bank)
Provides qualified signature certificates
Provides non-qualified attestations
Allows verification
Provides qualified attestations
Authentic sources of Annex VI: civil registry, diplomas database, tax authority, ...
Providers of registries of trust sources (e.g. PKD, trusted list, ...)
Provides registration services
Provides information for verification of EUDI Wallet, PID, QEAA, EAA, QES, Relying parties
Catalogues of attributes and EAA schemes providers
Provides registration services
Person identification data provider (civil registry, electronic identity card, ...)
Provides PID
EUDI Wallet
EUDI Wallet end user
Issues EUDI Wallet
Provides information for discovery of attestations
Provides interfaces to share PID, QEAA, EAA, QES
EUDI Wallet provider
Provides tools for EUDI Wallet issuance
Device manufacturers
Relying party (e.g. citizen portal, police officer, bank, online platform, airport, proxies)
Legend
Existing entities
Direct relationship with EUDI Wallets
Indirect relationship
New entities
New or existing entities
Optional entity
Arrow width highlights core EUDI Wallet functionalities

Figure 1 Overview of the EUDI Wallet roles

1 End Users of EUDI Wallets
2 EUDI Wallet Issuers
3 Person Identification Data Providers
4 Providers of registries of trusted sources
5 Qualified electronic attestation of attributes (QEAA) providers
6 Non-qualified electronic attestation of attributes (EAA) providers
7 Qualified and non-qualified certificate for electronic signature/seal providers
8 Providers of other trust services
9 Authentic sources
10 Relying parties
11 Conformity assessment bodies (CAB)
12 Supervisory bodies
13 Device manufacturers and related subsystems providers
14 Catalogue of attributes and schemes for the attestations of attribute providers

In the following, each role is described in more detail on the basis of the current state of play of discussions in the eIDAS expert group.

Please note that the interface to a QES provider may cover both a local or remote signing process.

This description will be updated and complemented in the course of the work on the toolbox.

3.1 End Users of EUDI Wallets

End users of EUDI Wallets are defined as natural or legal persons using the EUDI Wallet to receive, store and share attestations (PID, QEAA or EAA) and particular attributes about the user, including to prove their identity. The EUDI Wallet would enable end-users to create qualified electronic signatures and seals (QES).

Who can be a user of a EUDI Wallet depends on national law. The use of a EUDI Wallet by citizens would not be mandatory under the legislative proposal. However, Member States would be obliged to offer the EUDI Wallet to their citizens.

3.2 EUDI Wallet Issuers

EUDI Wallet Issuers are Member States or organisations either mandated or recognized by Member States making the EUDI Wallet available for end users. The terms and conditions of the mandate or recognition would be for each Member State to determine.

The EUDI Wallet can be seen as a combination of several products and trust services foreseen in the legal proposal, which as a whole give the user sole control over the use of their person identification data (PID) and qualified or non-qualified electronic attestations of attributes (EAA or QEAA), and any other personal data within their EUDI Wallet. From a technical viewpoint, this may also imply the user's sole control over sensitive cryptographic material (e.g. private keys) related to the use of these data in some scenarios, including electronic identification, signature / seal.

EUDI Wallet Issuers would be responsible for ensuring compliance with the requirements for EUDI Wallets, in particular the relevant definitions, functional and non-functional as well as security requirements.

3.3 Providers of Person Identification Data (PID)

PID providers would verify the identity of the EUDI Wallet user, maintain an interface to provide PID securely to the EUDI Wallet (in a harmonized common format) and make available information[9] for relying parties to verify the validity of the PID, without having an ability to receive any information about the use of the PID. The terms and condition of these services would be for each Member State to determine.

PID providers may e.g. be the same organisations that today issue official identity documents, electronic identity means, EUDI Wallet issuers etc. EUDI Wallet issuers may or may not be the same organisations as PID providers.

3.4 Providers of Registries of Trusted Sources

The specific status of a role in EUDI Wallet ecosystem **may** need to be verified in a trustworthy manner. Such roles **may** be:

- EUDI Wallet issuers
- Person Identification Data Providers
- Qualified electronic attestation of attributes (QEAA) providers
- Qualified certificate for electronic signature/seal providers
- Relying parties
- Non-qualified electronic attestation of attributes (EAA) providers
- Non-qualified certificate for electronic signature/seal providers
- Providers of other trust services
- Catalogue of attributes and schemes for the attestations of attribute providers

Other roles may be necessary and thus need to be defined and explicitly mentioned depending on the specific role and their criticality for example the different roles and actors involved with remote signing processes.

Trusted registries[10] would need to provide a registration service for the relevant entities, maintain a relevant registry and enable third party access to the registry information. The terms and conditions of entities to become registered would be for each registrar to determine unless specified in e.g. sectoral rules.

[9] Without prejudice to the actual mechanism how the information is provided, including whether directly or indirectly

[10] Further precisions to the specifics of trusted registries will be brought later on.

For example, the qualified status of QTSPs and the qualified trust service they provide (including the provision of QEAA) are recorded in trusted lists by Member States. Information about other roles may be provided in other forms of trusted registries.

