European Digital Identity Wallet

Architecture and Reference Framework

v2.6.0 20251013.130423

Contents

Architecture and Reference Framework

1 Introduction

1.1 Context

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

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

The Recommendation establishes a structured framework for cooperation between Member States, the Commission, and, where relevant, private sector operators to develop the Toolbox. The European Digital Identity Cooperation Group (EDICG), formerly known as the eIDAS Expert Group, is responsible for:

- exchange best practices and cooperate with the Commission on emerging policy initiatives in the field of digital identity wallets, electronic identification means and trust services;
- advising the Commission in the preparation of draft implementing and delegated acts;
- supporting Supervisory Bodies in the implementation of the [European Digital Identity Regulation];
- organising peer reviews of electronic identification schemes;
- engaging with the Commission and other relevant stakeholders to develop a Common Union Toolbox;

The European Digital Identity Cooperation Group's page can be found at the official page.

The European Digital Identity Cooperation Group has since further developed the concepts and specifications for the European Digital Identity Framework. The current ARF version is based on the legal text adopted by the co-legislators, including the adopted Commission Implementing Regulations:

- CIR 2024/2977 regarding PID and EAA,
- CIR 2024/2979 regarding integrity and core functionalities,
- CIR 2024/2980 regarding ecosystem notifications,
- CIR 2024/2981 regarding certification of Wallet Solutions,
- CIR 2024/2982 regarding protocols and interfaces,
- CIR 2025/846 regarding cross border identity matching,
- CIR 2025/847 regarding security breaches of European Digital Identity Wallets,
- CIR 2025/848 regarding registration of Wallet Relying Parties,
- CIR 2025/849 regarding the list of certified European Digital Identity Wallets,
- CIR 2025/1566 regarding the verification the identity and attributes of a QC or QEAA holder,
- CIR 2025/1567 regarding management of remote QSCDs as qualified trust services,
- CIR 2025/1568 regarding peer reviews of eID schemes,
- CIR 2025/1569 regarding QEAAs and EAAs provided by or on behalf of a public sector body responsible for an authentic source,
- CIR 2025/1570 regarding notification of information on certified QSCDs,
- CIR 2025/1571 regarding the formats and procedures for annual reports by supervisory bodies,
- CIR 2025/1572 regarding the format and procedures for notification of intention and verification with regard to the initiation of qualified trust services,
- CIR 2025/1929 regarding the binding of date and time to data and establishing the accuracy of the time sources for the provision of qualified electronic time stamps,
- CIR 2025/1942 regarding qualified validation services for qualified electronic signatures and qualified validation services for qualified electronic seals,
- CIR 2025/1943 regarding reference standards for qualified certificates for electronic signatures and qualified certificates for electronic seals,
- CIR 2025/1944 regarding reference standards for processes for sending and receiving data in qualified electronic registered delivery services and as regards interoperability of those services,
- CIR 2025/1945 regarding the validation of qualified electronic signatures and of qualified electronic seals and the validation of advanced electronic signatures based on qualified certificates and of advanced electronic seals based on qualified certificates,
- CIR 2025/1946 regarding qualified preservation services for qualified electronic signatures and for qualified electronic seals.

1.2 Purpose of this document

The purpose of this document is to explain the architecture of the EUDI Wallet ecosystem and all of its components, as well as how these components will interact to ensure the security of the ecosystem and the privacy of its Users. Also, it serves as background information to allow a better understanding of the the high-level requirements established in Annex 2.

Additionally, this document forms a reference to create uniform conditions for the implementation of the [European Digital Identity Regulation] and to define the technical specifications, standards and procedures that the Commission will develop for the purpose of implementing this Regulation.

Finally, this document is used to develop the Wallet Solution reference implementation.

The document presents a state-of-play of ongoing work of the European Digital Identity Cooperation Group and does not imply any formal agreement regarding its content. This document will be complemented and updated over time through the process of establishing the toolbox, as described in Chapter 9.

This document holds no legal value and does not prejudge the final mandatory legal requirements for the EUDI Wallet ecosystem. Only the adopted [European Digital Identity Regulation], and the implementing and delegated acts adopted under that Regulation, are mandatory. This document serves as a foundation for regularly updating the implementing acts, ensuring alignment with technological and standards developments.

1.3 Relation to the Large-Scale Pilots (LSP)

To support the development of a reference implementation of a Wallet Solution and to pilot its usage across different priority use cases, the Commission launched a call for proposals on 22 February 2022 under the Digital Europe Programme to pilot use cases for the EUDI Wallet ecosystem at a large scale.

The objective of the Large-Scale Pilots (LSP) call is to support the piloting of the EUDI Wallet ecosystem around a range of use cases involving both public and private sector stakeholders. The LSPs will test the EUDI Wallet ecosystem in both national and cross-borders contexts and integrate with the iterative development of the reference application.

The works of the LSPs will be aligned with the ARF, which will guide pilot system design and architecture development together with the release of the reference implementation.

The LSPs are expected to provide feedback on the ARF as they develop and interact with Relying Party services, Qualified or non-qualified Electronic Attestations of Attributes (Q)EAA Providers, Person Identification Data (PID) Providers, Qualified and non-qualified Trust Service Providers and Users in meaningful interactions under the proposed use cases.

1.4 Definitions

The definitions used in this document can be found in Annex 1 of this document.

1.5 Scope

The **EUDI Wallet Architecture and Reference Framework (ARF)** defines the architectural and functional aspects of the EUDI Wallet ecosystem, describing its main components and their interactions. It provides the technical foundation for ensuring **interoperability, security, and privacy** through the high-level requirements defined in **Annex 2**.

The ARF serves as a reference for the **harmonised implementation of the [European Digital Identity Regulation]**, guiding the development of **implementing acts, technical specifications, standards, and operational *procedures**.

This document applies exclusively to **EUDI Wallet ecosystems compliant with the [European Digital Identity Regulation]**, ensuring consistency in architecture and implementation. At the same time, it is designed to support the development of the Wallet Solution reference implementation while remaining adaptable to future technological and regulatory developments.

1.6 Change Log

In this version of the ARF:

- The Discussion Paper for Topic O was integrated into Section 5.5, and into Topic 25 and Topic 26 in Annex 2.
- The Discussion Paper for Topic Z was integrated into Sections 6.6.2.3.3 and 6.6.3.8, among others. Moreover, multiple requirements in Annex 2 where changed or slightly adapted to account for the fact that device binding is now recommended, not mandatory.

- Several issues raised via Confluence and GitHub have been resolved.

Apart from these changes, a limited number of editorial mistakes were corrected.

1.7 Additional topics

In this version of the **Architecture and Reference Framework (ARF)**, several areas still require further exploration and refinement. These topics will be addressed through discussions with Member States, the European Digital Identity Cooperation Group, civil society, industry representatives, and professionals, ensuring broad and comprehensive feedback from all relevant stakeholders.

The outcomes of these discussions will be incorporated into future versions of the ARF. The document will continue to evolve iteratively, improving its content and addressing new topics as they emerge. The process for providing feedback and details on how updates are managed is described in Chapter 9.

The current areas identified for further discussion include:

- Design of secure cryptographic interfaces between the Wallet Instance and the WSCA
- Design of user interfaces for Wallet Instances

- Authentication mechanisms for users to access their devices

- Implementation of certificate transparency

- Definition of support and maintenance responsibilities of Wallet Providers

A detailed list of these topics, along with progress updates, is available on GitHub.

1.8 Drafting Process and Discussion Papers

The development of the **Architecture and Reference Framework (ARF)** is guided by discussions with Member States and experts from the European Digital Identity Cooperation Group, as well as by feedback from industry and the wider community through GitHub.

For each discussion topic, a **Discussion Paper** is created and iteratively refined until consensus is reached. Once finalised, the paper is integrated into the next release of the ARF. An overview of all Discussion Papers and the ARF versions into which they were integrated can be found in the corresponding README file.

Once a Discussion Paper has been integrated into the ARF, it is **no longer updated**. Over time, its content may therefore become outdated, for example, when high-level requirements are modified in later ARF versions. This can happen for several reasons:

- **Editorial adjustments at integration**
  Requirements or descriptions may already be slightly modified when a Discussion Paper is integrated, to ensure consistency of language and style across the ARF. Sometimes further refinements are made in collaboration between the ARF editors and the authors of the paper.

- **Interdependence of topics**
  Discussion topics are not entirely separate. The introduction of new Discussion Papers may lead to adjustments of existing requirements or descriptions in the ARF.

- **Continuous feedback**
  The Commission receives feedback via Confluence, GitHub, and internal reviews. When accepted, these comments lead to further changes in the ARF.

Although the ARF may reference Discussion Papers as background information, **historic Discussion Papers (including their proposed high-level requirements) are not normative**. The authoritative requirements are those in the latest version of the Annex 2 of the ARF.

2 EUDI Wallet functionalities

2.1 Introduction

The EUDI Wallet ecosystem is designed as a secure, User-controlled digital environment that enables Users to use their Wallet Unit to manage and present their person identification data (PID) and attestations across both public and private services in the EU. Its functionalities are built around security, privacy, and User control, ensuring seamless interactions with Relying Parties and other entities, while adhering to data protection principles.

This chapter outlines the core functionalities of Wallet Solutions, as defined by the [European Digital Identity Regulation], and examines how the requirements for its implementation align with real-world use cases where Users will use their Wallet Unit.

The functionalities of a Wallet Unit can be grouped into the following categories:

- **Secure identification and authentication**, ensuring that Users can present person identification data in a trusted environment.
- **Exchanging qualified and non-qualified User attributes** through secure and verifiable electronic attestations of attributes.
- **Electronic signing of documents or data**, allowing Users to create legally recognised qualified electronic signatures and seals.
- **Generate and use pseudonyms** for authentication, to enhance privacy and prevent tracking.

These functionalities are discussed in the next four sections.

2.2 Identification and authentication

Using their Wallet Units, Users are able to:

- **Identify and authenticate** to online and offline services, while using **selective disclosure** of attributes as well as **User approval**. This *ensures that only necessary and User-approved attributes are presented to* Relying Parties, which minimises exposure of personal information.
- **Securely authenticate Relying Parties or other Wallet Units**, making sure that attributes are only presented to trusted entities.
- **Onboard seamlessly with PID Providers or attestation Providers** by leveraging existing electronic identification schemes, for a smooth and secure registration process.
- **Be informed** whether a Relying Party is authorised or registered to receive the requested attributes.
- **Access a transaction log via a dashboard**, allowing Users to:
  - **Review past interactions** with Relying Parties and Wallet Units.
  - **Request data erasure** under the GDPR Article 17 to maintain privacy.
  - **Report suspicious Relying Parties** to the relevant national data protection authority.

2.3 Attribute exchange mechanism using attestations

Using their Wallet Units, Users are able to:

- **Request, store, and present** personal identification data and electronic attestations of attributes under their sole control, ensuring secure usage in both online and offline scenarios.
- **Backup a list of their attributes, attestations, and configurations**, guaranteeing compliance with data portability rights.
- **Prevent tracking by Relying Parties** when using attestations, ensuring privacy-preserving interactions.

2.4 Qualified electronic signatures

Using their Wallet Units, Users are able to:

- **Create qualified electronic signatures and seals** for legally binding digital transactions.
- **Sign documents using qualified electronic signatures**, which are provided by default and free of charge within the Wallet Unit, ensuring universal accessibility and compliance with legal standards.

These functionalities are implemented by using the authentication and signing capabilities of the Wallet Unit as a part of a local QSCD, or a remote QSCD managed by a QTSP. See Topic 16 and Topic 37.

2.5 Pseudonyms

Pseudonyms can be used to authenticate a User when it is not necessary for a Relying Party to learn the identity of the User. As specified in [CIR 2024/2979], [W3C WebAuthn] defines the technical specification for pseudonyms. Passkeys are a widely used type of credential which are created and asserted using the WebAuthn API. Section 4.7 gives more information on the architecture and message flows of Passkeys.

A User uses a pseudonym when they wish to create an account at a Relying Party without identifying themselves. The Relying Party associates the pseudonym with the account, such that it can be used for subsequent authentication in later interactions with that Relying Party.

The User may additionally present attributes from a PID or attestation to the Relying Party, either during registration of the pseudonym or at a later interaction.

See also Topic 11 and the Discussion Paper on Topic E.

2.6 The role of use cases in the development of the Architecture and Reference Framework

2.6.1 Overview

The development of the Architecture and Reference Framework (ARF) is strategically driven by real-world use cases, ensuring that the User experience, value proposition, and requirements of the EUDI Wallet ecosystem are effectively addressed. To achieve this, the European Digital Identity Cooperation Group initially created service blueprints for each use case, which detail service touch points, components, and processes.

These blueprints serve a dual purpose: they play a crucial role in service design, enhancing both User experience and operational efficiency, while also identifying areas for improvement. As a foundational element, these blueprints shape the development of common specifications, providing comprehensive yet flexible solutions that can accommodate alternative approaches and optional steps.

It is important to note that User journeys may vary based on the specific implementation approach, influencing aspects such as data retrieval and User approval processes. The Annexes contain detailed descriptions of these blueprints, ensuring transparency and adaptability.

The European Digital Identity Cooperation Group has outlined service blueprints for the following main use cases:

- Identification and authentication to access online services, see Section 2.6.2,
- Qualified Electronic Signature, see Section 2.4,
- Mobile Driving Licence, see Section 2.6.3,
- Strong User Authentication for electronic payments, see Section 2.6.4
- A natural person representing another natural person, see Section 2.6.5.
- Additional use cases that will be introduced in the future, see Section 2.6.6.

These blueprints, along with all relevant information on use cases implementation, will be compiled in a standardised format within a dedicated document titled the “Use Cases Manual”, and distributed together with this document.

2.6.2 Identification and authentication to access online services using PID

One of the main use cases of the EUDI Wallet ecosystem is secure User identification and authentication. A User presents data from their PID, which is issued and managed at Level of Assurance (LoA) High, to various online services, both public and private. This capability is crucial, as it allows Relying Parties to confidently verify the identity of Users they interact with.

In this use case, a User utilises their Wallet Unit to present specific attributes from a PID to a Relying Party in order to access online services. Before doing so, the Wallet Unit first authenticates the User. The User is particularly mindful of the privacy and security implications of presenting data when accessing online services. Their primary objective is to securely and reliably access online services that require authentication, while maintaining full control over how their personal data is presented.

2.6.3 Mobile Driving Licence

A significant use case for the Wallet Unit involves allowing Users to request, store, and present a mobile Driving Licence (mDL) as an attestation in their Wallet Unit, allowing them mainly to prove their driving privileges. In this use case, the User employs a Wallet Unit to present an mDL to a Relying Party, for instance a police officer.

The use case description concentrates on proximity supervised and unsupervised flows, which involve scenarios where the User is physically near a Relying Party, and the mDL attribute exchange occurs using proximity technologies (e.g., NFC, Bluetooth). The two proximity flows have one significant difference: in the supervised flow, the Wallet Unit presents mDL attributes to a human Relying Party or under their supervision, whereas in the unsupervised flow, the Wallet Unit presents mDL attributes to a machine without human oversight.

In addition, like any other attestation type, an mDL can be presented online, over the internet.

For more details and high-level requirements for this use case, please see Topic 4.

2.6.4 Strong User Authentication for electronic payments

Users would like to be able to authenticate themselves and their electronic payments securely and conveniently using their Wallet Units, so that they can enjoy a seamless and protected shopping and payment experience.

A Wallet Unit facilitates complying with strong customer authentication (SCA) requirements for electronic payments, ensuring a high level of security and compliance with Article 97 of the PSD2 (and with the future PSD3/PSR).

Note: Whereas the PSD2 speaks about ‘strong *customer* authentication’, the [European Digital Identity Regulation], Article 5f(2), uses the term strong *user* authentication, and says that Relying Parties in (among others) the banking and financial sector shall accept EUDI Wallet Units to comply with legal requirements regarding strong user authentication. The ARF assumes that this means that Wallet Units must comply with the requirements for SCA in the PSD2.

Commission Delegated Regulation (EU) 2018/389 lays down the requirements for strong customer authentication (SCA), which needs to be complied with when accessing a payment account online and for initiating electronic payments, or carrying out any action through a remote channel which may imply a risk of payment fraud or other abuses. The use of a Wallet Unit for SCA will be in full compliance with those requirements. This implies that the Wallet Unit must enable the User to authenticate payment information, such as amount and payee, originating from a Relying Party, and to return the authenticated data to the Relying Party.

In general, the life cycle of a Wallet Unit in the role of an authenticator for strong User authentication comprises the following phases:

- **Registration**: The User registers the Wallet Unit as an authenticator for a service. This process includes:
  - User identification and authentication, for example by presenting a PID,
  - User consent for the registration,
  - Linking a Wallet Unit with the service and a User account in that service. This happens by issuing a dedicated SUA attestation to the Wallet Unit, containing User attributes relevant for the service. The issuance process for this SUA attestation complies with all requirements for attestation issuance in this ARF. The SUA attestation is device-bound, which means it contains a public key, and the associated private key is stored in a WSCA.
- **Strong User Authentication**: A Relying Party sends a presentation request to the Wallet Unit to request relevant attributes from the SUA attestation. This presentation request includes transactional data. In the context of electronic payments, the transactional data will include at least the payment amount and the payee. After presenting the data to the User and obtaining the User’s consent, the Wallet Unit signs the transactional data. It does so by including (a representation of) the transactional data in the signature

creation process used for device binding. Note that the syntax and semantics of the transactional data, as well as rules for how the data must be presented to the User and how the data will be prepared for inclusion in the device binding signature, will be defined in the Attestation Rulebook (or a Technical Specification) for the SUA attestation.

- **De-registration**: Unlinking the Wallet Unit from the service and/or the User's account in that service. This will involve deletion or revocation of the SUA attestation.

For more information, please refer to Sections 5.6.2 and 6.6.3.8. For high-level requirements, see Topic 20.

2.6.5 Natural person representing another natural person

The [European Digital Identity Regulation] considers the representation of one natural person by another.

One common use case is the legal representation of minors or individuals with diminished legal capacity. For example, parents or legal guardians must be empowered to make decisions and act on behalf of their children and represent them when accessing educational platforms, healthcare services, government benefits, or other services. The EUDI Wallet ecosystem must therefore accommodate such representation in a secure, verifiable manner.

Another significant use case is the management of affairs for elderly or incapacitated individuals. In these cases, individuals can be assigned as legal representatives to manage healthcare, financial, and personal matters. For instance, a caregiver or relative could hold a delegation to access health records or submit applications for social care services on behalf of the person they represent.

Power of attorney is another use case of a natural person (the agent) acting on behalf of another natural person (the principal).

For more details and high-level requirements for this use case, please see Topic 29.

2.6.6 Examples of other use cases

2.6.6.1 Health data

Easy access to health data is crucial in both national and cross-border contexts. A Wallet Unit may enable access to patient summary, ePrescriptions, etc.

2.6.6.2 Educational attestations and professional qualifications

Providing credentials for qualification recognition procedures can be costly and time-consuming for Users, Relying Parties (such as companies and employers), and Attestation Providers (such as education and training providers or academic institutions). A Wallet Unit may be a repository for educational credentials and a means for presenting them by the User to relevant Relying Parties.

2.6.6.3 Digital Travel Credential

Digital Travel Credential (DTC) Providers may issue DTCs to Wallet Units in a supported format, to enable Relying Parties to identify Users, thus facilitating a smooth travel experience and User journey. Relying Parties for a DTC may include governments, transportation providers, hospitality agents, or any other actors operating in a regulated environment which requires the use of a DTC.

2.6.6.4 Central Bank Digital Currencies

In the future, a Wallet Unit could also be used for payments with Central Bank Digital Currencies.

2.6.6.5 Social Security

Documents related to social security are important for many EU citizens to prove their rights and obligations under social security legislation in the EU. Examples include:

- **Portable Document ("PDA1")** This is a statement of applicable legislation which is useful to prove that a person pays social contributions in another EU country, for example if they are a posted worker or work in several countries at the same time.
- **Electronic Health Insurance Card ("EHIC")** This is a free card that provides every citizen with access to medically necessary government-provided healthcare during a temporary stay in one of the 27 EU countries, Iceland, Liechtenstein, Norway, and Switzerland, under the same conditions and at the same cost (free in some countries) as persons insured in that country. This includes, for example, services related to chronic or existing illnesses, as well as in connection with pregnancy and childbirth.

3. EUDI Wallet ecosystem

3.1 Introduction

This chapter describes the EUDI Wallet ecosystem as it is foreseen in the [European Digital Identity Regulation]. The different roles in the EUDI Wallet ecosystem are described in Figure 1 and detailed in the following sections.

Note that a single entity may combine multiple of the primary roles depicted in the figure, as long as that entity complies with all requirements, both legal and technical, for each of the roles. In addition, potential conflicts of interest are to be avoided, but this issue is outside the scope of this ARF.

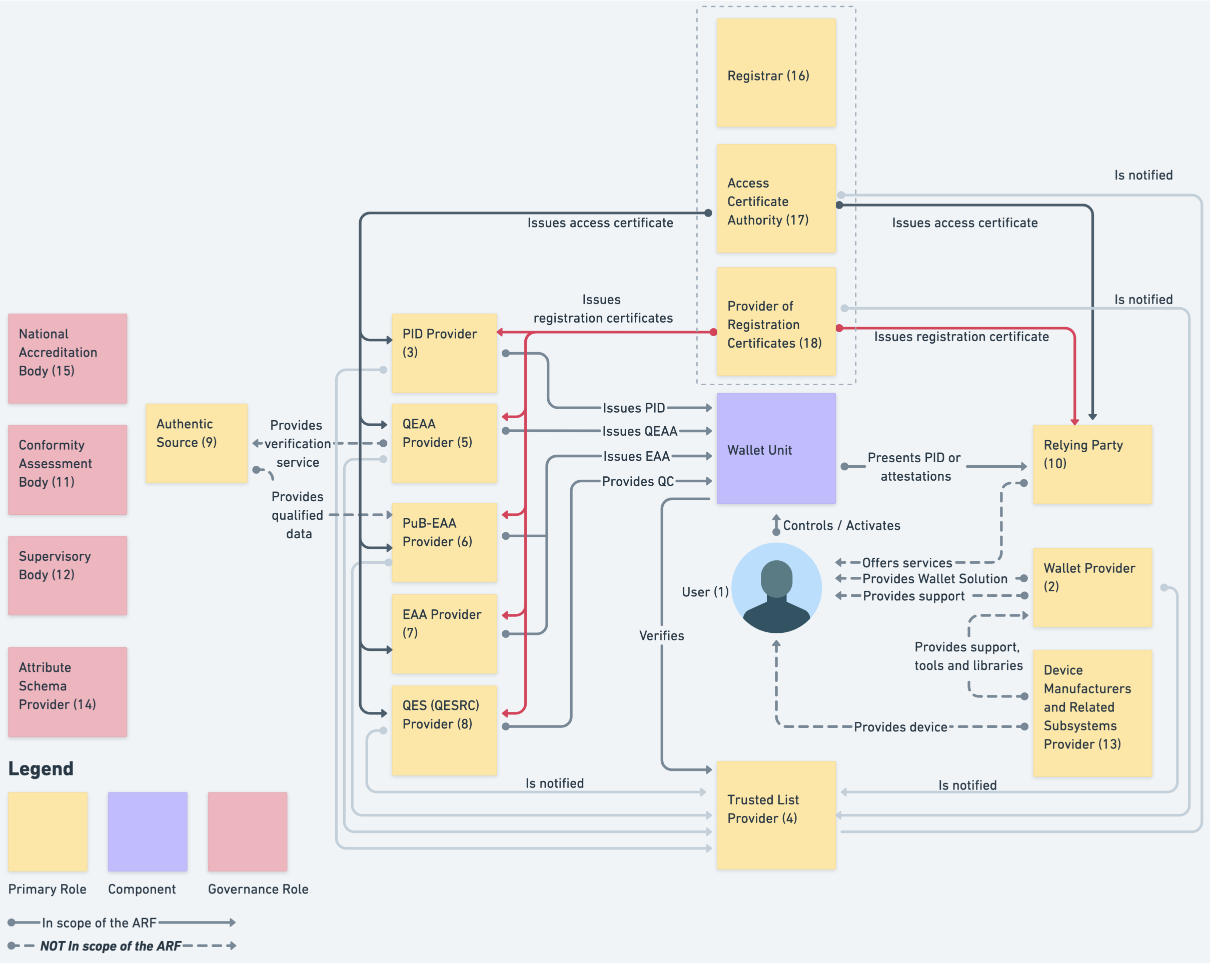


Figure 1: Overview of the EUDI Wallet ecosystem roles

1. Users of Wallet Units, see Section 3.2,

2. Wallet Providers, see Section 3.3,
3. Person Identification Data (PID) Providers, see Section 3.4,
4. Trusted List Providers, see Section 3.5,
5. Qualified Electronic Attestation of Attributes (QEAA) Providers, see Section 3.6,
6. Electronic Attestation of Attributes issued by or on behalf of a public sector body responsible for an authentic source (PuB-EAA) Providers, see Section 3.7,
7. Electronic Attestation of Attributes (EAA) Providers, see Section 3.8,
8. Qualified Electronic Signature Remote Creation Providers, see Section 3.9,
9. Authentic Sources, see Section 3.10,
10. Relying Parties, see Section 3.11,
11. Conformity Assessment Bodies (CAB), see Section 3.12,
12. Supervisory Bodies, see Section 3.13,
13. Device Manufacturers and Related Subsystems Providers, see Section 3.14,
14. Attestation Scheme Providers, see Section 3.15,
15. National Accreditation Bodies, see Section 3.16,
16. Registrars
17. Access Certificate Authorities, see Section 3.18.
18. Providers of registration certificates, see Section 3.19.

3.2 Users of Wallet Units

Users of Wallet Units use the Wallet Unit to receive, store, and present PID, QEAA, PuB-EAA, or non-qualified EAA to Relying Parties. Users can also create qualified electronic signatures and seals (QES) and create and present pseudonyms.

CIR 2024/2982 (among others) defines ‘wallet user’ as ‘a user who is in control of the wallet unit’. Being in control of the Wallet Unit implies being able to present a PID or attestation to a Relying Party. Within the use cases described in the current version of the ARF, the User is the subject of the PID(s) in the Wallet Unit. The User is also the subject of most of the attestations in the Wallet Unit, but there could be attestations that have no subject, such as vouchers, or that relate to objects owned or used by the User, such as a vehicle registration card.

Please note that this ARF assumes that a User device is a personal device, meaning that the User will not share it with other people, and that only the User can access and control the Wallet Unit. This also implies that all PIDs and attestations on the Wallet Unit pertain to that User (or to entities represented by, or objects owned by or linked to, that User).

The use of a Wallet Unit by citizens is not mandatory under the [European Digital Identity Regulation]. However, each Member State will provide at least one European Digital Identity Wallet within 24 months after the entry into force of the implementing acts referred to in the [European Digital Identity Regulation].

3.3 Wallet Providers

Wallet Providers are Member States or organisations either mandated or recognised by Member States making a Wallet Solution available to Users. All Wallet Solutions must be certified as described in Chapter 7.

A Wallet Provider makes a combination of several products and Trust Services available to a User, which give the User sole control over the use of their Person Identification Data (PID) and Electronic Attestations of Attributes (QEAA, PuB-EAA or EAA), and any other personal data within their Wallet Unit. This also implies guaranteeing a User sole control over sensitive cryptographic material (e.g., private keys) related to their Wallet Unit.

Wallet Providers are responsible for ensuring compliance with the requirements for Wallet Solutions.

From the viewpoint of the other actors in the EUDI Wallet ecosystem, the Wallet Provider is responsible for all components of the Wallet Unit. These components are described in Section 4.3.2. In particular, the Wallet Provider is responsible for ensuring that the Wallet Instance can access a Wallet Secure Cryptographic Device (WSCD) that has a level of security sufficient to ensure that the Wallet Unit can achieve Level of Assurance High, as required in the [European Digital Identity Regulation]. This is true even if the WSCD is not delivered by the Wallet Provider but is integrated into the User device. For more information, see Section 4.5. Other actors in the ecosystem do not need to interact with or explicitly trust a WSCA or WSCD supplier. As explained in Section 6.5.3.4), Wallet Providers provide Wallet Unit Attestations (WUA) to the Wallet Unit. The WUA attests that the Wallet Unit and all of its components, including the WSCA/WSCD, comply with the relevant requirements.

3.4 Person Identification Data (PID) Providers

PID Providers are trusted entities responsible for:

- verifying the identity of the User in compliance with LoA high requirements,

- issuing a PID to the Wallet Unit, and
- making available, in a privacy-preserving way, information for Relying Parties to verify the validity of the PID.

The terms and conditions of these services are for each Member State to determine.

PID Providers may be the same organisations that today issue official identity documents, electronic identity means, etc. PID Providers may be the same organisations as Wallet Providers. In case an organisation acts as both a PID Provider and a Wallet Provider, it complies with all requirements for both PID Providers and Wallet Providers.

3.5 Trusted List Provider

A Trusted List Provider (TLP) is a body responsible for maintaining, managing, and publishing a Trusted List. Within the EUDI Wallet ecosystem, Trusted Lists exist for the following entities:

- Wallet Providers, see Section 3.3,
- PID Providers, see Section 3.4,
- QEAA Providers, see Section 3.6,
- PuB-EAA Providers, see Section 3.7,
- Qualified Electronic Signature Remote Creation (QESRC) Providers, see Section 3.9,
- Access Certificate Authorities, see Section 3.18,
- Providers of registration certificates, see Section 3.19.

Notes:

- There is no Trusted List for Relying Parties. The expected number of Relying Party throughout the Union would make this infeasible. Instead, a Relying Party receives an access certificate from an Access Certificate Authority, and this certificate allows a Wallet Unit to authenticate the Relying Party.
- Wallet Providers, PID Providers, Access Certificate Authorities and Providers of registration certificates are not trust service providers in the sense of the [European Digital Identity Regulation]. Therefore, the Trusted Lists for these entities are -legally speaking-not trusted lists in the sense of Article 22. However, the technical requirements for all Trusted Lists and Trusted List Providers are the same. For that reason, the ARF does not distinguish between Trusted Lists for these entities and those for QEAA Providers and PuB-EAA Providers, who are trust service providers in the sense of the Regulation.

- Non-qualified EAA Providers are trust service providers in the sense of the [European Digital Identity Regulation]. Therefore, Trusted Lists and Trusted List Providers may also exist for non-qualified EAA Providers. However, this is out of scope of the ARF.

These Trusted Lists are described in more detail in Sections 6.2.2, 6.3.2 and 6.4.2. Some Trusted Lists contain the trust anchors of the relevant entities. A trust anchor is a combination of a public key and the identifier of the associated entity and may be used to verify signatures created by that entity.

An entity's status as a trusted entity can be verified by checking whether they are present on the relevant Trusted List. In order to be put on a Trusted List, relevant entities must be notified to the Commission by a Member State. This happens after the entity has been registered by a Registrar in the Member State, see Section 3.17.

For more information and high-level requirements, please refer to Topic 27 and to Topic 31.

3.6 Qualified Electronic Attestation of Attributes (QEAA) Providers

Qualified EAAs are provided by Qualified Trust Service Providers (QTSPs). The general trust framework for QTSPs (see Chapter III, Section 3 of the [European Digital Identity Regulation] applies also to QEAA Providers, but specific rules for the Trust Service of issuing QEAAs may be defined as well.

QEAA Providers maintain an interface to Wallet Units to provide QEAAs upon request. Potentially, they also maintain an interface towards Authentic Sources to verify attributes, as specified in Topic 42.

It is likely that for most QEAAs, a QEAA Provider will need to verify the identity of a User when issuing a QEAA. It is up to each QEAA Provider to implement the necessary User authentication processes, in compliance with all applicable national and Union legislation. Note that, when User identity verification is necessary, it is likely that the User requesting a QEAA already possesses a PID. This would enable the QEAA Provider to carry out User identification and authentication at LoA high, by requesting and verifying User attributes from the PID in the Wallet Unit.

The terms and conditions of these services are for each QEAA Provider to determine, beyond what is specified in the [European Digital Identity Regulation].

3.7 EAA issued by or on behalf of a public sector body responsible for an authentic source (PuB-EAA) Providers

As specified in the [European Digital Identity Regulation], an attestation may be issued by or on behalf of a public sector body responsible for an Authentic Source. This ARF calls such an attestation a PuB-EAA. For a description of Authentic Sources, see Section 3.10. A public sector body primarily is a state, regional or local authority, or a body governed by public law.

A PuB-EAA Provider, meaning a public sector body issuing PuB-EAAs, is not a QTSP. However, a PuB-EAA Provider has a qualified certificate, issued by a QTSP, that allows it to sign PuB-EAAs. A Relying Party verifies a PuB-EAA by first verifying the signature over the PuB-EAA, and subsequently verifying the signature of the qualified PuB-EAA Provider certificate. For more details, refer to Section 6.6.3.6. The [European Digital Identity Regulation] stipulates that PuB-EAAs, like QEAAs, have the same legal effect as attestations in paper form. It is up to the Member States to define terms and conditions for the provisioning of PuB-EAAs, but PuB-EAA Providers will comply with the same technical specifications and standards as Providers of PIDs and other attestations.

For the precise and legally binding definitions and obligations regarding the issuance of PuB-EAAs, please refer to the [European Digital Identity Regulation].

3.8 Non-Qualified Electronic Attestation of Attributes (EAA) Providers

Non-qualified EAAs can be provided by any (non-qualified) Trust Service Provider. While they will be supervised under the [European Digital Identity Regulation], it can be assumed that other legal or contractual frameworks will mostly govern the rules for provision, use and recognition of EAAs. Those other frameworks may cover policy areas such as educational credentials, digital payments, although they may also rely on Qualified Electronic Attestation of Attributes Providers. For non-qualified EAAs to be used, EAA Providers offer Users a way to request and obtain these EAAs. This implies that these non-qualified EAA Providers comply with the Wallet Unit interface specifications. The terms and conditions of issuing EAAs and related services are subject to sectoral rules.

3.9 Qualified Electronic Signature Remote Creation (QESRC) Providers

The Wallet Unit will allow the User to create qualified electronic signatures or seals over any data. This will also enhance the use of the Wallet Unit for signing, in a natural and convenient way. The creation of a qualified electronic signature or seal by means of the Wallet Unit can be achieved in several ways:

- the Wallet Unit itself could be certified as a qualified signature or seal creation device (QSCD), or
- the Wallet Unit could implement secure authentication into an electronic signature or electronic seal invocation capability, as part of a local QSCD or a remote QSCD managed by a QTSP.

As part of the ecosystem, the use of common interfaces and protocols for provisioning qualified electronic signatures and seals will create a unified European market for QTSPs offering remote signature services.

Besides providers of qualified electronic signatures and seals, also providers of non-qualified electronic signatures or seals may exist. However, such providers are out of scope of this ARF.

3.10 Authentic Sources

Authentic Sources are public or private repositories or systems, recognised or required by law, containing attributes about natural or legal persons. Authentic Sources are sources for attributes on, for instance, address, age, gender, civil status, family composition, nationality, education and training qualifications titles and licences, professional qualifications titles and licences, public permits and licences, or financial and company data.

Authentic Sources are required to provide an interface to QEAA Providers to verify the authenticity of the above attributes, either directly or via designated intermediaries recognised at national level. Authentic Sources may act as PuB-EAA Providers if they meet the requirements of the [European Digital Identity] Regulation, see Section 3.7. In Figure 1 this is indicated by the arrow ‘provides qualified data’.

3.11 Relying Parties and intermediaries

Within the scope of this ARF, a Relying Party is a service provider requesting attributes contained within a PID, QEAA, PuB-EAA or EAA from the Wallet Unit, subject to the approval of the User and within the limits of applicable legislation and rules.

Note: As specified in the [European Digital Identity Regulation], legally speaking, the term 'Relying Party' includes Attestation Providers (i.e., QEAA Providers, PuB-EAA Providers, and non-qualified EAA Providers), as well as service providers. However, technically speaking the responsibilities of Attestation Providers are quite different from those of service providers, as is the way they interact with Wallet Units. Therefore, for clarity the term 'Relying Party' is used in all parts of the ARF exclusively to mean a service provider interacting with a Wallet Unit to request and receive attributes from an attestation.

The reason for a Relying Party to rely on the Wallet Unit may be a legal requirement, a contractual agreement, or their own decision. In particular, the [European Digital Identity Regulation] requires that providers of very large online platforms must accept the EUDI Wallet for their user authentication processes.

Relying Parties maintain an interface with Wallet Units to request PIDs and attestations, using Relying Party authentication, as described in Section 6.6.3.2. If a Wallet Unit presents attributes from a PID or attestation to a Relying Party, the Relying Party can verify the authenticity of these attributes.

To rely on Wallet Units for the purpose of providing a service, Relying Parties register at a Registrar in the Member State where they are established. Registration includes the attributes that the Relying Party intends to request from Wallet Units. See Section 6.4.2 for more information on Relying Party registration. When processing a presentation request, a Wallet Unit verifies that the Relying Party only requests attributes that it registered, if the User has indicated that such a check must be performed. The Wallet Unit will warn the User if this is not the case. This is explained in Section 6.6.3.3.

In addition, an Attestation Provider may embed a disclosure policy in an attestation. Such a policy indicates to which Relying Parties a Wallet Unit should (or should not) present that attestation. When processing a presentation request, the Wallet Unit evaluates the policy based on data provided by the Relying Party, and warns the User if the outcome of that evaluation is negative. Please refer to Section 6.6.3.4 for more information.

So-called intermediaries form a special class of Relying Party. Article 5b (10) of the [European

Digital Identity Regulation] states "Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction". Such an intermediary is a party that offers services to Relying Parties to, on their behalf, connect to Wallet Units and request the User attributes that these Relying Parties need. The intermediary then sends the presented attributes to the intermediated Relying Party. This implies that an intermediary performs all tasks assigned to a Relying Party in this ARF on behalf of the intermediated Relying Party. In particular:

1. The intermediary registers once as a Relying Party with a Registrar (see Section 3.17) and obtains an access certificate (see Section 3.18 bearing its own name and Relying Party identifier. This access certificate is not different from an access certificate issued to a 'normal' Relying Party, since an intermediary is, as a matter of legal fact, a Relying Party. Note: In addition, the intermediary may receive a registration certificate (see Section 3.19), if the Registrar issues such certificates. However, this registration certificate will not be used in intermediated transactions.
2. Next, the intermediary separately registers each of the intermediated Relying Parties that uses its services. This includes registering the attributes the intermediated Relying Party wants to request for each of its intended uses. Note that each intermediated Relying Party is registered in the Member State where it is established. This implies that it is possible for an intermediary to register an intermediated Relying Party with a Registrar different from the Registrar where it is registered itself. To prove that the intermediated Relying Party is indeed using the services of the intermediary, the intermediary provides evidence to the Registrar, for example a contract. The Registrar evaluates the evidence, and, if all is correct, registers the fact that the intermediated Relying Party is using the services of the intermediary. If the Registrar (via a Provider of registration certificates) issues registration certificates, the intermediary receives one or more registration certificates for the intermediated Relying Party. These certificates contain an attribute stating that the intermediated Relying Party is using the services of the intermediary.
3. When asked by an intermediated Relying Party, the intermediary will request a presentation of attributes from a Wallet Unit, using one of the flows described in Section 4.4. For this, the intermediary will use their own access certificate (point 1. above) and the registration certificate of the intermediated Relying Party if available (point 2. above). If no registration certificate is available, the intermediary adds the user-friendly name and the unique identifier of the intermediated Relying Party directly in the presentation request. The intermediary also adds the URL of the Registrar of the intermediated Rely-

ing Party, as well as the identifier of its intended use. (Note: this will need an extension of [ISO/IEC 18013-5] and [OpenID4VP].) The Wallet Unit displays the name of both the intermediary and the intermediated Relying Party to the User when asking for User approval to present the requested attributes.

4. If the User has indicated that they want to verify the information registered about the Relying Party, and the Wallet Unit sees that the Relying Party uses the services of an intermediary (either in the registration certificate or because the information about the intermediated Relying Party is present in the request), it verifies that this Relying Party indeed uses the services of this intermediary. If the registration certificate is available, it does so by verifying that the name and the identifier of the intermediary listed in the registration certificate are identical to the name and identifier in the access certificate. If no registration certificate is available, the Wallet Unit contacts the Registrar of the intermediated Relying Party, indicated in the request, to do this verification online. If this verification was not successful, or the Wallet Unit was not able to retrieve the information registered about the Relying Party, the Wallet Unit informs the User.
5. When a Wallet Unit presents a PID or attestation to the intermediary, the intermediary verifies the authenticity of the PID or attestation, its revocation status, device binding (if expected), and User binding, as well as any combined presentation of attributes, if applicable, if the intermediary has agreed to do so with the Relying Party. Also, the intermediary may need to verify the authenticity of the Wallet Unit and its revocation status. Note that a Relying Party is not obliged to carry out all of these verifications. Therefore, the intermediary and any Relying Party using its services must agree on what verifications the intermediary will carry out.
6. If these verifications are successful, the intermediary forwards the User attributes it obtained from the Wallet Unit to the intermediated Relying Party. There must be an interface between an intermediary and a Relying Party, over which the intermediated Relying Party can request the intermediary to request some User attributes from a Wallet Unit and that the intermediary uses to send back the attribute values presented by the Wallet Unit. However, specifying this interface or the (security) requirements with which it needs to comply, is out of scope of the ARF. In particular, it is not required that the User attributes are end-to-end encrypted between the Wallet Unit and the intermediated Relying Party, such that an intermediary would not be able to see them.
7. The intermediary deletes any PIDs or attestations it obtained from the Wallet Unit, including any User attributes, immediately after it has sent the User attributes to the Relying Party. If the intermediary does not send any User attributes to the Relying

Party, for example because one of the verifications in the previous step failed, the intermediary deletes the PIDs or attestations immediately after it has completed all necessary verifications.

Note that this approach implies that an intermediated Relying Party using the services of an intermediary will not need an access certificate.

For high-level requirements on intermediaries, see Topic 52.

3.12 Conformity Assessment Bodies (CAB)

Conformity Assessment Bodies (CAB) are public or private bodies that are accredited by a national accreditation body, which itself is designated by a Member State according to Regulation 765/2008 Article 6c (3). In particular, CABs are accredited to carry out assessments on which Member States will rely before issuing a Wallet Solution or providing the 'qualified' status to a Trust Service Provider.

Wallet Solutions will be certified by CABs. QTSPs will be audited regularly by CABs.

The standards and schemes used by CABs to fulfil their tasks to certify Wallet Solutions are discussed in Chapter 7.

3.13 Supervisory Bodies

Supervisory Bodies review the proper functioning of Wallet Providers and other actors in the EUDI Wallet ecosystem. Supervisory Bodies will be created and appointed by the Member States. The Supervisory Bodies will be notified to the Commission by the Member States.

3.14 Device Manufacturers and Related Subsystems Providers

In the EUDI Wallet ecosystem, commercial actors such as device manufacturers and related subsystems providers fulfil an important role to enable a Wallet Unit to work smoothly and securely. Device manufacturers and related subsystem providers provide a platform on which a Wallet Unit can be built. Wallet Providers ensure that their Wallet Units use that platform to ensure usability, security, stability and connectivity. The components provided by device manufacturers and providers of related subsystems may include, among others, hardware, operating systems, secure cryptographic hardware, libraries, and app stores.

3.15 Attestation Scheme Providers for QEAAs, PuB-EAAs and EAAs

An Attestation Scheme Provider defines a specific attestation type (e.g., QEAA, PuB-EAA, or EAA) and publishes two complementary artefacts:

1. A human-readable Attestation Rulebook; see Section 5.4, the authoritative documentation that explains what the attestation represents and how it works, detailing identifiers, semantics, encodings, constraints, and processing rules, trust model; and
2. A machine-readable attestation scheme that mirrors the Rulebook so software can build requests to Wallet Units and validate responses at runtime.

Relying Parties use the Rulebook to decide whether and how to adopt an attestation and to prepare their systems, while their Relying Party Instances rely on the attestation scheme in production.

For PID, the European Commission publishes the applicable Rulebook.

Moreover, the Commission operates a catalogue of schemes and Rulebooks, setting the related technical specifications, standards, and procedures, so ecosystem participants can discover available attestations and understand how to request and verify their attributes; A broad array of attestation schemes, including sector-specific ones, is critical for interoperability and uptake. For more information see Section 5.5.

3.16 National Accreditation Bodies

National Accreditation Bodies (NAB), under Regulation (EC) No 765/2008, are the bodies in Member States that perform accreditation with authority derived from the Member State. NABs accredit CABs (Section 3.12) as competent, independent, and supervised professional certification bodies in charge of certifying Wallet Solutions against normative document(s) establishing the relevant requirements. NABs monitor the CABs to which they have issued an accreditation certificate.

3.17 Registrars

All PID Providers, QEAA Providers, PuB-EAA Providers, non-qualified EAA Providers and Relying Parties in the EUDI Wallet ecosystem are registered by a Registrar in the Member State where they reside. As a result of registering an entity,

- Data about the entity is registered by the Registrar and made available online in human-readable and machine-readable format to any interested party. In particular,
  - For a Relying Party, the Registrar mainly registers which attributes the Relying Party intends to request from Wallet Units, and for what purpose. The Registrar also registers if the Relying Party intends to use the services of an intermediary (see Section 3.11) to interact with Wallet Units, and if so, which one.
  - For a PID Provider, QEAA Provider, PuB-EAA Provider, or non-qualified EAA Provider, the Registrar registers the attestation type(s) this entity wants to issue to Wallet Units, for example, diplomas, driving licenses or vehicle registration cards.
- Registered entities receive an access certificate from an Access Certificate Authority, as described in Section 3.18.
- If supported by the Registrar, a registered entity also receives a registration certificate, as discussed in Section 3.19.

The process and terms and conditions for registering will be determined by each Member State.

3.18 Access Certificate Authorities

Access Certificate Authorities issue access certificate to all PID Providers, QEAA Providers, PuB-EAA Providers, non-qualified EAA Providers and Relying Parties in the EUDI Wallet ecosystem. When these entities interact with a Wallet Unit to issue or request a PID or attestation, they will present an access certificate to prove their authenticity and validity. In order to receive an access certificate, an entity must be registered by a Registrar as described in Section 3.17.

Access Certificate Authorities are notified by a Member State to the Commission. As part of the notification process, the trust anchors of the Access CA are included in a Trusted List by a Trusted List Provider. A trust anchor is the combination of a public key and an identifier for the associated entity. Wallet Units need these trust anchors to verify the signatures over the access certificates presented to them when a new PID or attestation is issued or when they receive an attribute presentation request from a Relying Party.

The Trusted List Provider signs and publishes the Access CA Trusted List and makes the URL of the Trusted List available to a common trust infrastructure maintained by the Commission, the so-called List of Trusted Lists. Using the common infrastructure, any entity in the EUDI Wallet ecosystem will be able to find all Trusted Lists in the ecosystem.

3.19 Providers of registration certificates

If a Registrar has a policy of issuing registration certificates, it has one or more associated Provider(s) of registration certificates. Such a Provider issues one or more registration certificates to each registered Relying Party, PID Provider, QEAA Provider, PuB-EAA Provider, and non-qualified EAA Provider. Each registration certificate contains (a subset of) the data registered for that entity, as described in Section 3.17.

Like Access Certificate Authorities (see previous section), Providers of registration certificates are notified by a Member State to the Commission. Their trust anchors are put on a Trusted List, such that they can be found by Wallet Units and used to verify a registration certificate received from a Relying Party.

4 High level architecture

4.1 Introduction

This chapter provides a broad overview of the EUDI Wallet ecosystem's core components, their interfaces, and the overall design principles. This chapter is structured as follows:

- Section 4.2 discusses the design principles that guided the design of the EUDI Wallet ecosystem, as described in this ARF.
- Section 4.3 presents an overview of the ecosystem's architecture, focussing on the components that make up a Wallet Unit and on the interfaces between a Wallet Unit and other entities, as well as the protocols used on these interfaces.
- Section 4.4 discusses the different attestation presentation flows enabled by this architecture, and in particular the mechanisms foreseen to enable and secure remote presentation flows in which the Wallet Unit and the Relying Party interact over the internet.
- Section 4.5 briefly discusses the different architecture types a Wallet Providers may use for implementing one or more Wallet Secure Cryptographic Device(s) into their Wallet Solutions.
- Section 4.6 presents state diagrams for all of the main entities and components in the EUDI Wallet ecosystem, discussing all of the states a particular component can be in, as well as the conditions triggering state transitions.

- Section 4.7 discusses how pseudonyms will be implemented and used within a Wallet Unit.

4.2 Design principles

To effectively translate the [European Digital Identity Regulation] into a User-friendly, privacy-focused, and secure technical architecture, establishing design principles is crucial. These principles, rooted in the regulatory framework and enriched by industry best practices, will serve as fundamental guidelines. This approach ensures compliance with requirements emphasising User-centricity, accessibility, privacy, security, and cross-border interoperability. It demonstrates a commitment to both regulatory alignment and excellence in the EUDI Wallet architecture's design.

4.2.1 User-centricity

The EUDI Wallet ecosystem prioritises User-centricity as a core design principle. This means placing User needs and experience at the forefront of every design decision. The Wallet Unit should be intuitive and easy to use, with seamless integration into existing use cases. Wallet Units make it easy for Users to exercise their legal rights to full control over their attributes and privacy, with transparent information about what attributes are being presented and to whom. Additionally, the Wallet Unit should be accessible and inclusive, catering to Users with varying technical backgrounds and abilities. By prioritising User-centricity, the EUDI Wallet ecosystem fosters trust and encourages widespread adoption, ultimately achieving its goal of empowering Users with secure and convenient digital identity management.

4.2.2 Accessibility

Regarding the accessibility of Wallet Units for Users, it is essential to ensure that these digital tools are inclusive by design and fully aligned with the applicable European legal and technical frameworks on accessibility. The same applies to any other User-facing component of the EUDI Wallet ecosystem, such as websites and User authentication methods of PID Providers and Attestation Providers, registries (see Section 3.17, et cetera). This is not only a matter of legal compliance but also a fundamental component of ensuring equal access, User trust, and widespread adoption across all segments of the population, including persons with disabilities.

For more information, please refer to Chapter 8.

4.2.3 Interoperability

The EUDI Wallet ecosystem prioritises interoperability as a core design principle. This ensures a Wallet Unit functions seamlessly across borders within the EU. Users can travel freely and confidently utilise their digital identity wallets for various services, from e-government platforms to private online interactions. Interoperability fosters secure data exchange through standardised protocols, allowing trusted entities to verify credentials effortlessly. This not only simplifies the User experience but also strengthens overall security within the system. Moreover, interoperability prevents market fragmentation by creating a level playing field for different Wallet Solutions. It fosters competition and collaboration, ultimately driving innovation in the EUDI Wallet ecosystem. By prioritising interoperability, the EUDI Wallet architecture lays the foundation for a trusted and universally accepted EUDI Wallet ecosystem across the EU.

4.2.4 Privacy by design

The EUDI Wallet architecture embodies the principle of privacy by design. This means that the protection of User data is a fundamental pillar of the architecture's design. The principle of data minimisation guides the collection of personal information, ensuring that Relying Parties gather only the attributes they need and have registered for. By enabling selective disclosure of attributes, the Wallet Unit empowers Users with granular control over what data is presented and to whom. Transparency is built into the system, with clear explanations of how data is used and protected. By making privacy a cornerstone from the beginning, the EUDI Wallet ecosystem aims to foster trust and protect the fundamental rights of its Users. Finally, measures are taken to prevent Users from being tracked by Relying Parties, PID Providers, or Attestation Providers.

For more information, please refer to Sections 7.4.3.4 and 7.4.3.5.

4.2.5 Security by design

The EUDI Wallet architecture embraces the principle of security by design. This means security considerations are woven into the very fabric of the architecture's design. Throughout the design process, potential vulnerabilities are identified and mitigated. Secure coding practices are mandated, and the architecture itself minimises attack surfaces by compartmentalising sensitive data and access controls. By prioritising security from the outset, the EUDI Wallet architecture aims to be inherently resistant to cyberattacks and data breaches, fostering trust and User confidence in this EUDI Wallet ecosystem.

For more information, please refer to Sections 7.4.3.2 and 7.4.3.3.