3.5 Qualified Electronic Attestation of Attributes Providers

Qualified EAA would be provided by QTSPs. The trust framework for QTSPs would apply also to QEAA. QEAA providers would maintain an interface for requesting and providing QEAA, including a mutual authentication interface with EUDI Wallets and potentially an interface towards authentic sources to verify attributes. QEAA providers would be required to provide information or the location of the services that can be used to enquire about the validity status of the QEAA, without having an ability to receive any information about the use of the attestations. The terms and conditions of these services would be for each QTSP to determine, beyond what is specified in the eIDAS Regulation.

3.6 Non-Qualified Electronic Attestation of Attributes Providers

Non-qualified EAA can be provided by any trust service providers. While they would be supervised under eIDAS, it can be assumed that other legal or contractual frameworks than eIDAS would mostly govern the rules for provision, use and recognition of EAA. Such other frameworks may cover policy areas such as driving licences, educational credentials, digital payments, although they may also rely on qualified Electronic Attestation of Attributes Providers. For EAA to be used, TSPs would need to offer users a way to request and obtain EAA, meaning they would need to be technically compliant with EUDI Wallet interface specifications. Depending on the domain rules, EAA providers may provide validity information about EAA, without having an ability to receive any information about the use of the EAA. The terms and conditions of issuing EAA-s and related services would be subject to sectoral rules.

3.7 Qualified and Non-Qualified Certificates for Electronic Signature/Seal Providers

Article 6a(3) of COM(2021)281 final requires the EUDI Wallet to enable the user to sign by means of qualified electronic signature or seal. This goal can be reached by several ways:

- The EUDI Wallet includes a qualified signature/seal creation device (QSCD), or
- It is a secure authentication tool as a part of a local or remote QSCD managed by a QTSP.

The EUDI Wallet may also enable the user to sign by means of non-qualified signatures or seals.

3.8 Providers of other Trust Services

Providers of other qualified or non-qualified trust services such as timestamps may be interacting with EUDI Wallet. The specifics of this role or roles in the EUDI Wallet ecosystem are subject to further discussion.

3.9 Authentic Sources

Authentic sources would be the public or private repositories or systems recognised or required by law to be recognised by relying parties to contain attributes about a natural or legal person. The authentic sources in scope of Annex VI of the legislative proposal are sources for attributes on: address, age, gender, civil status, family composition, nationality, education and training qualifications titles and licenses, professional qualifications titles and licenses, public permits and licenses, financial and company data. Authentic sources in scope of Annex VI would be required to provide interfaces to QEAA providers to verify the authenticity of the above attributes, either directly or via designated intermediaries recognised at national level. For this purpose, authentic sources may need to maintain an interface to collect user authorisation for QEAA providers' access to the person's data. Synergies with the Once Only Technical System of the Single Digital Gateway Regulation will be considered as a means to achieve this. The terms and conditions for the provisioning of these services would be for Member States to determine.

3.10 Relying Parties

Relying Parties are natural or legal persons that rely upon an electronic identification or a trust service. In the context of EUDI Wallets, they would request the necessary attributes contained within the PID dataset, QEAA and EAA from EUDI Wallet users in order to rely on the EUDI Wallet, subject to the acceptance by the holder of the Wallet and within the limits of applicable legislation and rules. The reason for reliance on the EUDI wallet may be a legal requirement, a contractual agreement or their own decision. To rely on the EUDI Wallet, relying parties would need to inform the Member State where they are established and their intention for doing so. Relying parties would need to maintain an interface with the EUDI Wallet to request attestations with mutual authentication. Relying parties are responsible for carrying out the procedure for authenticating the attestations they receive from the EUDI Wallet.

Relying parties may interact with EUDI Wallets via proxies or gateways like for example national authentication gateways or private sector authentication service providers.

3.11 Conformity Assessment Bodies (CAB)

The EUDI Wallets would have to be certified by accredited public or private bodies designated by Member States[11]. QTSPs need to be audited regularly by Conformity Assessment Bodies (CABs). CABs would be accredited by Member States as responsible for carrying out assessments on which Member States will have to rely before issuing a EUDI Wallet or providing the qualified status to a Trust Service Provider. The standards and schemes used by CABs to fulfil their tasks would be specified further in the Toolbox process.

3.12 Supervisory Bodies

The supervisory bodies shall be notified to the Commission by the Member States, which supervise QTSPs and take action if necessary in relation to non-qualified trust service providers. Supervisory bodies, depending on the approach, may need to allocate additional resources for fulfilling their responsibilities and design relevant processes such as reporting or carry out risk assessments.

3.13 Device Manufacturers and Related Entities

EUDI Wallets will have a number of interfaces with the devices they are based on, which may be for the following purposes:

- Local storage
- Online Internet access
- Sensors such as smartphone camera, IR sensors, microphones, etc.

[11] Article 6c (3)

- Offline communication channels such as Bluetooth Low Energy (BLE), WIFI Aware, Near Field Communication (NFC)
- Emitters such as screens, flashlights, speakers etc.

For secure cryptographic material storage, specific devices or services may be interfaced with. Other related entities may be service providers such as cloud service providers, app store providers etc.

The legal proposal sets constraints (e.g. compliance with level of assurance high) for which kinds of devices and services may be used for the purpose of issuing the EUDI Wallet. Likewise, the availability as well as terms and conditions of device interface providers and related service providers will set further constraints for EUDI Wallet issuers.

3.14 Catalogue of Attributes and Schemes for the Attestations of Attributes Providers

Providers of QEAA and EAA may publish relevant information about the attestations they provide in a catalogue or catalogues. It would potentially enable other entities such as relying parties to discover the attributes and schemes that are provided, and how to validate/verify them and also to differentiate between types of qualified electronic attestations of attributes. The Commission is required to set out the minimum technical specifications, standards and procedures for this purpose.

4 FUNCTIONAL REQUIREMENTS

This chapter provides an overview of the functional requirements of the EUDI Wallet. Based on the legislative proposal, EUDI Wallets shall provide the following functionalities, which are further explained in the respective sub-chapters:

1. Perform electronic identification, store and manage qualified electronic attestation of attributes (QEAA) and electronic attestation of attributes (EAA) **locally or remote;**
2. Request and obtain from attestations from providers, qualified electronic attestation of attributes (QEAA) and electronic attestation of attributes (EAA);
3. Provide or access cryptographic functions;
4. Mutual authentication between the EUDI Wallet and external entities;
5. Selecting, combining and sharing with relying parties PID, QEAA and EAA;
6. User interface supporting user awareness and explicit authorization mechanism;
7. Signing data by means of qualified electronic signature/seal (QES);
8. Provisioning of interfaces to external parties.

Figure 2 provides an overview of the EUDI Wallet functionalities as building blocks. The building blocks are divided into five categories: user interface (in blue), data storage (in yellow), complex functions/ cryptographic protocols (in purple), sensitive cryptographic material (in red) and eID means module (green outline). Some functionalities may be provided by the EUDI Wallet itself or by a EUDI Wallet subsystem or by an external entity via an interface.

Please note that the QES interface may cover both a local or remote signing process.

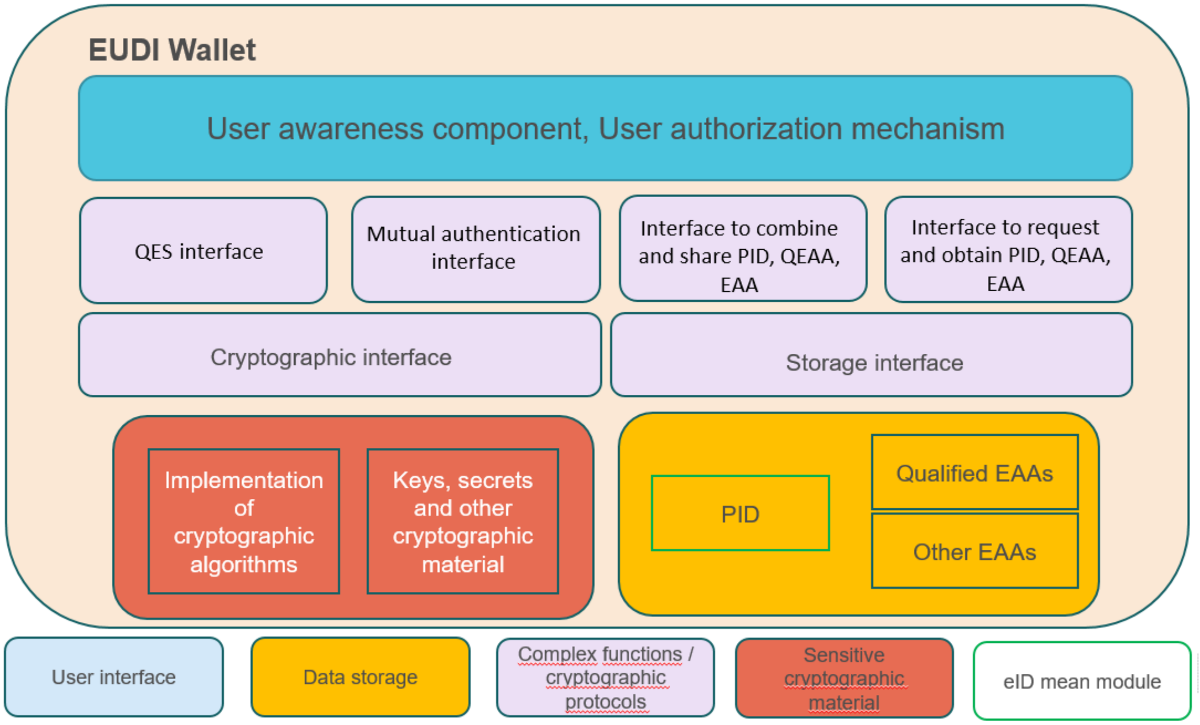

EUDI Wallet
User awareness component, User authorization mechanism
QES interface
Mutual authentication interface
Interface to combine and share PID, QEAA, EAA
Interface to request and obtain PID, QEAA, EAA
Cryptographic interface
Storage interface
Implementation of cryptographic algorithms
Keys, secrets and other cryptographic material
PID
Qualified EAAs
Other EAAs
User interface
Data storage
Complex functions / cryptographic protocols
Sensitive cryptographic material
eID mean module

Figure 2 Functionalities of the EUDI Wallet

This chapter differentiates between compulsory functions and interfaces ("**shall**") following the legal proposal and additional optional functions and interfaces that may be useful or desirable (**"may"**). This differentiation is subject to update and completion in the course of the work of the expert group on the toolbox.