4.3 Reference architecture

4.3.1 Overview

The figure below gives an overview of the architecture of the EUDI Wallet ecosystem and its components. In comparison to Figure 1, this figure presents more detail on the composition of a Wallet Unit and its interfaces to other entities. The depicted components of a Wallet Unit are described in Section 4.3.2, while the interfaces are described in Section 4.3.3. The other entities shown in the figure were already described in Chapter 3.

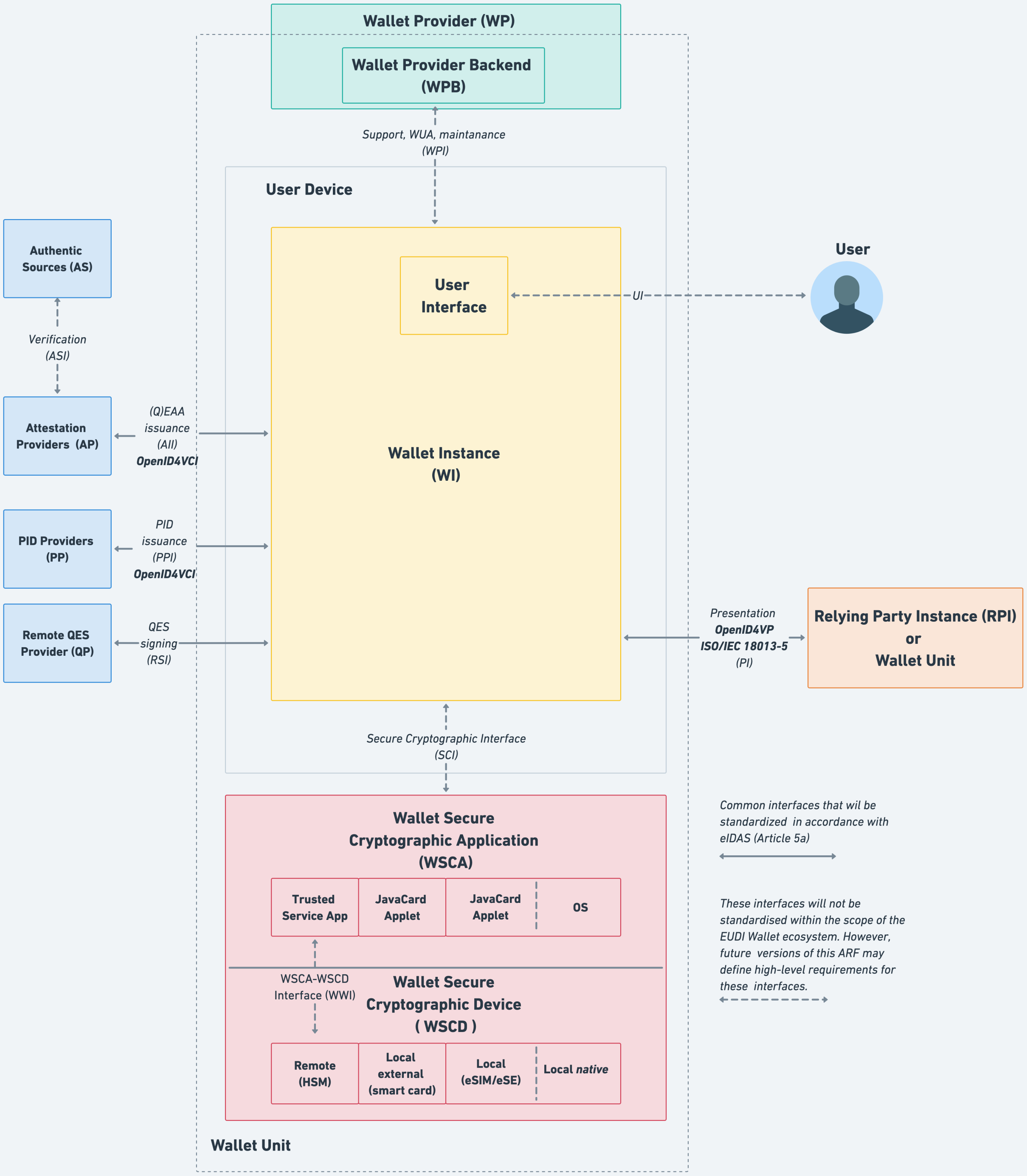

Wallet Provider (WP)
Wallet Provider Backend (WPB)
Support, WUA, maintanance (WPI)
User Device
Authentic Sources (AS)
Verification (ASI)
Attestation Providers (AP)
(Q)EAA issuance (AII) OpenID4VCI
PID Providers (PP)
PID issuance (PPI) OpenID4VCI
Remote QES Provider (QP)
QES signing (RSI)
User Interface
UI
User
Wallet Instance (WI)
Presentation OpenID4VP ISO/IEC 18013-5 (PI)
Relying Party Instance (RPI) or Wallet Unit
Secure Cryptographic Interface (SCI)
Wallet Secure Cryptographic Application (WSCA)
Trusted Service App
JavaCard Applet
JavaCard Applet
OS
WSCA-WSCD Interface (WWI)
Wallet Secure Cryptographic Device (WSCD)
Remote (HSM)
Local external (smart card)
Local (eSIM/eSE)
Local native
Wallet Unit
Common interfaces that wil be standardized in accordance with eIDAS (Article 5a)
These interfaces will not be standardised within the scope of the EUDI Wallet ecosystem. However, future versions of this ARF may define high-level requirements for these interfaces.

Figure 2: EUDI Wallet ecosystem reference architecture

Note that a User device can host more than one Wallet Unit, either provided by multiple Wallet Providers or by the same one, if supported by that Wallet Provider. If a User device hosts more than one Wallet Unit, all statements in this ARF regarding a Wallet Unit and its components hold for each Wallet Unit independently.

4.3.2 Components of a Wallet Unit

The following have been identified as the core components of a Wallet Unit:

- **User device (UD)**: A User Device comprises the hardware, operating system, and software environment required to host and execute the Wallet Instance. The minimum hardware and software requirements for the User device will be determined by the Wallet Provider.
- **Wallet Instance (WI)**: The app or application installed on a User device, which is an instance of a Wallet Solution and belongs to and is controlled by a User. This component implements the core business logic and interfaces as depicted in Figure 2. It directly interacts with the WSCA (which is interacting with the WSCD, see bullets hereafter) to securely manage cryptographic assets and execute cryptographic functions, ensuring a high level of assurance for authentication.
- **Wallet Secure Cryptographic Device (WSCD)**: A tamper-resistant device that provides an environment that is linked to and used by the Wallet Secure Cryptographic Application (WSCA) to protect critical assets and to securely execute cryptographic functions. This includes a keystore, but also the environment where the security-critical functions are executed. The WSCD is tamper-proof and duplication-proof. One WSCD may be a part of multiple Wallet Units, e.g. in case of a remote HSM. The WSCD consists of two parts: the WSCD hardware covers the hardware issued by the WSCD vendor and the WSCD firmware covers security-related software, such as an operating system and cryptographic libraries provided by the WSCD vendor. Figure 2 shows four different possible security architectures for the WSCD (for more details see Section 4.5):

  - a remote WSCD, which is a remote device, such as a Hardware Security Module (HSM), accessed over a network.
  - a local external WSCD, which is an external device, such as a smart card issued to the User specifically for this purpose,
  - a local internal WSCD, which is a component within the User device, such as a SIM, e-SIM, or embedded Secure Element,
  - a local native WSCD, which is a component embedded in the User device and accessed via an API provided by the operating system.

- **Wallet Secure Cryptographic Application (WSCA)**: an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the Wallet Secure Cryptographic Device. Different types of WSCD generally use different types of WSCA. For example, if the WSCD is a remote HSM, the WSCA may be (but does not have to be) a dedicated firmware module. If the WSCD is a external smartcard or an internal e-SIM or embedded Secure Element, the WSCA takes the form of a dedicated JavaCard applet running on the e-SIM or SE. If the WSCD is a local native WSCD, the WSCD is integrated into the OS of the User device. The WSCA interfaces directly with the Wallet Instance. For more details see Section 4.5.

- **Wallet Provider backend (WPB**): The Wallet Provider backend offers Users support with their Wallet Units, performs essential maintenance, and issues Wallet Unit Attestations through the Wallet Provider Interface (WPI).

4.3.3 Wallet Unit interfaces and protocols

Figure 2 shows the following interfaces between components of a Wallet Unit, or between the Wallet Unit and other entities in the EUDI Wallet ecosystem:

- The **Wallet Provider Interface (WPI)** is used by the Wallet Instance to communicate with the Wallet Provider to request and issue the Wallet Unit Attestation, as well as to provide support to the User and collect aggregated and User-consented information in a privacy-preserving manner to provision the Wallet Unit, in compliance with applicable legislation. Because the Wallet Provider is responsible for both sides of this interface, it will not be standardised in the scope of the EUDI Wallet ecosystem.
- The **User Interface (UI)** is the point of interaction and communication between the User and the Wallet Instance. This interface will not be standardised in the scope of the EUDI Wallet ecosystem.
- The **Presentation Interface (PI)** enables Relying Party Instances to securely request and receive PIDs, QEAAs, PuB-EAAs and EAAs from Wallet Units. This interface accommodates both remote and proximity interactions. For remote presentation flows, as detailed in Section 4.4.3, the Wallet Instance implements the OpenID for Verifiable Presentation protocol [OpenID4VP] in combination with the [W3C Digital Credentials API]. In contrast, for the proximity presentation flow, this interface adheres to the [ISO/IEC 18013-5] standard, see Section 4.4.2. The same interface can also be used by another Wallet Unit to request User attributes, see Section 6.6.4.
- The **Secure Cryptographic Interface (SCI)** enables the Wallet Unit to communicate with the Wallet Secure Cryptographic Application (WSCA). This interface is specifically

designed for managing cryptographic assets and executing cryptographic functions. In case the WSCA is delivered by the Wallet Provider, the Wallet Provider is responsible for both sides of this interface, and hence standardisation is not needed within the scope of the EUDI Wallet ecosystem. In case the WSCA is delivered by the provider of the WSCD, this interface will comply what an existing specification that is not specifically designed for the EUDI Wallet ecosystem. Rather, each type of WSCA/WSCD will expose a provider-defined interface to the Wallet Units. For example, in case the WSCD is a secure element, [CIR 2024/2979] requires support for the [GP OMAPI] interface specification (or an equivalent one). To be able to support different types of WSCA/WSCD, Wallet Units may therefore need to be able to handle multiple flavours of this interface.

- The **WSCA - WSCD Interface (WWI)** enables the WSCA to communicate with the WSCD. This interface is not specifically designed for the EUDI Wallet ecosystem. Rather, each type of WSCD will expose a manufacturer-defined interface to the WSCA making use of it, for example syscalls of the operating system. In case the WSCA is delivered by the Wallet Provider, the Wallet Provider is responsible for correctly implementing this interface.
- The **PID Issuance Interface (PII)** complies with the [OpenID4VCI] standard and is used when the Wallet Unit communicates with a PID Provider to request and receive PIDs to be stored within the Wallet Unit.
- The **Attestation Issuance Interface (AII)** complies with the [OpenID4VCI] standard and is used by the Wallet Unit to request various attestations that the User wants to include in their Wallet Unit.
- The **Remote Signing or Sealing Interface (RSI)** facilitates communication between the Wallet Unit and a Qualified Electronic Signature Remote Creation (QESRC) Provider. This interface is used by the Wallet Unit to generate a qualified electronic signature or seal.

*Note that the “Attribute Deletion Request to Relying Party Interface” and the “Reporting Relying Party to DPA Interface”, which are mentioned in the Regulation, are not depicted as interfaces in Figure 2. Functionality enabling a User to request a Relying Party to delete personal data (i.e., User attributes) obtained from the User’s Wallet Unit is seen as a feature of the Wallet Solution. The same applies to functionalities enabling the User to report a Relying Party to a Data Protection Authority.

4.4 Data presentation flows

4.4.1 Overview

This section defines four distinct communication flows that can be used when a Wallet Unit presents a PID or attestation to a Relying Party Instance:

- **Proximity Supervised Flow**: In this flow, the User and their User Device are physically near the Relying Part Instance. PIDs and attestations are exchanged using proximity technology (e.g., NFC, Bluetooth) between the Wallet Unit and the Relying Party Instance. Both devices may be with or without internet connectivity. A human representative of the Relying Party supervises the process.
- **Proximity Unsupervised Flow**: This flow is like the supervised flow, but the Wallet Unit presents attestations to a machine, without human supervision. The interfaces and protocols used in this flow are the same as for the proximity supervised flow, and are described in Section 4.4.2.
- **Remote Same-Device Flow**: In this flow, the User utilises a web browser or another application on their User device to access a Relying Party's a service. If consuming the service requires the Relying Party to obtain specific attributes from the User's Wallet Unit, the Relying Party sends a presentation request to the Wallet Unit. As explained in Section 4.4.3.2, this request is managed by the web browser on the User's device, utilising a solution like the [W3C Digital Credentials API].
- **Remote Cross-Device Flow**: In this flow, the User uses a web browser on a device other than the User device on which their Wallet Unit is installed to access the Relying Party's service. This other device could be for instance a desktop, laptop, or another mobile device. If the Relying Party needs to send a presentation request to the User's Wallet Unit, it presents this request to the web browser on the other device. Again using the [W3C Digital Credentials API], this web browser sets up a secure communication channel between the other device and the User's device. Section 4.4.3.3 explains this in more detail.

Specific use cases integrate one or more of these flows. Each of these flows is described in more detail in one of the next sections.

4.4.2 Proximity presentation flows

Figure 3 shows how attestation presentation works when the User and their User Device are physically near the Relying Part Instance. In this case, the [ISO/IEC 18013-5] standard specifies how a communication channel is set up and how a presentation request and the corresponding response are exchanged.

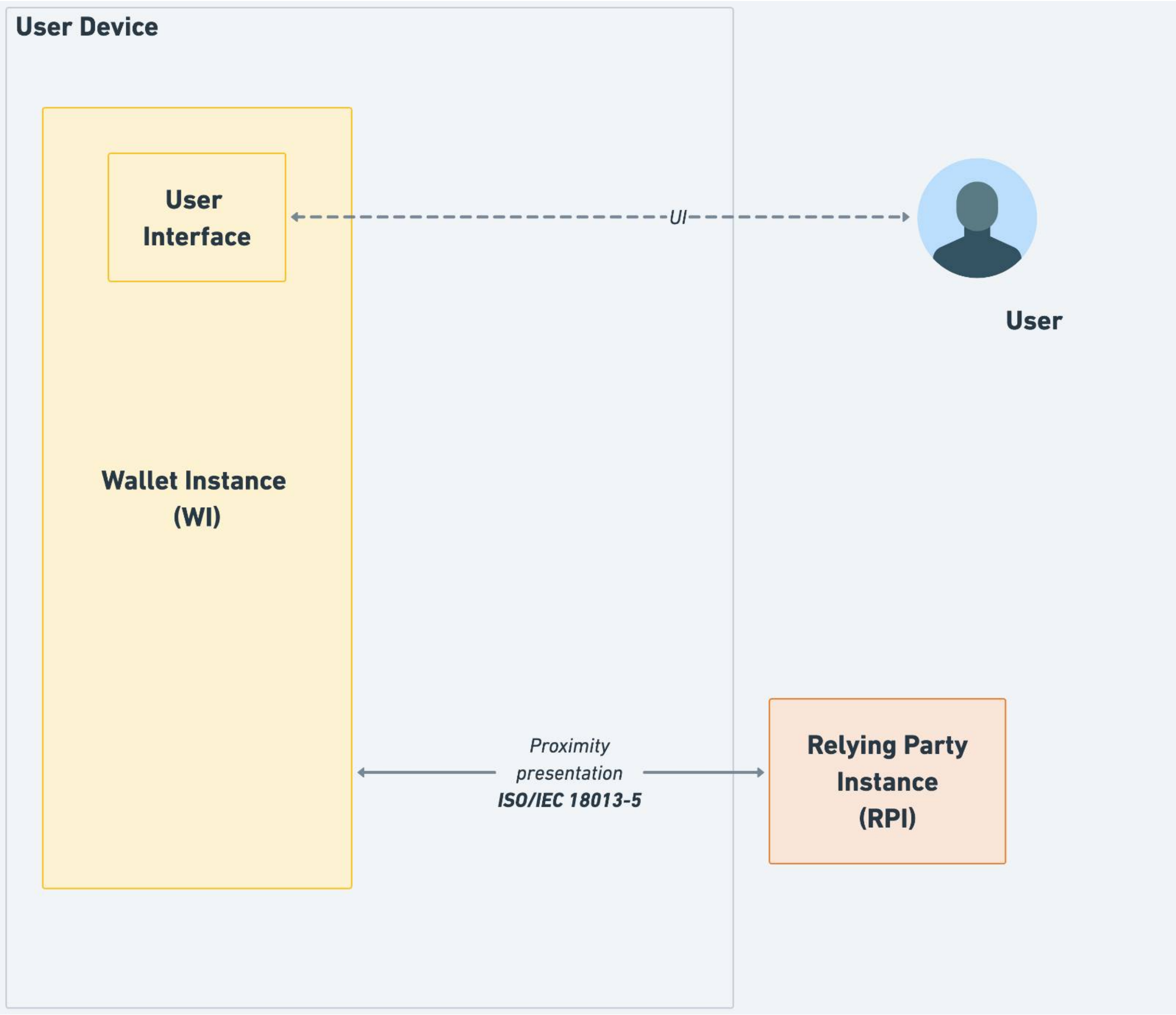

User Device
User Interface
UI
User
Wallet Instance (WI)
Proximity presentation ISO/IEC 18013-5
Relying Party Instance (RPI)

Figure 3: Proximity presentations

The attribute presentation flow begins when the User opens the Wallet Instance and instructs it to display a QR code or present an NFC tag. This QR code or NFC tag contains the information necessary to establish an NFC, BLE, or Wi-Fi Aware connection. The Relying Party Instance scans the QR code or the NFC tag and set ups the connection. The QR code or NFC tag also contains the information necessary to create an authenticated and encrypted secure channel between both entities.

4.4.3 Remote presentation transaction flows

4.4.3.1 Introduction

Remote presentation transaction flows are use cases in which the Relying Party Instance is remote from the User and the User device. The Relying Party Instance requests data from the Wallet Unit over the internet, using a browser. These use cases can be further distinguished as same-device flows, in which the browser is running on the same device as the Wallet Unit, and cross-device flows, where the browser is on a different device.

Remote presentation flows come with a number of challenges that are not present for proximity flows:

1. **Secure Cross-Device Flows**: Cross-device flows are vulnerable to phishing and relay attacks, necessitating enhanced security measures. Proximity checks, managed by the operating system of the User device, can mitigate the risks derived from these vulnerabilities by leveraging built-in security features to verify the authenticity of interactions, ensuring they are both secure and reliable.
2. **Wallet Unit Selection**: In remote flows, where interactions do not originate from the Wallet Unit, Users may encounter difficulties in selecting the appropriate Wallet Unit to fulfil a specific presentation request, particularly when multiple Wallet Units are present on the device. A unified interface provided by the web browser and the device operating system can streamline this process, offering a seamless and intuitive User experience.
3. **Invocation Mechanism**: Establishing a communication channel between the Wallet Unit and the remote Relying Party Instance presents challenges due to inconsistent invocation methods. One approach considered by standardisation bodies involves using custom URI schemes, such as “mdoc://” or “openid4vp://”. In this approach, the device operating system would trigger the Wallet Unit when the Relying Party Instance requests a connection via a custom URI. Another approach is the use of domain-bound universal links (a.k.a. app links). However, relying on custom URI schemes or universal links introduces variability in User experiences across different browsers and operating systems, resulting in operational inefficiencies and potential security risks. An interface provided by the web browser and the device OS does not need custom URL schemes or universal links for invoking a Wallet Unit.
4. **Clear Origin Verification**: Protecting against relay attacks requires precise identification of the Relying Party Instance’s origin. Including the origin information, such as the website domain or app package name, within the presentation request ensures the authenticity of the request and enhances trust for both Wallet Units and Users.
5. **Session binding**: When presenting a PID or attestation to a remote Relying Party Instance, Users have to switch contexts. Existing protocols may enable attacks where the

contexts are not bound to each other, resulting in session hijacking. Using an interface provided by the web browser and the device OS allows information about a session to be embedded in a presentation request. At the same time, the browser and the operating system handle proper context switching, preventing session hijacking.

The next sections describe how these challenges might be solved for both same-device and cross-device remote presentation flows, by using the [W3C Digital Credentials API]. This API is expected to establish a consistent method for invoking Wallet Units, addressing these challenges.

The current version of the [W3C Digital Credentials API] extends the Credential Management Level 1 API (the same API used by WebAuthn / Passkeys, see Section 4.7) to allow websites to request an attestation. This is achieved by providing a sequence of "presentation requests", where each presentation request includes an "exchange protocol" and "request data". The format of the request data are specific to the exchange protocol. The Digital Credentials API specifications will include a registry of supported protocols. For more information see the Topic F: Digital Credentials API discussion paper.

However, the [W3C Digital Credentials API] is still under development and has not yet been standardised. For the [W3C Digital Credentials API] to be mandated by this ARF in the future, it will have to align with the principles and expectations outlined in Chapter 3 of the Topic F discussion paper. Moreover, the API has not been implemented yet by all browsers and operating systems.

The use of this API by Wallet Units and Relying Parties is optional, and custom URL schemes may be used as well. If a Wallet Unit implements a custom URL scheme, it will need to implement mitigations for the challenges described in this section.

4.4.3.2 Same-device remote presentation flows

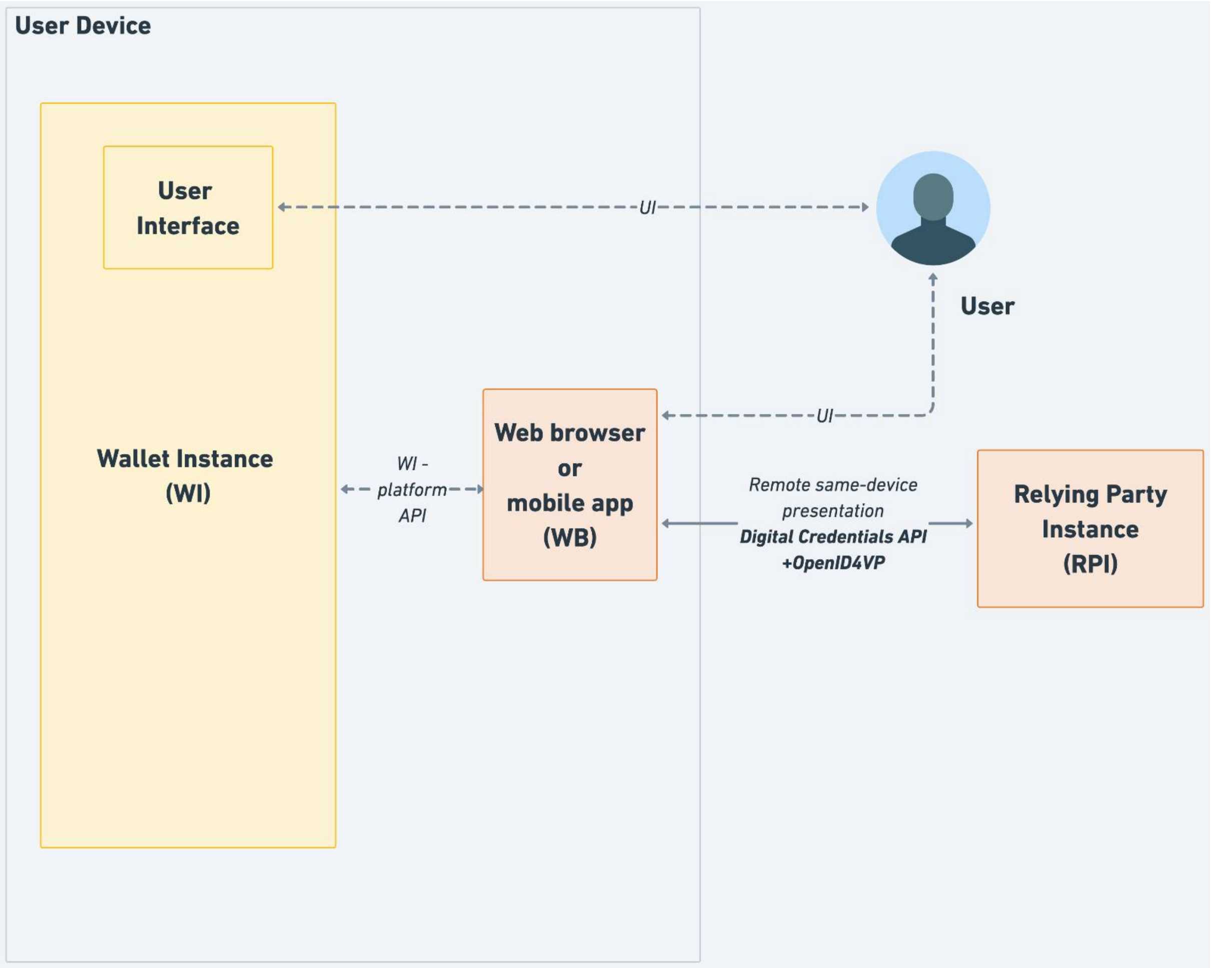

User Device
User Interface
UI
User
UI
Wallet Instance (WI)
WI - platform API
Web browser or mobile app (WB)
Remote same-device presentation
Digital Credentials API +OpenID4VP
Relying Party Instance (RPI)

Figure 4: Remote same-device presentations

Compared to Figure 2, Figure 4 shows additional detail. In particular, it shows the browser on the User device and the relevant interfaces of this browser:

- The **Remote same-device presentation** interface establishes communication between the web browser and a remote Relying Party Instance, which may operate on a server managed by the Relying Party. This interface may comply with the [Digital Credentials API], which is a browser API that is currently being standardised within the W3C.
- The **WI-platform API** interface is a mechanism provided by the device's operating system that may implement the Digital Credentials API mechanism at OS level. There are however no current plans to standardise this interface on the level of the API calls. These calls will be specified in the developer documentation for the respective OS. One of the main properties of this API is that a Wallet Unit receives reliable information regarding the origin of the presentation request.

Obviously, the browser also has a User interface allowing the User to interact with it. This interface will not be standardised in the context of the EUDI Wallet ecosystem.

A remote same-device attribute presentation flow begins when the User accesses the Relying Party's website using a browser on their device. The website may provide an option for the User to present attributes from their Wallet Unit, typically via a button or similar interface. When the User selects this option, the browser may ask the User for permission to initiate the presentation flow. Upon granting permission, the Relying Party Instance sends a presentation request compliant with the OpenID4VP specification to the browser via the Digital Credentials API. The browser, working in tandem with the device's operating system (OS), forwards the request to the Wallet Unit using the WI-platform API. If the device hosts multiple Wallet Units, the browser and OS will determine which Wallet Unit should handle the request. This decision may involve consulting the User.

The selected Wallet Unit processes the presentation request and seeks the User's approval before returning the requested attributes in an encrypted format to the browser. The browser then forwards this encrypted response to the remote Relying Party Instance.

Figure 4 also illustrates an inter-app attribute presentation flow. In this scenario, an application on the User's device, such as a banking or shopping app, interacts with the Wallet Unit over the WI-platform API. This app acts as the Relying Party Instance, possibly in cooperation with a remote server of the entity that provisioned the app. The app can use the User attributes retrieved from the Wallet Unit itself, for example for User authentication or to automatically fill in data fields like User name and address. Alternatively, the app can send these User attributes to the remote server. All requirements on Relying Parties in this ARF, such as those regarding Relying Party registration and authentication, User consent, and other aspects, are applicable in this use case as well.

In this use case, the attribute presentation flow begins when the User opens the app and initiates a request for attributes from the Wallet Unit via the WI-platform API. Notably, this is the same API used in remote same-device presentation flow involving a browser. The primary difference lies in the origin information included in the presentation request, which may vary.

4.4.3.3 Cross-device remote presentation flows

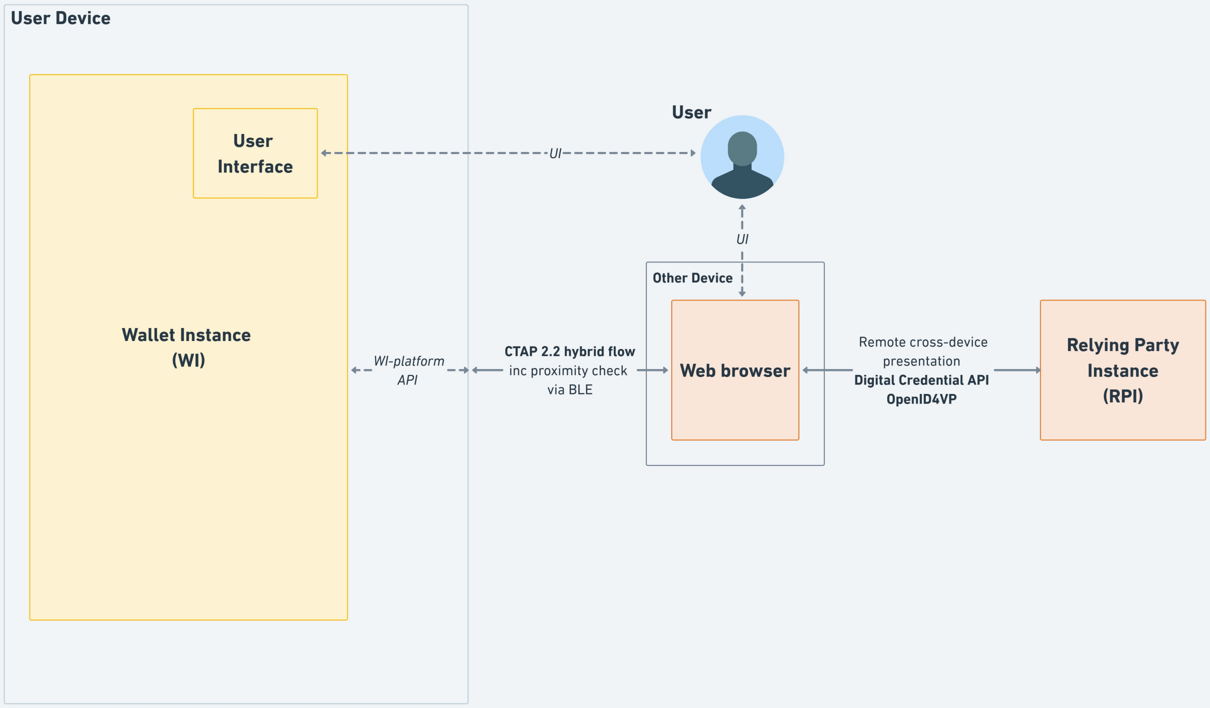


Figure 5: Remote cross-device presentations

A remote cross-device attribute presentation flow begins when the User uses a browser on a device different from their User device to visit the website of the Relying Party. The website may offer the User the possibility to present attributes from their Wallet Unit, for example by clicking a button. If the User does so, the browser may ask the User for permission to initiate the presentation flow. If the User allows this, the Relying Party Instance sends a presentation request to the browser over the Digital Credentials API. The browser then establishes a tunnel towards the User device, using the FIDO CTAP 2.2 hybrid flow, see section 11.5 of [CTAP]. Note that this flow is also used for FIDO Passkeys. This is done as follows:

1. The browser presents a QR code that includes information about the tunnel endpoint, as well as keys that will be used for establishing a secure channel over this tunnel.
2. The User scans the QR code using the camera on the User device.
3. The User device emits a BLE advertisement, which is received by the browser. The advertisement includes, in an encrypted form, information required for establishing the secure tunnel. This advertisement is used as a proximity check: the tunnel cannot be established if the User device and the device on which the browser runs are not close to each other.
4. A tunnel is established between the two devices.

The browser then sends the OpenID4VP-compliant presentation request to the User device. If there are multiple Wallet Instances present on the User device, the device OS will determine to which of these the request will be forwarded, possibly after consulting the User. The selected Wallet Unit will process the presentation request and, after requesting approval from the User, will return the requested attributes in encrypted format to the browser, using the established tunnel. The browser will forward the response to the remote Relying Party Instance.

Note that the Wallet Instance does not see any difference between the cross-device flow and the same-device flow. In both cases, it receives an OpenID4VP-compliant presentation request over the WI-platform API described in the previous section.

4.4.3.4 Profiling the use of [OpenID4VP] in remote presentation flows

As mentioned above, for both same-device and cross-device remote presentation flows, the messages used to request and present attestations comply with [OpenID4VP]. The OpenID Foundation is standardising a profile for the W3C Digital Credentials API, that will define how OpenID4VP will be used over this API.

In addition, there are two other profiles that will be used by Wallet Units and remote Relying Parties:

- [ISO/IEC 18013-7] Annex B contains a profile for OpenID4VP. Relying Parties and Wallet Unit will comply with the requirements in this profile when the format of the attestation complies with [ISO/IEC 18013-5].
- Otherwise, i.e. when the format of the attestation complies with [SD-JWT VC], Relying Parties and Wallet Unit will comply with the requirements in the profile for SD-JWT VCs specified in [HAIP].

4.5 WSCD architecture types

4.5.1 Introduction

Figure 2 showed four different types of architecture for the WSCD, which are:

- Remote WSCD, see Section 4.5.2
- Local external WSCD, see Section 4.5.3
- Local internal WSCD, see Section 4.5.4
- Local native WSCD, see Section 4.5.5

In addition, Section 4.5.6 describes a hybrid architecture. Within the EUDI Wallet ecosystem, a Wallet Provider is allowed to use any of these architectures.

Notes:

- Regardless of the chosen architecture, the **Wallet Provider** is responsible for ensuring that the Wallet Instance can access a WSCD with a security level sufficient to meet the **Level of Assurance High**, as required by the [European Digital Identity Regulation]. The Wallet Provider must also manage the cryptographic keys on the WSCD (through the WSCA) throughout the lifetime of the Wallet Unit, and attest the properties of the WSCD, including relevant certifications, in the Wallet Unit Attestation (see Section 6.5.3).
- User access to the WSCD always requires **two authentication factors**, irrespective of the architecture used:

  1. **Physical access** to the User device, and

  2. **An additional factor** verified by the WSCA.

  This second factor may be biometric, but is typically knowledge-based (e.g. a PIN or password).

  See also the requirements on User authentication in *Section C on Wallet Unit management* in Topic 40.

4.5.2 Remote WSCD

In this architecture, the Wallet Secure Cryptographic Device is situated remotely from the User device. Typically, it will be implemented by the Wallet Provider using an HSM running on a secure server. The Wallet Provider will also provide the WSCA with which the Wallet Unit interacts.

This architecture is typically used if the User device lacks sufficiently secure hardware, or if the Wallet Provider does not want to have a dependency on such hardware.

4.5.3 Local external WSCD

If the User device lacks sufficiently secure hardware, another option is to use a local external hardware component as the WSCD. This local external WSCD is typically a smart card or a secure token. It is connected to the User device via NFC or another short-range connection, and is able to perform all of the cryptographic operations required from a WSCA/WSCD in the ARF. Note that many existing smart cards, such as identity cards, will not be able to do this.

The WSCA typically takes the form of a Java Card applet. The WSCA is installed prior to issuance of the smart card or secure token to the User. The issuer of the WSCD and of the WSCA is the Wallet Provider or another entity acting on behalf of or in cooperation with the Wallet Provider.

4.5.4 Local internal WSCD

In this architecture, the Wallet Secure Cryptographic Device is integrated directly within the User's device. This includes solutions like UICCs, e-SIM/SAMs, or embedded Secure Elements. Such solutions typically are compliant with the GlobalPlatform Card Specifications [GP CS] or with the GSMA Secured Applications for Mobile [GSMA SAM] specification.

The WSCA will typically be a Java Card applet, and it is remotely issued to the WSCD by the Wallet Provider, at the moment the Wallet Unit is activated; see Section 6.5.3. In order to do this, the Wallet Provider may need to connect to and collaborate with other entities, such as a Trusted Service Manager employed by the owner of the WSCD.

The Wallet Provider is responsible for verifying that the local internal WSCD is compliant with all applicable requirements, prior to activating a Wallet Unit using such a WSCD.

4.5.5 Local native WSCD

A local native WSCD is integrated into the User device, just like the local internal WSCD discussed in the previous section. However, the API to access the WSCD is included in the operating system of the User device. Therefore, no separate WSCA is necessary. Alternatively, the API offered by the OS may be viewed as the WSCA.

The Wallet Provider is responsible for verifying that the local native WSCD is compliant with all applicable requirements, prior to activating a Wallet Unit using such a WSCD.

4.5.6 Hybrid architecture

In this architecture, two or more of the different types of WSCD described above are combined. For example, a remote HSM may manage the cryptographic keys of the Wallet Unit and of PIDs and device-bound attestations present in the Wallet Unit, while an embedded Secure Element is used to manage the access to the remote HSM.

4.6 State diagrams

4.6.1 Introduction

In this section, state diagrams are presented for Wallet Solutions, Wallet Units, PID Providers and Attestation Providers, PIDs and attestations, and Relying Parties.

4.6.2 Wallet Solution

A Wallet Solution has a state diagram of its own. The state of a Wallet Solution affects the state of all Wallet Units of that Wallet Solution. Figure 6 below shows the states of the Wallet Solution:

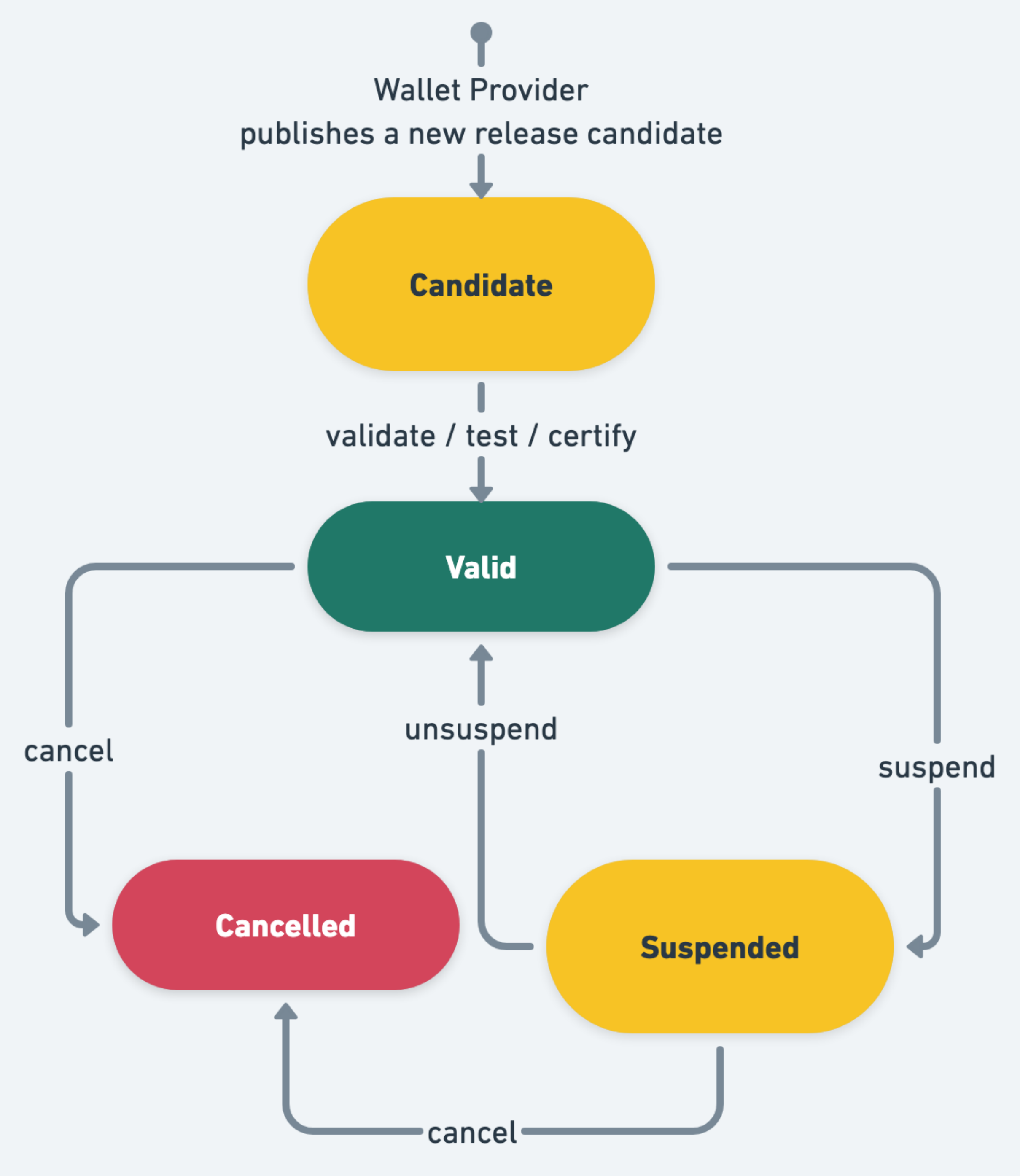


Figure 1: Figure 6

Figure 6: State diagram of Wallet Solution

The **Candidate** state is the first state of a Wallet Solution. This means it is fully implemented and the Wallet Provider requests the solution to be certified as a Wallet Solution as part of an EUDI Wallet eID scheme.

If all the legal and technical criteria have been met, a Member State may decide to allow a Wallet Provider to start providing the Wallet Solution to Users. The state of the Wallet Solution becomes **Valid**. This means the Wallet Solution can be officially launched, and can be provided to Users. The issuing Member State informs the Commission of each change in the certification status of their EUDI Wallet eID schemes and the Wallet Solutions provided under that scheme.

The issuing Member State can temporarily suspend a Wallet Solution. This would for example be the result of a critical security issue. This leads to the **Suspended** state. The issuing Member State can unsuspend the Wallet Solution, bringing the Solution back to the **Valid** state. The issuing Member State can also decide to completely cancel the Wallet Solution, which brings the Wallet Solution in the **Cancelled** state.

A Wallet Unit that is part of a suspended or cancelled Wallet Solution cannot request the issuance of a PID or attestation. Nor will a PID or attestation presented by such a Wallet Unit be accepted by a Relying Party.

4.6.3 Wallet Unit

Figure 7 below shows the states of a Wallet Unit.

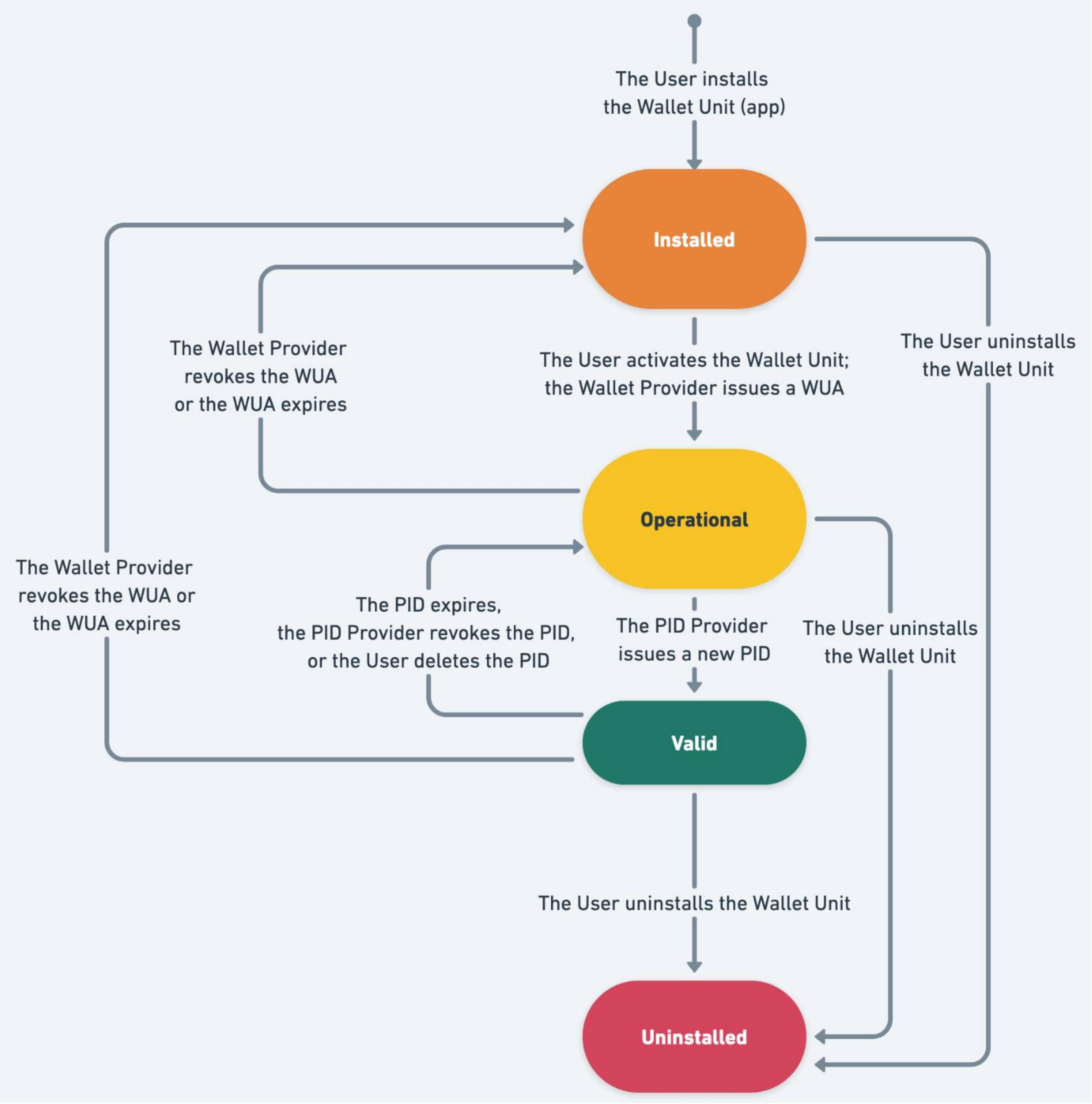

The User installs the Wallet Unit (app)
Installed
The Wallet Provider revokes the WUA or the WUA expires
The User activates the Wallet Unit; the Wallet Provider issues a WUA
The User uninstalls the Wallet Unit
Operational
The Wallet Provider revokes the WUA or the WUA expires
The PID expires, the PID Provider revokes the PID, or the User deletes the PID
The PID Provider issues a new PID
The User uninstalls the Wallet Unit
Valid
The User uninstalls the Wallet Unit
Uninstalled

Figure 2: Figure 7

Figure 7: State diagram of Wallet Unit

A Wallet Unit lifecycle begins when the User installs a Wallet Instance on their User device, see Section 6.5.2. The Wallet Unit's state is then **Installed**. In this state, the User and the Wallet Provider can perform only one action, namely activating the Wallet Unit, as described in Section 6.5.3. As part of the activation process, the Wallet Provider issues one or more

Wallet Unit Attestations (WUA) to the Wallet Unit.

Once a Wallet Unit is activated, it is in the **Operational** state. In this state, the User and the Wallet Provider manage the Wallet Unit and can perform the same actions as in the **Valid** state, see below. However, obviously, the User cannot identify nor authenticate themselves by presenting a PID to a Relying Party, nor can any other action with a PID be performed, because by definition no valid PID is present in this state.

If, in the **Operational** state, a PID Provider issues a PID to a Wallet Unit, it transitions to the **Valid** state. If, in either of these two states, the Wallet Provider revokes the WUA(s) or the WUA(s) expire(s) without being re-issued, the Wallet Unit moves back to **Installed**.

The following actions can be performed in the **Valid** state:

- The Wallet Provider updates the Wallet Unit to a new version,
- The Wallet Provider revokes the Wallet Unit, for instance at the User's request or if the security of the Wallet Instance is broken. Revocation of the Wallet Unit is accomplished by revoking the Wallet Unit Attestation (see Topic 9 and Topic 38).
- The User requests issuance of a PID, a QEAA, a PuB-EAA, or an EAA.
- The User presents attributes from a PID, a QEAA, a PuB-EAA, or an EAA to a Relying Party.
- The User deletes a PID, a QEAA, a PuB-EAA, or an EAA.
- A PID, a QEAA, a PuB-EAA, or an EAA is revoked by its Provider (if it is valid for more than 24 hours).
- The User uninstalls the Wallet Instance.

If the last or only PID in the Wallet Unit expires, is revoked, or is deleted, the Wallet Unit's state is moved back to **Operational**. Note that if there are multiple PIDs in the Wallet Unit, it does not move to the **Operational** state as long as at least one of them is valid.

4.6.4 PID Provider or Attestation Provider

Figure 8 shows the possible states of a PID Provider or Attestation Provider.

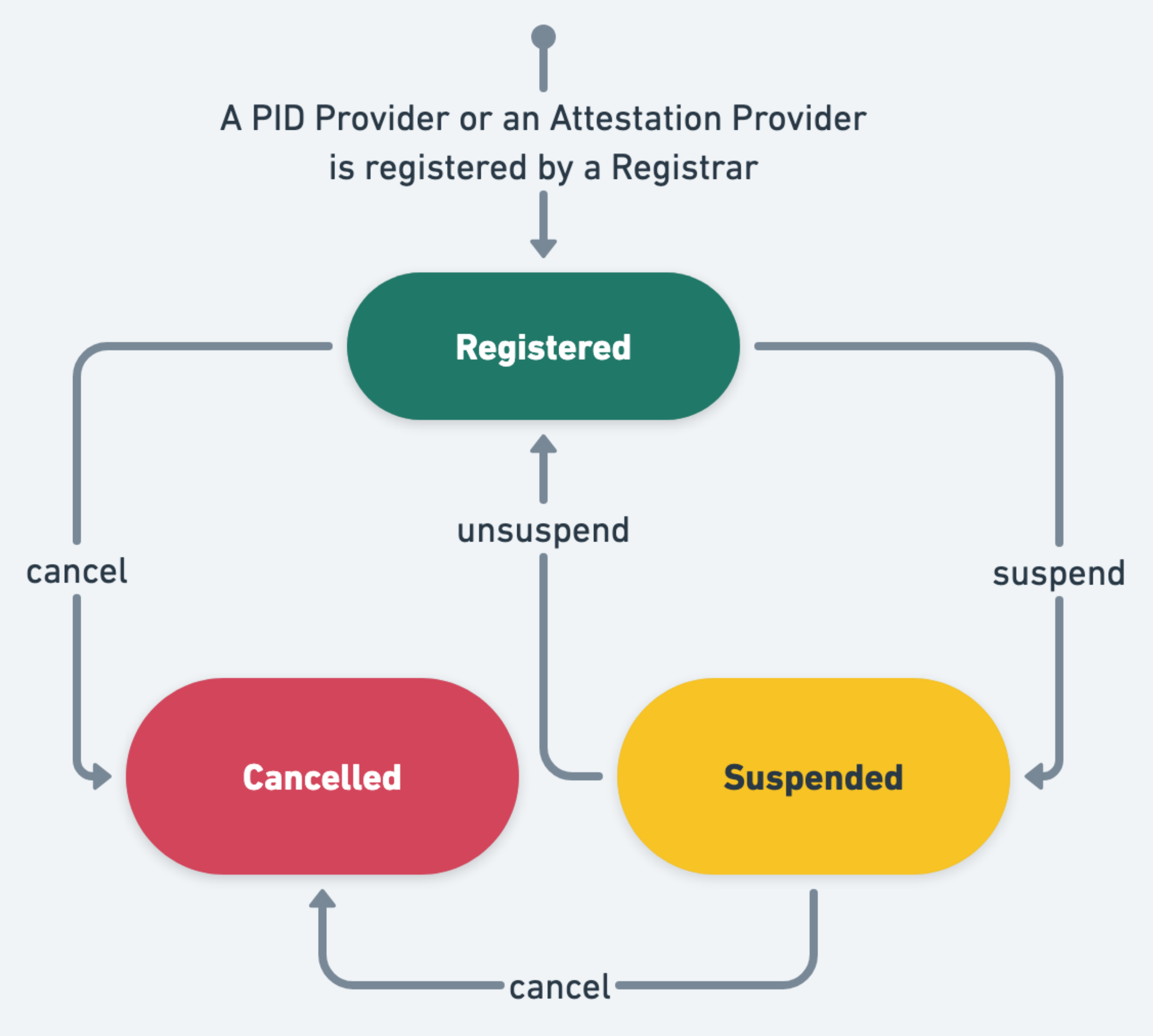

A PID Provider or an Attestation Provider is registered by a Registrar
Registered
cancel
unsuspend
suspend
Cancelled
Suspended
cancel

Figure 3: Figure 8

Figure 8: State diagram of PID Provider or Attestation Provider

The **Registered** state is the first state of a PID Provider or Attestation Provider. This means it is registered by a Member State Registrar and notified to the Commission, as described in Section 6.3.2.