4.1 Store Person Identification Data, Qualified Electronic Attestation of Attributes and Electronic Attestation of Attributes

The storage interface for the EUDI Wallet aims at delivering a storage capability for the received person identification data, QEAA and EAA in order for the user to be able on request to share them with relying parties, without requiring requests for the (Q)EAA or PID every time the information is needed. This reduces the ability of the electronic attestation provider to track the use of the provided electronic attestation on the user's side.

As stated by the legislative proposal, the EUDI Wallet storage can be local (located on a device the user holds) or remote (in a cloud-based infrastructure)[12]. The EUDI Wallet **shall** have either only a local storage, or a hybrid storage with at least pointers to a remote storage which are stored locally. Depending on the

[12] In the remote storage scenario, the offline sharing of the PID and (Q)EAA will present additional challenges requiring some minimum on device storage.

technical implementation choices, it **may** be needed to copy, synchronize and/or move data between different storage components, local or remote.

4.2 Request and obtain Person Identification Data, Qualified Electronic Attestation of Attributes and Electronic Attestation of Attributes

The EUDI Wallet **shall:**

- integrate a functionality to request and obtain PID of the user during on-boarding, for example, through an interface with electronic identifications means of assurance level high[13];
- enable the user to request and obtain qualified and non-qualified EAA, through an interface with (qualified and non-qualified) providers of EAA;
- enable the user to delete e.g. (Q)EAA, PID, cryptographic material, etc. from the Wallet.

The EUDI Wallet **may**:

- for use during the electronic identification/authentication process, rely on an interface with authoritative sources[14], for example official identity documents (e.g. through an access to the NFC interface of mobile phones in order to read identity documents with an NFC chip) or civil registries.

4.3 Cryptographic functions

Secure access to locally or externally stored cryptographic functions will be necessary to implement most of the functionalities of the EUDI Wallet (e.g. QES, authentication, selective disclosure). In case of externally stored cryptographic functions, the wallet shall provide a minimum set of local cryptographic functions that enables secure access to them. Overall cryptographic methods and functions **shall** fulfil existing and upcoming requirements originating in standards, implementing acts and certifications based on these.

These functions **shall** be used to manage:

- electronic identification of the user to relying parties;
- authentication of (Q)EAA and PID when those are linked to the EUDI Wallet;
- authentication of the EUDI Wallet itself towards third parties;
- the activation mean for the remote QSCD, if the EUDI Wallet relies on a remote QSCD for its QES functionality;
- the qualified certificates and its cryptographic keys, if the EUDI Wallet relies on a local QSCD for its QES functionality;

[13] As defined in Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) 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.

[14] Ibid, the list described is not exhaustive.

- the access mean to the EUDI Wallet remote storage if the EUDI Wallet relies on remote storage;
- as appropriate, secure storage of sensitive personal data on the device.

These functions **may** be used to manage:

- pseudonymous authentication of the user to relying parties.

4.3.1 Cryptographic material management

Cryptographic material management of the EUDI Wallet provides the capability to generate, store, use, modify and delete cryptographic material. Depending on the sensitivity of the cryptographic material, the cryptographic management interface **may** leverage on software and/or hardware solutions to provide the functionality.

Supported algorithms **shall** be sufficiently strong in terms of cryptography to ensure confidentiality, integrity and authenticity. Such a determination may be concluded by their inclusion in e.g. the SOG-IS Catalogue.

4.3.2 Trusted environments

Certain computations require an additional level of trust, which may not be provided by standard software execution environments. In those cases, the EUDI Wallet **may** rely on a Trusted Execution Environment (TEE) and Secure Elements (SE) locally or a remote equivalent or similar technology depending on the device to execute those computations.

Identifying means to enforce a common standard to access a TEE or SE in the EUDI Wallet will be defined as it will provide higher level of trust to the whole implementation.

4.4 MUTUAL AUTHENTICATION

To ensure informed actions from the user and adequate security levels, the EUDI Wallet **shall** implement mutual authentication capabilities[15]. The mutual identification and authentication capability **shall** cover both the EUDI Wallet end and the third party end as, depending on the use case, the EUDI Wallet **may** identify and authenticate itself or the user, however it shall be able to identify and authenticate the third party it is interacting with. Additionally, this mutual identification and authentication **shall** be possible both online (over the Internet) and offline.

To ensure that the EUDI Wallet can be used in a seamless way by TSPs and relying parties alike, a common authentication protocol **shall** be specified, ensuring interoperability at least at EU level and considering relevant European or international standards.

[15] Mutual authentication between wallets and relying parties should not be understood as mandatory for every transaction.

4.4.1 Identifying and authenticating the EUDI Wallet

The EUDI Wallet itself **shall** be able to prove to the relying party the origin and integrity of the individual EUDI Wallet being used and thereby contributing to an increase in trust and security of the ecosystem. This **shall** prove that a valid certification has been performed and the solution was installed on a suitable device with adequate security. Revocation checks still have to be done in addition.