The Registrar can temporarily suspend a PID Provider or Attestation Provider. This leads to the **Suspended** state. The Registrar can unsuspend the PID Provider or Attestation Provider, bringing it back to the **Registered** state. The Registrar can also decide to completely cancel registration of the PID Provider or Attestation Provider, which brings it in the **Cancelled** state.

For more information about suspension or cancellation, please refer to Section 6.3.3). A PID Provider or Attestation Provider with suspended or cancelled registration cannot issue PIDs or attestations to Wallet Units, nor will a PID or attestation issued by such a PID Provider or Attestation Provider be accepted by Relying Parties.

4.6.5 PID or attestation

Figure 9 shows the possible states of a PID or attestation.

In the context of the EUDI Wallet ecosystem, a PID or attestation begins its lifecycle when being issued to a Wallet Unit. Please note that this means that the management of attributes in the Authentic Source (adhering to national structures and attribute definitions) is outside the scope of the ARF.

For certain use cases, a PID or attestation may be pre-provisioned, meaning it is not yet valid when issued. In that case, its state is **Issued**, and it will transition to **Valid** when it reaches the beginning of its validity period. However, if a PID or attestation is issued on or after the validity start date, its state directly changes to **Valid**.

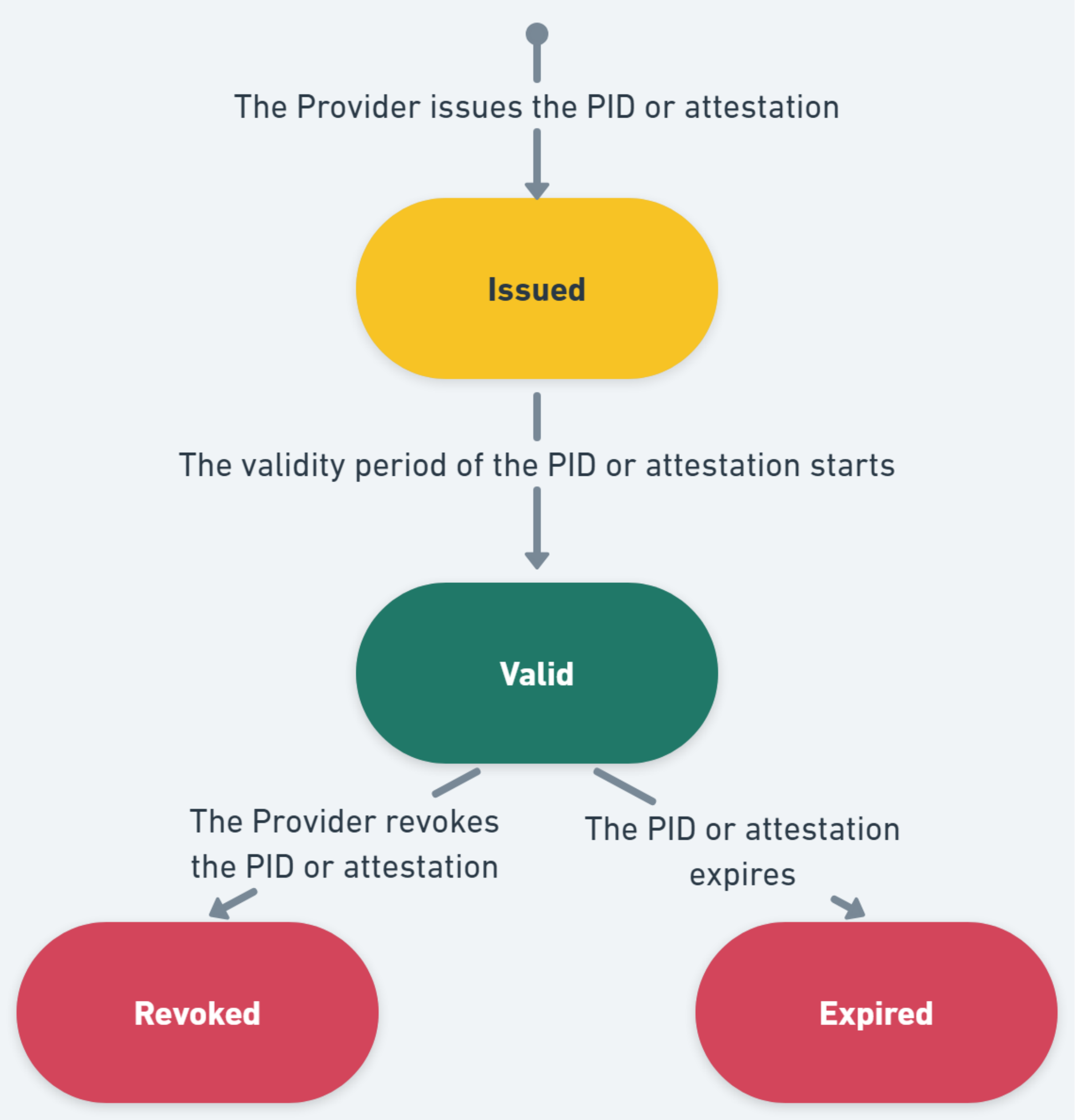

The Provider issues the PID or attestation
Issued
The validity period of the PID or attestation starts
Valid
The Provider revokes the PID or attestation
The PID or attestation expires
Revoked
Expired

Figure 4: Figure 9

Figure 9: State diagram of PID or attestation

There are two possible transitions for a valid PID or attestation: it expires by passing through the validity end date and transitions to the **Expired** state, or it is revoked by its PID Provider or Attestation Provider, ending up in the **Revoked** state. Expiration and revocation are independent transitions. Once a PID or attestation is expired or revoked, it cannot transition back to **Valid**.

4.6.6 Relying Party

Figure 10 shows the possible states of a Relying Party.

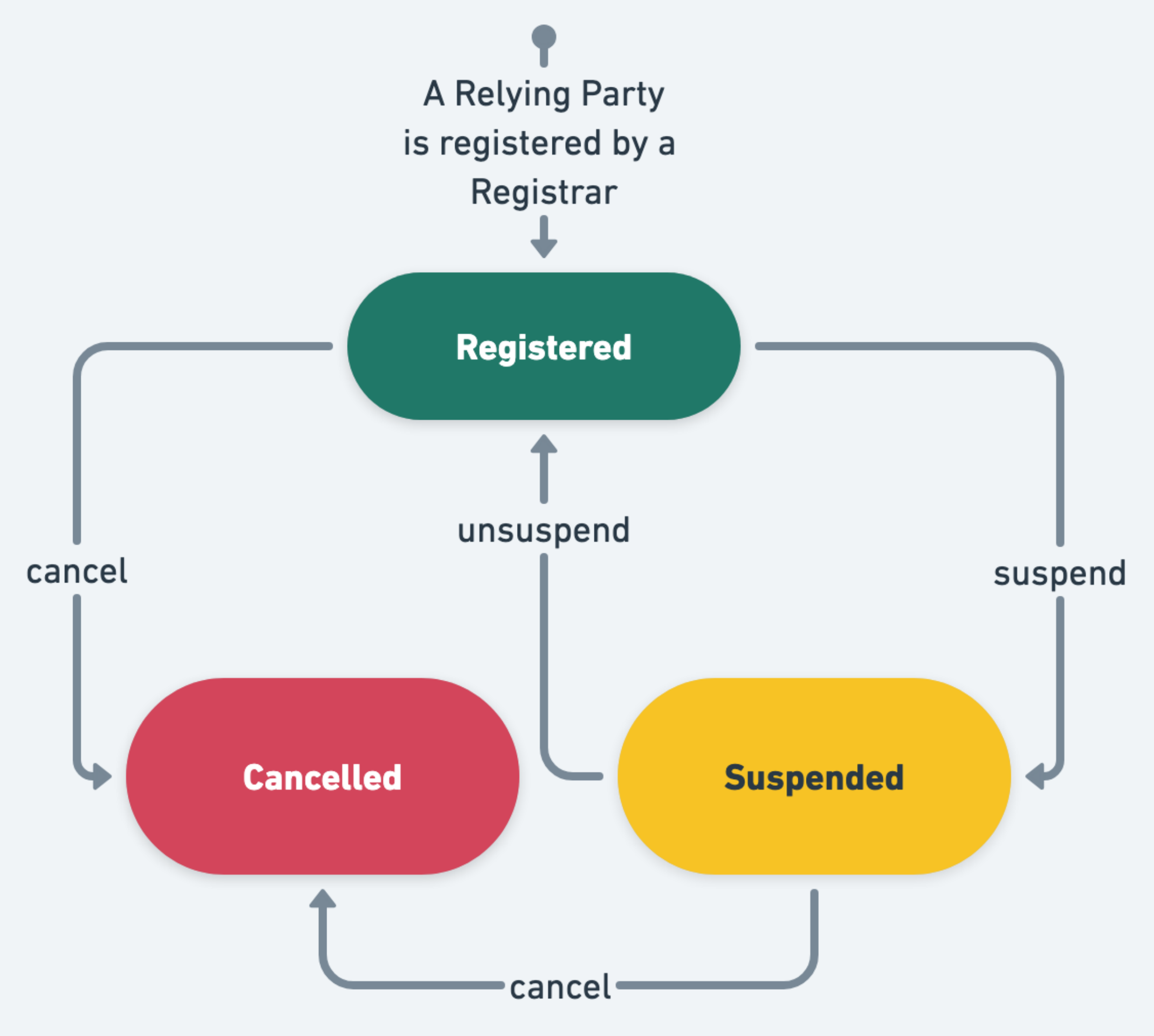


Figure 5: Figure 10

Figure 10: State diagram of Relying Party

The **Registered** state is the first state of a Relying Party. This means it has been registered by a Registrar, as described in Section 6.4.2.

The Registrar can suspend registration of a Relying Party. This leads to the **Suspended** state. The Registrar can unsuspend the Relying Party, bringing it back to the **Registered** state. The Registrar can also decide to completely cancel registration of the Relying Party, which brings it in the **Cancelled** state. For more information about suspension or cancellation, please refer to Section 6.4.3. A Wallet Unit will not present a PID or attestation to a Relying Party that has its registration suspended or cancelled.

4.7 Pseudonyms

4.7.1 Introduction to Passkeys

As specified in [CIR 2024/2979], [W3C WebAuthn] defines the technical specification for pseudonyms. Passkeys are a widely used type of credential which are created and asserted using the WebAuthn API.

Passkeys are to be seen as an alternative to passwords. The idea is that a User, when registering a user account at a service, uses a secure device to generate a public-private key pair, registers the public key at the service, and can then subsequently use the private key to authenticate towards the service at later points in time.

In a bit more detail, the flow for using Passkeys is as follows:

Registration:

1. The User generates a public-private key pair and stores both the public and the private key at their secure device (referred to as an Authenticator).
2. The User registers the public key at the desired Relying Party service.

Authentication:

1. When the User wishes to authenticate towards a service, the service will send them a challenge consisting of a random value.
2. The User uses the private key stored on their Authenticator to sign the challenge and sends this back to the service.
3. The service verifies that the signature on the challenge can be verified using the registered public key. If the signature verifies and the origin matches the expected origin, the User is considered authenticated and thereby granted access to the service.

For high-level requirements on the use of WebAuthn and Passkeys, see Topic 11. Note that the Commission will create or reference a technical specification containing all details necessary for Wallet Units and Relying Parties to generate, register, and use Pseudonyms.

4.7.2 Introduction to [W3C WebAuthn]

4.7.2.1 Overview

[W3C WebAuthn] defines an API for the creation and use of Passkeys. Conceptually, in addition to the User, there are four different logical components in this specification:

- **Relying Party Server:** The Relying Party that wishes to offer a service based on authentication using Passkeys.
- **Relying Party Client:** The program provided by the Relying Party that runs in the Client of the User and communicates with the Relying Party Server. The Relying Party Client is typically some JavaScript code, provided by the Relying Party, that runs on the Client (i.e., browser).
- **Client:** The client that the User uses to interact with the Relying Party's server and with the User's authenticator. The Client can be thought of as the browser that the User uses to access the Relying Party's service.
- **Authenticator:** The device controlled by the User to create, store, and use the Passkeys. In the context of the EUDI Wallet, the Wallet Unit is the Authenticator.

Note that the Relying Party Client and the Client are two programs that are executed on the same physical machine.

[W3C WebAuthn] defines a model dividing the responsibilities between these different entities and defines an interface between the Relying Party Client and the Client. Additionally, it defines a challenge/response protocol to authenticate with Passkeys. The interface is referred to as the *WebAuthn API*.

However, [W3C WebAuthn] does not specify how the Authenticator and the Client must communicate.

[W3C WebAuthn] relies on several different types of identifiers, including:

- **Relying Party ID:** An identifier unique to the Relying Party, which must be a valid domain string. This what the User will identify the Relying Party by and let the Authenticator learn which Relying Party is asking for registration/authentication.
- **Credential ID:** A unique identifier chosen by the Authenticator for each Passkey.

- **User ID:** An identifier unique to each User, which is assigned by the Relying Party. This will be provided to the Authenticator when registering a new Passkey. Subsequently, it will be provided by the Authenticator when authenticating towards the Relying Party. The Authenticator will keep track of which Passkeys are available for which User IDs and Relying Party IDs. The Relying Party keeps track of a User Name for each User ID.
- **User Name:** An alias that may be chosen by the User or the Relying Party and assigned to a specific Passkey on the Authenticator. This allows the User to easily distinguish and select which Passkey they want to authenticate with, if several are present in the Authenticator for the given Relying Party.

The next sections elaborate on how the different components work together to allow the registration and subsequent authentication using Passkeys.

4.7.2.2 Registration

The flow for registering a Passkey in [W3C WebAuthn] is the following:

0. The User requests (out of band of WebAuthn) the Relying Party to create a new Pseudonym.
1. The Relying Party Server creates a challenge and sends this along with the User ID, the Relying Party ID, and the User Name to the Relying Party Client.
2. The Relying Party Client forwards the information to the Client using the WebAuthnAPI.
3. The Client checks that the Relying Party ID is consistent with the caller's origin and forwards the information to the Authenticator along with other contextual data.
4. The Authenticator authenticates the User (for example using a PIN or via biometrics). It then generates a new key pair with a new Credential ID and set the scope of this to the specific Relying Party ID and User ID. Finally, the Authenticator may generate an attestation (explained in Section 4.7.2.3) and send this, as well as the public key and its Credential ID, to the Client.
5. The Client then forwards the information to the Relying Party Client that again forwards it to the Relying Party Server.
6. The Relying Party Server verifies the attestation (if present) and registers the received public key for this User ID.

Note that the Authenticator stores the public key in a way such that it is scoped uniquely to a specific Relying Party, aligning with the requirements of [CIR 2024/2979], Article 14 (2), which states that the pseudonyms must be unique to each Relying Party.

4.7.2.3 Pseudonym attestation

The term ‘attestation’ is here used differently than elsewhere in the ARF. In this context, the attestation is not about attributes of the User, but rather about attributes of the Authenticator. The attestation serves to ensure the Relying Party that they are talking with an Authenticator with certain attributes. The attestation often takes the form of a signature on the challenge as well as some other contextual data.

In [W3C WebAuthn], five different types of attestations are mentioned:

- **Basic Attestation:** The Authenticator stores a single master public and private key. The private key is used to sign all attestations and a certificate on the public key is included in the attestation data to allow the Relying Party to verify the signature.
- **Attestation CA:** Similar to the above, in the sense that the Authenticator stores a single master public and private key. However, instead of using this to attest Passkeys, the Authenticator uses this to authenticate towards a Certificate Authority (CA), which is configured to issue certificates to the Authenticator on multiple attestation key pairs. The Authenticator then uses these attestation private keys to sign attestations.
- **Anonymisation CA:** Similar to the second bullet above, except that it is explicit that the Authenticator requests a certificate for a new attestation key pair per generated Passkey.
- **Self Attestation:** The attestation is signed with the private key of the newly generated key pair in the Passkey. Note that this does not give any guarantees for the Relying Party about the Authenticator they are interacting with.
- **No Attestation Statement:** No attestation is given. Note that this does not give any guarantees for the Relying Party about the Authenticator they are interacting with.

Please note that Article 5a (5) a) viii) of the [European Digital Identity Regulation] states “*European Digital Identity Wallets shall, in particular support common protocols and interfaces: … for relying parties to verify the authenticity and validity of European Digital Identity Wallets;…*”. The latter two forms of attestation do not align with this requirement. Section 5.1 of the Discussion Paper for Topic E discusses how the other three possibilities relate to privacy risks about User surveillance identified in Section 7.4.3.5.

4.7.2.4 Authentication

The flow for authentication using a Passkey following [W3C WebAuthn] is:

1. The Relying Party Server creates a challenge and sends this along with its Relying Party ID to the Relying Party Client.
2. The Relying Party Client forwards the information to the Client using the WebAuthn API.
3. The Client checks that the Relying Party ID is consistent with the caller's origin and forwards the information to the Authenticator along with other contextual data.
4. The Authenticator authenticates the User (for example using a PIN or via biometrics). It then prompts the User to select one of the Passkeys scoped to this Relying Party ID, if there are multiple. For this step the User Name can be presented to the User. Finally, the Authenticator uses the private key of the chosen key pair (= Passkey) to sign the challenge as well as some contextual data including the User ID, Credential ID, and the Relying Party ID. The Authenticator then sends this to the Client.
5. The Client forwards the information to the Relying Party Client, which again forwards it to the Relying Party Server.
6. The Relying Party Server verifies the signature with the stored public key for this User ID and Credential ID, and, depending on the outcome of this verification, considers the User to be authenticated.

5 Data model and data exchange protocols

5.1 Attestation elements

Within the EUDI Wallet ecosystem, data is exchanged in the form of Electronic Attestations of Attributes (EAA), hereafter referred to as 'attestations.' Apart from EAA, the [European Digital Identity Regulation] explicitly defines another category of data, called Person Identification Data (PID), see Section 5.2.

The subject of a PID is a natural person. The subject of an attestation is a natural person, a legal person, or an object. For example, the subject of a digital product passport would be a product. In addition, some attestations do not have a subject. For example, a voucher may be valid for any User that can present it to a Relying Party. This is comparable to the concept of a 'bearer token'.

Each PID and attestation consists of the following key elements:

- A set of **attributes**, which provide information, typically about the subject of the attestation. A Relying Party will request one or more of these attributes to get the reliable information they need to provide some service to the User. The set of attributes that an attestation may contain is defined in an attestation scheme, see below.

- A set of **metadata**, meaning information about the attestation itself, such as its attestation type (PID, mDL, diploma, etc.), its Attestation Provider, and its administrative validity period, if applicable. This kind of metadata is also defined in an attestation scheme. In addition, metadata also includes information that is necessary to ensure the security of the attestation. This includes at least its technical validity period. For PIDs and device-bound attestations, it also includes a public key of the PID or attestation, which a Relying Party will use to verify that the PID or attestation was not copied, see Section 6.6.3.8. It may also include information allowing the Relying Party to verify that the PID or attestation was not revoked, see Section 6.6.3.7.
- A **proof**, which ensures the integrity, authenticity, and support of selective disclosure of the attestation. The format of the proof complies with the proof mechanism specified for this type of attestation, see below. The proof includes information that enables a Relying Party to verify the proof, for example a Attestation Provider certificate and a reference to a trust anchor that can be used to verify that certificate.

An **attestation scheme** defines the logical organisation of all mandatory and optional attributes within an attestation, as well as the format of each attribute, meaning its unique identifier, encoding, allowed values, and serialisation. In addition, an attestation scheme specifies some of the attestation metadata, such as its attestation type and information about its Attestation Provider, validity period, etc. Within the EUDI Wallet ecosystem, the attestation scheme for each attestation type may be specified by an Attestation Scheme Provider, next to an Attestation Rulebook; see Section 5.4.

A **proof mechanism** defines the method used to create the attestation proof. For example, a ‘standard’ digital signature is a proof ensuring integrity and authenticity, but not allowing selective disclosure. Proof mechanisms are specified in standards or technical specifications. The attestation formats listed in Section 5.3 either specify a proof mechanism that allows for selective disclosure, or leave it to other technical specifications to do so.

5.2 Attestation categories

5.2.1 Overview

Within the European Digital Identity Wallet ecosystem, the [European Digital Identity Regulation] distinguishes four legal categories of attestations:

- Person Identification Data (PID),
- Qualified Electronic Attestation of Attributes (QEAA),
- Electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source (PuB-EAA),
- Non-Qualified EAA.

The next subsections give more information about each of these categories. Please note that the differences between them are purely legal. For example, a diploma may be a QEAA or a non-qualified EAA, depending on whether it is issued by a qualified trust service provider (QTSP) or by an unqualified one. Similarly, an mDL may be issued as a PuB-EAA, a QEAA, or a non-qualified EAA, depending on the legal status of the party issuing mobile driving licences in each Member State. From a technical point of view, all PIDs, QEAAs, PuB-EAAs, and EAAs comply with one of the attestation formats listed in Section 5.3.

5.2.2 Person Identification Data (PID)

A PID is a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.

Besides the fact that the Regulation defines the PID as a category of data that is legally distinct from Electronic Attestations of Attributes (EAA), another difference between PID and EAA is that the presence or absence of a valid PID determines whether a Wallet Unit is in the Operational or the Valid state, as discussed in Section 4.6.3.

As implied in that section, it is possible for a Wallet Unit to contain multiple PIDs. If the User has multiple nationalities, they may be able to receive a PID from multiple PID Providers in a single Wallet Unit. However, please note that a Wallet Provider is free to decide that its Wallet Unit does not support all PID Providers, and that, conversely, a PID Provider may decide that it does not support all Wallet Solutions; see Section 6.5.2.3. Note that the subject of all PIDs in the Wallet Unit will be the same person, namely the User of the Wallet Unit.

For more information, please refer to Section 3.4.

5.2.3 Qualified Electronic Attestation of Attributes (QEAA)

A QEAA is an electronic attestation of attributes which is issued by a qualified trust service provider (QTSP) and meets the requirements laid down in Annex V of the Regulation. For more information, please refer to Section 3.6.

5.2.4 Electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source (PuB-EAA)

A PuB-EAA is an electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII of the Regulation.

For more information, please refer to Section 3.7.

5.2.5 Non-Qualified Electronic Attestation of Attributes (EAA)

A non-qualified EAA is an EAA which is not a QEAA or a PuB-EAA. For more information, please refer to Section 3.8.

5.3 Attestation formats and proof mechanisms

5.3.1 Overview

Section 5.1 listed a proof mechanism as one of the key elements needed to define a type of attestation. The proof mechanism for an attestation is closely related to the format of that attestation. Within the EUDI Wallet ecosystem, the following standardised formats for electronic attestations of attributes can be used:

- The format specified in [ISO/IEC 18013-5] and generalised in [ISO/IEC 23220-2],
- The format specified in 'SD-JWT-based Verifiable Credentials' [SD-JWT VC],
- The format specified in 'W3C Verifiable Credentials Data Model v2.0' [W3C VCDM 2.0].

The next subsections give more information about each of these formats and specifications, and explain where the different elements of an attestation, as explained in Section 5.1 are defined for that attestation format.

Within the EUDI Wallet ecosystem, Wallet Units will support the first two formats above. Support for the third format is optional and meant for non-qualified EAAs only. Topic 12 states the detailed requirements regarding support by Wallet Units, PID Providers, and Attestation Providers for these formats and specifications.

5.3.2 ISO/IEC 18013-5 and ISO/IEC 23220-2

The ISO/IEC 18013-5 standard was originally developed as a standard for mobile driving licences (mDL) and mDL readers. In terms of this ARF, an mDL is a Wallet Unit containing an mDL attestation (as defined in the mDL Rulebook), while an mDL reader is a Relying Party requesting such an attestation.

ISO/IEC 18013-5 specifies:

- An attestation scheme containing all attributes and metadata for an mDL. The scheme specifies the semantics of these attributes and metadata, as well as their encoding in Concise Binary Object Representation (CBOR), see [RFC 8949]. The standard also specifies the use of namespaces to avoid collision of attribute identifiers.
- A proof mechanism ensuring the authenticity and integrity of a PID or attestation, while allowing selective disclosure of attributes.
- A mandatory security mechanism enabling device binding of PIDs and attestations, see Section 6.6.3.8,
- All other aspects necessary to securely request, present, and verify an mDL attestation in proximity flows, see Section 5.6.1.2).

Points to note about ISO/IEC 18013-5:

- the mDL attestation scheme (see first bullet above) is the only aspect of ISO/IEC 18013-5 that is specific for mDLs. All other aspects are generic and can be used for any other attestation type, including PIDs. This means that another ISO/IEC 18013-5-compliant attestation type can be created simply by specifying an appropriate attestation scheme using CBOR, and referring to ISO/IEC 18013-5 for all other details. Please refer to Chapter 4 of the PID Rulebook for an example. Within the EUDI Wallet ecosystem, such an attestation scheme is specified in an Attestation Rulebook, see Section 5.4. ISO/IEC 23220-2 specifies a generic set of attributes for use in different attestation types, and also specifies how these can be encoded in CBOR.

- An ISO/IEC standard for mobile documents in general (not mDLs specifically) is in preparation and will become ISO/IEC 23220-4. This standard will generalise ISO/IEC 18013-5, in the sense that it will allow more options and communication flows. Once that standard is published, all references in this ARF to ISO/IEC 18013-5 may be replaced by appropriate references to ISO/IEC 23220-4. However, at the moment ISO/IEC 23220-4 is not finished yet and therefore cannot be referenced.

5.3.3 SD-JWT VC

'SD-JWT-based Verifiable Credentials' [SD-JWT VC] specifies a data format and processing rules to express verifiable credentials (i.e., attestations). "SD-JWT" here stands for 'Selectively Disclosable JSON Web Token'. As that name suggests, SD-JWTs are a special form of JWTs [RFC 7519] that are selectively disclosable. The mechanisms used to make them selectively disclosable is often described as using 'salted hashes', and is conceptually identical to the mechanism used for the same purpose in [ISO/IEC 18013-5].

[SD-JWT VC] specifies the following aspects:

- The encoding to be used for attributes and metadata, namely JSON, as well as rules to prevent collisions of claim names,
- A proof mechanisms ensuring the authenticity and integrity of a PID or attestation, while allowing selective disclosure of attributes, see above.
- A security mechanism enabling device binding of PIDs and attestations, see Section 6.6.3.8. This mechanism is optional in [SD-JWT VC].

In addition to these aspects, within the EUDI Wallet ecosystem,

- attestation schemes for specific SD-JWT VC-compliant attestation types will be specified in Attestation Rulebooks, see Section 5.4. Please refer to Chapter 5 of the PID Rulebook for an example.
- SD-JWT VC-compliant attestations will be requested and presented using [OpenID4VP], see Section 5.6.1.3.

Since [SD-JWT VC] contains a number of options, the use of the profile for SD-JWT VCs specified in [HAIP] is necessary to ensure interoperability between Wallet Units and Relying Parties.

5.3.4 W3C Verifiable Credentials

The W3C Verifiable Credentials Data Model [W3C VCDM 2.0] defines a general data model, offering a high-level structure but leaving many technical aspects open for further definition, including:

- Security mechanisms
- Signature formats
- Transport protocols

Key features of W3C VCDM are:

- JSON-LD (Linked Data)-based: The use of JSON-LD ensures structured and interoperable data exchange, but introduces complexity.
- Extensible Framework: Allows different implementations but requires additional specifications.
- Security and Signature Formats: Not inherently defined — must be specified separately.

To implement W3C VCDM-based attestations, separate specifications are needed for security mechanisms and signatures, such as:

1. 'Securing Verifiable Credentials using JOSE and COSE' [W3C VC-JOSE-COSE]: Defines how to use one of the following to secure attestations in the VCDM model:
    - a JWT (see [RFC 7519]),
    - a SD-JWT (see the previous section), or
    - a CBOR Web Token (CWT, see [RFC 8392]).
2. 'Verifiable Credential Data Integrity' [W3C VC Data Integrity]: Provides a cryptographic proof format independent of JWT or CWT, relying on detached proofs (not embedded signatures) for better flexibility.

These mechanisms offer different trade-offs, allowing PID Providers or Attestation Providers and Relying Parties to choose the appropriate security model based on their privacy, interoperability, and trust requirements. In order to achieve interoperability, the specification of a profile standard making specific choices will be necessary.

In addition to these aspects, within the EUDI Wallet ecosystem,

- attestation schemes for specific W3C VCDM-compliant attestation types (if any) will be specified in Attestation Rulebooks, see Section 5.4.
- W3C VCDM-compliant attestations may be requested and presented using [OpenID4VP], see Section 5.6.1.3. However, this ARF does not require this, and for any W3C VCDM-compliant attestation, the applicable transport protocol must be defined in the corresponding Rulebook.

See chapters 3 and 4 of the Discussion Paper for Topic V for more considerations regarding the SD-JWT VC and W3C Verifiable Credential formats and their interoperability within the EUDI Wallet ecosystem.

5.4 Attestation Rulebooks and Attestation schemes

5.4.1 Introduction

An **Attestation Scheme Provider** defines a type of attestation (e.g., PID, mDL, diploma) and publishes a **human-readable Attestation Rulebook** that explains what the attestation is and how it works: which attributes it contains, what each attribute means, how the attributes are encoded, how proofs are produced, and, where needed, how trust and presentation are handled. When the attestation is listed in the European Commission's **catalogue of attestation schemes** (the official index that lets ecosystem participants discover and reuse attestation types), the Attestation Scheme Provider also includes a **machine-readable attestation scheme**, so software can automatically build requests to Wallet Units and verify responses. In short: the **Rulebook** is the documentation for people, the **scheme** is the specification for software, and the **catalogue** is where everyone finds them.

Section 5.1 listed an attestation scheme as a key element of any attestation type. This section introduces the **Attestation Rulebook**, which, for each attestation type, **specifies**:

- the **attestation scheme** and proof mechanisms;
- where required, the **trust mechanisms** for authentication and authorisation;
- the **unique identifiers, syntax/encodings, and semantics** of all attributes that may appear in the attestation;

- the **presentation protocol(s)** that relevant attestations must support.
  The requirements for Rulebooks are defined in Topic 12.

5.4.2 Who defines Rulebooks and schemes

Attestation Rulebooks are defined by **Attestation Scheme Providers** (see Section 3.15). This role can be held by:

- **The European Commission**, in consultation with EDICG, currently the PID Rulebook and the mDL Rulebook.

- **Public Administration, sectoral or cross-border organisations** representing relevant stakeholders, to avoid duplicative Rulebooks (e.g., for diplomas) and unnecessary syntax/semantic divergence. Selection of the responsible organisation is out of scope for this document.

- **Individual Attestation Providers**, when they must include **domestic or provider-specific attributes** not covered by the EU-wide or sectoral Rulebook (see Topic 12).
- **Single organisations** for attestations intended solely for internal use.

5.4.3 Publication in the catalogue

An Attestation Scheme Provider may publish a new attestation in the **catalogue of attestation schemes** to enable discovery by Relying Parties and other actors (see Section 5.5.3). When doing so, the provider **also supplies the machine-readable attestation scheme** in accordance with Technical Specification 11.

5.5 Catalogue of attributes and catalogue of attestation schemes

5.5.1 Introduction

Article 45e(2) of Regulation (EU) 2024/1183 empowers the Commission to establish **specifications and procedures** for: (i) the **catalogue of attributes**, (ii) the **catalogue of attestation schemes**, and (iii) **verification procedures** for qualified electronic attestations of attributes.

The objective of this provision is to reach a high level of interoperability:

- **Technical interoperability** through common standards, protocols, and technical specifications enabling issuance, presentation, and processing of attestations (see Sections 5.3 and 5.6).
- **Semantic interoperability** through clear definitions of attestation contents, i.e., which attributes exist for each attestation type and their identifiers, syntax, and semantics (see Section 5.4).

To support discovery and re-use across the EUDI Wallet ecosystem, two Commission-run catalogues are defined:

- a **Catalogue of attributes** that draws on authentic public-sector sources (see Section 5.5.2); and
- a **Catalogue of attestation schemes** for QEAAs, PuB-EAAs, and EAAs (see Section 5.5.3).

5.5.2 Catalogue of attributes

The catalogue of attributes is exclusively intended for use by QTSPs issuing QEAAs, and enables them to find the access point of the Authentication Source responsible for a given attribute, at which the QTSP can verify the value of that attribute for a given User. This verification is discussed in Topic 42 in Annex 2.

See Topic 25 and Commission Implementing Regulation 2025/1569, particularly Article 7, for the high-level requirements for the catalogue of attributes.

For more details, see also the Discussion Paper on Topic O. Detailed interface specifications for registering and managing attributes in the catalogue and for querying the catalogue can be found in Technical Specification 11.

5.5.3 Catalogue of attestation schemes

The catalogue of attestation schemes is intended for use by Relying Parties, Attestation Providers, and other actors in the EUDI Wallet ecosystem. It enables them to discover which types of attestations already exist within the ecosystem, and to understand the identifiers, syntax, and semantics of all attributes within each type of attestation.

This section defines the following principles for the catalogue of attestation schemes:

- Attestation schemes are machine-readable, and each attestation scheme published in the catalogue refers to the corresponding human-readable Attestation Rulebook.
- Attestation schemes for QEAAs and PuB-EAAs used within the EUDI Wallet ecosystem may be registered and published in the catalogue of attestation schemes, but this is not mandatory.
- The catalogue of attestation schemes may also include attestation schemes for non-qualified EAAs. Registration and publication of non-qualified EEAs is not mandatory.
- The Commission will take measures to establish and maintain the catalogue of attestation schemes.
- The catalogue of attestation schemes will be publicly accessible.
- Registration of attestation scheme in the catalogue does not create any obligation for acceptance of the relevant type of attestation by any actor in the EUDI Wallet ecosystem. Neither does it automatically imply cross-border recognition of the type of attestation.
- Where possible, existing tools created by Member States, the Commission and cross-border organisations, will be used to connect to the catalogue and to interact with its

stakeholders. Also, mechanisms to add new and existing data sets to the catalogue will be implemented.

See Topic 26 and Commission Implementing Regulation 2025/1569, particularly Article 8, for the high-level requirements for the catalogue of attributes.

For more details, see also the Discussion Paper on Topic O. Detailed interface specifications for registering and managing attestation schemes in the catalogue and for querying the catalogue can be found in Technical Specification 11.

5.6 Protocols for secure data exchange between Wallet Units and Relying Parties

5.6.1 Attestation presentation

5.6.1.1 Introduction

Within the EUDI Wallet ecosystem, the protocol specified in ISO/IEC 18013-5 is used for proximity attestation presentation flows, while the protocol specified in OpenID4VP is used for remote attestation presentation flows. This section briefly describes both of these protocols.

5.6.1.2 Proximity attestation presentation using ISO/IEC 18013-5

ISO/IEC 18013-5 specifies the following aspects related to secure data exchange for attestation presentations:

1. Message structures and transaction flows allowing a Wallet Unit and a Relying Party to request and present attestations.
2. Proximity interface specifications, allowing a Wallet Unit and a Relying Party to set up a communication channel using QR code or NFC, and to subsequently communicate over BLE, NFC, or Wi-Fi Aware.
3. Security mechanisms ensuring
    - the confidentiality and authenticity of all data exchanged between a Wallet Unit and a Relying Party,
    - Relying Party authentication, see Section 6.6.3.2.

As already explained in Section 5.3.2, although ISO/IEC 18013-5 nominally specifies the mobile driving licence, all of the above aspects are generic and can be used for any type of attestation.

Whereas ISO/IEC 18013-5 specifies proximity transaction flows only. ISO/IEC 18013-7 specifies how to request and present ISO/IEC 18013-5-compliant attestations in remote transaction flows.

5.6.1.3 Remote attestation presentation using [OpenID4VP]

The [OpenID4VP] standard defines message structures, transaction flows, and an HTTP-based interface specification for attestation presentations by Wallet Units to Relying Parties. [OpenID4VP] also specifies security mechanisms ensuring:

- the confidentiality and authenticity of all data exchanged between a Wallet Unit and a Relying Party,
- Relying Party authentication.

[OpenID4VP] is suitable only for remote presentation transaction flows.

[OpenID4VP] can be used for presenting attestations in different formats, including especially the formats used within the EUDI Wallet ecosystem. Within this ecosystem, [SD-JWT VC]-compliant attestations are always requested and presented using [OpenID4VP], while [ISO/IEC 18013-5]-compliant attestations are requested and presented using [OpenID4VP] in remote transaction flows.

Since [OpenID4VP] contains a number of options, the use of the profile for ‘OpenID for Verifiable Presentations for IETF SD-JWT VC’ specified in [HAIP] is necessary to ensure interoperability between Wallet Units and Relying Parties.

5.6.2 Transactional data using [ISO/IEC 18013-5] and [OpenID4VP]

In some use cases, a Relying Party must be able to include additional data in the attestation presentation request. Primary examples include strong customer authentication for payments, see Section 2.6.4, and the creation of qualified electronic signatures, see Section 2.4. In the case of strong customer authentication for payments, the Relying Party sends payment information, such as the payment amount and the payee, to the Wallet Unit. In the case of electronic signatures, the Relying Party may send (a representation of) data to be signed to the Wallet Unit. In Topic 20, such data is called transactional data.

The Wallet Unit will process the transactional data in a use-case specific way, and, after consulting the User, will sign a (representation of the) transactional data to authenticate it.

The Wallet Unit will then return the signed data in the presentation response, together with the presented attributes, if any.

Both [ISO/IEC 18013-5] and [OpenID4VP] allow for sending, authenticating, and returning transactional data. In both protocols, the presentation request can be extended with use-case specific (proprietary) transactional data. The Wallet Unit can subsequently sign this data by including it in the device binding process, see Section 6.6.3.8. Therefore, no extensions of the presentation response are necessary to return the signed transactional data.

6 Trust model

6.1 Scope

This chapter explains how trust works in the EUDI Wallet system, how it is established, maintained, validated, and managed. It describes the rules and assumptions that decide whether different parts of the system, like a wallet app, a user's device, or a service provider, can be trusted.

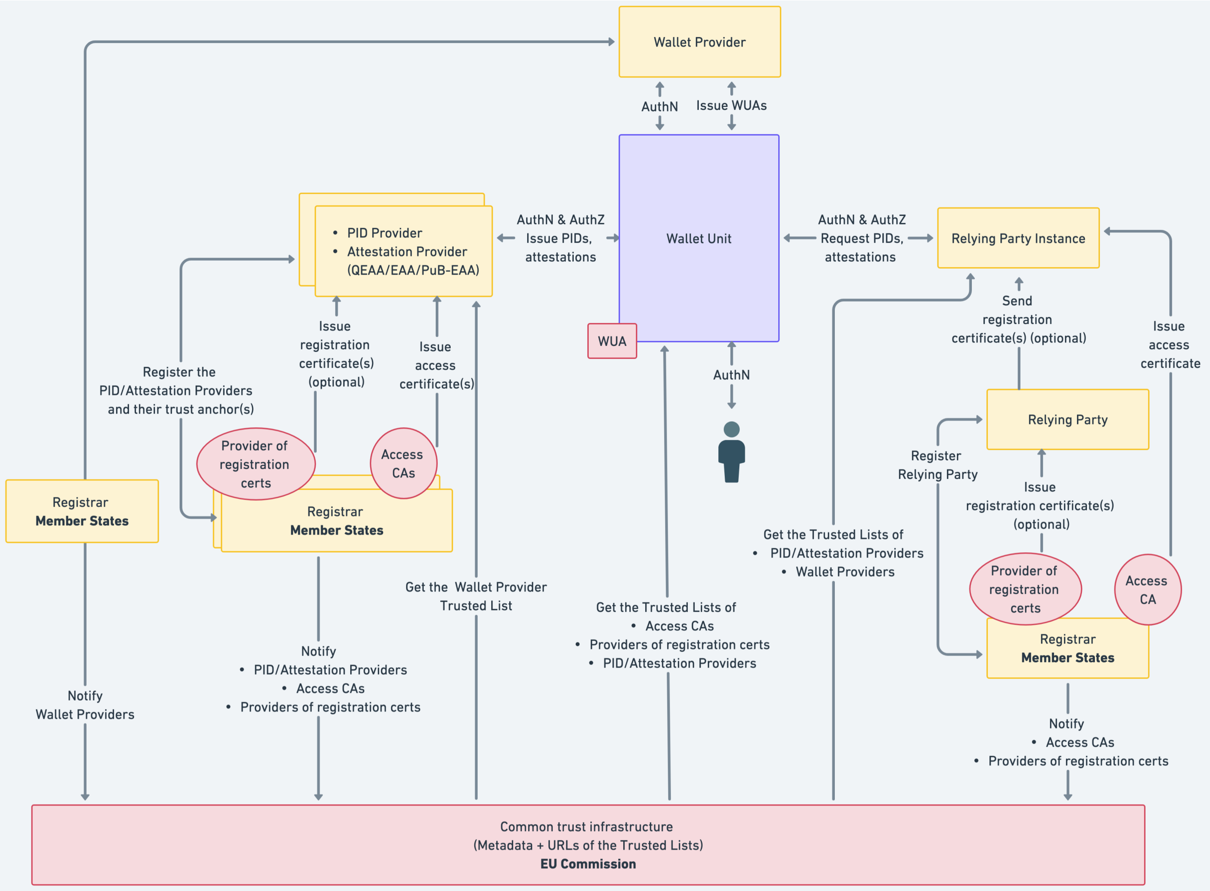

Wallet Provider
AuthN
Issue WUAs
Wallet Unit
WUA
AuthN
PID Provider
Attestation Provider (QEAA/EAA/PuB-EAA)
AuthN & AuthZ Issue PIDs, attestations
AuthN & AuthZ Request PIDs, attestations
Relying Party Instance
Send registration certificate(s) (optional)
Issue access certificate
Relying Party
Register Relying Party
Issue registration certificate(s) (optional)
Provider of registration certs
Access CA
Registrar Member States
Notify
• Access CAs
• Providers of registration certs
Get the Trusted Lists of
• PID/Attestation Providers
• Wallet Providers
Get the Trusted Lists of
• Access CAs
• Providers of registration certs
• PID/Attestation Providers
Get the Wallet Provider Trusted List
Issue registration certificate(s) (optional)
Issue access certificate(s)
Register the PID/Attestation Providers and their trust anchor(s)
Provider of registration certs
Access CAs
Registrar Member States
Notify
• PID/Attestation Providers
• Access CAs
• Providers of registration certs
Registrar Member States
Notify Wallet Providers
Common trust infrastructure
(Metadata + URLs of the Trusted Lists)
EU Commission

Figure 6: Figure 11

Figure 11 illustrates the main entities and their relationships in the trust model of the EUDI Wallet ecosystem.

At its core is the **Wallet Unit** (top middle, blue), which interacts with various entities throughout its lifecycle. The Wallet Unit lifecycle is detailed in Section 6.5 and consists of installation, activation, management, and uninstallation. Each Wallet Unit is a configuration of a **Wallet Solution**, comprising a **Wallet Instance** and one or more WSCA/WSCDs, provided by a **Wallet Provider**. The Wallet Provider oversees these components and manages their registration, cancellation, or suspension (see Section 6.2). The Wallet Provider ensures that a valid Wallet Unit is in possession of at least one **Wallet Unit Attestation (WUA)**, to enable other entities to authenticate the Wallet Unit. The Wallet Provider can revoke the WUAs if needed.

The Wallet Unit handles User **PIDs** and **attestations** (QEAAs, PuB-EAAs, and non-qualified EAAs). PIDs are issued by **PID Providers** and attestations by **Attestation Providers**, both positioned to the left of the Wallet Unit in Figure 11. Before interacting with a Wallet Unit, these Providers must be registered by a **Registrar**. Upon registration, they receive an **access certificate** from a **Access Certificate Authority** associated with the Registrar. They may optionally obtain a **registration certificate** from an associated **Provider of registration certificates**. See Section 6.3.

After a Wallet Unit has received a PID or attestation, it can present **User attributes** to **Relying Party Instances** (right side of Figure 11). These instances are hardware/software setups enabling **Relying Parties** to interact with Wallet Units. Like PID Provider or Attestation Providers, Relying Parties register with a **Registrar**, and receive an **access certificate** for each of their Relying *Party Instances. A Relying Party may optionally obtain one or more* **registration certificates** from a Provider of registration certificates *associated with the Registrar. This is discussed in Section 6.4.

Notes:

- This conceptual trust model may be implemented with slight variations across Member States, such as adopting one or multiple Certification Authorities or leveraging existing entities that already fulfil this role.
- For PIDs, qualified EAAs, PuB-EAAs, access certificates, and registration certificates, interoperability is essential (Section 4.2.3). Interoperability is achieved by using a PKI following X.509 certificate standards (RFC5280, RFC3647). Non-qualified EAAs may adopt alternative trust models and verification mechanisms.
- The model supports both remote and proximity use cases, though technical measures and authentication mechanisms may vary.
- This version of the ARF does not yet include trust interactions for qualified electronic signatures or seals; see Topic 16 and Topic 37 in Annex 2.
- Besides the trust relationships described in this chapter, other trust relations are established as well. For instance, Users, PID Providers, Attestation Providers, and Relying Parties trust certification bodies and Trusted List Providers. This trust is primarily rooted in authority and in procedural measures, such as public oversight, published security and operational policies, and audits, rather than in technical measures. To verify that entities are indeed interacting with a trusted authority, standard technical measures suitable for the context will be used.

6.2 Trust throughout a Wallet Solution lifecycle

6.2.1 Wallet Solution lifecycle

Section 4.6.2 presented the lifecycle of a Wallet Solution:

1. The Wallet Provider responsible for the Wallet Solution is notified to the Commission by a Member State. As a result, the Wallet Solution enters the Valid state. This is discussed in Section 6.2.2.
2. Under specific conditions, a Member State may decide to suspend or cancel a registered Wallet Provider. This is discussed in Section 6.2.3.

6.2.2 Wallet Provider registration and notification

Figure 11 depicts the Wallet Provider to the top of the Wallet Unit. To the left and below of this, the figure also shows that a Wallet Provider registers itself and its Wallet Solution with a Wallet Provider Trusted List Provider in its Member State. Subsequently, the Member State notifies the Wallet Provider to the European Commission.

The Wallet Solution provided by the Wallet Provider is certified as described in Chapter 7.

If the registration and notification processes are successful, the trust anchors of the Wallet Provider are included in a Wallet Provider Trusted List. During issuance of a PID or an attestation, the PID Provider or the Attestation Provider can use these trust anchors to verify the authenticity of a Wallet Unit Attestation signed by the Wallet Provider, so they can be sure they are dealing with an authentic Wallet Unit from a trusted Wallet Provider. See Section 6.6.2.3, Topic 9 and Topic 38.

If a certain entity offers multiple Wallet Solutions, they will register as a separate Wallet Provider for each of these Wallet Solutions. This implies that such an entity will register different trust anchors for each of their Wallet Solutions.

More details on the Wallet Provider notification process can be found in Topic 31.

6.2.3 Wallet Provider suspension or cancellation

Under specific conditions, a Member State may decide to suspend or cancel a Wallet Provider. This implies that the Wallet Provider’s status in the respective Trusted List will be changed to Invalid. As a result of this status change, PID Providers, Attestation Providers, and Relying Parties will no longer trust the trust anchors of the Wallet Provider and will therefore refuse to interact with any Wallet Unit provided by that Wallet Provider.

When a Member State cancels a Wallet Provider, the Wallet Provider revokes all valid WUAs for all Wallet Units.

If an entity has registered multiple Wallet Providers, each offering a different Wallet Solution, and one of these Wallet Providers is suspended or cancelled, only the applicable Wallet Solution will be impacted. It may happen that the reason for suspension or cancellation is applicable to all Wallet Solutions offered, in which case all of the Wallet Providers registered by that entity will be cancelled or suspended separately.

6.3 Trust throughout a PID Provider or an Attestation Provider lifecycle

6.3.1 PID Provider or Attestation Provider lifecycle

Section 4.6.4 presented the lifecycle of a PID Provider or Attestation Provider:

1. A PID Provider or an Attestation Provider is registered by a Trusted List Provider in its Member State. This is discussed in Section 6.3.2.
2. Under specific conditions, a Trusted List Provider may decide to suspend or cancel registration of a registered PID Provider or Attestation Provider. This is discussed in Section 6.3.3.

6.3.2 PID Provider or Attestation Provider registration and notification

6.3.2.1 Introduction

Figure 11 depicts the PID Providers and Attestation Providers to the left of the Wallet Unit. To the left and below of this, the figure also shows that each PID Provider and Attestation Provider will register itself with a Registrar in its Member State. The Member State notifies the PID Provider or Attestation Provider to the European Commission.

If the registration and notification processes are successful, at least the following happens:

- Data about the PID Provider or Attestation Provider is included in the registry of the relevant Registrar.
- The PID Provider or Attestation Provider receives an access certificate and optionally one or more registration certificates.
- The trust anchors of the PID Provider or Attestation Provider are included in a Trusted List.

These processes are discussed in the next subsections.

6.3.2.2 Data about the PID Provider or Attestation Provider is included in the registry

When a PID Provider or Attestation Provider is registered, the Registrar registers a set of data about the PID Provider or Attestation Provider in its register. The Registrar makes the contents of the register available to the general public, both in machine-readable and human-readable format.

The data to be registered about a PID Provider, QEAA Provider, PuB-EAA Provider, or EAA Provider includes the attestation type(s) that the Provider intends to issue to Wallet Units. This enables Wallet Units and Relying Parties to verify that a given PID Provider or Attestation Provider registered its intent to issue a specific attestation type. For example, a PuB-EAA Provider may have registered for issuing mDLs, but not to issue diplomas.

Regarding PID Providers or QEAA Providers it may be argued that Wallet Units do not have to do this verification, since these are trusted parties. Nevertheless, it is beneficial if a Wallet Unit verifies if a PID Provider or QEAA Provider is registered for issuing a PID or a particular type of QEAA, prior to requesting the issuance of such a PID or QEAA. Doing this helps to prevent attempts to issue a PID or attestation while not being entitled to do so, either fraudulently or as a result of an error.

6.3.2.3 PID Provider or Attestation Provider receives an access certificate and a registration certificate

When a PID Provider or Attestation Provider is registered by a Member State, a Access Certificate Authority (see Section 3.18 issues one or more access certificates to the PID Provider or to the Attestation Provider. A PID Provider or an Attestation Provider needs such a certificate to authenticate itself towards a Wallet Unit when issuing a PID or an attestation to it, as described in Section 6.6.2.2.

A PID Provider access certificate does not indicate that its subject is a PID Provider. Similarly, an Attestation Provider access certificate does not indicate that its subject is a QEAA Provider, a PuB-EAA Provider, or a non-qualified EAA Provider. Furthermore, the access certificate of a PID Provider or Attestation Provider does not contain the Provider’s registration to issue attestations of a specific type, for instance an mDL or diploma. Such information is included in the registration certificates (if issued), and in any case available in the Registrar's online service.

Such information is instead available via the Registrar's online service. Additionally, the same information is included in a registration certificate issued to the PID Provider or Attestation Provider by a Provider of registration certificates, if the Registrar has a policy of issuing such certificates - see Section 3.17. To manage both situations, either with use of a registration certificate or without, the access certificate of a PID Provider or Attestation Provider contains a URL to the Registrar's online service, which a Wallet Unit can use to obtain information on the Provider's registration. A Wallet Unit can use the information in the registration certificate (or obtained from the Registrar service) to verify that an Attestation Provider it is contacting to issue a specific type of attestation is in fact registered for that type of attestation.

See Section 6.6.3.3 to learn more about the registration certificate contents.

6.3.2.4 PID Provider or Attestation Provider trust anchors are included in a Trusted List

For a PID Provider, a QEAA Provider, or a PuB-EAA Provider, successful registration and notification also means that the Provider is notified to the European Commission and that its trust anchors are included in a Trusted List. Relying Parties can use these trust anchors to verify the authenticity of PIDs, QEAAs, and PuB-EAAs they obtain from Wallet Units.

Non-qualified EAA Providers are not included in a Trusted List by a Member State. However, if a Relying Party requests a non-qualified EAA from a Wallet Instance, it must know how to obtain the domain-specific trust anchor it needs to verify the signature over that EAA. To help with this, Topic 12 recommends that the applicable Rulebook specifies the mechanisms enabling this. This mechanism may be similar to the one for QEAAs, namely that the relevant non-qualified EAA Providers and their trust anchors are included in a trusted list. However, other methods may be used as well, and even if such a trusted list exists, it does not have to comply with the requirements in Topic 31.

More details on the PID Provider or Attestation Provider notification process, as well as on the information registered and published in the PID Provider Trusted List or Attestation Provider Trusted List, can be found in Topic 31.

6.3.3 Suspension or cancellation of the registration of a PID Provider or Attestation Provider

Under specific conditions, a Registrar may decide to suspend or cancel the registration of a PID Provider or Attestation Provider. The conditions for this will be specified by each Registrar.

Suspension or cancellation implies that the PID Provider or Attestation Provider access certificates are revoked. As a result, the PID Provider or Attestation Provider will no longer be able to issue PIDs or attestations to Wallet Units.

For a PID Provider, QEAA Provider, or PuB-EAA Provider, suspension or cancellation also implies that its status in the respective Trusted List will be changed to Invalid. As a result, Relying Parties will no longer trust PIDs or attestations issued by that Provider. For non-qualified EAA Providers, the applicable Rulebook (see Topic 12) may define similar mechanisms ensuring that Relying Parties will no longer trust the trust anchors of EAA Providers of which the registration was suspended or cancelled.

When a Registrar suspends or cancels registration of a PID Provider or Attestation Provider, the PID Provider or Attestation Provider revokes all of their PIDs or attestations as described in Section 6.6.3.7.

6.4 Trust throughout a Relying Party lifecycle

6.4.1 Relying Party lifecycle

Section 4.6.6 presented the lifecycle of a Relying Party:

1. A Relying Party is registered by a Registrar in the Member State where it resides. Relying Party registration is discussed in Section 6.4.2.
2. Under specific conditions, a Registrar may decide to suspend or cancel registration of a Relying Party. This is discussed in Section 6.4.3.

6.4.2 Relying Party registration

Figure 11 depicts the Relying Party Instance to the right of the Wallet Unit. A Relying Party Instance is a combination of hardware and software used by a Relying Party to interact with a Wallet Unit. A Relying Party can use multiple Relying Party Instances. This will happen especially in case the interactions with the Wallet Unit take place in proximity; for instance, a border control agency at an airport employing multiple lines (each operated by an agency employee) where arriving passengers can present their PID. However, a single Relying Party operating multiple Relying Party Instances can also happen in a remote context, for example if there is an operational system (including a remote Relying Party Instance) next to a fallback system used for business continuity purposes. A Relying Party may also use multiple remote Relying Party Instances for load distribution.

Figure 11 also shows the Relying Party. Below that, it shows that each Relying Party will register itself with a Registrar in its Member State. If the registration process is successful, the Registrar includes the Relying Party in its public registry.

A Relying Party may register in the context of several services, having different intended uses. Each intended use will require a different set of attributes to be obtained from a Wallet Unit. As a result, a single Relying Party may register multiple times and may be issued more than one registration certificate.

As a result of successful registration,

- a Provider of registration certificates (see Section 3.19) associated with the Registrar will issue one or more registration certificates to the Relying Party, if the Registrar has a policy of issuing such registration certificates. The purpose of the registration certificate is described in Section 6.6.3.3. It is up to each Registrar to decide if it issues registration certificates.
- an Access Certificate Authority (see Section 3.18) associated with the Registrar issues an access certificate to each Relying Party Instance of the Relying Party. A Relying Party Instance needs such a certificate to authenticate itself towards Wallet Units when requesting the presentation of attributes, as described in Section 6.6.3.2. Issuing access certificates to a registered Relying Party is mandatory.

More details on the Relying Party registration process can be found in Topic 27.

6.4.3 Relying Party suspension or cancellation

Under specific conditions, a Registrar may decide to suspend or cancel registration of a registered Relying Party. The conditions for this will be specified by each Registrar.

Suspension or cancellation involves revocation of all valid Relying Party Instance access certificates by the relevant Access CA, such that the Relying Party is no longer able to interact with Wallet Units.

6.5 Trust throughout a Wallet Unit lifecycle

6.5.1 Wallet Unit lifecycle

Section 4.6.3 above presented the lifecycle of a Wallet Unit:

1. The Wallet Instance that is part of the Wallet Unit is installed on a device by a User. The required trust relationships for installation are discussed in Section 6.5.2 below.
2. Next, the Wallet Unit is activated by the Wallet Provider and the User and becomes operational. The goals and required trust relationships for activation are discussed in Section 6.5.3.
3. Once in the **Operational** or **Valid** state, the Wallet Unit is managed by the User and the Wallet Provider. This management includes at least revoking the Wallet Unit when necessary. This is discussed in Section 6.5.4. Management will also include regular updates of the Wallet Instance application to ensure its continued security and functionality. However, this is not further defined in this chapter.
4. The User may uninstall the Wallet Instance; see Section 6.5.5.

6.5.2 Wallet Instance installation

6.5.2.1 Required trust relationships

The lifecycle of a Wallet Unit starts when a User decides to install a Wallet Instance application on their device. This application in an instance of a Wallet Solution, which is provided to the User by a Wallet Provider.

When downloading and installing the Wallet Instance, the following trust relationships are established:

1. On behalf of the User, the OS of the User's device and the relevant app store verify that the Wallet Instance (i.e., the application the User is installing) is genuine and authentic and does not contain any malware or other threats.
2. The User verifies that they can obtain the PID(s) they need in an instance of this Wallet Solution. If the relevant PID Provider does not support the Wallet Solution, the User will not be able to use the Wallet Unit for obtaining those PID(s).

The next two sections discuss these trust relationships.

6.5.2.2 Wallet Solution authenticity is verified

To ensure that the User can trust the Wallet Solution, Wallet Providers preferably make their certified Wallet Solutions available for installation via the official app store of the relevant operating system (e.g., Android, iOS). This allows the operating system of the device to perform relevant checks regarding the authenticity of the app. It also allows Users to use the same well-known channel for obtaining a Wallet Instance as they use for obtaining other apps. Finally, it avoids a situation where a User must allow side-loading of apps, which would increase the risk of unintentionally installing malicious apps.

If a Wallet Provider makes its Wallet Solution available for installation through other means than the official OS app store, it implements a mechanism allowing the User to verify the authenticity of the Wallet Unit. Moreover, the Wallet Provider provides clear instructions to the User on how to install the Wallet Unit, including:

- instructions on how to verify the authenticity of the Wallet Instance to be installed. This can be done, for example, by comparing the hash value of the application downloaded by the User with a hash value published by the Wallet Provider.
- instructions on bypassing of any operating system limitations on side-loading of apps, if applicable, and ensuring that these limitations are restored after the Wallet Instance has been installed.

Note: The [European Digital Identity Regulation] does not exclude the possibility that a Wallet Instance may be installed on a non-mobile device, for example a server. The requirements above also apply for the installation of a Wallet Unit on a User device that is not a mobile device, and for which no official operating system app store may exist.

6.5.2.3 User validates that Wallet Solution is usable with relevant PID

A User installs a Wallet Unit because they want to obtain and use one or more PIDs. However, PID Providers are not required to support all Wallet Solutions in the EUDI Wallet ecosystem. 'Support' here means that the PID Provider is willing to issue a PID to an instance of a given Wallet Solution on request of the User. Instead, a PID Provider may choose to support only a single Wallet Solution or a limited number of Wallet Solutions. Therefore, each PID Provider will publish a list of Wallet Solutions that they support, such that a User that wants to request a PID from that PID Provider knows which Wallet Unit they should install. This list could be published, for example, on the PID Provider's website.

Conversely, a Wallet Solution is not required to support all PID Providers, where 'support' means that it is able to request the issuance of a PID from a PID Provider. Each Wallet Provider will, prior to or during installation of a Wallet Instance, let the User know which PID Providers are supported by this Wallet Solution.

For QEAAs, PuB-EAAs, and non-qualified EAAs, the situation is different. Providers of such attestations will support all Wallet Solutions and are not allowed to discriminate between them when processing a request for the issuance of an attestation. Conversely, a Wallet Solution supports all Attestation Providers, and cannot discriminate between different Attestation Providers when requesting the issuance of an attestation at the User's request.

6.5.3 Wallet Unit activation

6.5.3.1 Introduction

After installation of the Wallet Instance, the new Wallet Unit (which includes that Wallet Instance) will contact the Wallet Provider to start the activation process. For successful EUDI Wallet Instance activation, the following trust relations are established:

1. The EUDI Wallet Instance authenticates the EUDI Wallet Provider, meaning that the instance is sure that it is dealing with the genuine Wallet Provider who provided it to the User.
2. The EUDI Wallet Provider authenticates the EUDI Wallet Instance. This means that the EUDI Wallet Provider is sure that the instance is indeed a true instance of their EUDI Wallet Solution, and not a fake app.

Both of these trust relationships are the responsibility of the Wallet Provider. The ARF does not specify how these trust relationships can be satisfied.

During the activation process, at least the following steps happen:

1. The Wallet Provider requests data about the User's device from the Wallet Instance.
2. The Wallet Provider requests the User to set up at least one User authentication mechanism.
3. The Wallet Provider issues one or more Wallet Unit Attestations to the Wallet Unit.
4. The Wallet Provider sets up a User account for the User.

These steps are described in the sections below.

6.5.3.2 Wallet Provider requests data about the User's device from the Wallet Instance

The Wallet Instance connects to the Wallet Provider to be activated. Then, the Wallet Provider requests data about the User's device from the Wallet Instance. This data may include the communication technologies supported by the device and the characteristics of the WSCD(s) available to the device for securely storing cryptographic keys and data associated with the Wallet Unit itself, as well as those associated with the PIDs and device-bound attestations in that Wallet Unit.

Notes:

- As discussed in Section 4.5, a WSCD may be integrated directly within the User's device. Examples of this include an e-SIM, a UICC, an embedded Secure Element, or native secure hardware accessible via the device's OS. If so, the Wallet Instance will discover the presence of such a WSCD during activation and will communicate the characteristics of the WSCD to the Wallet Provider. In some cases, the Wallet Provider will subsequently deploy a WSCA to the WSCD to facilitate communication between the Wallet Instance and the WSCD.
- Sometimes, the User's device does not contain a local WSCD, or the local WSCD does not have the security posture necessary to enable the Wallet Unit to be an identity means at LoA High, or the Wallet Provider does not want to use a local WSCD. In such a case, the Wallet Provider ensures the Wallet Unit gets access to a remote HSM operated by the Wallet Provider.

6.5.3.3 Wallet Unit requests User to set up at least one User authentication mechanism

User authentication will take place at several moments when a User uses their Wallet Unit:

1. When the User opens the Wallet Instance. This is necessary to prevent anyone except the User from accessing the Wallet Unit and inspecting the User's attestations and attribute values. This data is personal and might be sensitive.
2. When (or before) the Wallet Unit must perform any cryptographic operation involving private or secret keys in the WSCD. This will happen at least when

   - The User instructs the Wallet Unit to request the issuance of a new PID or device-bound attestation, see Section 6.6.2,

- The Wallet Unit asks the User for approval to present some attributes from a PID or device-bound attestation to a Relying Party, see Section 6.6.3.5,
- The User deletes a PID or device-bound attestation in their Wallet Unit, see Section 6.6

User authentication for opening the Wallet Instance (point 1 above) is done by an user authentication mechanism implemented by the OS of the User device, such as a lock screen. The only exceptions to this are situations where this is impossible (e.g. on some legacy devices) or in case the User decides that they want to use a User-specific PIN implemented by the Wallet Unit itself. In order to ensure that OS-level authentication is available and is sufficiently secure, during installation of the Wallet Unit, the Wallet Unit enforces the activation of an OS-level User authentication mechanism with adequate security policies. See the requirements on User authentication in Topic 40, Section C.

User authentication before requesting, presenting, or deleting PIDs or device-bound attestations (point 2 above) is always done by the WSCA/WSCD. It means that the User gives the WSCA/WSCD permission to create, use, or delete the cryptographic keys belonging to the Wallet Unit and to the PID or attestation for performing the cryptographic operations necessary for these actions.

Note that, as discussed in the first bullet in Section 6.6.3.9, the User authentication mechanisms implemented in the WSCA/WSCD will also play a role in ensuring User binding for PIDs or device-bound attestations. User binding allows a Relying Party to trust that the person presenting a PID or attestation is the User to whom the PID or the attestation was issued.

6.5.3.4 Wallet Provider issues one or more Wallet Unit Attestations to the Wallet Unit

During the activation of a Wallet Unit, the Wallet Provider issues one or more Wallet Unit Attestations to the Wallet Unit. The Wallet Unit Attestation (WUA) is described in Topic 9. More information on the WUA can also be found in the Discussion Paper for topic C and in the Technical Specification 3.

A WUA has three main purposes:

- It describes the capabilities and properties of the Wallet Unit, including a WSCD. This allows a PID Provider or an Attestation Provider to verify that the Wallet Unit complies with the Provider's requirements and therefore is fit to receive a PID or an attestation from the Provider. To ensure User privacy, the Wallet Unit presents the WUA only to PID Providers and Attestation Providers, but not to Relying Parties. This is because PID Providers and Attestation Providers have a valid business reason to know these properties, whereas Relying Parties do not.

- Moreover, the WUA is device-bound, meaning it contains a WUA public key. During the issuance of a PID or an attestation (see Section 6.6.2.3), a PID Provider or Attestation Provider can use this public key to verify that the Wallet Unit is in possession of the corresponding private key, and that this key is protected by the WSCA/WSCD described in the WUA.
- Lastly, a WUA contains information allowing a PID Provider or an Attestation Provider to verify that the Wallet Provider did not revoke the Wallet Unit Attestation, and hence the Wallet Unit itself. The WUA and the revocation mechanisms for Wallet Units are described in Topic 38.

Optionally, a fourth purpose of the WUA is the following. During the issuance of a PID or a device-bound attestation, the Wallet Unit will send a public key to the PID Provider or Attestation Provider. The Provider will include this public key in the issued PID or attestation. The WSCA/WSCD may be able to prove to the PID Provider or Attestation Provider that it manages both the private key belonging to this new public key and the private key belonging to the WUA public key. In that way, the PID Provider or Attestation Provider can trust that the level of security of this new key is the same as for the WUA key. Note that support for such a 'proof of cryptographic binding' between a WUA and a PID or attestation is not mandatory in this version of the ARF, since no such mechanism has been specified yet, let alone that this is widely supported by available WSCA/WSCDs. For more information, please refer to Topic 18.

The detailed format of the WUA is specified in the draft Technical Specification 3.

Regarding the WUA validity period, an important requirement in [CIR 2024/2977], Article 5, is that a PID Provider must revoke a PID when the Wallet Unit to which that PID was issued is revoked. This implies that a PID Provider, during the entire validity period of the PID, must be able to regularly check whether the Wallet Provider revoked the WUA the PID Provider obtained from the Wallet Unit during PID issuance. This implies that the validity period of a PID cannot exceed the end of validity of the WUA received by the PID Provider during issuance. Therefore, the validity period of WUAs will be long, perhaps as long as the expected lifetime of the Wallet Unit. This also implies that a WUA always needs to contain the information enabling the PID Provider to do a revocation check for the WUA. See also Section 6.6.2.4.

The responsibilities of the Wallet Provider regarding issuance of a WUA are similar to those of a PID Provider or Attestation Provider regarding the issuance of a PID or an attestation. This means that after the initial issuance of a WUA during activation, the Wallet Provider will manage the WUA and will issue new WUAs to the Wallet Unit as needed, during the lifetime of the Wallet Unit. In particular, the Wallet Provider will ensure that the risk of malicious Attestation Providers linking multiple presentations of the same WUA, with the goal of tracking the User, is minimised. For example, the Wallet Provider may set up the Wallet Unit in such a way that each Wallet Unit Attestation is presented to at most one PID Provider or Attestation Provider. Such a WUA is called a 'once-only' attestation, see Section 7.4.3.5.

6.5.3.5 Wallet Provider sets up a User account for User

The User needs a User account at the Wallet Provider to ensure that they can request the revocation of their Wallet Unit in case of theft or loss. The Wallet Provider associates the Wallet Unit with the User account. The Wallet Provider registers one or more backend-based User authentication methods that the Wallet Provider will use to authenticate the User. Note that:

- The Wallet Provider does not need to know any real-world attributes of the User. The User can use a pseudonym to register, for example an e-mail address. If the Wallet Provider wants to request additional User attributes, for instance to be able to provide additional services, they are free to do so if the User consents.
- In any case, User details registered by the Wallet Provider will not be included in the WUA. They are strictly for use by the Wallet Provider only.

6.5.3.6 Wallet Provider ensures User can verify they are using a trusted, certified Wallet Solution

According to the [European Digital Identity Regulation], the User needs to be provided with a means to verify that they are installing or (after activation) are indeed using a trusted, certified Wallet Solution. The solution specified in this ARF to comply with this requirement is a Trust Mark UI view. When the User invokes this Trust Mark in the Wallet Instance, it

- renders the official Trust Mark graphics and/or logo,
- shows an informational text about Wallet Solution certification, localised for the User's device language, and

- provides web links to a list of certified Wallet Solutions, as well as to a web page containing certification information of User's Wallet Solution.

The information in the third bullet is hosted and managed dynamically by the European Commission. The Technical Specification 1 on the EUDI Wallet Trust Mark concentrates on defining the exact technical contents and the provisioning process to enable the UI view rendering at the Wallet Instance. Topic 19 sets the high-level requirements for the Trust Mark as part of the Wallet Unit dashboard functionality. Topic 40 specifies what is required regarding the Trust Mark upon Wallet Unit activation and maintenance.

6.5.4 Wallet Unit management

Starting from Wallet Unit activation and until the Wallet Instance is uninstalled by the User, a Wallet Unit is managed by the User and the Wallet Provider. The Wallet Provider is responsible at least to:

- perform installation of a new version of the Wallet Solution as necessary.
- update the WUAs as necessary; see Topic 9.
- revoke the Wallet Unit in case its security is compromised; see Topic 38.

The User will be able to request the Wallet Provider to revoke the Wallet Unit at least in case of loss or theft of the User's device. See Topic 38.

If the Wallet Unit contains a PID, the PID Provider may request the Wallet Provider to revoke the Wallet Unit in case the natural person using the Wallet Unit has died or the legal person using the Wallet Unit has ceased operations. See Topic 38.

The Wallet Unit ensure that the Wallet Provider cannot access the contents of the Wallet Unit, in particular to learn the value of any User attestations or attributes, as well as the contents of the transaction log kept by the Wallet Unit.

Lastly, the Wallet Unit supports procedures for backing up and restoring the attestations it contains, or for migrating these attestations to a different Wallet Solution. See Topic 33 and Topic 34 respectively.

For high-level requirements regarding Wallet Instance installation and Wallet Unit activation and management, see Topic 40.

To allow Wallet Unit management, the following trust relations are established:

1. When contacting the Wallet Provider, for instance to request the revocation of the Wallet Unit, the User authenticates the Wallet Provider. This means the User is sure that they are visiting the website or the User portal of the genuine Wallet Provider who is responsible for the User's Wallet Unit, and not a spoofed website or portal. This risk can be partly mitigated by using standard mechanisms such as TLS server authentication. However, in addition the User will need to be vigilant as well, just as with any website on the internet.
2. When contacted by a User, the Wallet Provider authenticates the User. This means that the Wallet Provider is sure that the User is indeed the User that was associated with the Wallet Unit during activation. For this, the Wallet Provider uses the authentication methods established in the User's account during activation, see Section 6.5.3.A
3. When the Wallet Unit and the Wallet Provider set up a communication channel, the Wallet Unit authenticates the Wallet Provider, meaning that the Wallet Unit is sure that it is dealing with the genuine Wallet Provider. Similarly, the Wallet Provider authenticates the Wallet Unit. This means that the Wallet Provider is sure that the EUDI Wallet Instance is indeed a true instance of their Wallet Solution, and not a fake app. This will be ensured by the Wallet Provider. The ARF does not specify how these trust relationships can be satisfied.
4. When contacted by a PID Provider to request Wallet Unit revocation, the Wallet Provider authenticates the PID Provider. Section 6.6.2.2 below describes how a Wallet Unit can do this during PID issuance; a Wallet Provider can use the same mechanism.
5. To identify the Wallet Unit that is to be revoked, the PID Provider uses a Wallet Unit identifier provided by the Wallet Unit in the WUA during PID issuance; see Topic 9. This can be the same identifier used for enabling WUA revocation, for example an URI to a Status List plus an index in that list; see Topic 7.

6.5.5 Wallet Instance uninstallation

No trust relationships are required for Wallet Instance uninstallation; anybody able to access the device of the User will be able to do this.

If the User uninstalls the Wallet Instance, the Wallet Instance tries to ensure that the associated WSCA/WSCD(s) delete all sensitive data and cryptographic keys related to the Wallet Unit, as well as all keys of PIDs and device-bound attestations on the Wallet Unit. Note that in some cases this may be a challenge, for instance if the WSCD is an external smart card and the User does not present that card to the User device at the moment the User uninstalls the Wallet

Instance. Another example occurs when the WSCD is a remote HSM and the User device is offline at the moment the User uninstalls the Wallet Instance. In such cases, the cryptographic keys will probably remain present on the WSCD, even though they will never be used again. If needed, it is up to the Wallet Provider to define how the Wallet Unit should handle such situations. For example, an HSM manager could address such cases by deciding to delete cryptographic keys in the HSM that are too old or haven't been used for too long, while being aware of the risks in doing so.

If it supports the Digital Credentials API, see Section 4.4.3, the Wallet Instance also discloses the fact that it is uninstalled to the Digital Credentials API framework.

6.6 Trust throughout a PID or an attestation lifecycle

6.6.1 PID or attestation lifecycle

Section 4.6.5 above presented the lifecycle of a PID or attestation within a Wallet Unit:

1. Using their Wallet Unit, the User requests the issuance of a PID or an attestation from a PID Provider or an Attestation Provider. The required trust relationships for issuance are discussed in Section 6.6.2 below.
2. Once the PID or attestation is issued into the Wallet Unit, the User can present attributes from it to a Relying Party Instance, according to the User's decision and depending on successful authentication of the Relying Party. The required trust relationships for presenting PIDs and attestations, including User approval and Relying Party authentication, are discussed in Section 6.6.3.
3. Instead of presenting attributes to a Relying Party, a User can also present them to another User, meaning that their Wallet Unit is interacting with another Wallet Unit. This is discussed in Section 6.6.4.
4. The PID Provider or the Attestation Provider remains responsible for managing the PID or attestation over its lifetime. Management may include re-issuing the PID or attestation with the same or with different attribute values. The Provider can also revoke the PID or the attestation, possibly based on a request of the User. The management of PIDs and attestations is discussed in Section 6.6.5.
5. Finally, Section 6.6.6 discusses what happens if a User decides to delete a PID or an attestation from their Wallet Unit.

6.6.2 PID or attestation issuance

6.6.2.1 Required trust relationships

The lifecycle of a PID or an attestation starts when a User, using their Wallet Unit, requests a PID Provider or an Attestation Provider to issue the PID or an attestation to their Wallet Unit. The following trust relationships are established during issuance:

1. The Wallet Unit authenticates the PID Provider or Attestation Provider using the access certificate referred to in Section 6.3. This ensures that the User can trust that the PID or attestation they are about to receive, is issued by an authenticated PID Provider or Attestation Provider respectively. See Section 6.6.2.2 below describing how this will be done.
2. The PID Provider or Attestation Provider authenticates the User, meaning that the Provider is sure about the identity of the User. This is necessary to enable determination of the values of the attributes that the Provider will attest to. For instance, a PID Provider needs to authenticate the User to ensure it provides a PID containing the correct family name and date of birth. The method by which the PID Provider or Attestation Provider performs User identification and authentication is out of scope of the ARF, as these processes are specific to each PID Provider or Attestation Provider. However, they will satisfy the requirements for the Level of Assurance required for the PID or attestation issued.
3. The PID Provider or Attestation Provider authenticates and validates the Wallet Unit, see Section 6.6.2.3 below.
4. The PID Provider or Attestation Provider verifies that the Wallet Provider did not revoke the Wallet Unit. This is described in Section 6.6.2.4.
5. After the PID or attestation is issued to the Wallet Unit, the Wallet Unit verifies the authenticity of the PID or attestation; see Section 6.6.2.5.
6. The User will activate a PID before they can use it; see Section 6.6.2.6.
7. If an attestation contains an embedded disclosure policy, the Wallet Unit retrieves the policy and stores it locally, so that it can apply the policy in case a Relying Party requests attributes from the attestation. See Section 6.6.2.7.

More detailed requirements for the issuance process of PIDs and attestations, for instance regarding the issuance protocol, are included in Topic 10/23.

6.6.2.2 Wallet Unit authenticates the PID Provider or Attestation Provider

As shown in Figure 11, a Wallet Unit downloads the Access Certificate Authority Trusted List(s) it needs from the relevant Trusted List Provider(s), possibly after having located them via the Commission common trust infrastructure. See Section 6.3.2 for more information on these Trusted Lists.

Note: It is not mandatory for each Wallet Unit to possess all Access CA Trusted Lists for PID Providers, if there are multiple. Wallet Providers will choose which Trusted Lists they need to subscribe to, for example depending on the Member State(s) they are operating in. It is however mandatory to possess all Access CA Trusted Lists for Attestation Providers, since Wallet Units must support all QEAA Providers and PuB-EAA Providers in the EUDI Wallet ecosystem.

To start the process of requesting a PID or an attestation, the User directs the Wallet Unit to contact the PID Provider or Attestation Provider. The User may for example use the Wallet Unit to scan a QR code or tap an NFC tag to do so. Note that no centralised service discovery mechanism for PID or attestation issuance is foreseen.

Before requesting the issuance of a PID or an attestation, the Wallet Unit authenticates the PID Provider or the Attestation Provider. To do so, the Wallet Unit verifies the access certificate presented to it by the PID Provider or Attestation Provider in its Issuer metadata according to [OpenID4VCI]. Additionally, to verify the legal status of the Provider and the type(s) of attestation it issues), the Wallet Unit checks the registration information contained in the registration certificate (if available in the Issuer metadata) or in the online service of the Registrar indicated in the access certificate.

The Wallet Unit also verifies that the access certificate and registration certificate (if provided) are valid and authentic.

6.6.2.3 PID Provider or Attestation Provider validates the Wallet Unit

6.6.2.3.1 Verifies the authenticity of the Wallet Unit

As shown in Figure 11, a PID Provider or an Attestation Provider downloads the Wallet Provider Trusted List(s) it needs from the relevant Trusted List Provider(s), possibly after having located them via the Commission common trust infrastructure.

Note that for PID Providers it is not mandatory to possess all Wallet Provider Trusted Lists, if there are multiple. This is because it is not mandatory for a PID Provider to accept all certified Wallet Solutions in the EUDI Wallet ecosystem. Each PID Provider will choose which Trusted Lists they need to subscribe to. This is different for Attestation Providers: they must accept all Wallet Solutions and hence must possess all Wallet Provider Trusted Lists.

Section 6.5.3 above described that a Wallet Provider, during activation of a Wallet Unit, issues one or more Wallet Unit Attestations (WUA) to the Wallet Unit. When the Wallet Unit sends a request for a PID or an attestation to a PID Provider or to an Attestation Provider, it includes the WUA in the request. The PID Provider or Attestation Provider verifies the signature over the WUA, using the Wallet Provider trust anchor obtained from the Trusted List. Next, the PID Provider or Attestation Provider verifies that the Wallet Unit possesses the private key belonging to the public key in the WUA. This proves that the Wallet Unit is authentic and is provided by a trusted Wallet Provider. For more details see Topic 9.

6.6.2.3.2 Optionally, validates the properties of the WSCA/WSCD

The WUA describes the certifications and the other relevant properties of the WSCD, i.e., the secure cryptographic device included in the Wallet Unit to store and manage cryptographic keys. The security level of the WSCA/WSCD is a key determinant for the overall Level of Assurance (LoA) of the Wallet Unit. For obtaining a PID, the Wallet Unit and the WSCA/WSCD will comply with the requirements for LoA High. For other attestations, LoA High or Substantial will be needed, depending on the requirements of the Attestation Provider.

6.6.2.3.3 Verifies that PID key or device-bound attestation key is protected by the WSCD

Knowing the properties of the WSCA/WSCD is not very useful if the PID Provider or Attestation Provider cannot be sure that the private key for their new PID or device-bound attestation is indeed protected by that WSCA/WSCD. Topic 18 describes how the PID Provider or Attestation Provider may be able to obtain a proof that the WSCA/WSCD described in the WUA protects both the WUA private key and the private key of the new PID or attestation.

6.6.2.4 PID Provider or Attestation Provider verifies that WUA is not revoked

Section 6.5.3.4 above described that a Wallet Provider, during activation of a Wallet Unit, issues one or more Wallet Unit Attestations (WUA) to the Wallet Unit. A WUA contains revocation information. During the lifetime of the Wallet Unit, the Wallet Provider regularly verifies that the security of the Wallet Unit is not breached or compromised. If the Wallet Unit is no longer secure, the Wallet Provider revokes all of the corresponding WUAs. The WUA thus allows PID Providers and Attestation Providers to verify that the Wallet Unit is not revoked.

Moreover, Section 6.5.3.4 also explains that [CIR 2024/2977] requires that PID Providers must verify regularly, during the entire lifetime of the PID, whether the Wallet Unit on which that PID is residing is revoked by the Wallet Provider. They can do this using the revocation information in the WUA they received during PID issuance. PID Providers must also verify regularly whether the Wallet Provider has been suspended or cancelled in the associated Trusted List. If either of these events happens, the PID Provider must revoke the PID. Therefore, by verifying the revocation status of the PID, the Relying Party Instance implicitly verifies the revocation status of the Wallet Unit. See Technical Specification 3 for more information.

Attestation Providers can use the same mechanism to provide the same assurance to Relying Parties, although this is not required by the CIR. See also Section 6.6.3.12.

Topic 38 describes Wallet Unit revocation in more detail.

Once it has done all verifications, the PID Provider or Attestation Provider will issue the PID or attestation to the Wallet Unit.

6.6.2.5 Wallet Unit verifies PID or attestation

After the Wallet Unit receives the PID or attestation, it will

- verify that the PID or attestation it received matches the request.
- verify the signature of the PID or attestation, using the appropriate trust anchor, in the same way as described for a Relying Party Instance in Section 6.6.3.6.
- show the contents (i.e., attribute values) of the new PID or attestation to the User and request the User's approval for storing the new PID or attestation. When requesting approval, the Wallet Unit shows the contents of the PID or attestation to the User. The Wallet Unit also informs the User about the identity of the PID Provider or Attestation Provider, using the subject information from the PID Provider or Attestation Provider access certificate.

If one these verifications fail, the Wallet Unit will delete the PID or attestation, and will inform the User that issuance was not successful. Otherwise, the Wallet Unit will store the PID or attestation and will inform the User that issuance was successful. If it supports the Digital Credentials API, see Section 4.4.3, the Wallet Unit will also disclose the fact that it contains the new PID or attestation to the Digital Credentials API framework.

6.6.2.6 User activates the PID

As documented in Topic 9, to achieve Level of Assurance (LoA) High, Commission Implementing Regulation (EU) 2015/1502 requires that an activation process will be implemented to verify that a PID was in fact delivered into the possession of the person to whom it belongs.

However, in fact no additional step is needed in the issuance process to ensure this. This is because the User always starts the issuance process from the Wallet Unit into which they want the PID Provider to issue the new PID. The PID Provider sets up a secure communication channel towards this Wallet Unit, using the flow specified in [OpenID4VCI]. Additionally, the User uses an eID means on LoA High to authenticate towards the PID Provider. This process ensures that the new PID can only end up on the device used by the subject of the PID.

Note that activation is required only for PIDs, since the [European Digital Identity Regulation] only requires PIDs to be issued at LoA High.

6.6.2.7 Provisioning embedded disclosure policies

6.6.2.7.1 Introduction

During attestation issuance, an Attestation Provider can optionally create an embedded disclosure policy for the attestation, and provide it to Wallet Units during attestation issuance. Such an embedded disclosure policy contains rules determining which (types of) Relying Parties are allowed by the Attestation Provider to receive the attestation.

Note that the [European Digital Identity Regulation] does not contain a requirement for PIDs to be able to contain an embedded disclosure policy, but only for QEAAs and PuB-EAAs.

For more information regarding embedded disclosure policies, please refer to the Discussion Paper for Topic D.

6.6.2.7.2 Types of embedded disclosure policies

Annex III of [CIR 2024/2979] defines the following common embedded disclosure policies that must be supported:

> 1. ‘No policy’ indicating that no policy applies to the electronic attestations of attributes.
> 2. ‘Authorised relying parties only policy’, indicating that wallet users may only disclose electronic attestations of attributes to authenticated relying parties which are explicitly listed in the disclosure policies.
> 3. ‘Specific root of trust’ indicating that wallet users should only disclose the specific electronic attestation of attributes to authenticated wallet-relying parties with wallet-relying party access certificates derived from a specific root (or list of specific

> roots) or intermediate certificate(s).

The first of these policies is the default and will be applied if the Attestation Provider does not provide an embedded disclosure policy for an attestation.

For expressing conditions on Relying Parties, an embedded disclosure policy will refer to information included in the access certificate provided to the Wallet Unit by the Relying Party. Note that access certificates are signed and hence the information they contain is authenticated.

Wallet Units, as well as the mechanisms used for defining and evaluating policies, will provide support for at least policies 2. and 3. above. The Commission will ensure a technical specification is created that specifies how these policies will be formatted.

6.6.2.7.3 Distributing embedded disclosure policies

An Attestation Provider will provide an embedded disclosure policy, if any, in the Issuer metadata specified in [OpenID4VCI]. This does not require modifications to the attestation format. The Commission will ensure that a technical specification for issuing embedded disclosure policies is created.

Moreover, policies will be integrated directly into the metadata, rather than being "linked" using a URL and stored by the Attestation Provider. The approach does not require the Wallet Unit to communicate with the Attestation Provider in order to be able to obtain and evaluate a policy for an attestation requested by a Relying Party. Instead, during issuance of an attestation, the Wallet Unit retrieves any relevant disclosure policy from the metadata and stores it locally. A consequence of this approach is that an Attestation Provider will revoke an attestation if a relevant embedded disclosure policy must be updated.

6.6.2.8 Batch issuance

Batch issuance means that instead of issuing a single PID or attestation to a Wallet Unit, a PID Provider or Attestation Provider issues a batch of them. All PIDs or attestations in a batch have the same attestation type, attribute values and technical validity period. Apart from that, all of the descriptions in this section 6.6.2 apply regardless of the number of attestations issued (single or batch).

Batch issuance is discussed in more detail in the Discussion Paper for Topic B.

6.6.3 PID or attestation presentation to Relying Party

6.6.3.1 Required trust relationships

A Relying Party can request a User to present some attributes from a PID or from an attestation in their Wallet Unit. Figure 11 shows that a Relying Party uses a Relying Party Instance to interact with the Wallet Unit of the User. The relationship between the Relying Party and their Relying Party Instance is similar to the relationship between the User and their Wallet Unit.

When processing the request, the following trust relationships are established:

1. The Wallet Unit authenticates the Relying Party Instance, ensuring the User about the Relying Party's identity. Section 6.6.3.2 explains how this will be done.
2. The Wallet Unit verifies that the Relying Party does not request more attributes than it has registered for, and informs the User about the outcome of this verification. See Section 6.6.3.3 for more information.
3. The Attestation Provider, during issuance, may optionally embedded a disclosure policy in the attestation. If such a policy is present for the requested attestation, the Wallet Unit evaluates the disclosure policy and informs the User about the outcome of this evaluation. See Section 6.6.3.4.
4. The User approves or rejects the presentation of the requested attributes. User approval and selective disclosure are described in Section 6.6.3.5. Subsequently, after the Wallet Unit presents the selected attributes from the PID or attestation to the Relying Party Instance by sending a response to the request, the Relying Party validates the response. The following trust relationships are established:
5. The Relying Party Instance verifies the signature of the PID or attestation. This ensures that the Relying Party can trust that the PID or attestation it receives is issued by an authentic Provider and has not been changed. This is described in Section 6.6.3.6.
6. The Relying Party verifies that the PID Provider or Attestation Provider did not revoke the PID or attestation. This is described in Section 6.6.3.7.
7. For PIDs and device-bound attestations, the Relying Party verifies that the PID Provider or Attestation Provider issued this PID or attestation to the same Wallet Unit that presented it to the Relying Party. In other words, it checks that the PID or attestation was not copied or replayed. This is generally called device binding, and it is discussed in Section 6.6.3.8
8. In some use cases, the Relying Party verifies that the person presenting the PID or attestation is the User to whom the PID or the attestation was issued. This is called User binding. In other use cases, the Relying Party trusts that the Wallet Unit and the WSCA/WSCD have done this check. User binding is discussed in Section 6.6.3.9.

9. The Relying Party can request attributes from two or more attestations in the same interaction. This is called a **combined presentation of attributes**. If so, the Relying Party verifies that these attestations belong to the same User. This is discussed in Section 6.6.3.10.
10. Finally, after the interaction with the Relying Party Instance is over, the Wallet Unit enables the User to report unlawful or suspicious requests for personal data by a Relying Party, based on information logged by the Wallet Unit. In addition, the Wallet Unit enables the User to send a request to a Relying Party to delete personal data (i.e., User attributes) obtained from the Wallet Unit. This is discussed in Section 6.6.3.13.

6.6.3.2 Wallet Unit authenticates the Relying Party Instance

Relying Party authentication is a process whereby a Relying Party proves its identity to a Wallet Unit, in the context of an interaction in which the Relying Party requests the Wallet Unit to present some attributes. Relying Party authentication is discussed in Topic 6.

Relying Party authentication is included in the protocol used by a Wallet Unit and a Relying Party Instance to communicate. As documented in Topic 12, at least two different protocols can be used within the EUDI Wallet ecosystem, namely the ones specified in [ISO/IEC 18013-5] and [OpenID4VP]. Both protocols include functionality allowing the Wallet Unit to authenticate the Relying Party Instance. Although these protocols differ in the details, on a high level, they both implement Relying Party authentication as shown in Figure 12 below.

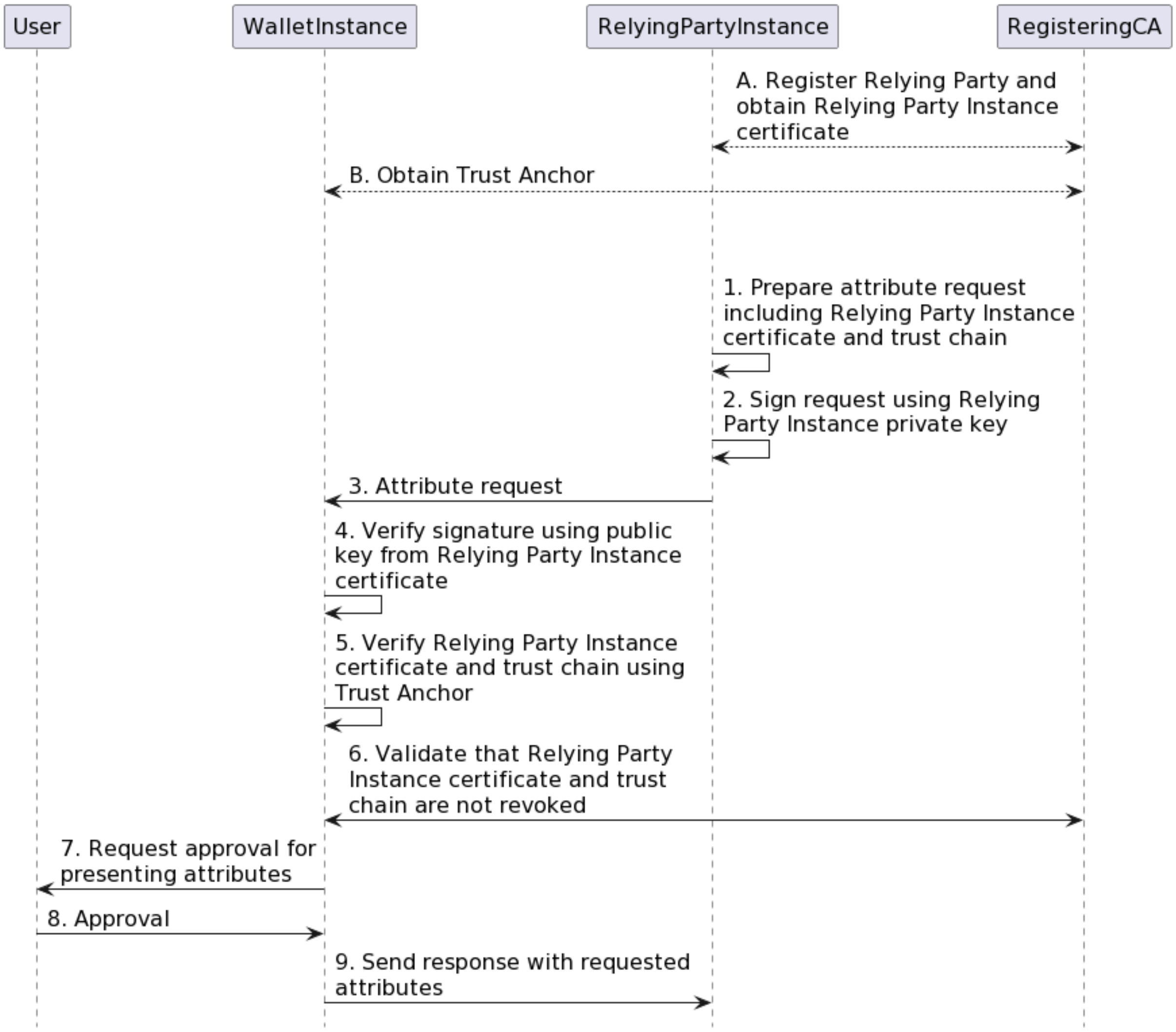

User
WalletInstance
RelyingPartyInstance
RegisteringCA
A. Register Relying Party and obtain Relying Party Instance certificate
B. Obtain Trust Anchor
1. Prepare attribute request including Relying Party Instance certificate and trust chain
2. Sign request using Relying Party Instance private key
3. Attribute request
4. Verify signature using public key from Relying Party Instance certificate
5. Verify Relying Party Instance certificate and trust chain using Trust Anchor
6. Validate that Relying Party Instance certificate and trust chain are not revoked
7. Request approval for presenting attributes
8. Approval
9. Send response with requested attributes

Figure 7: Figure 12

Figure 12 High-level overview of Relying Party authentication process

The figure shows the following:

First, there are two preconditions that need to be fulfilled before the Relying Party authentication process can begin. Note that these actions are not carried out for every presentation, but only once (excluding possible updates):

A) The Relying Party registered itself as described in Section 6.4.2 and obtained a Relying Party Instance access certificate.

B) The Wallet Unit obtained the trust anchor of the Relying Party Instance Access Certificate Authority.

Subsequently, during each presentation of attributes:

1. The Relying Party Instance prepares a request for some attributes to the Wallet Unit and includes its Relying Party Instance access certificate in the request, plus all intermediate certificates up to (but excluding) the trust anchor.
2. The Relying Party Instance signs some data in the attribute request using its private key.
3. The Relying Party Instance sends the request to the Wallet Unit.
4. The Wallet Unit checks the authenticity of the request by verifying the signature over the request using the public key in the Relying Party Instance access certificate.
5. The Wallet Unit checks the authenticity of the Relying Party by validating the Relying Party Instance access certificate and all intermediate certificates included in the request. For validating the last intermediate certificate, the Wallet Unit uses the trust anchor it obtained from the Trusted List.
6. The Wallet Unit validates that none of the certificates in the trust chain have been revoked. This includes the Relying Party Instance access certificate as well as all other certificates in the trust chain, including the trust anchor itself if applicable.
7. The Wallet Unit continues by requesting the User for approval.
8. The User approves the attributes that will be presented.
9. The Wallet Unit sends a response containing only the approved attributes to the Relying Party Instance.

6.6.3.3 Wallet Unit allows User to verify that Relying Party does not request more attributes than it registered

During registration, the Relying Party registered which attributes it intends to request from Wallet Units for each of the services (intended uses) it has. If the Registrar issues registration certificates, the Registrar listed these attributes in a separate certificate for each intended use and sent it to the Relying Party. Subsequently, the Relying Party distributed these to all of its Relying Party Instances. Finally, the Relying Party Instance sent a single registration certificate pertaining to the intended use relevant for the current presentation request to the Wallet Unit in the request.

Note that a single intended use may cover multiple attributes from multiple attestations. For example, a Relying Party selling alcoholic beverages online may register that for this intended use they will request an age verification attribute from the PID and a User address from some other attestation. However, if a Relying Party really has multiple intended uses for interacting with a Wallet Unit, it needs to send multiple presentation requests, each including the relevant registration certificate.

As a general setting or when processing a presentation request, the Wallet Unit offers to the User an option to verify the information registered for the Relying Party. If the User chooses to do so, the Wallet Unit obtains information about which attributes the Relying Party registered:

- If a registration certificate is included in the request, the Wallet Unit gets this information from the certificate.
- If no registration certificate is available, the Wallet Unit contacts the Registrar to obtain this information. To do so, the Wallet Unit needs the following:
  - the URL of the Registrar's online service,
  - the unique identifier of the Relying Party,
  - the identifier of the intended use of the Relying Party for this presentation request. This is needed because the list of registered attributes depends on the intended use. As specified in Technical Specification 5, the Registrar assigns a unique identifier to each intended use of a Relying Party during registration.

The Wallet Unit retrieves the first two pieces of information from the Relying Party access certificate, provided no intermediary is used in the presentation transaction. If an intermediary is used, the access certificate pertains to the intermediary and not to the intermediated Relying Party, see Section 3.11. Therefore, in such a case the intermediary includes the Registrar URL and Relying Party identifier directly in the presentation request. Regardless of whether an intermediary is used or not, the Relying Party Instance includes the identifier of the intended use separately in the presentation request.

Once it has retrieved the list of attributes registered by the Relying Party, the Wallet Unit compares this list to the attributes that the Relying Party requests in the presentation request. The Wallet Unit notifies the User in case the Relying Party requested attributes that it has not registered at the Registrar, when asking the User for approval, see Section 6.6.3.5. The Wallet Unit also notifies the User in case the Wallet Unit is not able to retrieve the Relying Party registration information.

The format of the registration certificate, as well as the way in which the Wallet Unit can verify that the registration certificate belongs to the authenticated Relying Party, will be specified in a technical specification. For more information, see Topic 44.

6.6.3.4 Wallet Unit evaluates embedded disclosure policy, if present

During attestation issuance, an Attestation Provider optionally created an embedded disclosure policy for the attestation, see Section 6.6.2.7. If such a policy is present for the requested attestation, the Wallet Unit evaluates the policy, together with information in the access certificate, to determine whether the Attestation Provider allows this Relying Party to receive the requested attestation. Note that the Wallet Unit verifies the authenticity of the access certificate before using any data contained in it.

The Wallet Unit presents the outcome of the disclosure policy evaluation to the User when requesting User approval, see Section 6.6.3.5.7. For example, “The issuer of your medical data does not want you to present data from <attestation name> to <Relying Party name>. Do you want to continue?” Note that the User can overrule the disclosure policy evaluation outcome.

For more details on the embedded disclosure policy, see Topic 43.

6.6.3.5 Wallet Unit obtains User approval for presenting selected attributes

6.6.3.5.1 Introduction

Note: In this document the term ‘User approval’ exclusively refers to a User’s decision to present an attribute to a Relying Party. Under no circumstances User approval to present data from their Wallet Unit should be construed as lawful grounds for the processing of personal data by the Relying Party or any other entity. A Relying Party requesting or processing personal data from a Wallet Unit must ensure that it has grounds for lawful processing of that data, according to Article 6 of the GDPR.

Before presenting any attribute to a Relying Party, the Wallet Unit requests the User for their approval. This is critical for ensuring that the User remains in control of their attributes.

A Wallet Unit requests User approval in all use cases, both in proximity flow and remote flow, and including:

- Use cases where the Relying Party could be assumed to be trusted, for example, when the Relying Party is part of law enforcement or another government agency.

- Use cases where the requested attributes are critical for the Relying Party to grant access to the User or deliver the requested services.
- Use cases where there is, according to the GDPR or other legislation, no legal need to ask for the User's approval because another legal basis exists for requesting the attributes.

A number of conditions must be fulfilled for effective User approval:

1. The Wallet Unit authenticated the User; see Section 6.6.3.5.2,
2. The Wallet Unit informed the User about the identity of the Relying Party; see Section 6.6.3.5.3,
3. The Wallet Unit informed the User about the attributes the Relying Party requested,
4. The Wallet Unit informed the User about the Relying Party's intended use and privacy policy for these attributes,
5. The Wallet Unit informed the User about the outcome of the evaluation of the requested attributes,
6. The Wallet Unit informed the User about the outcome of the evaluation of the embedded disclosure policy, if any,
7. The Wallet Unit enables the User to approve or deny the requested attributes.

These conditions are further discussed in the next subsections. After the User gives their approval, the Wallet Unit will present the approved User attributes to the Relying Party Instance.

More detailed requirements regarding User approval can be found in Topic 6

6.6.3.5.2 Wallet Unit authenticated the User

A prerequisite for requesting User approval is that the Wallet Unit is sure that the person using the Wallet Unit (and giving the approval) is in fact the User. Therefore, the WSCA/WSCD authenticates the User prior to or during requesting User approval, on request of the Wallet Unit. To do so, the Wallet Unit uses the User authentication mechanism set up during Wallet Unit activation, see Section 6.5.3.

6.6.3.5.3 Wallet Unit informs the User about the identity of the Relying Party

In order to be able to give approval, a User needs to be informed about the identity of the Relying Party. The Wallet Unit shows the User at least the User-friendly name registered by the Relying Party. It optionally also shows the Relying Party's registered unique identifier.

If the Relying Party does not use an intermediary, the Wallet Unit obtains this information from the access certificate presented by the Relying Party Instance. If the Relying Party uses an intermediary (see Section 3.11), the Wallet Unit informs the User about the name and optionally the unique identifier of both the intermediary and the intermediated Relying Party. In this case, the Wallet Unit obtains the information about the intermediary from the access certificate, while the information about the intermediated Relying Party is in the registration certificate, if present. If there is no registration certificate, the intermediary included the name and the unique identifier of the Relying Party in the presentation request, see requirement RPI_06 in Topic 52.

6.6.3.5.4 Wallet Unit informs the User about the attributes the Relying Party requested

In order to be able to give approval, a User also needs to know which attributes the Relying Party wishes to receive. Note that a Relying Party may request attributes from multiple attestations in a single request; for example information from a diploma and from a PID.

6.6.3.5.5 Wallet Unit informs the User about the Relying Party's intended use and privacy policy

According to the GDPR, a User must be informed about the Relying Party's intended use for the requested attributes. For each presentation request, the Relying Party can have only one intended use. If the Relying Party has multiple intended uses for requesting attributes from a Wallet Unit, it needs to send multiple presentation requests. In such a case, the Wallet Unit will request the User for their approval multiple times.

If the Relying Party Instance sends a registration certificate to the Wallet Unit in the presentation request, this certificate contains a User-friendly description of the Relying Party's intended use, as well as a URL to the applicable privacy policy of the Relying Party. The Wallet Unit shows this information to the User.

If there is no registration certificate, the Relying Party Instance includes the User-friendly description of the Relying Party's intended use in the presentation request, so that the Wallet Unit can show it to the User. In addition, if the User wants, the Wallet Unit will retrieve the information registered about the Relying Party from the respective Registrar. This information includes a URL to the applicable privacy policy of the Relying Party. The Wallet Unit then shows this URL to the User.