4.4.2 Identifying and authenticating the third party

For security and transparency reasons, the EUDI Wallet **shall** have the capability to identify and authenticate third parties it interacts with, in particular:

- qualified and non-qualified trust service providers (TSPs);
- relying parties including brokers and gateways;
- the EUDI Wallet issuer.

The EUDI Wallet **may** support several protocols from several recognized authentication standards. Governance rules and processes to add and remove protocols from the list of supported standards would be defined.

4.5 Selection, Combination and sharing of Person Identification Data, Qualified Electronic Attestation of Attributes and Electronic Attestation of Attributes

The legislative proposal states that the EUDI Wallet is an electronic identification means. Therefore, the EUDI Wallet **shall** be able to perform user identification and authentication with a specific set of PID thus performing identification with legal weight when required.

The Wallet **shall** leverage on a common protocol for identification and attribute sharing including verification of the integrity and authenticity of the information, irrespective of the set of attributes shared, in order to reduce the technical complexity of the solution and facilitate its deployment. This functionality will rely on QEAA and EAA, the data structures of those attestations and their sharing protocol reused for PID.

The functionality may take the existing eIDAS infrastructure and functions into consideration to support a seamless operation of EUDI and existing eID means.

The EUDI Wallet **shall** make it impossible to collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it.

The EUDI Wallet **shall** enforce privacy by design and selective disclosure of attributes.

Selective disclosure and combination of attestations can be handled in two different ways:

- the EUDI Wallet may hold a very broad collection of attributes as PID, QEAA and EAA, and each time a specific attribute or the derivation of a specific attribute is required, a new PID or (Q)EAA has to be requested from providers.
- The EUDI Wallet may have the intrinsic capability, based on the obtained PID and (Q)EAA, to selectively disclose, derivate a specific attribute and aggregate several single attributes, without the need for new PID, (Q)EAA or interactions with the PID and (Q)EAA providers. For instance, specific fit for purpose signature schemes in PID and (Q)EAA could enable such capabilities.

Attestation-sharing can be broken down to two types: offline and online sharing.

4.5.1 Offline sharing

The offline sharing scenario corresponds to a use case where the user share a PID, QEAA or EAA or a combination of these to a third party, which is in immediate proximity. If the electronic attestation is not linked to the EUDI Wallet, additional data out of the EUDI Wallet's scope, may be requested by the third party.

For instance:

- to ensure proper validation of an EU Health Certificate[16], the third party would require an ID document with biometric information such as a photograph as proof that the holder of the EU Health Certificate is the legitimate owner of the certificate;
- a proof of age could provide the age and photograph of a user, both authenticated by a trusted authority. In that case, the verifier can physically verify that the photograph matches the user, without any link between the proof of age and the EUDI Wallet, which, in this scenario, would only provide storage and sharing capabilities.

If the PID, QEAA or EAA data is linked to the EUDI Wallet, the holder of the EUDI Wallet will be able to prove that this data is subject of the attested attributes[17]. This avoids the need for the user to provide additional identification information to the relying party.

4.5.2 Online sharing

Online sharing **shall** require the user to prove ownership of the used (Q)EAA or PID by proving access and control over cryptographic material linked to the (Q)EAA or PID, if it is required for the usage scenario.

[16] Additional identification of persons showing certificates is specifically relevant for certificates that contain health-related information that is meant to be used outside the health sector.

[17] It will need to be discussed whether this link requires directly or indirectly an inclusion of cryptographic material that the holder of the EUDI Wallet can prove control over.

The authentication protocol **shall** be as common as possible in order to reduce the overall complexity of the solution and ease the adoption of the EUDI Wallet. This protocol would be such that it can meet the relevant requirements of level of assurance high[18] and may include a consideration of existing authentication infrastructures where relevant. Aiming for a common authentication protocol[19] between the EUDI Wallet and third parties does not preclude the existence of different underlying solutions to provide, verify and revoke (Q)EAA and PID.

4.6 User interface for user awareness and authorization mechanism

The user interface of the EUDI Wallet covers two main functionalities, user information and user authorisation. Both are needed in the context of identification, authentication, signing and attestation sharing.

4.6.1 User awareness component

The EUDI Wallet **shall**:

- display clear and unambiguous information to the user to enable properly informed decisions. The user shall in particular be clearly informed of:
    - The identity of the different parties the user will be interacting with[20]
    - The reason to share an electronic attestation of attribute including who is asking, which attributes are requested and for which purpose as defined by the relying party;
    - be clearly informed of the type of operation being executed.
    - her/his rights for data protection under the GDPR.
- allow the user to identify the attributes that are required as mandatory by the relying party and, if applicable, the attributes that are considered optional by the relying party;
- display an “EU Digital Identity Wallet trust mark” for the user;
- For QES display
    - who is asking,
    - to sign which document,
    - under which electronic signature policy etc.;
- display the events regarding the use of their EUDI Wallet (for instance via notification or display of the history of the EUDI Wallet events).

[18] as per CIR 2015/1502

[19] This common protocol shall aim at standardizing the data structures, the sequences of messages between parties and the underlying cryptographic mechanisms

[20] Qualified trust service providers, relying parties, Wallet issuers, trusted registries, other EUDI Wallets etc.