6.6.3.5.6 Wallet Unit informs the User about the outcome of the evaluation of the requested attributes

Section 6.6.3.3 above described how the Wallet Unit can verify the attributes requested by the Relying Party against the attributes that the Relying Party registered for the given intended use. The Wallet Unit will perform this verification only if the User desires this. If the Wallet

Unit performed this verification and the outcome is negative, the Wallet Unit will inform the User that this is the case. For example, "<Relying Party name> requested <attribute1>, but it did not register this attribute. Do you want to continue?" Note that the User can overrule a negative outcome of this verification and decide to approve the request.

6.6.3.5.7 Wallet Unit informed the User about the outcome of the evaluation of the embedded disclosure policy

Section 6.6.3.4 above described that an Attestation Provider can add an embedded disclosure policy for an attestation. It also described how a Wallet Unit can evaluate such a policy. The Wallet Unit presents the outcome of the disclosure policy evaluation to the User when asking for User approval. For example, "The issuer of your <attestation name> does not want you to present data to <Relying Party name>. Do you want to continue?" Note that the User can overrule a negative outcome of the disclosure policy evaluation and decide to approve the request.

6.6.3.5.8 Wallet Unit enables the User to approve or deny the requested attributes

After presenting all of the above mentioned information, the Wallet Unit enables the User to approve or deny the requested attributes. The User gives approval either to release all attributes requested, or none of them. This is because partial approval would mean that the Relying Party cannot deliver the service, but nevertheless receives some User attributes. This would be a violation of the User's privacy.

6.6.3.6 Relying Party Instance verifies the authenticity of the PID or attestation

The Relying Party Instance receives a PID or attestation, including some attributes, from the Wallet Unit. Subsequently, it verifies the signature over the PID or attestation. To do this for PIDs and QEAAs, the Relying Party Instance uses a trust anchor of the Provider obtained from a Trusted List. Note that the PID Provider or QEAA Provider may use an intermediate signing certificate to sign the PID or attestation, and use the trust anchor to sign the signing certificate, instead of signing the PID or attestation directly with the trust anchor.

For PuB-EAAs, the Relying Party Instance verifies a PuB-EAA by first verifying the signature of the PuB-EAA Provider over the PuB-EAA, using the PuB-EAA Provider certificate issued by a QTSP. Subsequently, the Relying Party Instance verifies the signature over this certificate, using the corresponding trust anchor from the QTSP Trusted List. Note that both the PuB-EAA Provider and the QTSP may use an intermediate signing certificate. All other things being equal, the verification of a PuB-EAA will therefore involve one or more extra certificates, compared to the verification of a PID or QEAA.

Finally, for non-qualified EAAs, the applicable Rulebook may describe how the Relying Party Instance obtains the relevant trust anchor.

The above implies that a Relying Party Instance is aware whether the attestation it is requesting from a Wallet Instance is a PID, a QEAA, a PuB-EAA, or a non-qualified EAA. Also, the Relying Party Instance stores trust anchors in such a way that, at the time of verification, it is able to distinguish between trust anchors usable either for PIDs, for QEAAs, for PuB-EAAs, or for non-qualified EAAs.

The technical implementation of the signature verification process depends on which of the standards mentioned in Topic 12 is supported by the Wallet Unit. Each of these standards specifies in detail how to carry out signature verification.

In addition, the Relying Party may want to verify that the Attestation Provider is registered to issue the type of attestation in question, as described in Section 6.3.2.3.

Notes:

- All PIDs and attestations in the EUDI Wallet ecosystem are digitally signed by the respective PID Provider or Attestation Provider, or by a WSCA/WSCD that is part of the Wallet Unit. If an attestation is digitally signed by a WSCA/WSCD, it is called a device-signed or self-issued attestation. Device-signed or self-issued PIDs or attestations are allowed for PIDs only if it can be shown that the WSCA/WSCD signs them at the required Level of Assurance (LoA) High. This implies that the level of security offered by the WSCA/WSCD is at least equivalent to the security level of the secure infrastructure used by the PID Provider for signing PIDs.
- The signature over the PID or attestation may or may not include the value of the presented attributes. If the attribute values are not included in the signature creation, the Relying Party trusts these attributes because they are presented over an authenticated channel set up between the secure environment (i.e., the WSCA/WSCD or the secure infrastructure used by the PID Provider or Attestation Provider, see previous bullet) and the Relying Party. One possible way to set up such an authenticated channel is by ensuring the authenticity and integrity (but not the non-repudiation) of the attributes by means of a Message Authentication Code (MAC). The MAC is created by the secure environment over the presented attribute values. The MAC key is generated from an

ephemeral key of the Relying Party (sent to the secure environment by the Wallet Instance) in combination with an ephemeral key created by the secure environment. The latter ephemeral key is sent to the Relying Party in such a way that the Relying Party can verify the authenticity of this key. Such a solution, or similar ones, can be used provided that:

- the solution is fully compliant with the relevant standards, i.e., [ISO/IEC 18013-5] or [OpenID4VP] and [SD-JWT VC].
- when used for PIDs, the solution can be certified for security at LoA High according to Chapter 7

6.6.3.7 Relying Party verifies that the PID or attestation is not revoked

To allow revocation checking of a PID or attestation, the PID Provider or Attestation Provider includes revocation information in the PID or attestation, if it is valid for longer than 24 hours. This revocation information includes a URL indicating the location where a Relying Party can obtain a status list or revocation list, and an identifier or index for this specific certificate or attestation within that list.

Notes:

- For attestations with a validity period of less than 24 hours, including revocation information is not necessary.
- A status list is a bit string or byte string in which each bit or group of bits denotes the current revocation status (valid or revoked) of one attestation. To get the status of the attestation it has received from the Wallet Unit, the Relying Party obtains the status list from the URL specified in the attestation and verifies the value encoded at the bit position given by the index value in the attestation.
- A revocation list is a list of PID identifiers or attestation identifiers revoked by the PID Provider or Attestation Provider. To get the status of the PID or attestation it has received from the Wallet Unit, the Relying Party obtains the revocation list from the URL specified in the attestation and verifies whether the identifier included in the attestation is on the list or not.
- In some cases, no reliable information regarding the revocation status of a PID or attestation will be available, for example in case a Relying Party Instance is offline and does not have access to a cached status list or revocation list, or if the requested attestation is non-qualified and the responsible Attestation Provider choose to not have a revoca-

tion service for the attestation. In such a case, a Relying Party performs a risk analysis considering all relevant factors for the use case, before taking a decision to accept or refuse the PID or attestation.

For more details and requirements on revocation, see Topic 7.

6.6.3.8 Relying Party Instance verifies device binding

Device binding is the property that a PID or an attestation is bound to a specific device (in fact, a WSCD) and cannot be used independent from that device. Device binding protects the attestation against copying or cloning, which enhances its security. As discussed in the next section, device binding can also be a prerequisite for User binding, namely when the Relying Party decides to trust the User authentication mechanisms of the Wallet Unit for verifying that the person that presents the PID or attestation to the Relying Party is in fact the User to whom the PID or the attestation was issued

Within the EUDI Wallet ecosystem, implementing device binding is mandatory for PIDs, since PIDs must be managed at Level of Assurance High, which is impossible without device binding. It is also mandatory for attestations complying with [ISO/IEC 18013-5], due to the fact that this is required in that standard. For [SD-JWT VC]-compliant attestations, implementing device binding is recommended but not mandatory. However, note that [OpenID4VP] enables the Relying Party to indicate if it wants to receive a proof of device binding for a requested attestations, via the `require_cryptographic_holder_binding` parameter in the request. It also stipulates that a Wallet Unit cannot return a non device-bound attestation in case the Relying Party requests such a proof.

A PID Provider or an Attestation Provider can implement device binding by including a cryptographic public key in the PID or attestation and signing it. The corresponding private key is protected by a certified WSCA/WSCD in the Wallet Unit.

Topic 9 explains that a WSCA/WSCD generates a public-private key pair for each PID and device-bound attestation upon request of the Wallet Unit, and that the Wallet Unit sends the public key to the PID Provider or Attestation Provider. Furthermore, it discusses how the PID or Attestation Provider can verify that the corresponding private key is really protected by the WSCA/WSCD.

After receiving a presentation response, the Relying Party verifies that a PID or device-bound attestation it received from a Wallet Unit is indeed bound to the WSCA/WSCD included in the

Wallet Unit. The Relying Party does so by requesting the Wallet Unit to sign some (pseudo-)random data provided by the Relying Party, using the private key corresponding to the public key in the PID or attestation. For this reason, device binding is also called 'proof of possession'. In [ISO/IEC 18013-5] it is called 'mdoc authentication'. In [SD-JWT VC] it is called 'key binding'.

The technical implementation of this verification depends on which of the standards mentioned in Topic 12 is supported by the Wallet Unit. Each of these standards specifies in detail how to carry out this verification.

The data signed by the Wallet Unit may include (a representation of) some transactional data which the Relying Party included in the presentation request, see Section 5.6.2. Note that neither [ISO/IEC 18013-5] nor [OpenID4VP] or [SD-JWT VC] specify the syntax and semantics of the transactional data. Nor do these standards specify how a Wallet Unit should process this data,or how it should be presented to the User prior to being signed. All of these aspects will need to be specified in the Attestation Rulebook or Technical Specification for the type of attestation that is being requested in the presentation request.

6.6.3.9 Relying Party Instance verifies or trusts User binding

User binding (sometimes also called 'holder binding') is the property that the person that presents the PID or attestation to the Relying Party is in fact the User to whom the PID or the attestation was issued. User binding prevents an attacker from successfully presenting a PID or an attestation that they are not legally allowed to use.

The mechanism(s) available for User binding depend on the presentation flow type (proximity or remote, supervised or unsupervised, see also Section 4.4), and on the attributes issued to the User by the PID Provider or Attestation Provider:

1. In the first place, for PIDs and device-bound attestations the Relying Party can always decide to trust the User authentication mechanisms implemented by the WSCA/WSCD (see Topic 9). This means that the Relying Party trusts that the the WSCA/WSCD has properly authenticated the User before allowing the User to present the attributes. Note that:

    - This trust is not based on the outcome of any verification by the Relying Party but on a a-priori trust in (in particular) the certified WSCA/WSCD that is part of the Wallet Unit.

   - Using this method implies that Relying Parties must verify device binding, as described in Section 6.6.3.8. The Relying Party Instance in fact first verifies that the PID or attestation is bound to a WSCA/WSCD trusted by the PID Provider or Attestation Provider, and then trusts that the WSCA/WSCD has properly authenticated the User.
   - As a matter of fact, this User binding method will always be carried out for PIDs and device-bound attestations, since the WSCA/WSCD must authenticate the User before it can carry out any cryptographic operations involving the private key of the PID or attestation.

2. In addition, in some cases, if a Relying Party does not want to only trust the above mechanism, it may be able to use User attributes to carry out an additional User binding process. For example, if the PID or attestation contains a User portrait, the Relying Party may be able to visually or biometrically compare that portrait to the face of the person presenting the attestation or by a photo taken of it by an automated machine or as a "selfie". This will generally be possible in supervised proximity presentations by human inspection, or in an unsupervised proximity flow if equipped with the appropriate equipment. It may also be possible to do this in unsupervised remote presentations by using face recognition technology, possibly even remotely. However, to generate trustworthy outcomes in such situations, special conditions and dedicated security measures are required, such as good lighting, clear instructions for the User for positioning their face and an approved liveness detection mechanism supporting Presentation Attacks Detection (PAD), as well as mechanisms for injection attack detection, in particular deepfake detection.
3. Lastly, if the person presenting the PID or attestation is able to present an identity document, the Relying Party may be able to verify User binding by comparing attributes from the PID or attestation, such as first and last name, to those in the identity document. However, this requires that the Relying Party can verify that the identity document is authentic and really belongs to the person presenting it. In practice this will often mean that the identity document is a photo ID, and the presentation must consequently be done in proximity and be supervised, or done remotely and supported by PAD.

6.6.3.10 Relying Party Instance verifies combined presentation of attributes

6.6.3.10.1 Introduction

According to the [European Digital Identity Regulation], a combined presentation of attributes is a request for attributes from two or more attestations in the same action. Scenarios where a User is asked to present different attributes from various physical documents are common in the real world, and are also relevant in the digital domain. Several examples, including university admissions, professional licencing, and rental or loan applications, are discussed in the Discussion Paper for Topic K. These scenarios can be addressed more efficiently through combined presentation, allowing a Relying Party to receive a consolidated set of attributes from different attestations.

In such cases, the Relying Party will need to verify that these attestations belong to the same User. This can be done in different ways, including (but not necessarily limited to):

- **Presentation-Based Binding**: A Relying Party may assume that attributes presented in a single presentation response are belonging to the same User. However, this means that the Relying Party trusts that the Wallet Unit is not hacked or fraudulent. In some high-security use cases, such trust may not be warranted.
- **Attribute-Based Binding**: Multiple attestations may include a shared unique identifier (e.g., a PID number), which can then serve as a binding reference across different attestations. Another possibility is the use of the same identifying data, such as full name and date of birth, in multiple attestations, which can be used to relate attestations to each other and to a User. This is analogous to many present-day processes using paper documents, which may be seen as an advantage. However, this method implies that identifying data of the User must be presented even in use cases where this is not necessary for the purposes of the use case itself. Moreover, this method may not be conclusive, for instance if multiple people share the same name.
- **Cryptographic Binding**: The WSCA/WSCD in the Wallet Unit may generate a cryptographic proof demonstrating that it manages the private keys associated with all of the involved PIDs and device-bound attestations. Since the WSCA/WSCD complies with stringent security requirements (possibly corresponding to LoA High), such a solution is more secure than presentation-based binding. It is more privacy-preserving than attribute-based binding, since no attributes more than strictly necessary for the use case have to be presented.

Cryptographic binding of attestations is discussed in the next section. For more information and high-level requirements, see Topic 18 and Topic 9.

6.6.3.10.2 Cryptographic binding between attestations

Cryptographic binding between attestations is an envisioned cryptographic mechanism that enables a WSCA/WSCD to prove that it manages the private keys corresponding to two (or more) public keys. Such a mechanisms can be used during attestation issuance, for instance to prove that the public key included in a PID and the public key to be embedded in a newly requested device-bound attestation are both managed by the same WSCD. A proof of cryptographic binding between attestations can be used as well during attestation presentation, e.g., to prove that the public keys associated with two (or more) device-bound attestations are managed by the same WSCA/WSCD and that, therefore, these attestations belong to the same User.

Note that:

- By definition, cryptographic binding between attestations can only be used for PIDs and device-bound attestations.
- This version of the ARF does not specify or reference a specific cryptographic mechanism to implement cryptographic binding between attestations.
- This ARF assumes that each Wallet Unit (and therefore each WSCA/WSCD) contains attestations for only one User (see also Section 3.2). Therefore, a proof of cryptographic binding between two attestations proves that these attestations belong to the same User. However, some additional actions must be done to use such a mechanism in practice:
  - During attestation issuance, an Attestation Provider must request the Wallet Unit to bind the new attestation to an existing PID or attestation. For this, the Attestation Provider must verify that the existing PID or attestation refers to the same User to whom the new attestation refers. How the Attestation Provider does this is out of scope of the ARF. For example, the Attestation Provider could request the User name and birth date from a PID on the Wallet Unit, verify that this information matches a record in its database, issue a attestation corresponding to the information in that record, and then request the Wallet Unit to bind the public key in that attestation to the public key in the PID.
  - A Relying Party that has verified a proof of cryptographic binding between two attestations needs to verify that these attestations belong to the User presenting them. This is User binding, as discussed in Section 6.6.3.9. Note that, if User binding is proven for one of the bound attestations, it is proven for all of them.

6.6.3.11 Relying Party Instance trusts issuer to have authenticated the Wallet Unit and the Wallet Provider

The Relying Party Instance does not have a way to directly verify the authenticity of the Wallet Unit and the Wallet Provider. Rather, the Relying Party trusts the PID Provider or the Attestation Provider to have done this during issuance of the PID or attestation.

6.6.3.12 Relying Party optionally trusts issuer to regularly verify that Wallet Unit is not revoked

Section 6.6.2.4 explained how a PID Provider or an Attestation Provider can verify that a WUA (and thus the Wallet Unit) is not revoked. That section also noted that the [CIR 2024/2977] requires PID Providers to verify regularly, during the entire lifetime of the PID, whether the Wallet Unit on which that PID is residing is revoked by the Wallet Provider. If that happens, the PID Provider must revoke the PID. Therefore, by verifying the revocation status of the PID, the Relying Party Instance can also trust the revocation status of the Wallet Unit.

Attestation Providers can use the same mechanism to provide the same assurance to Relying Parties, although this is not required by the CIR. It is up to a Relying Party to check, before starting requesting a particular type of attestation from Wallet Units to fulfil a particular use case, if the Attestation Provider of that attestation provides this assurance, and if not, to decide whether the associated risk is acceptable to the Relying Party.

6.6.3.13 Wallet Unit enables the User to report suspicious requests by a Relying Party and to request a Relying Party to erase personal data

A Wallet Unit enables the User to report unlawful or suspicious requests for personal data by a Relying Party to a Data Protection Authority (DPA). To allow this, a Wallet Unit provides a dashboard displaying all attestation presentation transactions performed by the Wallet Unit. For more information on this transaction log, see Topic 19.

The Wallet Unit enables the User to easily report a suspicious presentation request in the transaction log to a DPA. By default, this is the DPA that supervises the Relying Party, but if the Wallet Unit does not know which DPA this is (because this information was not available during the transaction), it will present the User with the contact details of at least the DPA of the region in which the Wallet Provider resides. The User can make such a report regardless of whether any attributes were actually presented to the Relying Party. Even if the Wallet Instance prevented the presentation of any attributes, for instance because Relying Party authentication failed, or if the User did not approve the presentation of any attributes, the User can still report the request to a Data Protection Authority.

For more information and requirements, see Topic 50.

The dashboard also enables the User to request a Relying Party to delete personal data in accordance with Regulation (EU) 2016/679 (the GDPR). In the context of EUDI Wallet, this personal data consists of attributes that were presented to the Relying Party by the User, using their Wallet Unit. Relying parties, which act as data processors or controllers, already have procedures, protocols, and interfaces in place to handle data deletion requests in accordance with the GDPR. Wallet Units re-use these already existing interfaces. As there are no standardised protocols and interfaces for this purpose (yet), this implies that a Wallet Unit can either

- open a specific URL with an external browser to ask for the deletion of data in a web form provided by the Relying Party.
- open an external mail client with a suitable template text,
- open an external phone client to enable the User to call the Relying Party.

The registration certificate of the Relying Party (see Section 6.4.2) contains the necessary contact information, including the URL of a web form for privacy-related enquiries, an e-mail address, and/or a phone number.

For more information and requirements on requesting a Relying Party to delete personal data, see Topic 48.

To be able to substantiate a report, or to list data that must be deleted, the User needs to be informed about which attributes were requested by which Relying Parties. To enable this, a Wallet Unit maintains a log of all transactions that are performed. For presentation transactions, this log includes the identifiers of the attributes that were requested and presented, but not their values. The aforementioned dashboard also enables the User to view the log and start a reporting process to a Data Protection Authority for any attestation presentation transaction in the log, or request the associated Relying Party to delete the attributes it received in that presentation transaction. More details about the logging functionality can be found in Topic 19.

6.6.4 PID or attestation presentation to another Wallet Unit

6.6.4.1 Introduction

Section 6.6.3 discussed the trust relationships necessary when a Wallet Unit receives a request from a Relying Party Instance and presents attributes to that Relying Party Instance. However, the [European Digital Identity Regulation] requires that a Wallet Unit is also able to receive such a request from another Wallet Unit, and present attributes to that requesting Wallet Unit. In this context, the requesting Wallet Unit is called the Verifier Wallet Unit, and the presenting Wallet Unit is called the Holder Wallet Unit. The User of a Holder Wallet Unit is called a Holder, and the User of a Verifier Wallet Unit is called a Verifier.

Wallet-to-Wallet interactions cover use cases where a natural person, the Holder, wishes to present a PID or attestation to another natural person, the Verifier, where both are using their Wallet Units. As an example, the use case could occur in a setting where one private person (the Verifier) wants to rent out their car to another private person (the Holder), provided the Holder has a valid driving licence.

Note that legal entities are not allowed to bypass the processes and rules governing Relying Parties, for example regarding the obligation to register, by using Wallet-to-Wallet interactions. Therefore,

- **Wallet-to-Wallet interactions will only take place in proximity, not remotely.** This ensures that both Users are aware of the device they are connecting to, because they have to present and scan a QR code or NFC tag. Being in proximity also allows for out-of-band communication and authentication possibilities between Holder and Verifier.
- **Wallet Units will be restricted in the number of times they can act as a Verifier per unit of time.** Since many Relying Parties will need to have frequent interactions with multiple Wallet Units, this ensures that it will not be feasible for a Relying Party to use a Wallet Unit for all of these interactions.
- **A User will need to select a dedicated 'Holder Wallet Unit' mode to start using Wallet-to-Wallet interactions.** If this mode is selected, a Holder Wallet Unit will clearly indicate to its User that they are presenting attributes to another natural person, and that they should not proceed if they are in fact interacting with a legal entity.

For more information, please refer to Technical Specification 9

6.6.4.1 General transaction flow

The following transaction flow will be used as the basis for Wallet-to-Wallet interactions:

1. The two EUDI Wallet Users meet in physical proximity and agree (out of band of the EUDI Wallet ecosystem), that one (the Holder) should present specific attributes from a PID or attestation to the other (the Verifier).
2. Both Users select a dedicated 'Wallet-to-Wallet mode' in their respective Wallet Unit and are asked to specify their role (Holder or Verifier).
3. The Holder Wallet Unit gives the Holder an option to suggest to the Verifier which PID or attestation, and which attributes. This suggestion is called a presentation offer.
4. A handshake protocol (called device engagement in ISO/IEC 18013-5) is performed and a data connection is established between the two devices as specified ISO/IEC 18013-5. This protocol also sends the presentation offer to the Verifier, if the User specified such an offer.
5. The Verifier now must specify to the Verifier Wallet Unit what attributes should be included in the presentation request:

   - If the Holder specified a presentation offer in step 3, the Verifier Wallet Unit displays the offer to the Verifier. The Verifier selects all or a subset of the offered attributes, but is not allowed to add additional attributes.
   - If there is no presentation offer in the handshake, the Verifier Wallet Unit assists the Verifier in creating a presentation request from scratch, by allowing the Verifier to select attributes from a pre-defined list populated by the Wallet Provider.

6. The Verifier Wallet Unit sends the presentation request to the Holder Wallet Unit.
7. The Holder Wallet Unit checks if the presentation request matches the presentation offer created in step 3 (if any), and aborts the transaction in case the request contains attributes that were not present in the offer. The Holder Wallet Unit informs the Holder about the reason for aborting. If no presentation offer was offer was sent in step 4, then this check is omitted.
8. The Holder Wallet Unit prompts the Holder for consent to present the requested attributes to the Verifier.
9. If the Holder approves the presentation, then a presentation is sent to the Verifier Wallet Unit.
10. The Verifier Wallet Unit verifies the received presentation in the same way a Relying Party Instance does, and presents the received attributes to the Verifier.
11. The Verifier makes a decision relevant to the use case, out of band of the EUDI Wallet ecosystem, but based (potentially among other factors) on the data presented by the Holder via their Wallet Units.

Notes:

- Step 2 ensures that both parties actively accept that a local data connection towards a natural person Wallet Unit should be established. For the Holder this is very important, because many if not all of the verifications usually done on a presentation request from a Relying Party will not be performed when a Wallet Unit acts as a Holder Wallet Unit; see the note to step 6 below. For the Verifier, this is necessary as well, since the functionality offered by a Verifier Wallet Unit is completely different then when acting a ‘normal’ Wallet Unit.
- In step 3, if the Holder wishes to let the Verifier specify the requested information, the presentation offer is left empty. However, the use of a presentation offer is recommended, as this increases the chance of success of the use case.
- Step 4 establishes a local data connection. [ISO/IEC 18013-5] requires that an mdoc reader(i.e., a Verifier Wallet Unit) must support QR code and NFC for device engagement, and BLE and NFC for data retrieval. A Holder Wallet Unit then chooses to use either QR code or NFC for device engagement, and either BLE or NFC for data retrieval. The requirements regarding supported technologies are therefore more stringent for a Verifier Wallet than for a Holder Wallet Unit. For the precise requirements, please refer to [ISO/IEC 18013-5]. This may mean that, depending on the device it’s installed on and the technologies chosen by the Holder, a Wallet Unit may not be able to act as a Verifier. For example, if a Holder Wallet Unit uses only NFC for device engagement, then a Wallet Unit on a device that does not have NFC will be not be able to act as a Verifier towards that Holder Wallet Unit. Technical Specification 9 will discuss ways to solve this challenge.
- In step 5, if the offered attributes do not fulfil the needs of the Verifier for the use case, the Verifier may decide to stop the transaction and return to step 1 to communicate (out of band) to the Holder which attributes the Holder should offer.
- In step 5, if there is no presentation offer, the Verifier Wallet Unit will present the Verifier with a list of ‘frequently used’ attributes to include in the presentation request. Conceivably, the Verifier Wallet Unit may limit the number of attributes in the list by asking the Verifier a set of predefined questions about the purpose of the use case. However, there is no guarantee that the Holder Wallet Unit contains these attributes.
- A user-friendly UI is important in steps 3 and 5 (when Users select what attributes to offer cq. request).
- In step 6, a presentation request from a Verifier Wallet Unit does not contain an access certificate (see Section 6.6.3.2) or a registration certificate (see Section 6.6.3.3). This

is because Verifiers are Users and are not required to register as a Relying Party. Additionally, because there is no access certificate in the presentation request, the Holder Wallet Unit is not able to evaluate an embedded disclosure policy, if existing, see Section 6.6.3.4. However, Technical Specification 9 will discuss if and how a Holder Wallet Unit might be able to authenticate the Verifier Wallet Unit. If this Technical Specification will specify such a mechanism, the Holder Wallet Unit will use it to make sure it is dealing with a Verifier using a certified Wallet Unit.
- In step 9, the Verifier Wallet Unit verifies the authenticity of the presented PID or attestation as specified in Section 6.6.3.6. This implies that the Verifier Wallet Unit needs to obtain the trust anchors of the relevant PID Provider or Attestation Provider from the respective Trusted List. Additionally, the Verifier Wallet Unit also verifies the revocation status of the presented PID or attestation as specified in Section 6.6.3.8.
- Only steps 2 to 9 are done within the Wallet Units. Steps 1 and 10 allow for additional actions to be taken and information to be exchanged between Holder and Verifier out of band.

For high-level requirements on this topic, please refer to Topic 30.

6.6.5 PID or attestation management

6.6.5.1 Overview

Starting from the issuance of a PID or attestation, the PID or attestation is managed by the User and the Wallet Provider. Management is performed until the PID or attestation, is deleted by the User (see Section 6.6.6) or the Wallet Instance is uninstalled by the User (see Section 6.5). Management includes at least the following processes:

1. Re-issuance of a PID or attestation when necessary.
2. Deletion of an unusable PID or attestation, typically after it has been replaced in a re-issuance process.
3. Revocation a the PID or attestation when necessary.

These processes are discussed in the next subsections.

6.6.5.2 PID or attestation re-issuance

6.6.5.2.1 Introduction

Re-issuance means the replacement of a PID or attestation that already exists in a Wallet Unit by a PID or attestation having the same attestation type. Re-issuance is always performed by the same PID Provider or Attestation Provider that issued the existing PID or attestation, and it is initiated by the Wallet Unit. The value of the attributes in the new attestation will typically be the same as in the original attestation. However, this is not required; the PID Provider or Attestation Provider may change one or more attribute values. Re-issuance is only applied within the administrative validity period of a document. As an example, a mobile driving licence (mDL) will typically be issued in the form of attestations which have a technical validity period shorter than the administrative validity period of the licence itself. Re-issuance is used for obtaining fresh attestations as needed during the administrative validity period, to ensure that the User can always present a valid mDL. When the administrative validity period ends, there will be an administrative process for obtaining a new driving licence, which is however out of scope of this document.

Note that, in general, if the original PID or attestation was issued in a batch, then the PID Provider or Attestation Provider will re-issue that PID or attestation in a batch as well.

There may be different reasons for re-issuing a PID or attestation, for example:

- The current PID(s) or attestation(s) are near the end of their technical validity period, or the Wallet Unit is running out of once-only attestations. This is done to mitigate the risk of Relying Party linkability. For more information, see Section 7.4.3.5.
- The value of one or more of the attributes in the PID or attestation has changed.
- The security architecture of the Wallet Solution uses PIDs and/or attestations that are issued just-in-time, at the moment that PID or attestation is being requested by a Relying Party. This is sometimes called synchronous issuing.

These reasons are discussed in the next subsections. Re-issuance is discussed in more detail in the Discussion Paper for Topic B.

6.6.5.2.2 Re-issuance to limit Relying Party linkability

As specified in [ISO/IEC 18013-5] or [SD-JWT VC], each PID or attestation contains metadata indicating its technical validity period. Determining the length of the technical validity period is the responsibility of the PID Provider or the Attestation Provider. The technical validity period chosen by the PID Provider or Attestation Provider will depend on several factors, primarily the security architecture of the Wallet Solution and the strategy chosen to mitigate Relying Party linkability, see Section 7.4.3.5.

Given the above factors, it can generally be assumed that the technical validity period of a

PID or attestations will be much shorter than their lifetime, meaning the period of time that a User wants to keep that PID or attestation in their Wallet Unit. That implies that new PIDs and attestations will need to be re-issued periodically, to replace the ones that are reaching end of their technical validity.

A similar reason for re-issuing PIDs and attestations occurs when the PID Provider or Attestation Provider uses once-only attestations (see Section 7.4.3.5), which can be presented only once to a Relying Party. In that case, the Wallet Unit, or rather the User, will regularly need new PIDs or attestations to avoid running out.

Re-issuance of PIDs or attestations for these reasons is a purely technical matter. To the maximum extent possible, the User does not notice that a PID or attestation has been re-issued, nor do they have to take any action to ensure that re-issuance happens in time. These conditions are very different from a first-time issuance of a PID or attestation, where the User must take the initiative to request the PID or attestation, and is potentially involved in the process in other ways as well.

This implies, among other, that no User authentication can take place during re-issuance of an existing attestation. Nevertheless, a Wallet Unit may offer the User the option to receive a notification of re-issuance.

In the absence of User authentication, and to prevent that a re-issued PID or attestation ends up at the wrong User, the PID Provider or Attestation Provider ensures that the re-issued PID or attestation is bound to the same WSCA/WSCD as the PID or attestation it replaces.

Finally, since the User is not involved, it is the Wallet Unit that triggers the re-issuance of PIDs and attestation when necessary.

6.6.5.2.3 Re-issuance because of a change of attribute values

During the lifetime of a PID or attestation, the value of some of the attributes may change. For example, at the date of birth of the User, an age attestation attribute (i.e., an attribute indicating whether the User has reached a certain age) may have to be changed from value False to value True. In another example, the User of a mobile driving licence may have passed the examination for a different vehicle category. In this case, the PID Provider or Attestation Provider re-issues the PID or attestation with the correct attribute values, and revokes the existing attestation.

Re-issuance of a PID or attestation for this reason will have an impact on the User, because they will notice that their attribute values have been changed. Therefore, in this case Users will be informed when re-issuance happens. Additionally, an Attestation Provider may state in their terms of conditions that re-issuance of an attestation may be used.

6.6.5.2.4 Re-issuance when using synchronous issuing

A third reason for re-issuing a PID or attestation is where the PID Provider or Attestation Provider uses synchronous issuing in their security architecture. In such an architecture, the Wallet Unit requests the re-issuance of a new PID or attestation after it has received a request for that PID or attestation from a Relying Party. Such a PID or attestation is very short-lived and is used only once.

The conditions on User awareness and authentication discussed in Section 6.6.5.2.2 are also valid for a synchronous re-issuance process.

6.6.5.3 Deletion of unusable PIDs or attestations

Some time after it is issued, a PID or attestation will become unusable, in the sense that the User cannot present it any longer to a Relying Party. For example, a PID or attestation expires, or a once-only PID or attestation (see Section 7.4.3.5) is already presented to a Relying Party. Typically (but not always), such a PID or attestation will already have been replaced in a re-issuance process as described in Section 6.6.5.2.2.

Wallet Providers need to decide what to do with unusable PIDs or attestations. Non device-bound attestation can be simply deleted, but for PIDs and device-bound attestations this is more complicated, as the Wallet Provider needs to manage the associated private keys in the WSCA/WSCD of the Wallet Unit. Typically, the amount of storage space available in a WSCA/WSCD is limited, and Wallet Providers will want to delete these keys to prevent an accumulation of unused private keys in the WSCA/WSCD. Deletion of private keys is a cryptographic key operation and cannot be done without User authentication; see Section 6.5.3.3. At the same time, for usability reasons the User should not be involved in such ‘cleaning up’ processes, just like the User does not have to take any action for re-issuance processes (Section 6.6.5.2.2).

The recommended solution for this challenge is to ensure that, whenever the WSCA/WSCD successfully authenticates the User, the Wallet Unit checks if there are any PIDs or device-bound attestations that cannot be presented any longer to Relying Parties. The Wallet Unit then requests the WSCA/WSCD to destroy all cryptographic key material in the WSCA/WSCD related to these PIDs or attestations. Thus, the Wallet Unit takes advantage of the fact that the User authenticates for another purpose, for example because they want to present a PID or device-bound attestation, to also carry out any necessary key deletion operations. See also Topic 40 in Annex 2.

6.6.5.4 PID or attestation revocation

PID or attestation management includes ensuring that PIDs and attestations can be revoked if necessary. Revocation is discussed in Topic 7. The User can request the PID Provider or Attestation Provider to revoke the PID or attestation at least in case of loss or theft. The PID Provider or Attestation can also decide itself to revoke a PID or attestation, for example in case the Wallet Unit on which the PID or attestation is residing is revoked; see Section 6.5.3.4.

6.6.6 PID or attestation deletion

In case the User no longer wants to retain a specific PID or attestation in their Wallet Unit, the User can delete it. If the PID Provider or Attestation Provider issued a batch of multiple PIDs or attestations that have the same content and are valid, the Wallet Unit deletes them all. Deleting a PID or a device-bound attestation also means that the WSCA/WSCD destroys the cryptographic key material associated with that PID or attestation. Before deleting the PID or attestation and the cryptographic keys, the WSCA/WSCD included in the Wallet Unit will authenticate the User.

If it supports the Digital Credentials API, see Section 4.4.3, the Wallet Unit also discloses the fact that it no longer contains the PID or attestation to the Digital Credentials API framework.

For high-level requirements on this topic, see Topic 51.

7 Certification and Risk Management

7.1 Introduction

This chapter briefly describes the certification of Wallet Solutions and the eID schemes under which they are provided, covering the overall certification approach, design principles, and main requirements outlined in the European Digital Identity Regulation and Commission Implementing Regulation CIR 2024/2981 laying down rules for on the certification of Wallet Solutions. Furthermore, references are made to the Annex I of CIR 2024/2981, the Risk Register, supporting the risk-based approach of the Wallet Solutions. For more detailed requirements, please refer to the CIR 2024/2981 itself.

The European Digital Identity Regulation requires certification of Wallet Solutions to ensure conformity of the Wallet Solutions with functional, security, and privacy related requirements, to achieve a high level of interoperability, security and trustworthiness. Certification applies to the Wallet Solutions and the eID schemes under which they are provided; for ease of reading this chapter only refers to Wallet Solutions. Furthermore, the object of certification includes software components, hardware components (in cases where they are provided directly or indirectly by the Wallet Provider) and the processes that support the provision and operation of a Wallet Solution, such as Wallet Unit activation, see Section 6.5.3.

The aim is to harmonise the implementation of the requirements laid down by the [European Digital Identity Regulation] and avoid divergent approaches to the maximum extent possible. For this reason, the Commission requested ENISA to prepare a candidate European certification scheme under the Cybersecurity Act, the CSA. As defining and adopting a dedicated, harmonised certification scheme for Wallet Solutions depends on agreements between Member States on detailed security requirements, on the availability of underlying certification schemes, and on established good practices in the Member States themselves, a transitory approach is foreseen by means of national certification schemes.

In other words, the certification approach for Wallet Solutions follows two phases. In the short-term, Member States provide national (transitory) certification schemes. In the medium term, a harmonised CSA scheme will be established. When the CSA-based scheme becomes available, it replaces the national schemes as for cybersecurity requirements. The schemes may continue to exist for functional requirements.

7.2. Certification of Wallet Solutions against national certification schemes

Until a dedicated Wallet Solution cybersecurity certification scheme under the CSA is available, the [European Digital Identity Regulation] requires Member States to establish national certification schemes. This will be done in time to make available the Wallet Solutions before the end of 2026. The Commission has adopted the CIR 2024/2981 to provide the main requirements on Member States for creation of national certification schemes. The CIR 2024/2981 and resulting national certification schemes are defined around a number of guiding principles:

First, the goal is to harmonise requirements to the extent possible. Member States are also encouraged to work together in the design and implementation of national schemes. Additionally, national schemes will leverage the use of relevant and existing certification schemes and standards for Wallet Solution certification and evaluation. Where available, relevant European

CSA schemes must be used. Currently, only the Common Criteria based European candidate cybersecurity certification EUCC scheme is available for the cybersecurity certification of ICT products, parts, or components for products. Upcoming CSA-based schemes include EUCS & EU5G. Additionally, other existing or upcoming schemes include schemes based on FITCEM (EN 17640), national schemes such as on remote identity verification, or other private schemes (e.g. for mobile devices and apps). For harmonisation of functional requirements, the Commission Implementing Regulations (CIRs) adopted under the European Digital Identity Regulation article 5(a) are referenced. For harmonisation of certification requirements, the ISO/IEC 17065 framework under Regulation [765/2008] is used, complemented by ISO/IEC 17067 on the definition of schemes.

Next, the CIR 2024/2981 refers to the composite nature of the Wallet Solutions as well as the potential different architectures in Member States, considering that the European Digital Identity Regulation is technology (and architecture) neutral. This means that a final ('top-level') certification of the Wallet Solution will yield a composite certificate, built on certification of separate components, such as EUCC certification. Wallet Solutions are always to be certified against assurance level High, as set out in the European Digital Identity Regulation as well as CIR (EU) 2015/1502. That assurance level has to be reached by the overall Wallet Solution. Under this Regulation, some components of the Wallet Solution may be certified at a lower assurance level, provided this is duly justified and without prejudice to the assurance level High reached by the overall Wallet Solution. For the use of assurance information from other certification schemes or sources, a dependency analysis will be performed.

Finally, in order to ensure a harmonised approach to cybersecurity and the assessment of the most critical risks that might affect the provision and operation of Wallet Units, a register of risks and threats is defined, see 7.4 Risk-based approach and risk register. The Risk Register contains high level risks and threats in relation to Wallet Solutions and the ecosystem, as well as detailed threat scenarios that will be taken into consideration when designing Wallet Solutions, independent of their specific architecture.

As a first step towards certification of Wallet Solutions under national schemes, Member States will assign a scheme owner, and design and roll out the scheme. As part of this process, Certification Bodies (CBs) will be accredited to carry out conformity assessments of Wallet Solutions against the requirements of the CIR 2024/2981 and the national scheme. Wallet Providers then request one or more designated CABs to assess and certify the conformity of their Wallet Solution. The CAB evaluates and certifies the conformity of the Wallet Solution if they meet the requirements.

The European Commission and ENISA support Member States in designing and implementing national certification schemes in the Cooperation Group.

7.3 Certification of Wallet Solutions against a dedicated CSA-based scheme

In parallel to the work described above, ENISA is requested to draft a dedicated European cybersecurity certification scheme for the Wallet Solutions under the CSA. Once available, this CSA-based scheme will replace the national transitory schemes mentioned above for the cybersecurity requirement it covers. This scheme will be based on available national schemes, harmonised requirements, and identify any additional requirements relevant for cybersecurity. The scheme will further detail the cybersecurity requirements, identify and set normative standards and define the target level of assurance or security for the relevant Wallet Solution components.

The work to develop the CSA-based scheme follows the milestones set out by the CSA and is supported by the Ad Hoc Working Group or 'AHWG'. This group is composed of selected experts from private organisations and industry, with extensive knowledge and experience in the areas of cybersecurity certification, digital wallets, electronic identification and trust services. The first step is to have a candidate scheme ready for public consultation and submitted for feedback of the European Cybersecurity Certification Group or ECCG. The ECCG's opinion serves as advisory input to ensure the candidate scheme aligns to EU cybersecurity objectives, standards and regulatory requirements. Although the ECCG's opinion is not binding, it will hold significant influence, as it reflects the collective expertise of national cybersecurity authorities, aiming to harmonise cybersecurity certification practices across Member States. Based on this input, the candidate scheme might be updated further. After finalisation of the ECCG opinion, the scheme will be transformed into a new Implementing Regulation and adopted by comitology procedure.

Finally, ENISA is also asked to facilitate the transition from national certification schemes to the dedicated cybersecurity certification scheme under the CSA.

7.4 Risk-based approach and risk register

7.4.1 Introduction

This section details the approach to develop harmonised guidelines for the development of the transitory national certification schemes. In addition to the requirements set out in the

European Digital Identity Regulation article 5c, cybersecurity risks and threats associated with the Wallet Solutions will be identified. Here, a risk-based approach is envisioned as the basis for certification by Member States, ensuring that the Wallet Solutions uphold confidentiality, availability and strong safeguards for User privacy and data protection. This is inspired by known processes, such as for the General Data Protection Regulation (GDPR) and related Data Protection Impact Assessments (DPIA).

The risk-based approach sets out a common Risk Register that contains a comprehensive but non-exhaustive list of risks and threats related to the Wallet Solution. These risks and threats are architecture-agnostic and provide a benchmark overview of the most critical risks and threats to Wallet Solutions. By adopting this common set of risks and threats, national transitory certification schemes will achieve a baseline level of harmonisation.

The risk register will be applied by scheme owners, Wallet Providers, and Certification Bodies (CBs). When establishing their certification schemes, scheme owners will perform a risk assessment to refine and complement the risks and threats listed in the register with those specific to their architecture, and consider how the applicable risks and threats can be appropriately treated. Wallet Providers will complement the scheme's risk assessment to identify any risks and threats specific to their implementation and propose appropriate mitigation measures for evaluation by the certification body.

7.4.2 High-level risks and threats

The following is an excerpt from [Risk Register]. To keep in line with the continuously evolving threat landscape, the risk register will be maintained and regularly updated in collaboration with the Cooperation Group.

High-level risks and threats

R1 Creation or use of an existing electronic identity R2 Creation or use of a fake electronic identity R3 Creation or use of fake attributes R4 Identify theft R5 Data theft R6 Data disclosure R7 Data manipulation R8 Data loss R9 Unauthorised transaction R10 Transaction manipulation R11 Repudiation R12 Transaction data disclosure R13 Service disruption R14 Surveillance

System-related risks

SR1 Wholesale surveillance SR2 Reputational damage SR3 Legal non-compliance

Technical threats

TT1 Physical attacks

1.1 Theft 1.2 Information leakage 1.3 Tampering

TT2 Errors and misconfigurations

2.1 Errors made when managing an IT system 2.2 Application-level errors or usage errors 2.3 Development-time errors and system misconfigurations

TT3 Use of unreliable sources

3.1 Erroneous use or configuration of wallet components

TT4 Failure and outages

4.1 Failure or dysfunction of equipment, devices or systems 4.2 Loss of resources 4.3 Loss of support services

TT5 Malicious actions

5.1 Interception of information 5.2 Phishing and spoofing 5.3 Replay of messages 5.4 Brute-force attack 5.5 Software vulnerabilities 5.6 Supply chain attacks 5.7 Malware 5.8 Random number prediction

7.4.3 Risks and mitigation measures discussed in Chapter 6 of this ARF

7.4.3.1 Introduction

This section briefly discusses some of the risks that were considered when the trust model in Chapter 6 was created, together with the mitigations for these risks and the residual risks that remain after these mitigations. This section is not intended to be a comprehensive risk register for the EUDI Wallet ecosystem as a whole; for that register, see [Risk Register] and Section 7.4.2 above. This section is limited to the scope of the ARF, namely, the Wallet Unit and its interactions with other entities in the ecosystem, as depicted in Figure 11 in Chapter 6.

7.4.3.2 Risks and mitigation measures related to confidentiality, integrity, and authenticity

Within the EUDI Wallet ecosystem, many interactions take place between entities in which one entity requests another entity to perform a task. For example, a User may ask a PID Provider or an Attestation Provider to provide a PID or an attestation to a Wallet Unit, or a Relying Party may ask a User to present attributes from an attestation in their Wallet Unit. For any of these interactions, the following risks apply:

- An attacker could impersonate one of the interacting entities. Therefore, the receiver of a message must be able to verify the identity of the sender, and vice versa. In other words, mutual authentication is needed. This authentication can be performed because valid entities in the EUDI Wallet ecosystem are put on a Trusted List by Member States. By verifying the signature over a message and verifying the associated public key certificates with a trust anchor included in a Trusted List, the receiver of a message can be sure about the identity of the message's sender.
- Messages between entities could be intercepted, meaning that they could be read by an attacker. To mitigate this risk, messages must be encrypted to ensure confidentiality.
- Intercepted messages could be changed by an attacker. To mitigate this risk, messages must be authenticated, so that the receiver can verify that originate from the authenticated sender and were not changed.

7.4.3.3 Risks and mitigation measures related to tampering of cryptographic keys and sensitive data

The mechanisms for authentication and confidentiality described in the previous section rely on the security of cryptographic keys, especially private and secret keys. If an attacker can obtain, use, or tamper with these keys, these security mechanisms would break down. Therefore, all cryptographic keys on Wallet Units are managed by dedicated secure applications (WSCAs), running on secure hardware (WSCDs), as described in Section 4.3. The security of WSCDs and WSCAs is ensured by means of an appropriate certification process.

Similar mitigation measures apply for all other entities in the EUDI Wallet ecosystem that use cryptographic keys, including Wallet Providers, PID Providers and Attestation Providers, Trusted List Providers, Providers of registration certificates, and Access Certificate Authorities. Such parties will typically use a certified Hardware Security Module (HSM) for managing private and secret keys. For Relying Parties and Relying Party Instances, such measures are formally not required.

WSCDs and WSCAs in a Wallet Unit may also be used to store other sensitive data except cryptographic keys. In particular, they could be used to store User attributes, in such a way that attackers, including malicious applications residing on the same User device as the Wallet Instance, cannot retrieve these attributes. This could be beneficial for User privacy.

7.4.3.4 Risks and mitigation measures related to authorisation

In certain cases, there is a risk that a legitimate entity within the EUDI Wallet ecosystem may attempt to perform actions beyond its authorised scope. This risk primarily affects two types of entities.

First, a non-qualified EAA Provider may attempt to issue attestations for which it lacks the necessary authorisation. For example, an Attestation Provider that has not been officially designated by a Member State or another relevant authority to issue diplomas may still attempt to generate an attestation of the diploma type. Within the EUDI Wallet ecosystem, this risk is limited to non-qualified EAA Providers, as PID Providers, QEAA Providers, and PuB-EAA Providers are assumed to be inherently trustworthy in this context. For more information, see Section 6.3.2.3.

This risk is mitigated by querying the Relying Party registry via an API. This registry, maintained by the Member State, contains comprehensive information about each Relying Party, allowing the system to verify the legitimacy of the issuer and ensure compliance with regulatory requirements.

In the context of the [European Digital Identity Regulation] Regulation, the term Relying Party encompasses both Attestation Providers and entities that provide services relying on attestations, ensuring a broad and consistent approach to trust and verification within the EUDI Wallet ecosystem.

Second, a Relying Party in the EUDI Wallet ecosystem may attempt to request attributes from a Wallet Unit without being registered or authorised to do so. This risk is mitigated mainly by three measures:

1. **Selective Disclosure and User Control** - The attestation formats and protocols specified in [ISO/IEC 18013-5] and [SD-JWT VC] (in combination with [OpenID4VP]) enable selective disclosure of attributes. This allows a Relying Party to specify which attributes within an attestation it wishes to receive while excluding others, a feature known as *collection limitation*. Additionally, selective disclosure ensures that the User retains control over their data, as they can approve or deny the presentation of requested attributes. More details on selective disclosure and User approval can be found in Section 6.6.3.5.
2. **Mandatory Relying Party Registration of Intended Requested Attributes** - The [European Digital Identity Regulation] mandates that each Relying Party register the attributes it intends to request from Users. According to CIR 2024/2982, these registered attributes must be included in a Relying Party registration certificate, which the Wallet Unit uses to

verify the legitimacy of the request and inform the User accordingly. This transparency ensures that Users can make an informed decision about whether to approve or deny the presentation of the requested attributes. More details on this requirement can be found in Section 6.6.3.3.

3. **Attestation Provider Disclosure Policy Enforcement** - The [European Digital Identity Regulation] also mandates that Attestation Providers can embed a disclosure policy within their attestations. This policy may include rules governing whether the Attestation Provider approves the presentation of this attestation to an authenticated Relying Party. The Wallet Unit evaluates this policy —if present— alongside authenticated data from the Relying Party, and informs the User of the outcome. This mechanism further supports the User in making a well-informed decision on whether to approve or deny attribute presentation. More information on disclosure policy enforcement can be found in Sections 6.6.2.7 and 6.6.3.4.

7.4.3.5 Risks and mitigation measures related to User privacy

7.4.3.5.1 Linkability

User privacy is a very important consideration in the design and implementation of the EUDI Wallet ecosystem. An important aspect of privacy is unlinkability. Unlinkability implies that, if a User presents attributes from an attestation multiple times, the receiving Relying Parties cannot link these separate presentations to conclude that they concern the same User.

Within the EUDI Wallet ecosystem, attributes are presented in electronic attestations containing unique, fixed elements such as hash values, salts, public keys, and signatures. Malicious Relying Parties could exploit these values to track Users by storing and comparing them across multiple transactions, identifying recurring patterns. This privacy threat, known as **Relying Party linkability**, can occur within a single Relying Party or among colluding entities. It can also occur when a third party attacks the systems of a Relying Party or of multiple Relying Parties resulting in a data breach. For that reason, Relying Parties will discard the unique fixed elements in received attestations as soon as they no longer need these elements.

A similar privacy threat arises when colluding Relying Parties share the unique values they obtained from an attestation with a malicious PID Provider or Attestation Provider. This allow the PID Provider or Attestation Provider to track User activity across multiple services. In this case, it’s called **Attestation Provider linkability**.

This topic is discussed in more detail in the Discussion Paper for Topic A.

7.4.3.5.2 Mitigating Relying Party linkability

Regarding the mitigation of Relying Party linkability: A trustworthy PID Provider or Attestation Provider can mitigate Relying Party linkability fully by issuing multiple PIDs or attestations to the same User. Wallet Units can use these attestations as disposable (single-use) attestations, which ensures attestations can never be linked by Relying Parties. Topic 10 in Annex 2 calls this 'once-only attestations', and requires Wallet Solutions to support this method. It also specifies how a PID Provider or Attestation Provider can indicate that they want a Wallet Unit to treat their PIDs or attestations in this way.

However, the 'once-only' approach increases issuance complexity and management overhead. Therefore, Topic 10 also mandates support for another solution, where PIDs and attestations are valid for a limited time only. This limits the amount of PIDs and attestations to be issued, but only partially mitigates Relying Party linkability. Topic 10/23 calls this 'limited-time attestations'.

Furthermore, Topic 10/23 describes two other approaches, which are optionally supported by Wallet Solutions, namely:

- the Attestation Provider issues attestations in batches to the Wallet Unit. The Wallet Unit then uses the attestations from a batch in a random order, until it has presented all attestations in the batch once. Then it 'resets' the batch and starts using them again in a random order. Topic 10/23 calls this 'rotating-batch attestations'.
- the Wallet Unit will present different attestations to different Relying Parties. However, in case a Relying Party requests attributes from this attestation multiple times, the Wallet Unit will present the same attestation to this Relying Party each time. Topic 10/23 calls this 'Per-Relying Party attestations'.

Additionally, organisational and enforcement measures can help deter Relying Parties from colluding and tracking Users. In particular, Relying Parties found in violation will have their access certificates revoked, preventing them from further interactions with Wallet Units.