In addition, the EUDI Wallet **may**:

- integrate a "constraint" code[21];
- validate qualified EAA and non-qualified EEA;
- grant the user an unambiguous way of distinguishing between qualified and non-qualified EAA as well as their validity status *(e.g. through the use of a visual indicator similar to the European trusted mark when displaying qualified EAA.);*
- restrict sharing certain sets of attributes with certain parties, or warn the user that the relying party may not be authorized to use/ask for these attributes[22].

4.6.2 User authorization mechanism

In order to protect the user's privacy and ensure full control of the user over their EUDI Wallet (including personal data and attributes), the EUDI Wallet **shall**:

- rely on a harmonized authorization mechanism ensuring security and privacy by design;
- get and store the user authorizations to perform actions for which they are prompted. This entails a specific action from the user, including an active operation proving that the legitimate user is indeed expressing consent[23].
- ensure that user authorization regarding the creation of QES shall be handled as part of the qualified signature/seal creation device (QSCD) on which the EUDI Wallet is relying[24].

Additionally, the EUDI Wallet **shall** require the user to use two-factor authentication in a combination of at least two authentication factors for certain use cases, satisfying the requirements for LOA high:

- a proof of knowledge;
- a proof of possession;
- a proof of inherence.

4.7 SIGN BY MEANS OF QUALIFIED ELECTRONIC SIGNATURE OR SEAL

When using the EUDI Wallet, it **shall** be possible to sign by means of a signature and a seal. An EUDI Wallet user **shall** be able to create qualified and non-qualified electronic signatures and seals either through:

[21] A "constraint" code is an alternative code to be entered when the user is acting under constraint, that would look like the real code has been entered, but that would trigger an alert or would block the transaction being performed.

[22] These "sharing policies" may be defined at different levels.

23 User authorisation may mean having full control (1) over the disclosed PID, QEAA or EAA, through the ability to select, combine, share or refuse sharing requested attributes to an identified third party, online or offline; (2) over the QES process, through the ability to access the document as well as the electronic signature policy and implications prior to perform the electronic signature.

[24] When the harmonized consent mechanism provided by the EUDI Wallet is be used, for convenience, to create QES, it may be certified as part of the QSCD.

- The Wallet being a QSCD;
- The use of a local QSCD as a core functionality;
- Through an interface with a qualified service for the management of remote QSCD. In this case the EUDI Wallet shall enable the user to activate its signature and seal private key.

4.8 Interfaces with external entities

In addition to the functionalities listed above, the EUDI Wallet will need to include certain interfaces with external entities to which specific requirements, specifications and standards will need to apply. They are presented in Figure 3 below.

Represented in green, the interfaces of the EUDI Wallet will need to be defined in dedicated technical specifications. These interfaces will impact the EUDI Wallet components' design and need to be specified at early stage of the design of the EUDI Wallet prototype.

Please note that the QES interface may cover both a local or remote signing process.