7.4.3.5.3 Zero-Knowledge Proofs

NOTE: Discussions on Zero-Knowledge Proofs are ongoing. No specific ZKP has *been selected to be supported by components in the EUDI Wallet ecosystem.

Attestation Provider linkability cannot be fully eliminated when using attestation formats based on salted hashes. The only viable mitigation is to adopt Zero-Knowledge Proofs (ZKPs) as a verification mechanism instead of relying on salted-attribute hashes. However, the integration of ZKPs in the EUDI Wallet ecosystem is still under discussion and development due to the complexity of implementing ZKP solutions in secure hardware and the lack of support in currently available secure hardware (WSCDs). As with Relying Party linkability, organisational and enforcement measures can help deter Attestation Providers from colluding and tracking Users. Additionally, many Attestation Providers are subject to regular audits, making it easier to detect collusion and tracking compared to Relying Parties.

Zero-Knowledge Proof (ZKP) mechanisms for verifying personal information are highly promising and essential for ensuring privacy in various use cases. They enable Users to prove statements such as “I am over 18” without disclosing any personal data, offering a robust solution for privacy-preserving authentication and verification.

One area of development is age verification, where the European Commission is actively exploring and testing ZKP-based solutions. The outcomes of this initiative could pave the way for the adoption of ZKPs within the EUDI Wallet ecosystem, further strengthening privacy protections in future implementations.

The Discussion Paper for Topic G (Zero-Knowledge Proofs) presents the (desired) privacy properties of Zero-Knowledge Proof schemes. It introduces the main families of Zero-Knowledge Proof schemes and gives an overview of representative solutions. Finally, it discusses topics related to the integration of Zero-Knowledge Proof schemes into the EUDI Wallet ecosystem.

High-level requirements for Zero-Knowledge Proofs to be used in the EUDI Wallet ecosystem are included in Topic 53 of Annex 2.

8 Accessibility

8.1 Introduction

Accessibility of all **User-facing components** of the EUDI Wallet ecosystem, such as Wallet Units, websites, User authentication methods of PID Providers and Attestation Providers, and registries (see Section 3.17), is essential to ensure that these digital tools are inclusive by design and aligned with the applicable European legal and technical frameworks.

Accessibility is not only a matter of **legal compliance** but also a fundamental condition for **equal access, User trust, and widespread adoption** across all segments of the population, including persons with disabilities.

For high-level requirements on accessibility, please refer to Topic 54.

This section will be updated in line with the developments of Discussion Topic Q: Interface between the User and the Wallet Instance.

8.2 Legal instruments and standards

The following main legislative instruments and standards apply:

- Directive (EU) 2016/2102 on the accessibility of websites and mobile applications of public sector bodies. This Directive establishes a common framework to harmonise accessibility requirements across Member States, ensuring that digital public services, including mobile applications, are perceivable, operable, understandable, and robust for all Users. In particular, it requires compliance with:
  - European Standard EN 301 549 V1.1.2, which defines accessibility requirements for ICT products and services, covering web content, software, mobile applications, hardware interfaces, and documentation.
- Directive (EU) 2019/882, the European Accessibility Act (EAA). This Directive extends accessibility obligations to a wider range of products and services placed on the EU market, including digital services beyond the public sector. It sets essential accessibility requirements for economic operators, including service providers and manufacturers, ensuring that solutions such as Wallet Units are accessible to persons with disabilities throughout their entire lifecycle, from design and development to marketing and after-sales support.

8.3 Wallet Units and other User-facing components

Together, these legal instruments create a **coherent legal and normative environment** that supports the development of accessible Wallet Units and related components. Compliance with these frameworks is both a regulatory obligation and a driver of **innovation, social inclusion, and digital equality**.

It is therefore crucial that accessibility is integrated into:

- Technical specifications

- User interface design

- Testing processes
- Procurement criteria

for all elements of the Wallet ecosystem.

Member States and implementing entities should also ensure **ongoing monitoring, effective feedback mechanisms, and continuous improvement** of accessibility practices. This requires close collaboration with Users, accessibility experts, and organisations representing persons with disabilities, to guarantee that Wallet Units and other User-facing components remain usable, effective, and inclusive for all.

9 Document development

9.1 Publication

This document is made publicly available at https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework (GitHub repository) where it will be regularly updated.

9.2 Contributing

We value your feedback and encourage you to share any thoughts, suggestions, or concerns you may have regarding this document.

9.2.1 Providing Feedback

To provide feedback on this document, please visit our GitHub repository. You can do so by navigating to the "Issues" tab and submitting a new issue or commenting on existing ones. Whether you've spotted a typo, have a suggestion for clarifying a section, or want to propose a new topic for inclusion, we welcome your feedback.

9.2.1.1 Guidelines for adding issues to the Github repository

When adding issues to the Github repository, please follow these general guidelines:

- Use **clear and descriptive titles** for your issues to provide a concise summary of the problem or task. This helps others quickly understand the issue at a glance.
- Provide a **detailed description of the issue**, including any relevant context, background information. The description should be comprehensive enough for others to understand the issue and take appropriate action.
- Use one or more of the following **labels** to categorise issues. Labels help organise and prioritise issues, making it easier to manage the repository.

Label	Description
Content Clarifications	Raise issues seeking clarification on specific content within the document. This could include explanations of concepts, definitions of terms, or examples to illustrate certain points.
Suggestions for Improvements	Propose suggestions to enhance the clarity, completeness, or accuracy of the document. This could involve restructuring sections, adding examples, or providing additional information.
Errors and Corrections	Identify errors such as typos, grammatical mistakes, or factual inaccuracies within the document and suggest corrections.
Compatibility and Integration	Issues related to how the document integrates with other systems or technologies, ensuring compatibility with different platforms or frameworks.
Enhancement Requests	Request new features, sections, or content to be added to the document to improve its usefulness or relevance.

Label	Description
Formatting and Styling	Feedback regarding the visual appearance, organisation, and consistency of formatting within the document.
Documentation Standards	Discussions around adhering to documentation standards, conventions, or guidelines.
Licence and Legal Concerns	Questions or concerns related to the licensing of the document, usage rights, attribution requirements, or legal implications for contributors and Users.
Technical Clarification	Raise issues seeking clarification on specific technical content within the document.

- **Attach** relevant files, screenshots, or links to additional resources that provide context or assist in resolving the issue. This can include **references** to related documentation or discussions.
- **Follow issue etiquette** by conducting a search to see if the issue has already been reported before creating a new one. This helps avoid duplicate issues.

9.2.1.2 Guidelines for discussing existing issues in the GitHub repository

When discussing existing issues in the Github repository, please follow these general guidelines:

- **Communicate with respect and courtesy** towards other contributors, maintain a professional tone, and avoid using language that could be interpreted as confrontational or inflammatory.
- Provide **context and background information** to help others understand your perspective. Explain the reasoning behind your comments.
- Communicate your intentions and motivations behind your comments or suggestions to **avoid misunderstandings**.

- Keep **discussions focused on the technical aspects of the issue** at hand.
- Provide **constructive feedback and suggestions** in a helpful and supportive manner. Instead of simply pointing out problems, offer solutions or alternative approaches to address the issue positively.
- Approach discussions with a **mindset of collaboration and problem-solving**.
- Be **open to different perspectives**, as contributors may have different viewpoints, experiences, and expertise levels.
- Contribute to a **positive and welcoming community atmosphere**.

9.2.2 Managing Issues and Pull Requests

Our team is committed to managing issues and pull requests related to this document in a transparent and efficient manner to ensure that all feedback is addressed promptly and effectively. Here's how we manage issues and pull requests to set the right expectations:

- Issue Management: When an issue is submitted, our team will review and prioritise it based on its relevance and impact. We'll keep you informed of the status of your issue and provide updates as it progresses. Once resolved, we'll close the issue and incorporate any necessary changes into the document.
- Pull Request Management: If you submit a pull request with proposed changes or improvements to the document, our team will review it carefully and provide feedback and suggestions for refinement. We'll work collaboratively with you to ensure that your contribution aligns with our document's objectives and maintains consistency and quality. Once approved, we'll merge your changes into the document and acknowledge your contribution.

Your feedback and contributions are essential in helping us maintain the quality and relevance of this document. We value your participation and strive to create a collaborative environment where everyone's contributions are valued and recognised.

9.3 Document Versioning

To avoid interoperability issues and changes to the ARF going unnoticed, a version control system and the following semantic versioning scheme (https://semver.org) will be used for the ARF.

The ARF document will be published under a standardised release versioning format, *MAJOR.MINOR.PATCH*, where:

MAJOR version is incremented (i.e., new version), when the ARF document has *undergone significant changes, for example introducing some breaking changes in* the architecture,

MINOR version is incremented when new information has been added to the *document or information has been removed from the document, and

PATCH version is incremented when minor changes have been made (e.g., fixing *typos).

10 References

Note: All standards and technical specifications (as opposed to Regulations and Implementing Regulations) in this list are undated. A reference is added to the entry for the respective document on the Standards and Technical Specifications Roadmap, which contains the latest information regarding the targeted version.

Item Reference	Standard name/details
[2015/1505]	COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) 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.
[European Digital Identity Regulation]	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

Item Reference	Standard name/details
[Risk Register]	Regulation (EU) 2024/2981, Annex I of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets
[CIR 2024/2977]	Commission Implementing Regulation 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets
[CIR 2024/2979]	Commission Implementing Regulation 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets
[CIR 2024/2980]	Commission Implementing Regulation 2024/2980 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem
[CIR 2024/2981]	Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets

Item Reference	Standard name/details
[CIR 2024/2982]	Commission Implementing Regulation 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework
[CIR 2025/846]	Commission Implementing Regulation 2025/846 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards cross-border identity matching of natural persons
[CIR 2025/847]	Commission Implementing Regulation 2025/847 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets
[CIR 2025/848]	Commission Implementing Regulation 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties
[CIR 2025/849]	Commission Implementing Regulation 2025/849 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the submission of information to the Commission and to the Cooperation Group for the list of certified European Digital Identity Wallets

Item Reference	Standard name/details
[CIR 2025/1566]	Commission Implementing Regulation 2025/1566 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for the verification of the identity and attributes of the person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued
[CIR 2025/1567]	Commission Implementing Regulation 2025/1567 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the management of remote qualified electronic signature creation devices and of remote qualified electronic seal creation devices as qualified trust services
[CIR 2025/1568]	Commission Implementing Regulation 2025/1568 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards procedural arrangements for peer reviews of electronic identification schemes and for cooperation on the organisation of such reviews within the Cooperation Group and repealing Commission Implementing Decision (EU) 2015/296

Item Reference	Standard name/details
[CIR 2025/1569]	Commission Implementing Regulation 2025/1569 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards qualified electronic attestations of attributes and electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source
[CIR 2025/1570]	Commission Implementing Regulation 2025/1570 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notification of information on certified qualified electronic signature creation devices and certified qualified electronic seal creation devices
[CIR 2025/1571]	Commission Implementing Regulation 2025/1571 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the formats and procedures for annual reports by supervisory bodies
[CIR 2025/1572]	Commission Implementing Regulation 2025/1572 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the format and procedures for notification of intention and verification with regard to the initiation of qualified trust services

Item Reference	Standard name/details
[CIR 2025/1929]	Commission Implementing Regulation 2025/1929 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the binding of date and time to data and establishing the accuracy of the time sources for the provision of qualified electronic time stamps
[CIR 2025/1942]	Commission Implementing Regulation 2025/1942 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards qualified validation services for qualified electronic signatures and qualified validation services for qualified electronic seals
[CIR 2025/1943]	Commission Implementing Regulation 2025/1943 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for qualified certificates for electronic signatures and qualified certificates for electronic seals
[CIR 2025/1944]	Commission Implementing Regulation 2025/1944 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for processes for sending and receiving data in qualified electronic registered delivery services and as regards interoperability of those services

Item Reference	Standard name/details
[CIR 2025/1945]	Commission Implementing Regulation 2025/1945 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the validation of qualified electronic signatures and of qualified electronic seals and the validation of advanced electronic signatures based on qualified certificates and of advanced electronic seals based on qualified certificates
[CIR 2025/1946]	Commission Implementing Regulation 2025/1946 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards qualified preservation services for qualified electronic signatures and for qualified electronic seals
[ISO/IEC 18013-5]	ISO/IEC 18013-5, Personal identification — ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application
[ISO/IEC 18013-7]	ISO/IEC 18013-7, Personal identification — ISO-compliant driving licence - Part 7: Mobile driving licence (mDL) add-on functions
[ISO/IEC 23220-2]	ISO/IEC 23220-2, — Cards and security devices for personal identification — Building blocks for identity management via mobile devices - Part 2: Data objects and encoding rules for generic eID systems
[ISO 3166-1]	ISO 3166-1: Codes for the representation of names of countries and their subdivisions – Part 1: Country codes: alpha-2 country

Item Reference	Standard name/details
[ISO 3166-2]	ISO 3166-2:2020: Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code
[ETSI TS 119 612]	ETSI TS 119 612: Electronic Signatures and Infrastructures (ESI); Trusted Lists
[ETSI TS 119 431-1]	ETSI TS 119 431-1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.
[ETSI TS 119 431-2]	ETSI TS 119 431-2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation
[ETSI TS 119 432]	ETSI TS 119 432 - Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation
[ETSI EN 319 132-1]	ETSI EN 319 132-1 - Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures (XAdES)
[ETSI TS 119 182-1]	ETSI TS 119 182-1 - Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures
[ETSI EN 319 122-1]	ETSI EN 319 122-1 - Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures

Item Reference	Standard name/details
[ETSI EN 319 162-1]	ETSI EN 319 162-1 - Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers
[ETSI EN 319 142]	ETSI EN 319 142-1 - Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
[CEN EN 419 241-1]	CEN EN 419 241-1 – Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements
[SD-JWT VC]	SD-JWT-based Verifiable Credentials (SD-JWT VC). Retrievable from: https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/
[RFC 2119]	RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels. S. Bradner, March 1997.
[RFC 3339]	RFC 3339 - Date and Time on the Internet: Timestamps, G. Klyne et al., July 2002
[RFC 9562]	RFC 9562 - Universally Unique IDentifiers (UUIDs), P. Leach et al., May 2024
[RFC 5280]	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, D. Kooper et al., May 2008
[RFC 3647]	RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, S. Chokhani et al., November 2003
[RFC 7519]	RFC 7519 - JSON Web Token (JWT), M. Jones et al., May 2015

Item Reference	Standard name/details
[RFC 8259]	RFC 8259 - The JavaScript Object Notation (JSON) Data Interchange Format, T. Bray, Ed., December 2017
[RFC 8610]	RFC 8610 - Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures, H. Birkholz et al., June 2019
[RFC 8943]	RFC 8943 - Concise Binary Object Representation (CBOR) Tags for Date, M. Jones et al., November 2020
[RFC 8949]	RFC 8949 - Concise Binary Object Representation (CBOR), C. Bormann et al., December 2020
[CSC API]	Cloud Signature Consortium API Specification v2.0, 20 April 2023
[GP OMAPI]	GPD_SPE_075 Open Mobile API Specification, v3.3, July 2018, GlobalPlatform
[GP CS]	GPC_SPE_034 Card Specification, v2.3.1, March 2018, GlobalPlatform
[GSMA SAM]	GSMA Secured Applications for Mobile, v1.1, 03 November 2023, GSM Association
[W3C VCDM v2.0]	Sporny, M. *et al,* Verifiable Credentials Data Model v2.0, W3C Recommendation
[W3C VC-JOSE-COSE]	Jones, M. *et al,* Securing Verifiable Credentials using JOSE and COSE, W3C Recommendation
[W3C VC Data Integrity]	Sporny, M. *et al,* Verifiable Credential Data Integrity 1.0, W3C Recommendation
[W3C Digital Credentials API]	Caceres, M., Cappalli, T., Goto, S. *et al,* Digital Credentials API, Draft Community Group Report

Item Reference	Standard name/details
[W3C WebAuthn]	Jeff Hodges *et al,* Web Authentication, An API for accessing Public Key Credentials Level 2, W3C Recommendation
[CTAP]	Client to Authenticator Protocol (CTAP) Review Draft, March 21, 2023. Available: https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/issues/365
[OpenID4VCI]	Lodderstedt, T. et al., OpenID for Verifiable Credential Issuance, OpenID Foundation.
[OpenID4VP]	Terbu, O. et al., OpenID Connect for Verifiable Presentations, OpenID Foundation.
[OIDC]	Sakimura, N. et al., OpenID Connect Core 1.0, OpenID Foundation.
[EKYC]	Lodderstedt, T. et al., OpenID Connect for Identity Assurance Claims Registration 1.0, OpenID Foundation.
[EKYC Schema]	Lodderstedt, T. et al., OpenID Identity Assurance Schema Definition 1.0, OpenID Foundation.
[HAIP]	Yasuda, K. et al, OpenID4VC High Assurance Interoperability Profile, OpenId Foundation.
[IANA-JWT-Claims]	IANA JSON Web Token Claims Registry
[Topic 6]	Annex 2 - Relying Party authentication and User approval
[Topic 7]	Annex 2 - Attestation revocation and revocation checking
[Topic 9]	Annex 2 - Wallet Unit Attestation
[Topic 10]	Annex 2 -Issuing a PID or attestation to a Wallet Unit
[Topic 11]	Annex 2 - Pseudonyms
[Topic 12]	Annex 2 - Attestation Rulebooks

Item Reference	Standard name/details
[Topic 16]	Annex 2 - Signing documents with a Wallet Unit
[Topic 18]	Annex 2 - Combined presentations of attributes
[Topic 19]	Annex 2 - User Navigation requirements (Dashboard logs for transparency)
[Topic 23]	Annex 2 - PID issuance and (Q)EAA issuance
[Topic 25]	Annex 2 - Unified definition and controlled vocabularies for attributes
[Topic 26]	Annex 2 - Catalogue of attestations
[Topic 27]	Annex 2 - Registration of PID Providers, Providers of QEAAs, PuB-EAAs, and (non-qualified) EAAs, and Relying Parties
[Topic 30]	Annex 2 - Interaction between Wallet Units
[Topic 31]	Annex 2 - PID Provider, Wallet Provider, Attestation Provider, and Access Certificate Authority notification and publication
[Topic 33]	Annex 2 - Wallet Unit backup and restore
[Topic 34]	Annex 2 - Migrate to a different Wallet solution
[Topic 37]	Annex 2 - QES – Remote Signing - Technical Requirements
[Topic 38]	Annex 2 - Wallet Unit revocation
[Topic 40]	Annex 2 - Wallet Instance installation and Wallet Unit activation and management
[Topic 42]	Annex 2 - Requirements for QTSPs to access Authentic Sources
[Topic 43]	Annex 2 - Embedded disclosure policies
[Topic 44]	Annex 2 - Relying Party registration certificates
[Topic 48]	Annex 2 - Blueprint for requesting data deletion to Relying Parties

Item Reference	Standard name/details
[Topic 50]	Annex 2 - Blueprint to report unlawful or suspicious request of data
[Topic 51]	Annex 2 - PID or attestation deletion
[Topic 52]	Annex 2 - Relying Party intermediaries

11 Annexes

- Definitions - Annex 1
- High Level Technical Requirements - Annex 2
- Rulebooks - Annex 3:
  - PID Rulebook - Annex 3.1
  - mDL Rulebook - Annex 3.2
- Service Blueprints - Annex 4:
  - Blueprint Initialisation and activation - Annex 4.1
  - Blueprint Online identification and authentication - Annex 4.2
  - Blueprint Issuing mDL - Annex 4.3
  - Blueprint Presenting mDL (proximity-supervised) - Annex 4.4
  - Blueprint Presenting mDL (proximity-unsupervised) - Annex 4.5
  - Blueprint Remote QES – Creating a signature for authentication / authorisation - Annex 4.6
  - Blueprint Remote QES - Enrolment - Annex 4.7
  - Blueprint Remote QES - Creating a signature channelled by a Wallet Unit - Annex 4.8
  - Blueprint Remote QES - Creating a signature channelled by Relying Party - Annex 4.9
  - Blueprint QES – View history of signatures - Annex 4.10
  - Blueprint Local QES - Enrolment - Annex 4.11
  - Blueprint Local QES – Creating a signature - Annex 4.12
- Design Guides - Annex 5:

  - Wallet Unit design guide - Annex 5.1
  - Wallet Unit design guide – data sharing scenarios - Annex 5.2

ANNEX 1 - Definitions

A.1 Introduction

In the Architecture Reference Framework (ARF) many terms are used that need a precise definition. This Annex contains the definitions of these terms.

In fact, there are three sources for these definitions:

- In the first place, the [European Digital Identity Regulation] defines several of these terms. For convenience, these definitions are listed in Section A.2.
- Secondly, the adopted Commission Implementing Regulations CIR 2024/2977, CIR 2024/2979, CIR 2024/2980, CIR 2024/2981, and CIR 2024/2982 also contain a list of definitions. Again for convenience, these definitions are included in Section A.3
- Thirdly, in writing the ARF, additional technical terms and corresponding definitions are used. These are listed in Section A.4.

A.2 Definitions from the [European Digital Identity Regulation]

The following terms are defined in the [European Digital Identity Regulation] and used in the ARF.

Term	Definition in [European Digital Identity Regulation]
Electronic attestation of attributes (EAA)	An attestation in electronic form that allows attributes to be authenticated.
Attribute	A characteristic, quality, right or permission of a natural or legal person or of an object.

Term	Definition in [European Digital Identity Regulation]
Authentic Source	A repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union law or national law, including administrative practice.
Authentication	An electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form.
Conformity Assessment Body (CAB)	A conformity assessment body as defined in Article 2, point 13, of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides, or as competent to carry out certification of European Digital Identity Wallets or electronic identification means.
Electronic attestation of attributes issued by or on behalf of a public sector body (PuB-EAA)	An electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII.

Term	Definition in [European Digital Identity Regulation]
Electronic identification scheme	A system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons.
(Electronic) signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
(Electronic) seal	Data in electronic form which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity
Person Identification Data (PID)	A set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.
Public Sector Body	A state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate.
Qualified Electronic Attestation of Attributes (QEAA)	An electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V.

Term	Definition in [European Digital Identity Regulation]
Qualified Electronic Signature (QES)	An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.
Qualified Electronic Signature Creation Device (QSCD)	Configured software or hardware used to create an electronic signature that meets the requirements laid down in Annex II of the [European Digital Identity Regulation].
Qualified Trust Service Provider (QTSP)	Qualified Trust Service Provider means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
Relying Party	A natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service
strong User authentication	An authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

Term	Definition in [European Digital Identity Regulation]
User	A natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with the [European Digital Identity Regulation].

Table 1: Definition of terms used in the ARF originating from the [European Digital Identity Regulation]

A.3 Definitions from the adopted Commission Implementing Regulations

The following terms are defined in the adopted Commission Implementing Regulations and used in the ARF. Note that small differences exist in the way in which terms are written, for example regarding capitalisation. The table contains the term as used in the ARF.

Term	Definition
(Wallet) User	A user who is in control of the Wallet Unit
Wallet Unit	A unique configuration of a Wallet Solution that includes Wallet instances, Wallet Secure Cryptographic Applications and Wallet Secure Cryptographic Devices provided by a Wallet Provider to an individual Wallet User
Wallet Solution	A combination of software, hardware, services, settings, and configurations, including Wallet Instances, one or more Wallet Secure Cryptographic Applications and one or more Wallet Secure Cryptographic Devices

Term	Definition
Provider of person identification data (PID Provider)	A natural or legal person responsible for issuing and revoking the person identification data and ensuring that the person identification data of a user is cryptographically bound to a Wallet Unit
Wallet Unit Attestation (WUA)	A data object that describes the components of the Wallet Unit or allows authentication and validation of those components;
Embedded disclosure policy	A set of rules, embedded in an electronic attestation of attributes by its provider, that indicates the conditions that a wallet-relying party has to meet to access the electronic attestation of attributes
Registrar (of wallet-relying parties)	The body responsible for establishing and maintaining the list of registered wallet-relying parties established in their territory who has been designated by a Member State
Wallet Instance	The application installed and configured on a Wallet User's device or environment, which is part of a Wallet Unit, and that the Wallet User uses to interact with the Wallet Unit
Wallet Secure Cryptographic Application (WSCA)	An application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the Wallet Secure Cryptographic Device

Term	Definition
Wallet Secure Cryptographic Device (WSCD)	A tamper-resistant device that provides an environment that is linked to and used by the Wallet Secure Cryptographic Application to protect critical assets and provide cryptographic functions for the secure execution of critical operations
Wallet Provider	A natural or legal person who provides Wallet Solutions
critical assets	Assets within or in relation to a Wallet Unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, this would have a very serious, debilitating effect on the ability to rely on the Wallet Unit
(Wallet-) Relying Party	A Relying Party that intends to rely upon Wallet Units for the provision of public or private services by means of digital interaction
(Wallet-relying party) access certificate	A certificate for electronic seals or signatures authenticating and validating the (Wallet-) Relying Party, issued by a provider of wallet-relying party access certificates
Provider of wallet-relying party access certificates (Access Certificate Authority, Access CA)	A natural or legal person mandated by a Member State to issue Relying Party access certificates to (Wallet-) Relying Parties registered in that Member State.
Provider of (wallet-relying party) registration certificates	a natural or legal person mandated by a Member State to issue (wallet-relying party) registration certificates to (wallet-)relying parties registered in that Member State

Term	Definition
(Wallet-relying party) registration certificate	A data object that indicates the attributes the Relying Party has registered to intend to request from Users

A.4 Additional definitions used in the ARF

Note: The technical terms and definitions in Table 3 below are intended to be defined in such a way that they are aligned with the definitions used in the [European Digital Identity Regulation] and the Commission Implementing Regulations in Tables 1 and 2, and should be interpreted as such. In case any definition in Table 3 contradicts a definition from the [European Digital Identity Regulation] or the Commission Implementing Regulations, the latter take precedence.

In some cases, a term has its origin in the context of a specific Topic in Annex 2. In such a case, the topic number is mentioned in a note. If the definition relies on an external source, such as a standard or a formal publication, that source is mentioned.

Term	Definition
Administrative validity period (of a PID or attestation)	The date(s) from and/or up to which the attributes in the attestation are valid, which are represented as attribute(s) in the attestation. *Note: Some attestations, for instance diplomas, do not have an administrative validity period.*
Attestation	When not further qualified, a collective term for a QEAA, PuB-EAA, or (non-qualified) EAA.
Attestation Provider	When not further qualified, a collective term for QEAA Provider, PuB-EAA Provider, or (non-qualified) EAA Provider.

Term	Definition
Attestation Revocation List	A mechanism provided by a PID Provider or an Attestation Provider (or a trusted party acting on its behalf) for communicating the revocation status of PIDs and attestations, by publishing a list of identifiers of revoked PIDs or attestations. *Note: See Topic 7.*
Attestation Rulebook	A document describing the attestation type, namespace(s), and other features for a specific attestation type. *Note: See Topic 12.*
Attestation Status List	A mechanism provided by a PID Provider or an Attestation Provider (or a trusted party acting on its behalf) for communicating the revocation status of PIDs and attestations, by publishing status information (Valid or Invalid) for all relevant PIDs or attestations. *Notes: -See Topic 7. -Which PIDs or attestations are relevant is determined by the entity publishing the status list. For example, a status list may contain all PIDs or attestations whose validity period is not over yet at the time of publication of the list.*
Attestation type	An identifier for a type of attestation, unique within the context of the EUDI Wallet ecosystem. *Note: See Topic 12.*
Certificate Authority (CA)	An entity which is trusted by one or more parties in the EUDI Wallet ecosystem to create and seal certificates.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Term	Definition
Holder (when used in the context of Wallet-to-Wallet interactions)	A User wishing to use their Wallet Unit to present attributes from a PID or attestation to the User of another Wallet Unit. *Notes: See also Verifier. - See Topic 30.*
Holder Wallet Unit	A Wallet Unit used by a Holder.
Intermediary	A Relying Party that offers services to other (intermediated) Relying Parties to, on their behalf, connect to Wallet Units and request the User attributes that these intermediated Relying Parties need. *Note: See Topic 52*
Namespace	A specification of the attribute identifier, syntax and semantics of attributes that can be used in an attestation, having an identifier that is unique within the context of the EUDI Wallet ecosystem. *Note: See Topic 12.*
National Accreditation Bodies (NAB)	A body that performs accreditation with authority derived from a Member State under Regulation (EC) No 765/2008.
Notification	The act of transferring information to the European Commission. *Note: see Topics 31.
Pseudonym	Data uniquely representing a User which in itself does not allow to infer the User's attributes or person identification data, without the use of additional information that is kept separately by the issuer of the data uniquely representing the user. *Note: See Topic 11.*

Term	Definition
Public Key Infrastructure (PKI)	Systems, software, and communication protocols that are used by EUDI Wallet ecosystem components to distribute, manage, and control public keys. A PKI publishes public keys and establishes trust within an environment by validating and verifying the public keys mapping to an entity.
Qualified Electronic Signature Remote Creation Provider	A natural or a legal person that offers services related to the remote creation, validation, and management of qualified electronic signatures that meet legal requirements and standards in the [European Digital Identity Regulation] to be considered as legally equivalent to handwritten signatures.
Relying Party Instance	A software and/or hardware module with the capability to interact with a Wallet Unit and to perform Relying Party authentication, that is controlled by a Relying Party.
Selective Disclosure	The capability enabling the User to present a subset of the attributes included in a PID or attestation.
SUA attestation	An attestation used for strong user authentication in the context of electronic payments, such that, when a Relying Party sends a presentation request for the attestation to a Wallet Unit, it includes transactional data in the request. *Note: See Topic 20*

Term	Definition
Technical validity period (of a PID or attestation)	The dates (and possibly times) from and up to which the attestation is valid, which are represented as metadata of the attestation. *Note: All PIDs and attestations have a technical validity period, which is typically much shorter than its administrative validity period (if existent). The technical validity period is chosen based on a risk analysis, e.g. with regard to User privacy.*
Trust Anchor	An authoritative entity represented by a public key and associated data. *Note: based on RFC 5914.*
Trusted List	Repository of information about authoritative entities in a particular legal or contractual context which provides information about their current and historical status.
Verifier (when used in the context of Wallet-to-Wallet interactions)	A User wishing to use their Wallet Unit to request attributes from a PID or attestation from the User of another Wallet Unit. *Note: See Topic 30*
Verifier Wallet Unit	A Wallet Unit used by a Verifier.

ANNEX 2 - High-Level Requirements

A.2 High-level requirements

A.2.1 Introduction

A.2.1.1 Overview

This annex to the ARF main document includes high-level requirements (HLRs) related to the EUDI Wallet ecosystem. The requirements define the responsible actor that should implement each requirement. There are no requirements imposed on the Users.

All requirements in this Annex only apply in the context of the EUDI Wallet ecosystem.

A.2.1.2 Key words

This Annex uses the capitalised key words ‘SHALL’, ‘SHOULD’ and ‘MAY’ as specified in RFC 2119, i.e., to indicate requirements, recommendations and options specified in this annex.

In addition, ‘must’ (non-capitalised) is used to indicate an external constraint, i.e., a requirement that is not mandated by this document, but, for instance, by an external standard or specification. The word ‘can’ indicates a capability, whereas other words, such as ‘will’, and ‘is’ or ‘are’, are intended as statements of fact.

A.2.2 Structure and order of presentation of the HLRs

Topics presented in Section A.2.3 are ordered by a Topic number.

Each Topic includes a short description, followed by the High-Level Requirements (HLRs), identified by a unique identifier. The identifier includes a prefix which signifies the context of the HLRs (e.g. ISSU for issuance), an underscore and a numerator, e.g. ISSU_10.

A.2.3 High-Level Requirements

A.2.3.1 Topic 1 - Accessing Online Services with a Wallet Unit

Description

One of the main use cases of the EUDI Wallet ecosystem is to enable Users to access online services and to enable Relying Parties offering such services to, where needed, identify and authenticate Users with a high level of assurance. This essential functionality ensures that Relying Parties can confidently verify that they are interacting with the correct User.

Note: As specified in the [European Digital Identity Regulation], legally speaking, the term ‘Relying Party’ also include QEAA Providers, PuB-EAA Providers, and non-qualified EAA Providers. However, for clarity this Annex uses the term ‘Relying Party’ exclusively in the meaning of a service provider interacting with a Wallet Unit to request and receive attributes from an attestation.

In this use case, a User is using their Wallet Unit to present attributes in order to access online services offered by Relying Parties. The User is concerned about presenting such attributes during online interactions. Their objectives include maintaining control over the presentation of personal attributes from PIDs and attestations.

HLRs

Index	Requirement specification
OIA_01	A Wallet Unit SHALL support [SD-JWT VC] for remote presentation flows and [ISO/IEC 18013-5] for proximity presentation flows, to receive and respond to presentation requests for person identification data (PID) and attestations by Relying Parties.
OIA_02	A Wallet Unit SHALL support proving cryptographic device binding between a WSCA/WSCD included in the Wallet Unit and a PID or attestation, in accordance with [SD-JWT VC] or [ISO/IEC 18013-5]. *Note: Such a mechanism is called ‘mdoc authentication’ in [ISO/IEC 18013-5] and ‘key binding’ in [SD-JWT VC].*
OIA_03	Empty
OIA_03a	Wallet Providers SHALL ensure that their Wallet Solution supports the protocol specified in ‘OpenID for Verifiable Presentations’, see [OpenID4VP], with additions and changes as documented in this Annex and in technical specifications referenced in this Annex.

Index	Requirement specification
OIA_03b	For remote presentation flows, when the format of the requested attestation complies with [ISO/IEC 18013-5], Relying Parties and Wallet Units SHALL comply with the requirements in the profile for OpenID4VP specified in [ISO/IEC 18013-7] Annex B.
OIA_03c	For remote presentation flows, when the format of the requested attestation complies with [SD-JWT VC], Relying Parties and Wallet Units SHALL comply with the requirements in the ‘OpenID for Verifiable Presentations for IETF SD-JWT VC’ profile specified in [HAIP].
OIA_04	A Wallet Unit SHALL verify and process PID or attestation presentation requests from Relying Parties in accordance with the protocols and interfaces specified in [OpenID4VP] for remote flows.
OIA_05	After verifying and processing a PID or attestation request, the Wallet Unit SHALL display to the User the identity of the requesting Relying Party and the requested attributes.
OIA_06	A Wallet Unit SHALL present the requested attributes only after having received the User’s authorisation. *Note: See also OIA_07*.
OIA_07	A Wallet Unit SHALL support selective disclosure of attributes from PIDs and attestations to be released to the requesting Relying Parties.

Index	Requirement specification
OIA_08	Wallet Units and Relying Party Instances SHOULD support the [W3C Digital Credentials API]](https://wicg.github.io/digital-credentials/) for remote presentation flows, provided that a) this API is fully standardised, b) this API complies with the expectations outlined in Chapter 3 of the Topic F discussion paper, and c) this API is broadly supported by relevant browsers and operating systems.
OIA_08a	If Wallet Units and Relying Party Instances do not support the [W3C Digital Credentials API], they SHALL implement adequate mitigations for the challenges described in Section 4.4.3.1 of the ARF main document.
OIA_08b	If a Wallet Unit supports the [W3C Digital Credentials API], it SHALL disclose the presence of all stored attestations and attributes to the Digital Credentials API framework, but it SHALL NOT disclose the value of the attributes in these attestations. *Note: The latter restriction applies even if such disclosure would enhance the services provided by the operating system to the Wallet Unit, for example, attestation selection in the context of the Digital Credentials API.*

Index	Requirement specification
OIA_08c	If a Relying Party supports the [W3C Digital Credentials API], the Relying Party's presentation request MAY be processed by the browser for searching available attestations, for preventing fraud targeting the user, or for troubleshooting purposes. Moreover, the request SHOULD be processed by the browser for User security purposes. However, the request SHALL NOT be processed by the browser for market analysis purposes (including as a secondary purpose) or for the browser's own purposes.
OIA_09	For remote presentation flows the Wallet Unit SHALL ensure that the attributes included in the presented attestation are accessible only to the Relying Party Instance, by encrypting the presentation response. The technical specification meant in OIA_03a SHALL specify mechanisms preventing decryption of the presentation response via Man-in-the-Middle attacks by the browser, the operating system, or other components between the Wallet Unit and the Relying Party.
OIA_10	For both proximity and remote presentation flows, if a Wallet Unit contains two PIDs having the same encoding (e.g. ISO/IEC 18013-5 or SD-JWT VC-compliant) and a Relying Party requests a PID, the Wallet Unit SHALL ask the User which of these PIDs they want to release, unless the Wallet Unit can decide from context.

Index	Requirement specification
OIA_11	For both proximity and remote presentation flows, if a Wallet Unit contains two attestations having the same encoding (e.g. ISO/IEC 18013-5 or SD-JWT VC-compliant) and the same attestation type, and a Relying Party requests an attestation of that type and encoding, the Wallet Unit SHALL ask the User which of these attestations they want to release, unless the Wallet Unit can decide from context. *Note: Attestation types are explained in [Topic 12].*
OIA_12	For both proximity and remote presentation flows, a Relying Party SHALL validate the signature of a PID using a trust anchor provided in a PID Provider Trusted List made available in accordance with [Topic 31].
OIA_13	For both proximity and remote presentation flows, a Relying Party SHALL validate the qualified signature of a QEAA in accordance with Art.32 of the [European Digital Identity Regulation]. For the verification, the Relying Party SHALL use a trust anchor provided in a QEAA Provider Trusted List made available in accordance with Art. 22 of the [European Digital Identity Regulation].

Index	Requirement specification
OIA_14	For both proximity and remote presentation flows, a Relying Party SHALL validate the qualified signature of a PuB-EAA in accordance with Art.32 of the [European Digital Identity Regulation]. For that verification, the Relying Party SHALL use the public key provided in the qualified certificate of the QTSP supporting the qualified signature. The Relying Party SHALL also validate the qualified certificate of the QTSP using a trust anchor provided in a Trusted List made available in accordance with Art. 22 of the [European Digital Identity Regulation]. The Relying Party SHALL also verify the certified attributes of the qualified certificate, as specified in Article 45f.

Index	Requirement specification
OIA_15	For both proximity and remote presentation flows, a Relying Party SHALL validate the signature of a non-qualified EAA using a trust anchor provided according to the mechanism(s) specified in the applicable Rulebook, see [Topic 12]. *Notes: - OIA_12 - OIA_15 imply that a Relying Party Instance must know if the attestation it is requesting from a Wallet Instance is a PID, a QEAA, a PuB-EAA, or a non-qualified EAA. These requirements also imply that the Relying Party Instance must store trust anchors in such a way that, at the time of verification, it is able to distinguish between trust anchors usable either for PIDs, for QEAAs, for PuB-EAAs, or for non-qualified EAAs. - PID Providers, QEAA Providers, and PuB-EAA Providers are trusted by other actors in the EUDI Wallet ecosystem to not fraudulently issue attestations (or PIDs) that they are not legally allowed to issue. This trust is warranted since these kinds of providers operate within a regulated framework and are regularly audited. However, non-qualified EAA Providers are unregulated and may not be completely trustworthy. Therefore, when it receives an non-qualified attestation, a Relying Party Instance may have to verify that the non-qualified EAA Provider is authorised or registered to issue this type of attestation, in addition to verifying the signature over the attestation using the EAA Provider's trust anchor. Mechanisms allowing to do this should be defined in the applicable Rulebook, see ARB_26.*

Index	Requirement specification
OIA_16	When receiving a PID or attestation, a Relying Party Instance SHALL discard the values of all unique elements, including at least the ones mentioned in requirement ISSU_35 in Topic 10, as well as any timestamps, as soon as they are no longer needed. The Relying Party Instance SHALL NOT communicate these values to the Relying Party or to any other party inside or outside the EUDI Wallet ecosystem.

A.2.3.2 Topic 2 - Mobile Driving Licence within the EUDI Wallet ecosystem

Description

A User can obtain their mobile Driving Licence (mDL) from an mDL Provider and store it in an Wallet Unit. The User can then present the mDL to a Relying Party upon request to prove their driving rights conveniently, securely, and in compliance with the Driving Licences Directive, once it is adopted.

This Topic contains high-level requirements related to a User presenting a mobile Driving Licence (mDL) to a Relying Party in a supervised or unsupervised scenario, and also in an unsupervised scenario, in proximity mode.

HLRs

No high-level requirements are identified for this Topic, as the mDL is an attestation that must comply with all relevant requirements in other Topics.

A.2.3.3 Topic 3 - PID Rulebook

Description

The Person Identification Data (PID) Rulebook contains requirements specific to the PID within the EUDI Wallet ecosystem.

The PID Rulebook contains the PID scheme, which describes the structure, the type, the identifiers, and the logical organisation of the mandatory and optional attributes and metadata of the PID, as specified in Commission Implementing Regulation (EU) 2024/2977. It also describes how Member States can specify any national PID attributes. Two encodings for these attributes are specified, one compliant with [ISO/IEC 18013-5], the other compliant with [SD-JWT VC].

For more information, see Annex 3 - [PID Rulebook].

A. Generic HLRs

The requirements in the table below are valid for all PIDs in the EUDI Wallet ecosystem, regardless of the encoding used.

Index	Requirement specification
PID_01	PIDs and PID Providers SHALL comply with all requirements in [PID Rulebook].

Index	Requirement specification
PID_02	A PID Provider SHALL issue any PID in both the format specified in ISO/IEC 18013-5 [ISO/IEC 18013-5] and the format specified in [SD-JWT VC]. *Note: [CIR 2024/2977] mentions the W3C Verifiable Credentials Data Model v1.1 instead of [SD-JWT VC]. The latest stable version of this standard is [W3C VCDM 2.0]. However, W3C VCDM is not a complete specification of an attestation format. In particular, it does not specify a specific proof method to be used. Without additional specification, such as those in [W3C VC-JOSE-COSE] or [W3C VC Data Integrity], and making further choices, it is impossible to implement a PID based on W3C VCDM. This Rulebook considers [SD-JWT VC] to essentially be such an additional specification. See also Section 5.3.4 of the ARF main document.*
PID_03	The portrait in a PID SHALL consist of a single portrait image in JPEG format. The portrait image SHALL comply with the quality requirements for a Full Frontal Image Type in ISO/IEC 19794-5 clauses 8.2, 8.3, and 8.4. However, the attribute portrait SHALL NOT comply with the format requirements in ISO/IEC 19794-5 clauses 8.1 and 8.5, meaning it SHALL NOT contain any of the headers or blocks specified in clause 5 except for the image data itself (a JPEG).

B. HLRs for ISO/IEC 18013-5-compliant PIDs

The requirements in the table below are valid for PIDs in the EUDI Wallet ecosystem that are compliant with [ISO/IEC 18013-5].

Index	Requirement specification
PID_04	PID Providers SHALL use “eu.europa.ec.eudi.pid.1” as the attestation type for ISO/IEC 18013-5-compliant PIDs. *Notes: - This identifier uses the general format [Reverse Domain].[Domain Specific Extension]. Since the European Commission controls the domain ec.europa.eu, this attestation type identifier will not collide with any attestation type identifiers defined by other organisations in other Attestation Rulebooks. - The Commission may use the version number “1” in this identifier to distinguish between the first version of the PID, defined in the PID Rulebook, and any future version, which will then have an incremented version number.*
PID_05	When issuing a PID compliant with [ISO/IEC 18013-5], a PID Provider SHALL use the value “eu.europa.ec.eudi.pid.1” for the identifier of the namespace for the PID attributes specified in Section 4.2 of the PID Rulebook. *Notes: - The version number “1” allows for future extension(s) or change(s) of the ISO/IEC 18013-5-compliant PID attributes. - This namespace has the same value as the attestation type specified in requirement PID_04. This is allowed according to ISO/IEC 18013-5.*

Index	Requirement specification
PID_06	When issuing a PID compliant with [ISO/IEC 18013-5], a PID Provider MAY include attributes that are not defined in the PID Rulebook. If so, these attributes SHALL be defined within a domestic PID namespace as meant in requirement ARB_10 in Topic 12. The PID Provider SHALL generate the identifier for this domestic PID namespace by appending the applicable ISO 3166-1 alpha-2 country code or the ISO 3166-2 region code, separated by a period, to the PID namespace identifier specified in PID_05, excluding the version number. The PID Provider MAY include a version number in the domestic PID namespace identifier. *Note: For example, the identifier of the first domestic PID namespace for Germany could be "eu.europa.ec.eudi.pid.de.1".*
PID_07	A PID Provider that defines a domestic namespace SHALL publish the namespace, including all attribute identifiers, their definition, presence and encoding format, in an Attestation Rulebook complying with all applicable requirements in Topic 12.
PID_08	When issuing a PID compliant with [ISO/IEC 18013-5], a PID Provider SHALL include both the attributes and the metadata specified in [CIR 2024/2977] in the PID as (issuer-signed or device-signed) data elements. *Note: This implies that technically speaking, there is no difference between these attributes and metadata.*

Index	Requirement specification
PID_09	When issuing a PID compliant with [ISO/IEC 18013-5], a PID Provider SHALL encode each attribute or metadata in the PID as specified in the third column of the tables in Section 4.2.1 of the PID Rulebook.
PID_10	When issuing a PID compliant with [ISO/IEC 18013-5], a PID Provider SHALL encode each attribute or metadata in the PID in Concise Binary Object Representation (CBOR) according to [RFC 8949].
PID_11	When issuing a PID compliant with [ISO/IEC 18013-5], a PID Provider SHALL ensure that each PID contains at most one attribute with the same attribute identifier.
PID_12	When issuing a PID compliant with [ISO/IEC 18013-5], a PID Provider SHALL ensure that the value of all attributes and metadata in the PID is valid at the value of the timestamp in the validFrom element in the MSO, see [ISO/IEC 18013-5] clause 9.1.2.4. *Note: The value of the age_over_18, age_over_NN, or age_in_years attributes, if present, changes whenever the User to whom the person identification data relates has a relevant birthday. The value of many other attributes will also change over time.*
PID_13	When issuing a PID compliant with [ISO/IEC 18013-5], a PID Provider SHALL ensure that the issuance_date attribute, if present, is not later than the validFrom element in the MSO, see [ISO/IEC 18013-5] clause 9.1.2.4.

C. HLRs for SD-JWT VC-compliant PIDs

The requirements in the table below are valid for PIDs in the EUDI Wallet ecosystem that are compliant with [SD-JWT VC].

Index	Requirement specification
PID_14	A PID Provider issuing [SD-JWT VC]-compliant PIDs SHALL include the vct claim in their PIDs, where the vct claim SHALL be a URN within the `urn:eudi:pid:` namespace. The type indicated by the vct claim SHALL be `urn:eudi:pid:1` for the type defined in this document or a domestic type that extends it.
PID_15	Empty
PID_16	A PID Provider that defines a domestic type SHALL publish information about the type, including all claim identifiers, their definition, presence and encoding format, in an Attestation Rulebook complying with all applicable requirements in Topic 12.
PID_17	When issuing a PID compliant with [SD-JWT VC], a PID Provider SHALL include both the attributes and the metadata specified in [CIR 2024/2977] in the PID as claims. *Note: This implies that technically speaking, there is no difference between these attributes and metadata.*
PID_18	When issuing a PID compliant with [SD-JWT VC], a PID Provider SHALL encode each attribute or metadata in the PID as specified in the tables in Section 5.2 of the PID Rulebook.
PID_19	When issuing a PID compliant with [SD-JWT VC], a PID Provider SHALL ensure that the value of all attributes and metadata in the PID is valid at the value of the timestamp in the nbf claim, if present. *Note: The value of the age-related claims, if present, changes whenever the User to whom the person identification data relates has a relevant birthday. The value of many other attributes will also change over time.*

Index	Requirement specification
PID_20	When issuing a PID compliant with [SD-JWT VC], a PID Provider SHALL ensure that the date_of_issuance claim, if present, is not later than the value of the timestamp in the nbf claim, if present.
PID_21	When issuing a PID compliant with [SD-JWT VC], a PID Provider SHALL make all claims (i.e., all top-level properties, all nested properties, and all array entries) selectively disclosable individually, except those claims defined as non-selectively disclosable in [SD-JWT VC].

A.2.3.4 Topic 4 - mDL Rulebook

Description

The mobile driving licence (mDL) Rulebook contains requirements specific to the mDL use case within the EUDI Wallet ecosystem.

Mobile driving licences are legally specified in the proposed EC Regulation 2023_127 (4th Driving Licence Regulation). This Regulation specifies that mDLs must comply with the ISO/IEC 18013-5 standard. It does not mention any other standards, in particular not [SD-JWT VC]. Consequently, mDLs issued to a Wallet Unit will not be implemented as [SD JWT VC]- compliant documents. The mDL Rulebook therefore specifies only an ISO/IEC 18013-5 compliant encoding.

For more information, see Annex 3 - [mDL Rulebook].

HLRs

Index	Requirement specification
mDL_01	mDLs and mDL Providers SHALL comply with all requirements in [mDL Rulebook].

A.2.3.5 Topic 5 - Wallet Unit Design Guide

There are no HLRs for this Topic.

A.2.3.6 Topic 6 - Relying Party authentication and User approval

Description

Relying Party authentication is a process whereby a Relying Party proves its identity to a Wallet Unit, in the context of a transaction in which the Relying Party requests the Wallet Unit to present some attributes.

To perform Relying Party authentication, the Wallet Unit verifies a Relying Party Instance access certificate offered by the entity with which it communicates, which is called a “Relying Party Instance”. Note that there could be multiple Relying Party Instances for each Relying Party.

The Wallet Unit communicates the outcome of Relying Party authentication to the User when it requests the User for approval to present the requested attributes. High-level requirements for User approval are also included in this Topic. If requested by the User, the Wallet Unit also communicates the outcome of the verification of the information in the Relying Party registration certificate or obtained from the Registrar, see Topic 44. The Wallet Unit also informs the User about the outcome of the evaluation of an embedded disclosure policy, if present, see Topic 43.