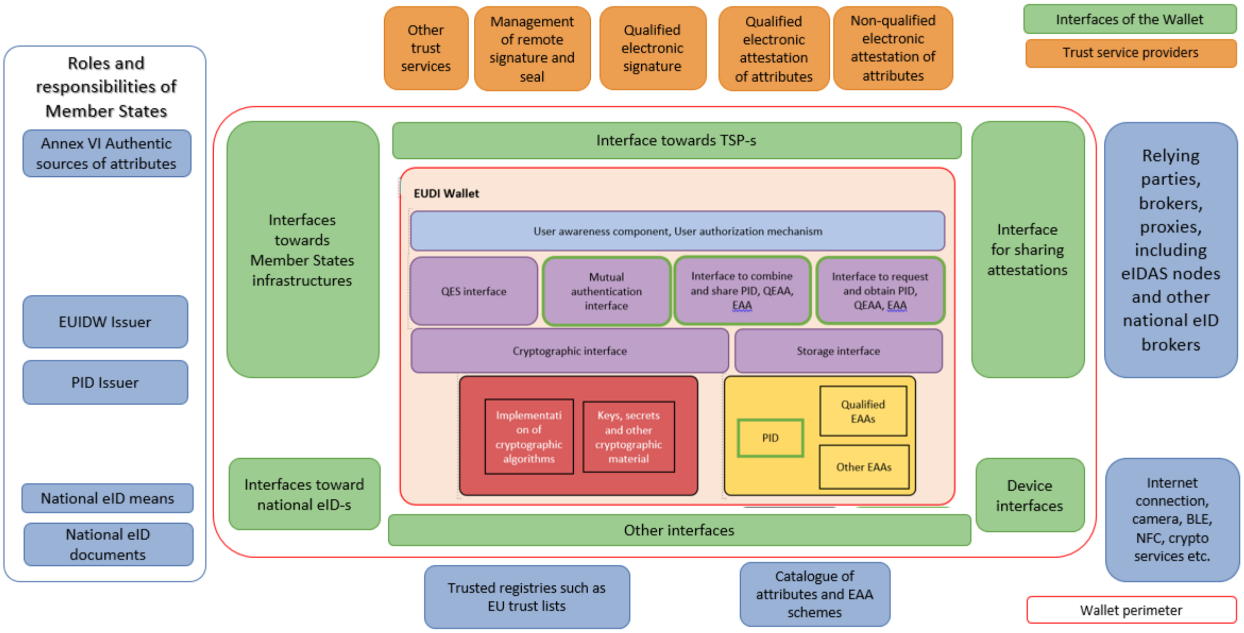

Other trust services
Management of remote signature and seal
Qualified electronic signature
Qualified electronic attestation of attributes
Non-qualified electronic attestation of attributes
Interfaces of the Wallet
Trust service providers
Roles and responsibilities of Member States
Annex VI Authentic sources of attributes
EUIDW Issuer
PID Issuer
National eID means
National eID documents
Interfaces towards Member States infrastructures
Interfaces toward national eID-s
Interface towards TSP-s
EUDI Wallet
User awareness component, User authorization mechanism
QES interface
Mutual authentication interface
Interface to combine and share PID, QEAA, EAA
Interface to request and obtain PID, QEAA, EAA
Cryptographic interface
Storage interface
Implementation of cryptographic algorithms
Keys, secrets and other cryptographic material
PID
Qualified EAAs
Other EAAs
Other interfaces
Interface for sharing attestations
Device interfaces
Relying parties, brokers, proxies, including eIDAS nodes and other national eID brokers
Internet connection, camera, BLE, NFC, crypto services etc.
Trusted registries such as EU trust lists
Catalogue of attributes and EAA schemes
Wallet perimeter

Figure 3 Interfaces of the EUDI Wallet

4.8.1 Interface towards Member States' infrastructures

The existing infrastructures involved in the processes described above includes:

- authentic sources of attributes under the responsibility of the Member States in accordance with the eIDAS Regulation;
- issuance infrastructure of the EUDI Wallet;
- identity proofing infrastructure associated with the EUDI Wallet issuance;

- relying parties, brokers, proxies including eIDAS nodes and other national eID brokers and gateways;
- notified electronic identity means.

Several processes and entities are under the responsibility of the Member States and as such interfaces between the EUDI Wallet and the Member States corresponding infrastructures **shall** be established to handle in particular:

- performing high level of assurance identity proofing during the onboarding process;
- issuing the EUDI Wallet with the user's PID during the on boarding process;
- provisioning PID relying on authentic sources of attributes;
- more generally providing an interface / proxy between existing electronic identity infrastructures and the EUDI Wallet to authenticate its user.

4.8.2 Interface towards Member States identity cards

Following Regulation 2019/1157[25], Member States ID cards contain attested PID in digital format, accessible through a contactless interface. The EUDI Wallet **may** leverage on this data in its workflows for instance in order to:

- Retrieve electronically attested PID;
- Help with the identity proofing process;
- Strengthen identification or authentication claims.

National infrastructures **may** be needed in addition to the contactless interface to the identity card chip, for instance to provide PID on the basis of the PID contained in the ID cards.

Passports and national identity documents which contain electronic components **may** also be considered for interfaces.

4.8.3 Interface towards relying parties, brokers or proxies[26]

Some relying parties **may** be considered as brokers that act as proxies between the EUDI Wallet, (Q)EAA or PID sharing protocol and other identification and authentication protocols. When one relying party acts

[25] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (OJ L 188, 12.7.2019, p. 67).

[26] **'proxy/broker/gateway'**: is used to denote an intermediary role between a EUDI Wallet and a service provider in a digital infrastructure. Service providers may introduce a proxy/broker/gateway which implements the EUDI Wallet interface for the service provider and therefore acts as relying party for the EUDI Wallet.

as a proxy for another relying party, the reliability of the authentication mechanism **shall** not be affected. The present document does not distinguish between relying parties which are directly accessible and brokers. Both are considered relying parties to which the same technical requirements apply.

The (Q)EAA sharing protocol **may** be unified with the identification and authentication protocol of the electronic identity means of the EUDI Wallet for simplicity, ease of adoption, security and maintainability reasons.

4.8.4 Trusted registries interfaces

The EUDI Wallet interacts with a complex ecosystem in which sources of trust are crucial. Trusted registries **shall** provide the EUDI Wallet and its user with adequate information and trust regarding[27]:

- trusted authorities such as the EU trusted lists, providers of PID, sectorial non-qualified EAA providers, trusted relying parties, the list of certified EUDI Wallet etc.;
- PID, (Q)EAA and EUDI Wallets validity status, comprised of:
  - the validity status of a particular individual EUDI Wallet,
  - the validity of an PID or (Q)EAA which the provider or the user may choose to revoke or suspend at a given time.

4.8.5 Device interfaces

The EUDI Wallet will be comprised of one or several software and/or hardware components. Besides CSP (Cryptography Services Provider) components, which **may** provide cryptography services and storage capabilities (such as SE, SIM or appropriately evaluated software solutions), other hardware components on which the EUDI Wallet software runs, **may** be external to the EUDI Wallet and accessible through standardized interfaces.

A non-exhaustive list of those interfaces includes:

- Online Internet network access (via broadband cellular network, Wi-Fi or LAN connection);
- Sensors, such as smartphone cameras, IR sensors, microphones etc.;
- Offline communication channels (such as Bluetooth Low Energy, Wi-Fi Aware, NFC etc.);
  Emitters such as screens, flashlights, speakers etc.

[27] Empowerments for implementing acts are proposed in COM(2021)281 final, Art 6b(4), 6c(6), 6d(3).

5 NON-FUNCTIONAL REQUIREMENTS OF THE EUDI WALLET

This chapter outlines the principal constraints within which the EUDI Wallet functionalities shall be able to operate. It identifies compulsory non-functional requirements ("**shall**") following the legal proposal. This description may be updated and amended and optional functions that may be useful or desirable (**"may"**) may be identified in the course of the work of the expert group on the toolbox.

The EUDI Wallet **shall** meet the requirements set out in Article 8 of the eIDAS Regulation with regards to assurance level high, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication, as defined in CIR 2015/1502.[28]

As provided by the legislative proposal, EUDI Wallets **shall** be interoperable across the European Union and have externally oriented interfaces specified by common, technical standards. Certain use cases **may** require further international interoperability.

The EUDI Wallet **shall** ensure full control of the user over their data held within their individual EUDI Wallet by integrating security and privacy by design. Therefore, the core functions of the EUDI Wallet such as identification, authentication, signature, seal and attributes sharing **shall** not occur without the consent[29] of the user. However, suspension and revocation may not require consent of the user who may be informed.

The EUDI wallet **shall** have an easy to use interface and user experience and **shall** address accessibility, usability and inclusion.

The EUDI Wallet **shall** enable awareness of the user, and in particular allow the user to know when and how their EUDI Wallet is being or has been used, to be informed of the nature of all the operations carried on with their EUDI Wallet, and to present these elements in form of a history. In this context, the user **shall** also be notified of breaches of control, or be reasonably able to detect breaches of control. The implementation of this capability will require further discussion in order to preserve user privacy. It will

[28] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) 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.

[29] "Consent" of the user represents the informed willingness of the user to carry on an operation, such as performing an electronic identification, performing a qualified electronic signature, sharing attributes etc.

also be necessary to further discuss alternative approaches to content and cryptographic material recovery by the user.

The EUDI Wallet **shall** enable the user to share only the information they intend to share. The Wallet **shall** ensure an appropriate level of privacy, implementing policies about non-traceability and unlinkability of user's activities for third parties as appropriate considering:

- the applicable legal context for identity providers and attestation providers;
- the need to retain evidence for dispute resolution purpose;
- the right for the user to be informed of the use of their EUDI Wallet.

In order to bring trust to EUDI Wallet users and relying parties, conformity of the critical components of the implementations of the EUDI Wallet (including both the EUDI Wallet core functionalities and the implementation of interface protocols) **shall** be ensured by the EUDI Wallet issuer and confirmed by a recognized certification of the EUDI Wallet[30]. The security of critical components integrated within the EUDI Wallet or used by the EUDI Wallet, which protect against misuse or alteration of identification data, authentication mechanism or consent mechanism **shall** be certified in accordance with the legal proposal[31].

In addition, the mechanism for relying parties to verify whether a EUDI Wallet used is genuine and certified, **shall** not enable the relying party to distinguish between two certified EUDI Wallets, in order to preserve the privacy of the user when performing pseudonymous authentication. Trust service providers **shall** not receive any information about the use of provided attestations.

The issuer of the EUDI Wallet **shall** not collect information about the use of the EUDI Wallet, which are not necessary for the provision of the EUDI Wallet services. In addition, the Wallet issuer **shall** not combine PID and any other personal data stored or relating to the use of the EUDI Wallet with personal data from any other services offered by this issuer or from third-party services, which are not necessary for the provision of the EUDI Wallet services, unless the user has expressly requested it. Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held.

[30] Article 6c of COM(2021)281 final.

[31] Article 6c(1) provides that European Digital Identity Wallets that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and the references of which have been published in the Official Journal of the European Union shall be presumed to be compliant with the cybersecurity relevant requirements set out in Article 6a paragraphs 3, 4 and 5 in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.

6 POTENTIAL BUILDINGS BLOCKS OF THE EUDI WALLET

The implementation of the EUDI Wallet functionalities presented in Chapter 4 of this document can be provided by different technologies. These existing technologies can be segmented into building blocks in order to identify the set of components, which can compose the core of the EUDI Wallet.

The different functions of the EUDI Wallet can be implemented using existing technologies such as:

- Form factors
  - Form factor 1: Mobile application
  - Form factor 2: Web application
  - Form factor 3: Secure Application on PC
- Supporting building blocks
  - Building block 1: Backend server including evaluated HSM
  - Building block 2: Official electronic identity documents
  - Building block 3: Secure External Hardware Token
  - Building block 4: Cryptographic Service Provider
  - Building block 5: Trusted execution environment (TEE)

The form factors can in addition to the user interface provide:

- User authentication to ensure consent.
- Storage (level of security depending on building block used).
- Access to QSCD and cloud based functionalities (level of security depending on building block used).

The supporting blocks, depending on the implementation, can together with the form factor provide:

- Secure storage on the building block (with limitations);
- Strong user authentication;
- Secure and encrypted storage;
- Mutual authentication;
- Qualified electronic signatures;
- Secure access to cloud services.