HLRs

A. Relying Party authentication

Index	Requirement specification
RPA_01	The Wallet Unit used by a User, as well as the Relying Party Instance used by the Relying Party, SHALL implement a mechanism for Relying Party authentication in PID or attestation presentation transactions. This mechanism SHALL: - enable the Wallet Unit to identify and authenticate the Relying Party, - enable the Wallet Unit to verify that the request from the Relying Party was not copied and replayed, - use Relying Party Instance access certificates issued in accordance with [Topic 27].
RPA_01a	If a Wallet Unit supports the [W3C Digital Credentials API] for remote presentation flows, it SHALL retain full authority over the process meant in RPA_01. In particular, this process SHALL NOT be handled by a third party, including the browser and the operating system.
RPA_02	The Commission SHALL ensure that technical specifications for the Relying Party authentication mechanism mentioned in RPA_01 are created both for Wallet Units complying with [ISO/IEC 18013-5] and for Wallet Units complying with [OpenID4VP]. These specifications SHALL comply with applicable requirements in these standards.
RPA_02a	The technical specifications mentioned in RPA_02 SHALL ensure that a Relying Party Instance includes its access certificates in the presentation request by value, not by reference. *Note: This ensures that no external requests are necessary to carry out Relying Party authentication, and that transactions are atomic and self-contained.*

Index	Requirement specification
RPA_03	A Wallet Unit and a Relying Party Instance SHALL perform Relying Party authentication in all PID or attestation presentation transactions to Relying Parties, whether proximity or remote, using a Relying Party Instance access certificate. *Note: The actions both entities perform differ. For example, while the Relying Party creates a signature over some data in the request, the Wallet Unit validates that signature.*
RPA_04	For the verification of Relying Party Instance access certificates, a Wallet Unit SHALL accept the trust anchors in the Trusted List(s) of Relying Party Access Certificate Authorities of all Member States. *Note: For more information about Relying Party Access Certificate Authorities, please see [Topic 31].*
RPA_05	If Relying Party authentication fails for any reason, the Wallet Instance SHALL inform the User that the identity of the Relying Party could not be verified and that therefore the request is not trustworthy.
RPA_06	If Relying Party authentication succeeds, the Wallet Instance SHALL display to the User the name of the Relying Party as included in the Relying Party access certificate, together with the attributes requested by the Relying Party. The Wallet Instance SHALL do so when asking the User for approval according to RPA_07. *Note: If the Relying Party is an intermediary acting on behalf of an intermediated Relying Party, the Wallet Instance displays the names of both the intermediary and the intermediated Relying Party to the User, see RPI_07.*

Index	Requirement specification
RPA_06a	If Relying Party authentication fails for any reason, the Wallet Unit SHALL notify the User. In addition, the Wallet Unit SHALL either not present the requested attributes to the Relying Party, or give the User the choice to present the requested attributes or not. *Note: It is up to the Wallet Provider to make a choice for one of these two options.*

B. User approval

Index	Requirement specification
RPA_07	A Wallet Unit SHALL ensure the User approved the release of any attribute(s) in the Wallet Unit to a Relying Party, prior to releasing these attributes. A Wallet Unit SHALL always allow the User to refuse releasing an attribute requested by the Relying Party.
RPA_07a	If a Wallet Unit supports the [W3C Digital Credentials API] for remote presentation flows, it SHALL retain full authority over the process meant in RPA_07. In particular, this process SHALL NOT be handled by a third party, including the browser and the operating system.
RPA_08	A Wallet Unit SHALL ensure that (one of) its WSCA(s) has authenticated the User before allowing the User to give or refuse approval for releasing any attributes. *Note: See [Topic 09] for information about the WSCA.*

Index	Requirement specification
RPA_09	A Relying Party SHOULD communicate in the request which attributes are needed for which purpose (use case, service), if this is supported by the protocol used for communication with the Wallet Unit. *Notes: - This could be done, for instance, by grouping the attributes and describing the use case, service, or purpose of each group. - The purpose of this recommendation is that a Relying Party makes clear to the User what the intended use, the service being accessed, or the specific purpose is of each requested attribute. For example, a service may legally require attributes for age verification (e.g., birthdate), but the Relying Party may additionally want a User address (e.g., street, location, PObox, country) in order to offer added-value services. Age verification attributes and address attributes should be grouped separately, and the purposes should be clearly distinguished. This allows the User to be better informed about the request, and also allows them to approve one purpose but deny the other; see RPA_10.*

Index	Requirement specification
RPA_10	If a Wallet Unit receives a request indicating one or more purposes (use cases, services) for requesting attributes, the Wallet Instance SHOULD show these to the User when asking for User approval. Moreover, the Wallet Unit SHOULD ensure that for each purpose, the User gives approval either to release all attributes requested for that purpose, or none of them. *Note: This means that a User should either approve the release of all attributes in a given group or to deny the entire group. The Wallet Unit should not allow partial approval within a group. Partial approval would mean that the Relying Party cannot deliver the service, but nevertheless receives some User attributes. This would be a violation of the User's privacy.*
RPA_11	When the presentation of an attestation is denied by the User, the Wallet Unit SHALL behave towards the Relying Party as if the attestation did not exist.
RPA_12	When asking for User approval, the Wallet Unit MAY indicate to the User whether the attestation requested by a Relying Party is device-bound or not. *Note: The intent of this indication is to warn the User than a non-device bound attestation may be copied by the Relying Party and presented to a third party.*

A.2.3.7 Topic 7 - Attestation revocation and revocation checking

Description

This Topic contains the high-level requirements (HLRs) relating to the (possible) revocation of PIDs, QEAAs, PuB-EAAs, non-qualified EAAs, and WUAs by their providers. It also contains

HLRs relating to the (possible) checking of the revocations status of a PID or attestation by a Relying Party.

Note: This Topic does not pertain to access certificates for Relying Parties, PID Providers, or Attestation Providers as discussed in [Topic 31]. Neither does it apply to any intermediate certificates establishing trust between these certificates and the respective trust anchors. These access certificates are part of a Public Key Infrastructure, and rules for revoking these certificates will be established within the respective PKI.

HLRs

Index	**Requirement specification**
VCR_01	A PID Provider, QEAA Provider, or PuB-EAA Provider SHALL use one of the following methods for revocation of a PID, QEAA, or PuB-EAA: - Only issue short-lived attestations having a validity period of 24 hours or less, such that revocation will never be necessary, - Use an Attestation Status List mechanism specified per VCR_11, or - Use an Attestation Revocation List mechanism specified per VCR_11. *Note: The 24-hour period originates from ETSI EN 319 411-1 V1.4.1, requirement REV-6.2.4-03A. This requires that the process of revocation must take at most 24 hours. Consequently, revocation may make no sense if the attestation is valid for less than 24 hours, because it may reach the end of its validity period before it is revoked.*
VCR_01a	A Wallet Provider SHALL use either the second or the third of the methods specified in VCR_01 for revocation of a WUA. *Note: Due to requirement WUA_08 in Topic 9, it is not possible to issue short-lived WUAs. This implies that all WUAs are revocable.*

Index	Requirement specification
VCR_02	For non-qualified EAAs, the relevant Rulebook SHALL specify whether that type of EAA must be revocable. If a non-qualified EAA type must be revocable, the relevant Rulebook SHALL determine which of the methods mentioned in VCR_01 must be implemented by the relevant EAA Providers for the revocation of such an EAA.
VCR_03	If a PID or attestation is revocable, the PID Provider of a given PID, or the Attestation Provider of a given attestation, SHALL be the only party in the EUDI Wallet ecosystem responsible for executing the revocation of that PID or attestation. *Note: A PID Provider, Attestation Provider MAY outsource the operation of the revocation process to a third party.
VCR_03a	The Wallet Provider of a given WUA SHALL be the only party in the EUDI Wallet ecosystem responsible for executing the revocation of that WUA. *Note: A Wallet Provider MAY outsource the operation of the revocation process to a third party.*
VCR_04	A PID Provider, Attestation Provider or Wallet Provider that revoked a PID, attestation, or WUA SHALL NOT reverse the revocation.
VCR_05	If a PID, attestation, or WUA is revocable, the PID Provider, Attestation Provider, or Wallet Provider SHALL have a policy specifying under which conditions a PID, attestation, or WUA it issued will be revoked.

Index	Requirement specification
VCR_06	If a PID, attestation, or WUA is revocable, the PID Provider, Attestation Provider, or Wallet Provider SHALL revoke a PID, attestation, or WUA when its security has been compromised.
VCR_07	A Wallet Provider SHALL revoke all valid WUAs issued to a Wallet Unit upon the explicit request of the User to revoke their Wallet Unit.
VCR_07a	If a PID or attestation is revocable, the PID Provider or Attestation Provider SHOULD revoke that PID or attestation upon the explicit request of the User to whom the PID or the attestation was issued.
VCR_07b	If a PID or attestation is revocable, the PID Provider or Attestation Provider SHOULD revoke that PID if the Wallet Unit on which it resides is revoked, in compliance with requirement WURevocation_18 in Topic 38.
VCR_08	If a PID is revocable, the PID Provider SHALL revoke a PID upon the death of the natural person who is the subject of the PID, or the cease of activity of the legal person who is the subject of the PID.

Index	Requirement specification
VCR_09	If a PID, attestation, or WUA is revocable, the PID Provider, Attestation Provider or Wallet Provider SHALL revoke a PID, attestation, or WUA if the value of one or more attributes in the PID, attestation, or WUA was changed (including attributes being added or deleted) and it is still valid for at least 24 hours. Subsequently, if the User's contact details are known, the PID Provider, Attestation Provider, or Wallet Provider SHOULD, via an out-of-band manner, notify the User about the revocation and ask the User to request re-issuance of the PID, attestation, or WUA using their Wallet Unit. *Note: If the value of the attributes is determined by a party different from the Provider, such as an Authentic Source, the Provider is responsible for ensuring that this third party notifies them about such changes.*
VCR_10	Wallet Providers SHALL implement the attestation revocation mechanisms specified per VCR_11 in their Wallet Solutions.

Index	Requirement specification
VCR_11	The Commission SHALL create or reference technical specifications providing all necessary details for PID Providers, Attestation Providers, and Wallet Providers to implement an Attestation Status List mechanism or an Attestation Revocation List mechanism for the PIDs, attestations, and WUAs they issue. These technical specifications SHALL also contain all details necessary for Relying Party Instances, Relying Parties, and Wallet Units interacting with other Wallet Units to use these mechanisms to verify the revocation status of PIDs, attestations, and WUAs. *Note: 'Attestation Status List' and 'Attestation Revocation List' are specific mechanisms, defined in Annex 1. Attestation Revocation Lists are sometimes referred to as 'Identifier Lists'.*
VCR_12	If a Relying Party decides it needs to be able to verify the revocation status of PIDs or attestations, it SHALL support both the Attestation Status List mechanism and the Attestation Revocation List mechanism specified per VCR_11. *Note: Per VCR_13, it is recommended but not mandatory for a Relying Party to verify whether a PID or attestation is revoked.*
VCR_12a	A PID Provider or Attestation Provider SHALL support both the Attestation Status List mechanism and the Attestation Revocation List mechanism specified per VCR_11 for verifying the revocation status of a WUA.

Index	Requirement specification
VCR_13	A Relying Party Instance SHOULD verify the revocation status of a PID or attestation upon obtaining it from a Wallet Unit, following the steps specified per VCR_11.
VCR_14	When no reliable information regarding the revocation status of a PID or attestation is available, a Relying Party SHOULD perform a risk analysis considering all relevant factors for the use case, before taking a decision to accept or refuse the PID or attestation.
VCR_15	A Relying Party Instance SHOULD NOT request the relevant Attestation Status List or Attestation Revocation List each time an attestation is presented to it by a Wallet Unit. Rather, the Relying Party operating the Relying Party Instance SHOULD download each new version of the list once, at a time and from a location unrelated to the presentation of a PID or attestation by a User. The Relying Party SHOULD then distribute the list to all of its Relying Party Instances, using an Relying Party-internal distribution mechanism.
VCR_16	A PID Provider, Attestation Provider or Wallet Provider SHALL NOT require the Relying Party or Relying Party Instance to authenticate itself before downloading an Attestation Status List or Attestation Revocation List.

Index	Requirement specification
VCR_17	When using an Attestation Status List for revocation, the PID Provider, Attestation Provider or Wallet Provider SHALL randomly assign the index for each PID or attestation, to prevent this index from becoming a correlator. *Note: Randomly assigning indices within a bitstring or byte array is more complicated than creating random identifiers (e.g. serial numbers) for attestations, as is needed for an Attestation Revocation List. This is because duplicate indices and unnecessarily long bitstrings or byte arrays must be prevented.*
VCR_18	When using an Attestation Status List for revocation, the PID Provider, Attestation Provider, or Wallet Provider SHALL represent a sufficiently large number of PIDs, attestations, or WUAs on each Attestation Status List to ensure herd privacy. *Note: In this context, herd privacy means that if an entity requests a particular status list, the PID Provider, Attestation Provider, or Wallet Provider is not able to deduce which PID, attestation or WUA (likely) was presented to that entity.* Note: Complying with this requirement may be difficult in case the number of PIDs, attestations, or WUAs to be represented on the list is small. In such a case, decoy entries can be added to the list to obfuscate the real number of referenced PIDs, attestations, or WUAs.*
VCR_19	A Wallet Unit SHOULD regularly check the revocation status of its PIDs, attestations, and WUAs, and notify the User if a PID, attestation, or WUA (i.e, the Wallet Unit itself), is revoked.

A.2.3.8 Topic 8 - Design Solutions on Data Sharing scenarios

There are no HLRs for this Topic.

A.2.3.9 Topic 9 - Wallet Unit Attestation

Note to this Topic: The Commission received many comments on the ideas described in this Topic, particularly relating to revocation and the differing needs of Relying Parties on one side and PID Providers and Attestation Providers on the other. Further details on these subjects will be provided in Technical Specification 3 and the high level requirements in Topic 9 intentionally do not go into these technical details.

Description

When a User's Wallet Unit interacts with other actors in the EUDI Wallet ecosystem, in particular PID Providers, Attestation Providers, or Relying Parties, these actors may want to verify if the Wallet Unit is authentic and has not been revoked.

Furthermore, when a PID Provider or Attestation Provider receives a request from a User to issue a PID or attestation to the User's Wallet Unit, the PID Provider or Attestation Provider needs to decide whether it can comply with this request. To determine this, the PID Provider or Attestation Provider needs to know (among other things) if the Wallet Unit offers the functional capabilities required by the PID Provider or Attestation Provider in its PID or attestation issuing policy. In addition, the PID Provider or Attestation Provider needs to know if the Wallet Secure Cryptographic Application(s) (WSCA) and the corresponding Wallet Secure Cryptographic Device(s) (WSCD) that are part of the Wallet Unit offer the required level of security. Therefore, the PID Provider or Attestation Provider needs to receive trustworthy information about these capabilities and security posture.

This Topic introduces an information object that contains the necessary information to allow PID Providers and Attestation Provider to verify if he Wallet Unit is authentic and has not been revoked, and that also contains the information needed by the Provider to take a decision on issuance. This object is called the Wallet Unit Attestation (WUA). The WUA also contains a public key. By including this public key in the WUA, the Wallet Provider attests that the corresponding private key is protected by a certified WSCA/WSCD that has the properties and security posture described in the WUA. The PID Provider or Attestation Provider then asks the Wallet Unit to create a key pair for its new PID or attestation, and to prove that both this new private key and the private key corresponding to public key in the WUA are in possession of the Wallet Unit.

A topic related to the WUA is the following. It would be useful for the Wallet Unit to be able to provide a proof that the PID or attestation private key is protected by the same WSCA/WSCD as the WUA private key. Because if that is the case, the PID Provider or Attestation Provider can be sure that the security level of the new PID or attestation key is the same as the security level of the WUA key. A mechanism for providing such a proof is discussed in Topic 18, where it is used to give assurance to a Relying Party that multiple attestations originate from the same WSCA/WSCD and thus are related to the same User. The same mechanism could also be used here.

HLRs

A. Support for WUA Use Cases

Index	Requirement specification
WUA_01	The WUA SHALL provide a PID Provider or Attestation Provider with information about the capabilities of the WSCA and WSCD of the Wallet Unit, such that they are able to take a well-grounded decision on whether to issue a PID or attestation to the Wallet Unit.
WUA_02	The WUA SHALL enable PID Providers and Attestation Providers to verify the authenticity and revocation status of the Wallet Unit.
WUA_03	A Wallet Provider SHALL ensure that a non-revoked Wallet Unit at all times can present a WUA, when requested by a PID Provider or Attestation Provider.
WUA_04	Empty

Index	Requirement specification
WUA_05	During issuance of a PID or device-bound attestation, a Wallet Unit SHALL retrieve the requirements of the PID Provider or Attestation Provider regarding User authentication and key storage by the WSCA/WSCD from the Issuer metadata (as specified in [OpenID4VCI]). The Wallet Unit SHALL determine which of its WSCA/WSCD(s), if any, comply with these requirements. If a compliant WSCA/WSCD is available to the Wallet Unit, the Wallet Unit SHALL request it to generate a new key pair for the new PID or attestation. The Wallet Unit SHALL provide the PID Provider or Attestation Provider with the WUA describing the properties of the WSCA/WSCD that generated the new PID or attestation private key.
WUA_06	If a Wallet Unit contains multiple WSCAs, it SHALL, internally and securely, keep track of which PIDs and attestations are bound to which WSCA.
WUA_07	A Wallet Unit SHALL present a WUA only as part of the issuance of a PID or an attestation.
WUA_08	The WUA SHALL enable PID Providers to request a Wallet Provider to revoke a Wallet Unit, in accordance with requirement WURevocation_11, by including an identifier for the Wallet Unit in the WUA. The Wallet Provider SHALL ensure that this Wallet Unit identifier does not enable tracking of the User. *Notes: - This is a legal requirement from [CIR 2024/2977]. See also Section 6.5.3.4 of the ARF main document. - The Wallet Unit identifier meant here can be the same as the one used for revoking the WUA, for instance a URI and index to an Attestation Status List (see Topic 7).*

B. WUA in relation Cryptographic Keys

Index	Requirement specification
WUA_09	A WUA SHALL contain a public key, and the corresponding private key SHALL be generated by the WSCA/WSCD described in the WUA.
WUA_10	Empty (moved to Topic 18)

Index	Requirement specification
WUA_11	During PID or attestation issuance, the PID Provider or Attestation Provider SHALL verify that the WSCA/WSCD described in the WUA received from the Wallet Unit has proven possession of the private key corresponding to the public key in the WUA.
WUA_11a	During issuance of a PID or a device-bound attestation, the PID Provider or Attestation Provider SHALL verify that a WSCA/WSCD has proven possession of the new PID or attestation private key.
WUA_11b	During issuance of a PID or a device-bound attestation, the PID Provider or Attestation Provider SHOULD verify a proof of cryptographic binding generated by the WSCA/WSCD per requirement ACP_01, if present, to verify that the new PID or attestation private key is managed by the same WSCA/WSCD as the WUA private key. *Note: The three proofs mentioned in WUA_11, WUA_11a and WUA_11b MAY be implemented as a single cryptographic proof.*
WUA_12	The Wallet Unit SHALL be able to prove that it possesses the private key corresponding to the public key in the WUA.
WUA_13	Empty
WUA_14	Empty (moved to Topic 18)
WUA_15	Empty
WUA_16	If a WSCA/WSCD is able to export a private key, the Wallet Provider SHALL specify this capability as an attribute in the WUA.

C. Requirements regarding privacy

Index	Requirement specification
WUA_17	A Wallet Provider SHALL consider all relevant factors, including offline usage, interoperability, and the risk of a WUA becoming a vector to track the User, when deciding on the validity period of a WUA. *Regarding interoperability, see ISSU_12c, which limits the validity period of PIDs issued based on the validity period of the WUA.*
WUA_18	A Wallet Unit SHALL release a WUA only to a PID Provider or Attestation Provider, and not to a Relying Party or any other entity.

D. Miscellaneous requirements

Index	Requirement specification
WUA_19	Empty
WUA_20	A Wallet Provider SHALL ensure that its Wallet Units comply with all relevant requirements specified in Technical Specification 3.
WUA_20a	A PID Provider or Attestation Provider SHALL comply with all relevant requirements specified in Technical Specification 3.
WUA_21	Empty

A.2.3.10 Topic 10 - Issuing a PID or attestation to a Wallet Unit

Description

PID Providers and Attestation Providers issue PIDs and attestations to Wallet Units. This Topic lists the high-level technical requirements related to PID and attestation issuance.

This Topic also contains the high-level requirements for Topic 23.

HLRs

A - Generic HLRs

Index	Requirement specification
ISSU_01	Wallet Providers SHALL ensure that their Wallet Solution supports the OpenID4VCI protocol specified in [OpenID4VCI], as profiled by the ‘OpenID for Verifiable Credential Issuance’ profile specified in [HAIP], and with additions and changes as documented in this Annex (see e.g. this Topic and [Topic 9]) and in future technical specifications created by or on behalf of the Commission.
ISSU_01a	PID Providers and Attestation Providers SHALL support the OpenID4VCI protocol specified in [OpenID4VCI], as profiled by the ‘OpenID for Verifiable Credential Issuance’ profile specified in [HAIP], and with additions and changes as documented in this Annex (see e.g. this Topic and [Topic 9]) and in future technical specifications created by or on behalf of the Commission.

Index	Requirement specification
ISSU_02	Wallet Providers SHALL ensure that their Wallet Solution supports the attestation formats specified in ISO/IEC 18013-5, see [ISO18013-5], and in “SD-JWT-based Verifiable Credentials (SD-JWT VC)”, see [SD-JWT-VC], with additions and changes as documented in this Annex and in future technical specifications created by or on behalf of the Commission.
ISSU_03	Wallet Units, PID Providers, and Attestation Providers SHALL support the [W3C Digital Credentials API]](https://wicg.github.io/digital-credentials/) for issuance of PIDs and attestations, provided that a) this API is fully standardised, b) this API complies with the expectations outlined in Chapter 3 of the Topic F discussion paper, and c) this API is broadly supported by relevant browsers and operating systems.
ISSU_04	The OpenID4VCI protocol referenced in requirement ISSU_01, or an EUDI Wallet-specific extension or profile thereof, SHALL enable PID Providers and Attestation Provider to issue to a Wallet Unit a batch of multiple PIDs or attestations that are simultaneously valid and contain the same attributes.

Index	Requirement specification
ISSU_05	A Wallet Unit SHALL support a process to activate a newly issued PID, in accordance with the requirements for LoA High in Commission Implementing Regulation (EU) 2015/1502 Section 2.2.2. The Wallet Unit SHALL NOT allow a User to use a non-activated PID. *Notes: - The goal of the activation process is to verify that the PID was delivered into the Wallet Unit and WSCA/WSCD of the User who is the subject of the PID. - This requirement is not applicable for QEAAs, PuB-EAAs or non-qualified EAAs, since these are not identity means in the sense of Commission Implementing Regulation (EU) 2015/1502.*
ISSU_06	After a Wallet Unit receives a PID or an attestation from a PID Provider or Attestation Provider, it SHALL verify that the PID or attestation it received matches the PID or attestation requested by the Wallet Unit.
ISSU_07	After a Wallet Unit receives a PID from a PID Provider, it SHALL validate the signature of the PID using a trust anchor provided in a PID Provider Trusted List made available in accordance with [Topic 31], unless this would result in the validation of the PID signature being done by the same component that created the signature. *Note: This could be the case in architectures where the Wallet Provider is also the PID Provider and the Wallet Units use a remote HSM as their WSCD.*

Index	Requirement specification
ISSU_08	After a Wallet Unit receives a QEAA from a QEAA Provider, it SHALL validate the qualified signature of the QEAA in accordance with Art.32 of the [European Digital Identity Regulation]. For the verification, the Wallet Unit SHALL use a trust anchor provided in a QEAA Provider Trusted List made available in accordance with Art. 22 of the [European Digital Identity Regulation].
ISSU_09	After a Wallet Unit receives a PuB-EAA from a PUB-EAA Provider, it SHALL validate the qualified signature of the PuB-EAA in accordance with Art. 32 of the [European Digital Identity Regulation]. For that verification, the Wallet Unit SHALL use the public key provided in the qualified certificate of the QTSP supporting the qualified signature. The Wallet Unit SHALL also validate the qualified certificate of the QTSP using a trust anchor provided in a Trusted List made available in accordance with Art. 22 of the [European Digital Identity Regulation]. Finally, the Wallet Unit SHALL also verify the certified attributes of the qualified certificate, as specified in Article 45f.

Index	Requirement specification
ISSU_10	After a Wallet Unit receives a non-qualified EAA from an EAA Provider, it SHALL validate the signature of the EAA using a trust anchor provided according to the mechanism(s) specified in the applicable Rulebook, see [Topic 12]. *Notes: - Requirements ISSU_07 to ISSU_10 are equivalent to requirements OIA_12 to OIA_15 in Topic 1. These requirements imply that a Wallet Instance must be aware whether the attestation it is requesting from an issuer is a PID, a QEAA, a PuB-EAA, or a non-qualified EAA. These requirements also imply that the Wallet Unit must store trust anchors in such a way that, when it receives an issued attestation, it is able to distinguish between trust anchors usable either for PIDs, for QEAAs, for PuB-EAAs, or for non-qualified EAAs. - PID Providers, QEAA Providers, and PuB-EAA Providers are trusted by other actors in the EUDI Wallet ecosystem to not fraudulently issue attestations (or PIDs) that they are not legally allowed to issue. This trust is warranted since these kinds of providers operate within a regulated framework and are regularly audited. However, non-qualified EAA Providers are unregulated and may not be completely trustworthy. Therefore, before requesting an non-qualified attestation, a Wallet Unit may need to verify that the non-qualified EAA Provider is authorised or registered to issue this type of attestation. Mechanisms allowing to do this may be defined in the applicable Rulebook, see ARB_26.*

Index	Requirement specification
ISSU_11	A Wallet Unit SHALL request the User's approval before storing a PID or attestation obtained from a PID Provider or Attestation Provider. When requesting approval, the Wallet Instance SHALL display the contents of the PID or attestation to the User. The Wallet Instance SHALL also inform the User about the identity of the PID Provider or Attestation Provider, using the subject information in the PID Provider's or Attestation Provider's access certificate.
ISSU_11b	In case one or more of the verifications in ISSU_06 - ISSU_11 fail, the Wallet Unit SHALL immediately delete the PID or attestation it received. The Wallet Instance SHALL notify the User about the fact that issuance of the PID or attestation was not successful, including the reason for this failure.
ISSU_12	A PID Provider or Attestation Provider SHALL offer its PIDs or attestations in all formats required in the PID Rulebook or the applicable Attestation Rulebook, see [Topic 12]. *Note: Examples include the mdoc format specified in [ISO/IEC 18013-5] and the SD-JWT VC-format specified in [SD-JWT VC].*
ISSU_12a	A Wallet Provider SHALL ensure that, when a User instructs their Wallet Unit to request a PID or attestation from a PID Provider or Attestation Provider, the Wallet Unit requests that PID or attestation in all formats offered by the PID Provider or Attestation Provider. *Note: Examples include the mdoc format specified in [ISO/IEC 18013-5] and the SD-JWT VC-format specified in [SD-JWT VC].*

Index	Requirement specification
ISSU_12b	During issuance of a PID or device-bound attestation, a WSCA/WSCD SHALL generate a new key pair for a new PID or attestation, on request of the PID Provider or Attestation Provider via the Wallet Instance. *Note: In case of synchronous issuing in a remote HSM architecture, re-use of an existing key pair for the new PID or attestation may be acceptable and it may not be necessary to generate a new key pair for each new PID or attestation.*
ISSU_12c	The expiration date of a PID SHALL be no later than the expiration date of the WUA presented as part of the PID issuance process. *Note: This requirement is an implication of WURevocation_18 in Topic 38. If the PID would be valid for longer than the WUA, the PID Provider would not be able to use the revocation information in the WUA to verify the revocation status of the Wallet Unit.*
ISSU_12d	If an Attestation Provider supports revocation chaining for its attestations per WURevocation_19 in Topic 38, the expiration date of an attestation SHALL be no later than the expiration date of the WUA presented as part of the attestation issuance process. *Note: See note in ISSU_12c.*

B - HLRs for PID issuance

Index	Requirement specification
ISSU_13	A Wallet Provider SHALL ensure that at least one PID Provider is willing to issue a PID complying with [PID Rulebook] to Users of the Wallet Units it provides.
ISSU_14	A PID Provider SHALL ensure that all PIDs it issues to Wallet Units comply with the requirements specified in [PID Rulebook].
ISSU_15	A PID Provider SHALL support the OpenID4VCI protocol referenced in ISSU_01 for issuing PIDs.
ISSU_16	Empty
ISSU_17	A PID Provider SHALL implement device binding for all PIDs it issues, meaning it SHALL ensure that a PID is cryptographically bound to a WSCA/WSCD included in the Wallet Unit, as specified in requirements WUA_11 - WUA_11b in [Topic 9]. *Note: Device binding is called 'mdoc authentication' in [ISO/IEC 18013-5] and 'key binding' in [SD-JWT-VC].*
ISSU_18	A PID Provider SHALL verify the identity of the subject of the PID in compliance with Level of Assurance (LoA) High requirements. *Note: These requirements will be determined by the relevant eID scheme.*
ISSU_18a	A PID Provider SHALL ensure that the attributes attested in the PID issued are valid for the identified PID subject at any point of time of PID validity.

Index	Requirement specification
ISSU_19	For the verification of a WUA, a PID Provider SHALL accept the trust anchors in the Wallet Provider Trusted List it needs. *Notes: - The Wallet Provider Trusted List is explained in [Topic 31]. - It is not mandatory for a PID Provider to accept all Wallet Provider Trusted Lists, if there are multiple. This is because it is not mandatory for a PID Provider to accept all certified Wallet Solutions in the EUDI Wallet ecosystem. Each PID Provider will choose which Trusted Lists they need to subscribe to.*
ISSU_19a	A PID Provider SHALL support at least one Wallet Solution, meaning that it is willing and able to issue a PID to a Wallet Unit on request of the User.
ISSU_20	To inform its potential PID subjects about the Wallet Solution(s) they can use for requesting a PID, a PID Provider SHALL publish a list of supported Wallet Solutions in such a way that it can be easily found, for example on the PID Provider’s website.

Index	Requirement specification
ISSU_21	Before issuing a PID, a PID Provider SHALL verify that the Wallet Provider mentioned in the Wallet Unit's WUA is present in a Wallet Provider Trusted List. The PID Provider SHALL also authenticate and validate the WUA using the trust anchor(s) registered for the Wallet Provider in the Wallet Provider Trusted List. Moreover, it SHALL verify that the Wallet Units's WUA is not revoked. *Notes: - For the WUA, see [Topic 9] and [Topic 38]. - CIR 2024/2977, Article 3 (9), also allows "another authentication mechanism in accordance with an electronic identity scheme notified at assurance level high." However, the ARF does not further specify such other authentication mechanisms, which means that in general they will not be interoperable.*
ISSU_22	A PID Provider SHALL include its PID Provider access certificate in its Issuer metadata used in the common OpenID4VCI protocol referenced in ISSU_01.
ISSU_22a	A PID Provider SHALL sign its metadata (as defined in OpenID4VCI) using the private key corresponding to its PID Provider access certificate.
ISSU_22b	The common OpenID4VCI protocol referenced in requirement ISSU_01, or an EUDI Wallet-specific extension or profile thereof, SHALL enable a PID Provider or Attestation Provider to include its access certificate and registration certificate in its Issuer metadata, according to requirement ISSU_22 and RPRC_22, respectively.

Index	Requirement specification
ISSU_23	For the verification of PID Provider access certificates, a Wallet Unit SHALL accept the trust anchors in the Trusted List(s) of Access Certificate Authorities it needs. *Notes: - Access Certificate Authority Trusted Lists are explained in [Topic 27]. -It is not mandatory for a Wallet Unit to accept all Access Certificate Authority Trusted Lists, if there are multiple. Wallet Providers will choose which Trusted Lists they need to subscribe to, for example depending on the Member State(s) they are operating in.*
ISSU_23a	A Wallet Provider SHALL support at least one PID Provider, meaning that its Wallet Units SHALL be capable of requesting the issuance of a PID from these PID Provider(s), and that the Wallet Provider has agreed with the PID Provider(s) that the PID Provider(s) will process such a request according to the agreed rules and procedures.
ISSU_23b	Prior to or during installation of a Wallet Instance, the Wallet Provider SHALL notify the User about the PID Provider(s) that are supported by the Wallet Unit.
ISSU_24	A Wallet Unit SHALL authenticate and validate the PID Provider access certificate before requesting the issuance of a PID. The Wallet Unit SHALL verify that the access certificate is authentic and is valid at the time of validation, and that the issuer of the access certificate is a CA that is in a Access Certificate Authority Trusted List.

Index	Requirement specification
ISSU_24a	Before requesting the issuance of a PID, the Wallet Unit SHALL verify that the PID Provider is indeed a registered PID Provider. The Wallet Unit SHALL do so using information contained in the PID Provider registration certificate, if available. If the registration certificate is not available, the Wallet Unit SHALL use the URL of the Registrar's online service, contained in the PID Provider access certificate, to obtain the necessary information from the Registrar. If the registered information does not confirm that the PID Provider is indeed properly registered as a PID Provider, the Wallet Unit SHALL display a warning to the User, and SHALL NOT request the issuance of a PID.

C - HLRs for Attestation Issuance

Index	Requirement specification
ISSU_25	An Attestation Provider SHALL ensure all attestations issued to Wallet Units comply with the requirements specified in the applicable Rulebook, as described in [Topic 12].
ISSU_26	An Attestation Provider SHALL support the OpenID4VCI protocol referenced in ISSU_01 for issuing attestations.

Index	Requirement specification
ISSU_27	An Attestation Provider SHOULD implement device binding for all attestations it issues. If an issued attestation is device-bound, the Attestation Provider SHALL ensure that the attestation is cryptographically bound to a WSCA/WSCD included in the Wallet Unit, as specified in requirement WUA_11 - WUA_11b in [Topic 9]. *Notes: Device binding is called 'mdoc authentication' in [ISO/IEC 18013-5] and 'key binding' in [SD-JWT-VC]. - Implementing mdoc authentication is mandatory in [ISO/IEC 18013-5]; therefore, it is mandatory for attestations complying with that standard.*
ISSU_27a	If the subject of the attestation is a natural person, an Attestation Provider SHALL verify the identity of the subject of the attestation, in compliance with applicable requirements and in accordance with relevant standards or Implementing Regulations. *Note: Not every attestation has a natural person as its subject. For example, a holiday voucher may be valid for any User that can present it to a Relying Party and therefore has no subject. This is comparable to the concept of a 'bearer token'.*
ISSU_27b	If applicable, an Attestation Provider SHALL ensure that the attributes attested in the attestation issued are valid for the identified attestation subject.
ISSU_27c	The Attestation Provider SHALL verify that the User requesting the attestation has the right to receive it.

Index	Requirement specification
ISSU_28	For the verification of a WUA, an Attestation Provider SHALL accept the trust anchors in the Wallet Provider Trusted List. *Note: The Wallet Provider Trusted List is explained in [Topic 31].*
ISSU_29	A QEAA Provider or PuB-EAA Provider SHALL support all Wallet Solutions, except in case the attestation in question is a Strong User Authentication (SUA) attestation as meant in Topic 20 and the Wallet Provider does not support processing of the transactional data associated with the SUA attestation. Except for such cases, A QEAA Provider or PuB-EAA Provider SHALL NOT discriminate between Wallet Solutions when processing a request for the issuance of an attestation. *Note: This requirement is not applicable for non-qualified EAA Providers. For example, a non-qualified EAA Provider may choose to issue attestations in the format specified in [W3C VCDM], see ARB_01a. In that case, it will support only those Wallet Solutions that have implemented this attestation format.*
ISSU_30	Before issuing an attestation, an Attestation Provider SHALL: - verify that the Wallet Provider mentioned in the Wallet Unit's WUA is present in the Wallet Provider Trusted List. - authenticate and validate the WUA using the trust anchor(s) registered for the Wallet Provider in the Wallet Provider Trusted List. - verify that the Wallet Unit's WUA is not revoked. *Note: For the WUA, see [Topic 9] and [Topic 38].*
ISSU_31	Empty

Index	Requirement specification
ISSU_32	An Attestation Provider SHALL include its Attestation Provider access certificate and registration certificate(s) in its Issuer metadata used in the common OpenID4VCI protocol referenced in ISSU_01.
ISSU_32a	An Attestation Provider SHALL sign its metadata (as defined in OpenID4VCI) using the private key corresponding to its Attestation Provider access certificate.
ISSU_33	For the verification of Attestation Provider access certificates, a Wallet Unit SHALL accept the trust anchors in all applicable Access Certificate Authority Trusted List(s). *Note: Access Certificate Authority Trusted Lists are explained in [Topic 27]. There may be separate Access Certificate Authority Trusted Lists for QEAA Providers, PuB-EAA Providers, and EAA Providers.*
ISSU_33a	For the verification of Attestation Provider registration certificates, a Wallet Unit SHALL accept the trust anchors in all Trusted List(s) for Providers of registration certificates.
ISSU_33b	A Wallet Provider SHALL support all Attestation Providers, except possibly if the attestation in question is a Strong User Authentication (SUA) attestation as meant in Topic 20 and the Wallet Provider chooses to not support processing of the transactional data associated with that attestation. Except for such cases, Wallet Units SHALL be capable of requesting the issuance of a QEAA, PuB-EAA, or non-qualified EAA from all Attestation Providers at the User’s request.

Index	Requirement specification
ISSU_34	A Wallet Unit SHALL authenticate and validate the Attestation Provider access certificate before requesting the issuance of an attestation. The Wallet Unit SHALL verify that the access certificate is authentic and is valid at the time of validation, and that the issuer of the access certificate is a CA that is in an Access Certificate Authority Trusted List, as documented in [Topic 27].
ISSU_34a	Before requesting the issuance of an attestation, the Wallet Unit SHALL verify that the Attestation Provider is a registered QEAA Provider, PuB-EAA Provider, or EAA Provider. The Wallet Unit SHALL also verify the Provider's sub-entitlements, i.e., whether the Provider properly registered for the issuance of the type of attestation that the User wants to obtain. The Wallet Unit SHALL do these checks using information contained in the Attestation Provider registration certificate, if available. If the registration certificate is not available, the Wallet Unit SHALL use the URL of the Registrar's online service, contained in the Attestation Provider access certificate, to obtain such information. If the registered information does not confirm that the Provider is registered as a QEAA Provider, PuB-EAA Provider, or EAA Provider, or if the registered information does not confirm that the Provider registered for the relevant type of attestation, the Wallet Unit SHALL display a warning to the User, and SHALL NOT request the issuance of an attestation.

D - HLRs for Privacy Risks and Mitigation

These HLRs were added as a result of the discussions of Topic A, Privacy risks and mitigation. For more background information on these requirements, please refer to Section 7.4.3.5 of the ARF main document and to the Discussion Paper for Topic A.

Index	Requirement specification
ISSU_35	A PID Provider or Attestation Provider SHALL ensure that all unique elements in a PID or attestation have a negligible chance of having the same value across all PIDs or attestations issued by that Provider. This SHALL include at least a) the salt used for hashing every attribute, b) the hash values of all attributes, c) the attestation identifier or index used for revocation purposes (if applicable), d) the attestation public key used for device binding (if applicable), and e) the value of the Attestation Provider signature. *Notes: - The list of unique elements is based on [ISO/IEC 18013-5] and [SD-JWT VC]. - This requirement can be achieved, for example, by ensuring that salt values, indexes and attestation identifiers are pseudo-random numbers generated by a cryptographically secure pseudo-random number generator (CSPRNG).*
ISSU_35a	A Wallet Provider SHALL ensure that all unique elements in a WUA have a negligible chance of having the same value across all WUAs issued by that Wallet Provider. This SHALL include at least a) the attestation identifier or index used for revocation purposes, b) the WUA public key used for device binding, and c) the value of the Wallet Provider signature. *Note: The list of unique elements is based on Technical Specification 3.*

Index	Requirement specification
ISSU_35b	After issuing a PID, attestation, or WUA, a PID Provider, Attestation Provider or Wallet Provider SHALL discard the values of all unique elements, including at least the ones mentioned in requirement ISSU_35 or ISSU_35a (as applicable) above, as well as any timestamps, as soon as they are no longer needed. The Provider SHALL NOT communicate these values to any other party inside or outside the EUDI Wallet ecosystem.
ISSU_36	When issuing PIDs, attestations, or WUAs in a batch to a Wallet Unit, a PID Provider, Attestation Provider, or Wallet Provider SHALL ensure that the timestamps in these PIDs, attestations, or WUAs do not enable Relying Parties to conclude that they are part of the same batch (and therefore belong to the same User). *Note: This can be done, for example, by making timestamps sufficiently imprecise that a high number of batches, each issued to a different Wallet Unit, share the same timestamp values (herd privacy).*

Index	Requirement specification
ISSU_37	A Wallet Provider SHALL ensure that its Wallet Solution supports the following methods for limiting the number of times a User can present the same PID or attestation to Relying Parties: Method A (Once-only attestations, as specified in requirement ISSU_43 - ISSU_47) and Method B (Limited-time attestations, as specified in requirement ISSU_48 - ISSU_50). In addition, a Wallet Provider MAY ensure that its Wallet Solution supports Method C (Rotating-batch attestations, as specified in requirement ISSU_51 - ISSU_54) or Method D (Per-Relying Party attestations, as specified in requirement ISSU_55 - ISSU_57). *Note: Wallet Solutions, PID Providers, Attestation Providers, and Wallet Providers are free to define and use other methods as well. However, such other methods are out of scope of the ARF.*

Index	Requirement specification
ISSU_38	A PID Provider, Attestation Provider, or Wallet Provider SHALL have a policy describing which of the methods A, B, C, or D, it will use to limit the number of times a Wallet Unit may present a single PID, attestation, or WUA. For each supported method, the policy SHALL also specify how the values for respective parameters for that method, such as technical validity period and batch size, will be chosen. The goal of the policy SHALL be to ensure that the risk of linkability is mitigated to an acceptable level, given the (expected) usage of the PID, attestation, or WUA by the User. To determine what an acceptable level of risk is, the PID Provider, Attestation Provider, or Wallet Provider SHALL carry out a risk analysis regarding linkability. *Notes: If an Attestation Provider issues multiple attestation types, these requirements apply for each type of attestation separately.*

Index	Requirement specification
ISSU_39	The Commission SHALL create or reference a profile or extension of the OpenID4VCI specification enabling a PID Provider, Attestation Provider, or Wallet Provider to indicate in their OpenID4VCI Issuer metadata which of the methods A, B, C, or D the Wallet Unit must use for the PID, attestation, or WUA issued. Indicated methods SHALL be ordered by preference. This profile or extension SHALL also enable the PID Provider, Attestation Provider, or Wallet Provider to set the value of parameters to be used by the Wallet Unit for each method (if applicable). *Note: For example, the parameters to be set for method A include the lower limit for unused attestations and the batch size to be requested.*

Index	Requirement specification
ISSU_40	PID Providers, Attestation Providers, and Wallet Providers SHALL indicate in their OpenID4VCI Issuer metadata at least that either method A or method B must be used for a given type of PID, attestation, or WUA. PID Providers, Attestation Providers, and Wallet Providers MAY additionally indicate that it prefers using method C and/or method D over method A or method B. In such a case, a Wallet Unit supporting method C and/or method D SHALL use that method, while a Wallet Unit not supporting these methods SHALL use method A or method B, as applicable. *Example: An Attestation Provider indicates methods {D, C, A} in their metadata, in that order. A Wallet Unit that supports methods C and D (as well as A and B) then uses method D for this type of attestation. A Wallet Unit supporting methods A, B and C uses method C. A Wallet Unit supporting only methods A and B uses method A.*
ISSU_41	To the maximum extent possible, Wallet Providers, PID Providers, and Attestation Providers SHALL ensure that Users do not notice which of the methods A, B, C, or D is used for their PIDs, attestations, or WUAs.
ISSU_42	To the maximum extent possible, Wallet Providers, PID Providers, and Attestation Providers SHALL ensure that no User action is needed for the re-issuance of WUAs, PIDs, or attestations. *Note: For the topic of re-issuance, see also the Discussion Paper for Topic B.*

Method A: Once-only attestations

The requirements in this subsection specify the Wallet Unit's behaviour when it is using Method A for a given type of PID, attestation, or WUA. For more information on this method, please refer to Section 3.2 of the Discussion Paper for Topic A.

Index	Requirement specification
ISSU_43	The Wallet Unit SHALL request the PID Provider, Attestation Provider, or Wallet Provider to issue PIDs, attestations, or WUAs in batches to the Wallet Unit. All PIDs, attestations, or WUAs in a batch SHALL have the same attribute values and the same technical validity period.
ISSU_44	The Wallet Unit SHALL present each PID, attestation, or WUA only once to a Relying Party, except when it has fallen back to Method B as specified below, or to another available method.
ISSU_45	The Wallet Unit SHALL have a lower limit for the number of unused PIDs, attestations, or WUAs it holds, and SHALL request the issuance of a new batch when this limit is reached. During the first issuance of a new PID, attestation, or WUA, see requirement ISSU_39, the PID Provider, Attestation Provider or Wallet Provider SHALL inform the Wallet Unit about the value of the lower limit and the size of the batch to be requested.
ISSU_46	If the Wallet Unit must request a new batch of PIDs, attestations, or WUAs, but is not able to do so because it is offline, the Wallet Unit SHALL warn the User that they are about to lose the possibility to present this PID or attestation to a Relying Party (or request (re-)issuance of a PID or attestation, in case of the WUA) and request them to connect their device to the internet.

Index	Requirement specification
ISSU_47	If the Wallet Unit has run out of unused PIDs, attestations, or WUAs, but is not able to request a new batch because it is offline, it SHALL fall back to method B (see requirement 6), or another available method. This means that, when requested by a Relying Party or Attestation Provider, the Wallet Unit SHALL again present one of the already used PIDs, attestations or WUAs. The Wallet Unit SHALL return to using method A as soon as it is able to go online and request a new batch of PIDs, attestations, or WUAs.

Method B: Limited-time attestations

The requirements in this subsection specify the Wallet Unit's behaviour when it is using Method B for a given type of PID, attestation, or WUA. See also Section 3.3 of the Discussion Paper for Topic A.

Index	Requirement specification
ISSU_48	The Wallet Unit SHALL request the PID Provider, Attestation Provider, or Wallet Provider to issue a single PID, attestation, or WUA to the Wallet Unit.
ISSU_49	The Wallet Unit SHALL present that PID, attestation, or WUA multiple times to the same Relying Party or Attestation Provider, or to different Relying Parties or Attestation Providers, when requested to do so.

Index	Requirement specification
ISSU_50	The Wallet Unit SHALL request the PID Provider, Attestation Provider, or Wallet Provider to re-issue a PID, attestation, or WUA some time before the one existing in the Wallet Unit expires. The PID Provider, Attestation Provider, or Wallet Provider SHALL inform the Wallet Unit about the moment at which the Wallet Unit must request the re-issuance of a PID, attestation, or WUA, relative to the expiration date of the existing one. *Note: It is the responsibility of the Relying Party receiving a PID or attestation (or the Attestation Provider receiving a WUA) to validate whether a presented PID, attestation, or WUA is temporally valid. A Wallet Unit is allowed to present a PID, attestation, or WUA even if its expiration date is in the past.*

Method C: Rotating-batch attestations

The requirements in this subsection specify the Wallet Unit's behaviour when it is using Method C for a given type of PID, attestation, or WUA. See also Section 3.4 of the Discussion Paper for Topic A.

Index	Requirement specification
ISSU_51	The Wallet Unit SHALL request the PID Provider, Attestation Provider, or Wallet Provider to issue PIDs, attestations, or WUAs in batches to the Wallet Unit. All PIDs, attestations, or WUAs in a batch SHALL have the same attribute values and the same technical validity period.

Index	Requirement specification
ISSU_52	When a presentation of attributes is requested by multiple Relying Parties, the Wallet Unit SHALL present each PID or attestation in a batch once, in a random order. Similarly, when a WUA is requested by multiple Attestation Providers, the Wallet Unit SHALL present each WUA in a batch once, in a random order.
ISSU_53	When all PIDs, attestations, or WUAs in a batch have been presented once, the Wallet Unit SHALL reset the batch, and start presenting each PID, attestation, or WUA in the batch again in a random order.
ISSU_54	The Wallet Unit SHALL request the PID Provider, Attestation Provider, or Wallet Provider to re-issue a batch of PIDs, attestations, or WUAs, some time before the batch in the Wallet Unit expires. The PID Provider, Attestation Provider, or Wallet Provider SHALL inform the Wallet Unit about the size of the batch and about the moment at which the Wallet Unit must request the re-issuance of a batch, relative to the expiration date of the existing one.

Method D: Per-Relying Party attestations

The requirements in this subsection specify the Wallet Unit's behaviour when it is using Method D for a given type of PID, attestation, or WUA. See also Section 3.5 of the Discussion Paper for Topic A.

Index	Requirement specification
ISSU_55	The Wallet Unit SHALL present a different PID, attestation, or WUA to each different Relying Party or Attestation Provider upon their request. This means that it SHALL comply with Method A for such Relying Parties or Attestation Providers.
ISSU_56	In case a given Relying Party requests attributes from a given type of PID or attestation multiple times, the Wallet Unit MAY present the same PID or attestation to this Relying Party each time. If it does, it SHALL comply with Method B or Method C for such a Relying Party.
ISSU_56a	In case a given Attestation Provider requests a WUA multiple times, the Wallet Unit MAY present the same WUA to this Attestation Provider each time. If it does, it SHALL comply with Method B or Method C for such an Attestation Provider.
ISSU_57	The Wallet Unit SHALL keep track of which PID or attestation it has presented to which Relying Party, using the unique identifier from the respective access certificate, unless the Relying Party is an intermediary. If the Relying Party is an intermediary, the Wallet Unit SHALL use the unique identifier obtained from the registration certificate or from the extension of the presentation request meant in RPI_06. *Note: The Wallet Unit can see that a presentation request is from an intermediary either because this is indicated in the registration certificate or because the extension meant in RPI_06 and RPI_06a is present.*

Index	Requirement specification
ISSU_57a	The Wallet Unit SHALL keep track of which WUA it has presented to which Attestation Provider, using the unique identifier obtained from the respective access certificate.

E - HLRs for re-issuance and batch issuance of PIDs, attestations and WUAs

These HLRs were added as a result of the discussions of Topic B, re-issuance and batch issuance of PIDs, attestations and WUAs. For more background information on these requirements, please refer to Sections 6.6.2.7 and 6.6.5.2 of the ARF main document, and to the Discussion Paper for Topic B.

Index	Requirement specification
ISSU_58	A Wallet Unit SHALL give its User the option to manually initiate a re-issuance process for any of the PIDs or attestations in their Wallet Unit. *Note: This requirement does not apply for WUAs, since Users must not be involved in the management of WUAs.*
ISSU_59	After a successful re-issuance, a Wallet Unit SHALL compare the attribute values of the re-issued PID or attestation with those of the existing PID or attestation, and SHALL notify the User in case of any differences. *Note: This requirement does not apply for WUAs, since Users must not be involved in the management of WUAs.*
ISSU_60	A Wallet Unit SHALL gracefully handle situations in which re-issuance of a PID, attestation, or WUA is refused by the PID Provider, Attestation Provider, or Wallet Provider,for example by attempting a retry after an appropriate delay.

Index	Requirement specification
ISSU_61	A Wallet Unit SHALL support PID or attestation first-time batch issuance with a single User authentication, regardless of the size of the batch. *Notes: - See also requirement WIAM_14. - This requirement does not apply for WUAs, since Users must not be involved in the management of WUAs.*
ISSU_62	If a PID, attestation, or WUA was successfully re-issued because the value of one or more of its attributes was changed (including attributes being added or deleted), a Wallet Unit SHOULD delete the correct pre-existing PID, attestation, or WUA. *Notes: - It is up to the Wallet Unit, possibly using metadata provided by the PID Provider, Attestation Provider, or Wallet Provider using the [OpenID4VCI] protocol, to determine the PID, attestation, or WUA to be deleted. - Additionally, per requirement VCR_09, the PID Provider, Attestation Provider, or Wallet Provider revokes the pre-existing PID, attestation, or WUA.*
ISSU_63	PID Providers, Attestation Providers, Wallet Providers, and Wallet Units SHALL support the features of [OpenID4VCI] enabling the re-issuance of PIDs, attestations, and WUAs.
ISSU_64	PID Providers, Attestation Providers, Wallet Providers, and Wallet Units SHALL support the features of [OpenID4VCI] enabling the batch issuance of PIDs, attestations, and WUAs.

Index	Requirement specification
ISSU_65	The common OpenID4VCI protocol referenced in requirement ISSU_01, or an EUDI Wallet-specific extension or profile thereof, SHALL enable a PID Provider, Attestation Provider or Wallet Provider to verify that a re-issued device-bound PID, attestation, or WUA is bound to the same WSCA/WSCD to which the existing device-bound PID, attestation, or WUA is bound. *Note: This can be done, for instance, by requiring that OAuth 2.0 Demonstrating Proof of Possession (DPoP) [RFC 9449] is used for each Refresh Token, and that the public key of the Refresh Token and the public key of the existing PID, attestation, or WUA are stored in the same WSCA/WSCD.*
ISSU_66	The common OpenID4VCI protocol referenced in requirement ISSU_01, or an EUDI Wallet-specific extension or profile thereof, SHALL enable an Attestation Provider to verify that the Refresh Token used for the re-issuance of a non device-bound attestation is bound to a WSCA/WSCD included with the Wallet Unit in which the replaced attestation is stored. *Notes: - This requirement implies that if an Attestation Provider enables re-issuance of an attestation by issuing Refresh Tokens, these tokens must be device-bound, even in case the attestation itself is not device-bound. - This requirement does not apply to PIDs and WUAs, since these are bound to a WSCA/WSCD because they must be issued and managed at Level of Assurance High.*

A.2.3.11 Topic 11 - Pseudonyms

Description

Wallet Units will support generating pseudonyms for Users in compliance with the W3C WebAuthn API specification, W3C WebAuthn. On a high level, this means that the WSCA/WSCD in the Wallet Unit will be able to create key pairs. The public keys of these pairs function as pseudonyms for the User. Only the User can use these pseudonyms, since the WSCA/WSCD authenticates the User before allowing a pseudonym to be used, see requirement WIAM_14. The Wallet Unit will keep an internal structure to associate each pseudonym (public key) with a specific Relying Party, based on the Relying Party unique identifier in the Relying Party Instance access certificate mentioned in requirement Reg_32.

Pseudonyms were discussed with Member States in Topic E. These discussions included the use cases for which Wallet Units must support pseudonyms and the HLRs for the technical specification of how it must be implemented. The below HRLs are the result of this discussion. For more background information on these requirements, please refer to the Discussion Paper for Topic E.

NOTE: As specified in requirement PA_21, the Commission will create or reference a technical specification containing a profile or extension of the [W3C WebAuthn] specification. The HLRs below are in fact requirements to be fulfilled by this technical specification. Discussions on the pseudonyms are ongoing.

A. HLRs related to Use Cases

Index	Requirement specification
PA_01	A Wallet Unit SHALL enable a User to generate a Pseudonym and register it at a Relying Party.
PA_02	A Wallet Unit SHALL enable a User to authenticate with a Pseudonym towards a Relying Party if the Wallet Unit was used previously to register the Pseudonym for the same Relying Party.
PA_03	A Wallet Unit SHALL be able to perform the actions specified in the above two requirements independently of whether the interaction with the Relying Party is initiated on the same device hosting the Wallet Instance or on a device different from the one hosting the Wallet Instance.
PA_04	A Wallet Unit SHALL enable the User to use multiple different Pseudonyms at a given Relying Party.

Index	Requirement specification
PA_05	A Wallet Unit SHOULD enable a User to freely choose a User alias for each Pseudonym registered at a Relying Party. Setting an alias SHOULD be optional for the User. The User SHOULD be able to change the alias for any Pseudonym.
PA_06	A Wallet Unit SHALL enable a User to choose which Pseudonym to authenticate with towards a Relying Party, if multiple Pseudonyms are registered for this Relying Party. The Wallet Unit SHOULD present the User with the aliases of the applicable Pseudonyms, if assigned, when making this choice.
PA_07	A Wallet Unit SHALL enable a User to delete a Pseudonym.
PA_08	A Wallet Unit SHALL enable the User to manage Pseudonyms within the Wallet Unit in a user-friendly and transparent manner.
PA_08a	A Wallet Unit SHALL log Pseudonym registration and presentation transactions as specified in Topic 19.
PA_09	A Wallet Unit SHALL enable the User to see all existing pseudonyms, including the associated Relying Party.

B. HLRs related to Relying Parties

Index	Requirement specification
PA_10	A Relying Party SHALL be able to verify that a User is registering a Pseudonym using a non-revoked Wallet Unit.
PA_11	A Relying Party SHALL be able to verify that a User is authenticating with a Pseudonym using a non-revoked Wallet Unit.
PA_12	If Wallet Unit is used to register a Pseudonym at a Relying Party in combination with a PID, attestation or WUA being presented to the same Relying Party, then this Relying Party SHALL be able to verify that the same User performed both actions.
PA_13	The Relying Party SHALL be able to validate that the pseudonym presented to them belongs to the User presenting it.

C. HLRs related to privacy

Index	Requirement specification
PA_14	A Wallet Unit SHALL store the information necessary for authenticating with a Pseudonym in its WSCA/WSCD.
PA_15	A Relying Party SHALL NOT be able to derive the User’s true identity, or any data identifying the User, from the Pseudonym value received by the Relying Party.
PA_16	A Wallet Unit SHALL NOT reveal the same Pseudonym to different Relying Parties unless the User explicitly chooses otherwise.
PA_17	It SHALL NOT be possible to correlate Pseudonyms based on their values nor on other metadata sent by the Wallet Unit during registration and authentication, meaning that colluding Relying Parties SHALL NOT able to conclude that different Pseudonyms belong to the same User.
PA_18	The Wallet Unit SHALL ensure that Pseudonyms contain sufficient entropy to make the chance of colliding Pseudonyms (meaning two Users having the same Pseudonym value for the same Relying Party) negligible.
PA_19	A Wallet Unit SHALL NOT share the User’s optionally assigned Pseudonym aliases with any Relying Party.
PA_20	The Wallet Unit SHALL verify the identity of a Relying Party when a User registers a Pseudonym or authenticates with a Pseudonym, provided the profile or extension of [W3C WebAuthn] meant in PA_21 enables the Wallet Unit to do this. In case the profile or extension does not enable this, the Wallet Unit SHALL trust the WebAuthn Client (i.e., the browser) to verify the Relying Party identity. *Notes: - [W3C WebAuthn] currently does not offer a way for an Authenticator (i.e., the Wallet Unit) to authenticate a Relying Party. Instead, the Client (i.e., the browser) will authenticate the Relying Party, using TLS.*

D. HLRs related to interoperability

Index	Requirement specification
PA_21	The Commission SHALL create or reference a technical specification containing a profile or extension of the [W3C WebAuthn] specification compliant with the HLRs specified in this Topic. This specification SHALL contain all details necessary for Wallet Units and Relying Parties to generate, register, and use Pseudonyms.
PA_22	Wallet Providers SHALL ensure that their Wallet Solution supports the [W3C WebAuthn] specification and the technical specification meant in requirement PA_21.

A.2.3.12 Topic 12 - Attestation Rulebooks

Description

Article 45e of the [European Digital Identity Regulation] sets up the legal basis for the Commission to "where necessary, establish specifications and procedures for the catalogue of attributes and schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes". As described in Section 5.5 of the ARF main document, these 'schemes for the attestations of attributes' will be described in so-called Attestation Rulebooks. A separate Rulebook will be created for each type of attestation. This Topic describes the high-level requirements for the Attestation Rulebooks that will specify the details of new types of attestations.

Attestation Rulebooks will be written by Attribute Schema Providers, a role which can be assumed by different types of organisation. The goal of this Topic is to ensure that all Rulebooks that will be written in the future will contain the same type of information and the same level of detail, such that all attestations are interoperable.

An attestation scheme is a machine-readable companion to an Attestation Rulebook. Attestation schemes may be registered and published in a publicly accessible catalogue, as described in Topic 26.

HLRs

A. Requirements regarding attestation formats

Index	Requirement specification
ARB_01	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a QEAA or a PuB-EAA SHALL specify that one or more of the following two common format(s) must be used for these attestations: - The format specified in ISO/IEC 18013-5, see [ISO18013-5]. - The format specified in "SD-JWT-based Verifiable Credentials (SD-JWT VC)", see [SD-JWT-VC].
ARB_01a	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a non-qualified EAA SHALL specify that one or more of the following three common format(s) must be used for these attestations: - The format specified in ISO/IEC 18013-5, see [ISO18013-5]. - The format specified in "SD-JWT-based Verifiable Credentials (SD-JWT VC)", see [SD-JWT-VC]. - The format specified in "W3C Verifiable Credentials Data Model", see [W3C VCDM v2.0].
ARB_01b	The Schema Provider for an Attestation Rulebook describing attestations using the format specified in [SD-JWT VC] SHALL ensure that these attestations comply with the 'SD-JWT VCs' profile specified in [HAIP].

Index	Requirement specification
ARB_02	The Schema Provider for an Attestation Rulebook SHALL analyse whether it must be possible for a User to present that type of attestation when the Wallet Unit and the Relying Party are in proximity and attestations are presented without using the internet. If so, the Attestation Rulebook SHALL specify that the attestations must be issued in the ISO/IEC 18013-5-compliant mdoc format. *Note: In theory, it is possible to use SD-JWT VC-compliant attestations in proximity use cases. In practice, however, the only protocol available to request and release SD-JWT VC-compliant attestations between a Wallet Unit and a Relying Party Instance is OpenID4VP. That protocol cannot be used without internet connectivity.*
ARB_03	The Schema Provider for an Attestation Rulebook MAY specify in the Attestation Rulebook that that type of attestation must be issued in the [SD-JWT VC]-compliant format, provided the [SD-JWT VC] specification has been approved by an EU standardisation body or by the European Digital Identity Cooperation Group established pursuant to Article 46e(1) of the [European Digital Identity Regulation].

Index	Requirement specification
ARB_04	If an Attestation Rulebook specifies that a type of attestation can be issued in a format compliant with [W3C VCDM v2.0], the Schema Provider for that Attestation Rulebook SHALL ensure the Rulebook references one or more documents specifying in detail how a Relying Party can request attributes from a such an attestation, and how a User can selectively disclose attributes from such an attestation. Moreover, these referenced documents SHALL be approved by an EU standardisation body or by the European Digital Identity Cooperation Group established pursuant to Article 46e(1) of the [European Digital Identity Regulation].

B. Requirements regarding attestation types

Index	Requirement specification
ARB_05	The Schema Provider for an Attestation Rulebook SHALL specify a value for the attestation type, which SHALL be unique within the scope of the EUDI Wallet ecosystem. *Notes: - In ISO/IEC 18013-5, the attestation type is called ‘document type’ and is included as a “docType” key-value pair in both the mdoc request and the mdoc response. Also, a method for generating unique attestation type values is recommended. - In OpenID4VP, the attestation type is included in the “meta” property of a Credential Query in a presentation request. - In [SD-JWT VC], the attestation type is called ‘SD-JWT VC type’ and is included as a ‘vct’ claim in the SD-JWT VC.*

C. Requirements regarding attestation schemes

Index	Requirement specification
ARB_06	The Schema Provider for an Attestation Rulebook SHALL define all attributes that an attestation of that type may contain. This definition SHALL first describe the semantics of each attribute in an encoding-independent manner and SHALL subsequently for each attribute specify an ISO/IEC 18013-5-compliant format, an SD-JWT VC-compliant format, or both, as needed given the choices made according to ARB_01 - ARB_04.

Index	Requirement specification
ARB_06a	For ISO/IEC 18013-5-compliant attestations, the Attestation Rulebook SHALL define each attribute within an attribute namespace. An attribute namespace SHALL fully define the identifier, the syntax, and the semantics of each attribute within that namespace. An attribute namespace SHALL have an identifier that is unique within the scope of the EUDI Wallet ecosystem, and each attribute identifier SHALL be unique within that namespace. *Note: In ISO/IEC 18013-5, namespaces are discussed and a method for generating unique namespace identifiers is recommended.*
ARB_06b	For [SD-JWT VC]-compliant attestations, the Schema Provider for the Attestation Rulebook SHALL ensure that each claim name is either: - included in the IANA registry for JWT claims, - is a Public Name as defined in [RFC 7519], or is a Private Name specific to the attestation type. *Note: [SD-JWT VC] does not discuss how to avoid conflicting claim names. Since SD-JWTs are a special kind of JWTs, the methods specified in RFC 7519 are applicable.*
ARB_07	When determining the attributes to be included in a new attestation type, the Schema Provider for the applicable Attestation Rulebook SHOULD consider referring to attributes that are already included in the catalogue of attributes specified in Topic 25 or specified in an attestation scheme included in the catalogue of attestation schemes specified in Topic 26, rather than unnecessarily re-defining all attributes.

Index	Requirement specification
ARB_08	The Schema Provider for an Attestation Rulebook SHOULD, when specifying a new attribute, take into consideration existing conventions for attribute identifier values and attribute syntaxes. *Note: These conventions may depend on the format of the attestation, i.e., CBOR for ISO/IEC 18013-5-compliant attestations or JSON for SD-JWT VC-compliant attestations.*
ARB_09	The Schema Provider for an Attestation Rulebook SHALL specify, for each attribute in the attestation, whether the presence of that attribute is mandatory, optional, or conditional.
ARB_10	The Schema Provider for an Attestation Rulebook for an ISO/IEC 18013-5 compliant attestation MAY define a domestic namespace to specify attributes that are specific to that Rulebook and are not included in the applicable EU-wide or sectoral namespace. All requirements for namespaces in this Topic SHALL also apply for domestic namespaces.
ARB_11	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a QEAA or a PuB-EAA SHALL include in the Rulebook an attribute as meant in Annex V point a) and Annex VII point a) of the [European Digital Identity Regulation]. This attribute SHALL reference the technical specification meant in ARB_25.
ARB_12	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a non-qualified EAA SHOULD include an attribute in the Rulebook indicating that the attestation is an EAA. This attribute SHALL reference the technical specification meant in ARB_25.

Index	Requirement specification
ARB_13	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a QEAA SHALL include in the Rulebook one or more attributes or metadata representing the set of data meant in Annex V point b) of the [European Digital Identity Regulation].
ARB_14	The Schema Provider for an attestation Rulebook describing a type of attestation that is a PuB-EAA SHALL include in the Rulebook one or more attributes or metadata representing the set of data meant in Annex VII point b) of the [European Digital Identity Regulation].
ARB_15	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a non-qualified EAA SHOULD include in the Rulebook one or more attributes or metadata representing the set of data meant in Annex V point b) of the [European Digital Identity Regulation].
ARB_16	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a QEAA or a PuB-EAA SHALL include in the Rulebook one or more attributes representing the set of data meant in Annex V point c) or Annex VII point c) of the [European Digital Identity Regulation].
ARB_17	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a non-qualified EAA SHOULD include in the Rulebook one or more attributes representing the set of data meant in Annex V point c) of the [European Digital Identity Regulation].

Index	Requirement specification
ARB_18	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a QEAA or a PuB-EAA SHALL include in the Rulebook one or more attributes or metadata representing the set of data meant in Annex V point e) or Annex VII point e) of the [European Digital Identity Regulation].
ARB_19	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a non-qualified EAA SHOULD include in the Rulebook one or more attributes representing the set of data meant in Annex V point e) of the [European Digital Identity Regulation].
ARB_20	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a QEAA or a PuB-EAA SHALL include in the Rulebook one or more attributes or metadata representing the location meant in Annex V point h) or Annex VII point h) of the [European Digital Identity Regulation]. For a QEAA, this location SHALL indicate at least the URL at which a machine-readable version of the trust anchor to be used for verifying the QEAA can be found or looked up. For a PuB-EAA, this location SHALL indicate at least the URL at which a machine-readable version of the qualified certificate that signed the PuB-EAA can be found or looked up.

Index	Requirement specification
ARB_21	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a non-qualified EAA SHOULD include in the Rulebook one or more attributes or metadata representing the location at which a machine-readable version of the trust anchor to be used for verifying the EAA can be found or looked up.*Note: What this location indicates precisely is dependent on the nature of the mechanism used for distributing trust anchors; see requirement ARB_26.*

D. Miscellaneous requirements

Index	Requirement specification
ARB_22	The Schema Provider for an Attestation Rulebook SHALL specify all technical details necessary to ensure interoperability, security, and privacy of that attestation. *Note: An Attestation Rulebook may also specify requirements regarding how the Wallet Unit must display the attestation and the attributes in it to the User.*
ARB_23	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a QEAA or a PuB-EAA SHALL specify which of the revocation mechanisms specified in Topic 7 SHALL be supported by that attestation.
ARB_24	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a non-qualified EAA SHALL specify whether that type of EAA must be revocable. If an EAA type must be revocable, the relevant Rulebook SHALL determine which of the revocation mechanisms specified in Topic 7 SHALL be supported by that attestation.

Index	Requirement specification
ARB_25	The Commission SHALL take measures to ensure that the following information is included in a technical specification: - The identifier of the attribute containing the indication meant in Annex V point a) and Annex VII point a). - The syntax and semantics of this attribute in case the attestation is a QEAA, in case it is PuB-EAA, and in case it is a non-qualified EAA.
ARB_26	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a non-qualified EAA SHOULD define in the Rulebook: - mechanisms allowing a Wallet Unit to verify that the EAA Provider is authorised or registered to issue this type of EAA. - mechanisms allowing a Relying Party to obtain, in a trustworthy manner, the trust anchor(s) of the EAA Providers issuing this type of EAA.
ARB_27	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a QEAA, PuB-EAA, or non-qualified EAA SHOULD specify in the Rulebook whether a Relying Party receiving the attestation must request and verify a PID and verify the cryptographic binding between the PID and the attestation. *Note: Relying Parties can only do so in a trustworthy manner if Wallet Units are able to provide a proof of cryptographic binding showing that the private keys of the attestation and the PID are stored in the same WSCD, in accordance with the requirements in Topic 18.*

Index	Requirement specification
ARB_28	An Attribute Schema Provider SHOULD specify an attribute in an Attestation Rulebook that indicates whether the Attestation Provider during attestation issuance requested a cryptographic binding (as specified in Topic 18) between the new attestation and an existing PID or attestation. If present in a Rulebook, the identifier for this attribute SHALL be "cryptographically_bound_to", and its contents SHALL be an attestation type or vct (see ARB_05). *Note: The meaning of this attribute, if present, is "This attestation is cryptographically bound to one or more attestations of the given attestation type or vct on this Wallet Unit." If a Relying Party receives this attribute from a Wallet Unit, it can subsequently request the Wallet Unit to send a proof of cryptographic binding between the attestation and an attestation indicated in the "cryptographically_bound_to" attribute.*
ARB_29	The Schema Provider for an Attestation Rulebook describing a type of attestation that is a QEAA, PuB-EAA, or non-qualified EAA SHOULD ensure that the structure and contents of the Attestation Rulebook follow the descriptions in the Attestation Rulebook template.

Index	Requirement specification
ARB_30	If an Attestation Rulebook specifies a [SD-JWT VC]-compliant attestation, the Schema Provider for that Attestation Rulebook SHALL specify for all claims (i.e., all top-level properties, all nested properties, and all array entries) whether an Attestation Provider MUST, MAY, or MUST NOT make that claim selectively disclosable. *Notes: - This requirement does not apply to claims defined as non-selectively disclosable in [SD-JWT VC]. - There will be use cases where a specific claim must not be disclosed without simultaneously disclosing one or more other claims. Such cases should be solved by making all of these claims members of the same JSON object (or elements of the same JSON array). That JSON object (or array) is then the claim that must be selectively disclosable, while the nested properties (or individual array elements) must not be selectively disclosable. - This requirement does not apply to [ISO/IEC 18013-5]-compliant attestations, since in such attestations, by definition all data elements are selectively disclosable, while none of the key-value pairs or array elements inside a data element (if any) are selectively disclosable.*

Index	Requirement specification
ARB_31	If an Attestation Rulebook specifies a [SD-JWT VC]-compliant attestation, the Schema Provider for that Attestation Rulebook SHOULD consider defining a Type Metadata Document for it, as defined in Chapter 6 of [SD-JWT VC]. If the Schema Provider defines such a document, it SHOULD contain the Claim Selective Disclosure Metadata (defined in Section 9.3 of [SD-JWT VC]) for each of the claims, in order to specify if that claim is selectively disclosable (see requirement ARB_30). *Note: Although a Type Metadata Document is a highly technical document, defining it has a number of advantages for developers, Attestation Providers, Relying Parties,. and Wallet Units, as spelled out in Chapter 6 of [SD-JWT VC].*
ARB_32	If an Attestation Rulebook specifies a [SD-JWT VC]-compliant attestation, the Schema Provider for that Attestation Rulebook SHOULD consider defining a JSON Schema for it, as defined in Section 6.5 of [SD-JWT VC], and include or reference that Schema in the Type Metadata Document meant in ARB_31. *Note: requirements for validation of a Schema (if present) by Wallet Units or Relying Party are specified in Section 6.5.2 of [SD-JWT VC].*
ARB_33	If a Schema Provider for an Attestation Rulebook registers an attestation scheme in the catalogue of attestation schemes meant in Topic 26, the registration SHALL include a reference to the corresponding Attestation Rulebook. *Note: By definition, an attestation scheme is machine-readable, whereas an Attestation Rulebook is human-readable.*
ARB_34	The Schema Provider for an Attestation Rulebook SHALL specify whether that attestation is device-bound or not.

A.2.3.13 Topic 13 - Developing a Wallet Unit architecture based on Secure Element

There are no HLRs for this Topic.

A.2.3.14 Topic 14 - Developing a Wallet Unit architecture based on External Token

There are no HLRs for this Topic.

A.2.3.15 Topic 15 - Developing a Wallet Unit architecture based on Remote HSM

There are no HLRs for this Topic.

A.2.3.16 Topic 16 - Signing documents with a Wallet Unit

Description

A Wallet Unit SHALL enable its User to create qualified electronic signatures or seals. This goal can be reached by using signature or seal creation capabilities of the Wallet Unit as a part of a local QSCD, or by using a remote QSCD managed by a QTSP.

This Topic contains high-level requirements related to the creation of Qualified Electronic Signatures using a Wallet Unit.

HLRs

A. Requirement for Wallet Providers

Index	Requirement specification
QES_01	Wallet Providers SHALL ensure that each User has the possibility to receive a qualified certificate for Qualified Electronic Signatures, bound to a QSCD, that is either local, external, or remotely managed in relation to the Wallet Instance.

Index	Requirement specification
QES_02	Wallet Providers SHALL ensure that each User who is a natural person has, at least for non-professional purposes, free-of-charge access to a Signature Creation Application which allows the creation of free-of-charge Qualified Electronic Signatures using the certificates referred to in QES_01. Wallet Providers SHALL ensure that: - The Signature Creation Application SHALL, as a minimum, be capable of signing or sealing User-provided data and Relying Party-provided data. - The Signature Creation Application SHALL be implemented as part of a Wallet Solution or external to it (by providers of trust services or by Relying Parties). - The Signature Creation Application SHALL be able to generate signatures or seals in formats compliant with at least the mandatory formats referred to in QES_08. *Notes: - Signature Creation Application (SCA): see definition in the ETSI TS 119 432 standard. - If the SCA is external to the Wallet Solution, it may be for example a separate mobile application, or be hosted remotely, for instance by the QTSP or by a Relying Party.*
QES_03	For the use of the qualified certificate referred to in QES_01, Wallet Providers SHALL ensure that a Wallet Unit implements secure authentication of the User, as well as signature or seal invocation capabilities, as a part of a local, external or remote QSCD.

Index	Requirement specification
QES_04	Wallet Providers SHALL enable their Wallet Units to interface with QSCDs using protocols and interfaces necessary for the implementation of secure User authentication and signature or seal functionality. *Note: In a Relying Party-centric flow, the remote QTSP will likely be selected by the Relying Party, which implies the QSCD is managed by the remote QTSP. In a Wallet Unit-driven flow, the User should be able to choose the QSCD.*
QES_05	Wallet Providers SHALL enable their Wallet Units to be used for User enrolment to a remote QES Provider (i.e., a QTSP offering remote QES), except where the Wallet Unit interfaces with local or external QSCDs.
QES_06	Wallet Providers SHALL ensure that their Wallet Solution supports at least one of the following options for remote QES signature creation: - remote QES creation through secure authentication to a QTSP signature web portal, - remote QES creation channelled by the Wallet Unit, - remote QES creation channelled by a Relying Party.
QES_07	Wallet Providers SHALL ensure that, where a Signature Creation Application relies on a remote Qualified Signature Creation Device and where it is integrated into a Wallet Instance, it supports the Cloud Signature Consortium API Specification 2.0 [CSC API].

Index	Requirement specification
QES_08	Wallet Providers SHALL ensure that their Wallet Units are able to create signatures or seals in accordance with the mandatory PAdES format as specified in ETSI EN 319 142-1 V1.1.1 (2016-04). In addition, Wallet Providers SHOULD ensure that their Wallet Units are able to create signatures or seals in accordance with the following formats: - XAdES as specified in ETSI EN 319 132-1 V1.2.1 (2022-02), - JAdES as specified in ETSI TS 119 182-1 V1.2.1 (2024-07), - CAdES as specified in ETSI EN 3191 22-1 V1.3.1 (2023-06), and - ASiC as specified in ETSI EN 319 162-1 V1.1.1 (2016-04) and ETSI EN 319 162-2 V1.1.1 (2016-04).
QES_09	Empty
QES_10	Wallet Providers SHALL ensure that, where the Signature Creation Application is implemented as part of the Wallet Unit and is used to generate signatures or seals of the representation of the document or data to be signed or sealed, the Wallet Unit presents the representation of the document or data to be signed or sealed to the User.
QES_11	Wallet Providers SHALL ensure that, where the Signature Creation Application is implemented as part of the Wallet Unit, a Wallet Unit computes the hash or digest of the document or data to be signed through a Signature Create Application component.

Index	Requirement specification
QES_12	Wallet Providers SHALL ensure that a Wallet Unit is able to create the signature value of the document or data to be signed either using a local or a remote signing application. *Note: a local signing application is on-device. It may either be embedded in the Wallet Unit or be an external application.*
QES_13	Wallet Providers SHALL ensure that a Wallet Unit provides a log of transactions related to qualified electronic signatures or seals generated by or through the Wallet Unit, allowing the User to view the history of previously signed data or documents, according to requirement DASH_04 in Topic 19. *Note: If the signature is generated by a remote Signature Creation Application, the Wallet is at minimum used to authenticate the User to the remote QTSP and to obtain the User's consent for the usage of the private signing key. The logs then record information about these processes.*
QES_14	Wallet Providers SHALL ensure that the User will be able to explicitly authorise the creation of a qualified electronic signature or seal through their Wallet Unit.
QES_15	Wallet Providers SHALL ensure that a Wallet Unit can verify, in remote signature creation scenarios, that the qualified electronic signature or seal creation device is part of a qualified service, which is carried out by a qualified trust service provider.

Index	Requirement specification
QES_16	Wallet Providers SHOULD ensure that a Wallet Unit supports multiple-signing scenarios where multiple signatories are required to sign the same document or data.
QES_17	Wallet Providers SHALL ensure that Wallet Units provide a signature creation confirmation upon the creation of a qualified electronic signature, informing the User about the outcome of the signature creation process. *Note: See also QES_17a.*
QES_17a	If the Signature Creation Application is external to the Wallet Unit, after the User authorises the usage of the private signing key, the Signature Creation Application SHALL return the outcome of the signature creation process to the Wallet Unit.
QES_18	Wallet Providers SHALL configure at least one default qualified signing service in the Wallet Unit.
QES_19	Wallet Providers SHALL ensure that, where the Signature Creation Application is implemented as part of the Wallet Unit, a Wallet Unit supports ETSI TS 119 101 (Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation) when using signing keys managed by the QSCD, whether locally, externally, or remotely in relation to the Wallet Instance.
QES_20	Empty
QES_21	Empty

Index	Requirement specification
QES_22	Empty

B. Requirements for QTSPs

Index	Requirement specification
QES_23	QTSPs providing the remote QES part of a Wallet Solution SHALL support: 1. ETSI TS 119 431-1 (Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev), 2. ETSI TS 119 431-2 (Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation), 3. ETSI TS 119 432 (Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation). Wallet Providers and QTSPs providing the remote QES part of a Wallet Solution SHALL comply with Sole Control Assurance Level (SCAL) 2 as defined in CEN EN 419 241-1 (Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements).
QES_24	QTSPs providing the Signature Creation Application as part of the remote QES part of a Wallet Solution SHALL support ETSI TS 119 101 (Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation).

C. Requirements for Relying Parties

Index	Requirement specification
QES_24a	Relying Parties providing the Signature Creation Application in a Relying Party-centric flow SHALL support ETSI TS 119 101 (Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation).

D. Requirements for the Commission

Index	Requirement specification
QES_25	Empty
QES_26	Empty

A.2.3.17 Topic 17 - Identity matching

Description

Users would like to use their PID in their Wallet Unit to access their existing online account(s), even if their PID attribute values are not exactly the same as those in their account(s). Users regularly need to log in to cross-border services offered by public sector bodies. Identity matching enables them to use their Wallet Unit to do so.

HLRs

There are no HLRs for this Topic.

A.2.3.18 Topic 18 - Combined presentations of attributes

Description

Note: The text in this section and the high-level requirements in the next section were adapted from the Discussion Paper for Topic K. All high-level requirements were changed compared to the situation prior to integration of Topic K.

The concept of *combined presentation* refers to a process where a Relying Party requests multiple attributes concerning a single User, drawn from separate attestations (e.g., PID and/or (Q)EAAs), and receives a consolidated response. The key functional goal is to enable the Relying Party to verify that all presented attributes pertain to the same User, without compromising trust, privacy, or data integrity.

A combined presentation of attributes, when designed with privacy in mind, becomes a powerful tool for protecting individuals from unnecessary exposure. Rather than relying on full identification for each presented attestation, we can instead implement solutions that enable Users to prove only what is strictly necessary — without revealing who they are. This aligns directly with the commitments laid out in the [European Digital Identity Regulation]: access to digital services must be privacy-protective by design (recital 4), supported by privacy-enhancing technologies (recital 14), and uphold the principle of unobservability (recital 32).

In this light, Article 5a(16)(b) provides a clear obligation: when attributes are presented together, this must be done in a way that avoids unnecessary identification of the User. Instead, a privacy-preserving combined presentation of attributes opens the door to new possibilities. It enables the transition of many real-world processes — currently performed under full identification — into more private digital equivalents.

Consider, for example, eligibility checks for educational programs. A student should be able to prove they reside in a particular city and have qualifying grades *without revealing their name, gender, or exact address*. The same logic applies more broadly: renting a car or a bicycle, or purchasing restricted goods like alcohol, often requires only proof of eligibility — but not a proof of identity. With the right cryptographic mechanisms in place, we can minimize data exposure while maintaining trust in the presented attributes

This Topic describes high-level requirements for such a Cryptographic Binding of Attestations scheme. For more information, also see Section 6.6.3.10.

HLRs

Index	Requirement specification
ACP_01	A Cryptographic Binding of Attestations scheme SHALL enable a WSCA/WSCD to prove that it manages two or more private keys, paired with two or more public keys provided to it by the Wallet Unit. *Notes: -These public keys may be included in WUAs, PIDs, attestations, or pseudonyms. - The proof may be transitive, so a proof that two keys are stored/managed in the same WSCA/WSCD may be done by proving these keys relate to each other via a third key (also stored in the WSCA/WSCD).*
ACP_02	A Cryptographic Binding of Attestations scheme SHALL rely solely on algorithms standardised by a standardisation organisation recognised by the Commission or in a standard recognised by the Commission.
ACP_03	A Cryptographic Binding of Attestations scheme SHOULD be implemented using a Zero-Knowledge Proof mechanism that satisfies the requirements specified in Topic 53.
ACP_04	A Cryptographic Binding of Attestations scheme SHALL be compatible with the requirements for attestation issuance in this document, in particular Topic 10, as well as with requirements for both remote and proximity presentation flows in this document, in particular Topic 1 and Topic 24.

Index	Requirement specification
ACP_05	A Cryptographic Binding of Attestations scheme SHALL enable an Attestation Provider, during the issuance of an attestation, to request and obtain proof that the private key for the new attestation is managed by the same WSCA/WSCD as the private key of a PID or another attestation already existing on the Wallet Unit. *Note: ACP_05 and ACP_06 may require an addition to the common OpenID4VCI protocol referenced in requirement ISSU_01, or an extension or profile thereof.*
ACP_06	A Cryptographic Binding of Attestations scheme SHALL enable a PID Provider or Attestation Provider, during the issuance of a PID or attestation, to request and obtain proof that the private key for the new PID or attestation is managed by the same WSCA/WSCD as the private key of the WUA received.
ACP_07	Before making a request according to ACP_05, an Attestation Provider SHALL verify that the new attestation indeed belongs to the User of the existing PID or attestation.

Also see requirements ARB_27 and ARB_28 in Topic 12.

A.2.3.19 Topic 19 - User navigation requirements (Dashboard logs for transparency)

Description

In this use case, the User is accessing a dashboard of the Wallet Unit, which provides a record of all transactions executed through the Wallet Unit. The User is concerned about data privacy, and thus the function of a dashboard ensures a higher degree of transparency, privacy and control of the User over their personal data.

This Topic lists high-level requirements related to the functions of such a dashboard.

HLRs

Index	**Requirement specification**
DASH_01	A Wallet Provider SHALL enable a User to access a user-friendly dashboard functionality in their Wallet Unit.
DASH_02	The Wallet Unit SHALL log all transactions executed through the Wallet Unit, including any transactions that were not completed successfully. This log SHALL include all types of transaction executed through the Wallet Unit: a) PID or attestation issuance and re-issuance transactions, b) PID or attestation presentation transactions, c) Wallet-to-Wallet transactions (see Topic 30), d) pseudonym registration or presentation transactions, e) signature or seal creation transactions (see Topic 16), f) data deletion requests sent to a Relying Party (see Topic 48), g) reports sent to a Data Protection Authority (see Topic 50), h) PID or attestation deletions by the User. *Note: For the data to be logged for a data deletion request to a Relying Party or a report sent to a DPA, see Topic 48 and Topic 50, respectively. For other types of transaction, the data to be logged is specified in the requirements in this Topic.*
DASH_02a	The Wallet Unit SHALL retain transactions in the log at least for the minimum retention period specified in applicable legislation. If the Wallet Unit must delete transactions from the log, for instance because of size limitations, the Wallet Unit SHALL notify the User via the dashboard before doing so, indicating the potential consequences for the User’s data protection rights, and SHALL instruct the User how to export the transactions that are about to be deleted; see DASH_07.

Index	Requirement specification
DASH_02b	The dashboard SHALL include a functionality to display to the User an overview of all transactions in the log.
DASH_02c	The transaction log meant in DASH_02 SHALL comply with all relevant requirement in Technical Specification 10, including measures to ensure and/or verify its confidentiality, integrity, and authenticity.

Index	Requirement specification
DASH_03	For a PID or attestation presentation transaction executed through the Wallet Unit, the log SHALL contain at least: a) the date and time of the transaction, b) the name and unique identifier of the corresponding Relying Party, and the Member State in which that Relying Party is established, c) the name, contact details (if available), and unique identifier of the intermediary, if an intermediary is involved in the transaction, d) the attestation type(s) and the identifier(s) of the attribute(s) that were requested, as well as those that were presented, e) in the case of non-completed transactions, the reason for such non-completion, f) the URL of the online service of the Relying Party's Registrar. *Note: if no intermediary is involved, this URL can be retrieved from the access certificate, see Reg_33. If an intermediary is involved, it can be retrieved from the registration certificate, if available (see RPRC_04a) or from the presentation request (see RPI_06).* g) the web form URL (if available), e-mail address (if available), and telephone number (if available) provided by the Relying Party for sending data deletion requests, see requirement RPRC_11 in Topic 44, h) the name and country of the Data Protection Authority supervising the Relying Party, as well as the web form URL (if available), e-mail address (if available), and telephone number (if available) provided by this DPA for reporting suspicious attribute presentation requests. i) information on the intended use and the URL to the applicable privacy policy (if available). *Note: The information in points g), h), and i) may be retrieved from the registration certificate or from the Registrar's online service (see Topic 44).*

Index	Requirement specification
DASH_03a	For a PID or attestation presentation transaction or a Wallet-to-Wallet transaction executed through the Wallet Unit, the log SHALL NOT contain the value of any attributes presented to the Relying Party or the Verifier Wallet Unit, or the value of any transactional data included in the presentation request.
DASH_03b	For a Wallet-to-Wallet transaction executed through the Wallet Unit, the log SHALL contain at least: a) the date and time of the transaction, b) the role of the Wallet Unit (Holder Wallet Unit or Verifier Wallet Unit), c) the attestation type(s) and the identifier(s) of the attribute(s) that were requested, as well as those that were presented, d) in the case of non-completed transactions, the reason for such non-completion.
DASH_03c	For a pseudonym registration or presentation transaction executed through the Wallet Unit, the log SHALL contain at least: a) the date and time of the transaction, b) identifying information about the Relying Party, if known to the Wallet Unit, c) whether it is a pseudonym registration or pseudonym presentation transaction, d) in the case of non-completed transactions, the reason for such non-completion. *Note: Regarding point b), see PA_20 in Topic 11.*
DASH_04	For a signature or seal creation transaction executed through the Wallet Unit, the log SHALL contain at least: a) the date and time of the transaction, b) the document or data signed or sealed (if available to the Wallet Unit), c) in the case of non-completed transactions, the reason for such non-completion.

Index	Requirement specification
DASH_05	For a PID or attestation issuance or re-issuance transaction executed through the Wallet Unit, the log SHALL contain at least: a) the date and time of the transaction, b) the name, contact details (if available), and unique identifier of the corresponding PID Provider or Attestation Provider, c) the attestation type requested, as well as the attestation type issued, d) the number of attestations requested and issued (i.e., the size of the batch in case of batch issuance). d) in the case of non-completed transactions, the reason for such non-completion. e) for a re-issuance transaction, whether it was triggered by the User or by the Wallet Unit without involvement of the User, f) the URL of the associated Registrar’s online service. *Note: this URL can be retrieved from the access certificate.*
DASH_05a	For the deletion of a PID or attestation by the User, the log SHALL contain at least: a) the date and time of the deletion event, b) the attestation type of the deleted PID or attestation. c) The name and unique identifier of the corresponding PID Provider or Attestation Provider. *Note: This requirement is not about deletion of transactions from the log, as per DASH_06a.*
DASH_06	The Wallet Provider SHALL ensure the confidentiality, integrity, and authenticity of all transactions included in the log.

Index	Requirement specification
DASH_06a	Via the dashboard, the Wallet Unit SHALL enable the User to delete any transaction in the log. Before deleting any transactions, the Wallet Unit SHALL indicate to the User the potential consequences for the User's data protection rights. *Note: This requirement applies even in case the minimum retention period specified in applicable legislation (see DASH_02a) is not yet over.*
DASH_06b	The Wallet Unit SHALL ensure that no entity other than the User can delete transactions from the log, except possibly for the reason mentioned in DASH_02a.
DASH_07	The dashboard SHALL allow the User to export the details of one or more transactions in the log to a file, using the common format specified according to DASH_02c, while ensuring their confidentiality, authenticity and integrity. The file SHALL be stored in an external storage or remote storage location of the User's choice, from among the storage options supported by the Wallet Unit and SHALL use the common format and security measures specified according to DASH_02c.
DASH_08	For a natural-person User, a Wallet Instance SHALL provide a User interface.
DASH_09	The User interface referred to in DASH_08 SHALL provide a view with - the EU Digital Identity Wallet Trust Mark, - accompanying general information on the certification of Wallet Solutions, - links to the certification status information as defined in the Technical Specification 1.

Index	Requirement specification
DASH_09a	Positioning of the view meant in DASH_09 in the Wallet UI navigation SHALL follow design guidelines provided by the European Commission.
DASH_09b	Wallet Providers and Wallet Units SHALL comply with all relevant requirements in Technical Specification 1 for the EUDI Wallet Trust Mark.
DASH_10	Empty. *Note: See requirement WIAM_12a in Topic 40.*
DASH_11	A Wallet Unit issued to a legal person SHALL allow the legal person to interact with the Wallet Unit in the appropriate interface provided by the Wallet Provider.
DASH_12	The User interface referred to in DASH_08 SHALL enable the User, for each presentation transaction in the log, to easily request the Relying Party to delete any or all attributes presented to it in that transaction, or to send a report about that particular transaction to a DPA.

A.2.3.20 Topic 20 - Strong User authentication for electronic payments

Description

Note: The description in this section was adapted from the Discussion Paper for Topic W. The high-level requirements in the next section were taken from this paper as well.

The [European Digital Identity Regulation] requires Wallet Units to provide a functionality of strong User authentication (SUA), among others in the context of payments.

For more information, please refer to Section 2.6.4 of the ARF main document.

HLRs

Index	Requirement specification
SUA_01	The Wallet Units SHALL be able to process the transactional data included in a presentation request for that an attestation, according to all requirements in the associated Attestation Rulebook.
SUA_02	The Attestation Rulebook (see Topic 12 of a SUA attestation SHALL specify the syntax and semantics of the transactional data associated with that attestation, as well as all necessary requirements for Wallet Units to process that transactional data, at least regarding a) displaying the data to the User when obtaining consent for signing the data, b) processing (e.g., hashing) the data for inclusion in the device binding signature, and c) the scope of information to be logged about a SUA attestation presentation transaction by a Wallet Unit.
SUA_03	The Attestation Provider of a SUA attestation SHALL NOT issue such an attestation to a Wallet Unit that does not comply with all relevant requirements in the Attestation Rulebook for that attestation.
SUA_04	In the response to a presentation request that includes transactional data, a Wallet Unit SHALL include (a representation of) that data, according to requirements included in the Attestation Rulebook or in information provided to the Wallet Unit in the presentation request. In the latter case, the rules to interpret such information SHALL be included in the Attestation Rulebook. *Note: This requirement, as well as SUA_05, only applies if the requested SUA attestation is present on the Wallet Unit and if the User consents to signing the transactional data and presenting the requested attributes.*

Index	Requirement specification
SUA_05	The Wallet Unit SHALL include (a representation of) the transactional data received in a presentation request in the signature creation process used for device binding, using the private key of the requested SUA attestation, using the mechanisms provided for key binding in [SD-JWT-VC] and mdoc authentication in [ISO/IEC 18013-5], and complying with the applicable requirements in the Attestation Rulebook, see SUA_02. *Notes: - The resulting signature value constitutes a proof of transaction and fulfils the requirement of the authentication code required in [PSD2]. - See also requirement OIA_02 in Topic 1.*
SUA_06	The Wallet Unit SHALL be able to adapt the dialogue message(s) displayed to the User (like font size and colour, background colour, text position, labels in the buttons to ‘approve’ or ‘reject’ a transaction), according to requirements in an Attestation Rulebook or in information provided to the Wallet Unit in the presentation request. In the latter case, the rules to interpret such information SHALL be included in the Attestation Rulebook.

A.2.3.21 Topic 21 - Diplomas within the EUDI Wallet ecosystem

There are no HLRs for this Topic.

A.2.3.22 Topic 22 - Digital Travel Credentials within the EUDI Wallet ecosystem

There are no HLRs for this Topic.

A.2.3.23 Topic 23 - PID issuance and (Q)EAA issuance

Description

See Topic 10.

HLRs

See Topic 10.

A.2.3.24 Topic 24 - User identification in proximity scenarios

Description

In this use case, the User is using their Wallet Unit for identification purposes in proximity scenarios. As explained in Section 4.4.2 of the ARF main document, in a proximity flow, the User and their Wallet Instance are physically near the Relying Part Instance. PIDs and attestations are exchanged using proximity technology (e.g., NFC, Bluetooth) between the Wallet Unit and the Relying Party Instance. Note that this definition does not imply that a Wallet Unit and a Relying Party have to use proximity technologies if they are close together. They are free to use a remote flow (according to Topic 1). However, there may be situations where either the Wallet Unit or the Relying Party Instance does not have an internet connection. In such cases, they must be able to use a proximity flow, if they are close together.

The User is concerned about sharing personal data in proximity, while the User's objectives include identifying themselves to services requiring User identification and maintaining control over their personal data sharing.

This topic lists high-level requirements related to User identification in proximity use cases where Users utilise their Wallet Units.

HLRs

Index	Requirement specification
ProxId_01	To enable identification using proximity flows, Wallet Units SHALL support device retrieval as specified in ISO/IEC 18013-5 for presenting PID or attestation attributes. Wallet Units SHALL comply with the requirements for mDLs and mdocs ISO/IEC 18013-5. *Note: Nominally, ISO/IEC 18013-5 is intended only for mDLs and mDL readers. The corresponding standard for mobile documents in general (including Wallet Units with the EUDI Wallet ecosystem) will be ISO/IEC 23220-4, which is based on ISO/IEC 18013-5. However, the latter standard is not finished yet and therefore cannot be referenced at the moment. To guarantee interoperability between Wallet Units and Relying Party Instances in proximity scenarios, it is necessary to make choices from among the possibilities specified in ISO/IEC 18013-5. Making the same choices as for mDLs ensure this.*
ProxId_01a	If a Relying Party supports using proximity flows, its Relying Party Instances SHALL support device retrieval as specified in ISO/IEC 18013-5 for requesting PID or attestation attributes. Such Relying Party Instances SHALL comply with the requirements for mDL readers and mdoc readers in ISO/IEC 18013-5. *Note: See note to ProxId_01. Support for proximity flows by Relying Parties is not mandatory.*

Index	Requirement specification
ProxId_02	Wallet Units, PID Providers, Attestation Providers, Wallet Providers, and Relying Parties SHALL NOT support server retrieval as specified in ISO/IEC 18013-5 for requesting and presenting PID or attestation attributes. *Note: Using server retrieval, a Relying Party would request User attributes directly from a PID Provider or Attestation Provider, after having received an authentication and/or authorisation token from the User's Wallet Unit.*
ProxId_03	A Wallet Unit SHALL present the presentation request and the identity of the Relying Party to the User when processing the request.
ProxId_04	A Wallet Unit SHALL request its User to approve the presentation of attributes from their Wallet Unit for proximity identification before presenting them to the Relying Party.
ProxId_05	A Wallet Unit SHALL transmit the requested User attributes to the requesting Relying Party Instance securely in accordance with ISO/IEC 18013-5 for proximity flows.
ProxId_06	Empty

A.2.3.25 Topic 25 - Unified definition and controlled vocabularies for attributes (Catalogue of attributes)

Description

See Section 5.5 for a description of the catalogue of attributes and the distinction between this catalogue and the catalogue of attestation schemes discussed in Topic 26.

CIR 2025/1569 contains requirements for the catalogue of attributes, especially in Article 7. These requirements are not repeated in this Topic.

HLRs

Index	Requirement specification
CAT_01	Empty
CAT_01a	Empty
CAT_01b	Empty
CAT_02	Empty
CAT_03	Empty
CAT_03b	Empty
CAT_04	A request to include or to modify an attribute in the catalogue of attributes SHALL indicate how a QTSP can use the verification point for that attribute. *Note: this could be, for instance, in the form of (a reference to) an endpoint description text.*

A.2.3.26 Topic 26 - Catalogue of attestation schemes

Description

See Section 5.5 in the ARF main document for a description of the catalogue of attestation schemes and the distinction between this catalogue and the catalogue of attributes discussed in Topic 25. [Section 5.5] also discusses the relationship between an attestation scheme and the corresponding Rulebook.

CIR 2025/1569 contains requirements for the catalogue of attestation schemes, especially in Article 8. These requirements are not repeated in this Topic.

HLRs

Index	Requirement specification
CAT_05	Empty
CAT_05a	Empty

Index	Requirement specification
CAT_05b	Empty
CAT_06	Empty
CAT_07	Empty
CAT_08	Empty
CAT_09	Empty
CAT_10	Empty
CAT_11	Empty

A.2.3.27 Topic 27 - Registration of PID Providers, Providers of QEAAs, PuB-EAAs, and non-qualified EAAs, and Relying Parties

Description

PID Providers, QEAA Providers, PuB-EAA Providers, non-qualified EAA Providers, and Relying Parties register with a Registrar in their Member State. The main goal of the registration process is for the Registrar to register relevant information about the registering entity, and make this information available online to interested parties.

In addition, a registering Relying Party will receive an access certificate for each of the Relying Party Instances it uses to interact with Wallet Units to request the presentation of attestations. The Relying Party Instance can communicate to a Wallet Units in order to be authenticated by the Wallet Unit. Similarly, a QEAA Provider, PuB-EAA Provider, or non-qualified EAA Providers will receive an access certificate for each of the service supply point(s) it uses to interact with Wallet Units to issue attestations.

Finally, the registering entity will receive one or more registration certificates containing the registered information, if the Registrar has a policy of issuing such registration certificates. For requirements regarding the issuance and use of registration certificate, please refer to Topic 44.

This Topic specifies high-level requirements related to the registration of the above mentioned entities.

HLRs

A. *General requirements for Member State registration processes*

Index	Requirement specification
Reg_01	Member States SHALL provide processes and mechanisms for PID Providers, QEAA Providers, PuB-EAA Providers, non-qualified EAA Providers, and Relying Parties to register in a registry. *Note: Member States may choose to implement a single registry for all these roles, or a separate registry for each of these roles.*
Reg_01a	Member States SHALL register a common set of data about a) PID Providers, b) QEAA Providers, c) PuB-EAA Providers, d) non-qualified EAA Providers. and e) Relying Parties, according to the relevant requirements in Technical Specification 6. *Note: For PID Providers, QEAA Providers, PuB-EAA Providers, and non-qualified EAA Providers, the common set of data specified in [Technical Specification 6] include the attestation type(s) that the provider intends to issue to Wallet Units.*
Reg_01b	Empty
Reg_02	Member States SHALL make publicly available all necessary details and documentation about the registration processes for their registry.
Reg_03	Member States SHALL publish the registry entries online, in a sealed or signed machine-readable common format suitable for automated processing, according to the relevant requirements in Technical Specification 5, for the purpose of transparency to Users and other stakeholders.

Index	Requirement specification
Reg_04	Member States SHALL make the registry entries available online, in a human-readable format. The website used for this purpose SHALL use a secure channel protecting the authenticity and integrity of the information in the registry during transport. Member States SHALL NOT require authentication or prior registration and authorisation of any person wishing to retrieve the information in the registry.
Reg_05	Empty
Reg_06	Member States SHALL support the common API specified in Technical Specification 5 for to enable automated retrieval of registry entries from the Member States' registries. *Note: [Technical Specification 5] specifies the use of a secure channel protecting the authenticity and integrity of the information in the registry during transport, and does not require authentication or prior registration and authorisation of any entity wishing to retrieve the information in the registry.*
Reg_07	A Member State SHALL enable a registered PID Provider, QEAA Provider, PuB-EAA Provider, non-qualified EAA Provider, or Relying Party to update the information registered on it, using a process comparable to the original registration process. For Relying Parties, this SHALL be possible using the API or user interface mentioned in Reg_24.
Reg_08	A registered PID Provider, QEAA Provider, PuB-EAA Provider, non-qualified EAA Provider, or Relying Party SHALL make any updates necessary to ensure the continued correctness of the registered information without undue delay.

Index	Requirement specification
Reg_09	Member States SHALL log all changes made on the information registered regarding a PID Provider, QEAA Provider, PuB-EAA Provider, non-qualified EAA Provider, or Relying Party, including at least initial registration, updates, deletion of information, and suspension or cancellation.

B. *General requirements for the issuance of access certificates*

Index	Requirement specification
Reg_10	A Member State SHALL ensure that an Access Certificate Authority notified according to [Topic 31] issues an access certificate to all PID Providers, QEAA Providers, PuB-EAA Providers, non-qualified EAA Providers, and Relying Parties registered in one of the Member State's registries.
Reg_11	A Member State SHALL ensure that the issuance process of access certificates by their notified Access Certificate Authority(s) complies with a common Certificate Policy for Access Certificate Authority.
Reg_12	The Commission SHALL provide technical specifications establishing the common Access Certificate Authority Certificate Policy mentioned in Reg_11.
Reg_13	The common Certificate Policy mentioned in Reg_12 SHALL require that an Access Certificate Authority logs all issued certificates for Certificate Transparency (CT). *Note: This requirement is still under discussion and might be changed or removed in a future version of this ARF.*

Index	Requirement specification
Reg_14	The common Certificate Policy mentioned in Reg_12 SHALL require that an Access Certificate Authority provides one or more method(s) to revoke the access certificates it issued.
Reg_15	The common Certificate Policy mentioned in Reg_12 SHALL include a policy for revocation, which SHALL require that an Access Certificate Authority revokes an access certificate at least when: - the certificate subject which is a Relying Party is suspended or cancelled by the respective Registrar, - the certificate subject which is a PID Provider, QEAA Provider, PuB-EAA Provider, or non-qualified EAA Provider is suspended or cancelled by the respective Registrar, - on request of the certificate subject, or - on request of a competent national authority.
Reg_16	The common Certificate Policy mentioned in Reg_12 SHALL specify the profile of access certificates in detail.
Reg_17	Empty
Reg_18	The common Certificate Policy mentioned in Reg_12 SHALL define the minimum change history information to be stored for resolving possible disputes regarding registration.

C. *Requirements for the registration of PID Providers*

Index	Requirement specification
Reg_19	A Member State SHALL approve a PID Provider according to a well-defined policy before including it in its PID Provider Registry. To that end, a Member State SHALL define specific vetting processes and rules of acceptance for inclusion of PID Providers in its Registry.
Reg_20	A Member State SHALL identify PID Providers at a level of confidence proportionate to the risk arising from the potential harm a fraudulent PID Provider could cause to Users and other stakeholders in the EUDI Wallet ecosystem.
Reg_20a	A Registrar SHALL provide a method to suspend or cancel a registered PID Provider.
Reg_20b	A Registrar SHALL have a policy for the suspension or cancellation of a registered PID Provider, which SHALL specify that a PID Provider is suspended or cancelled at least on request of the PID Provider or of a competent national authority.

D. *Requirements for the registration of Attestation Providers*

Index	Requirement specification
Reg_21	A Member State SHALL approve an Attestation Provider according to a well-defined policy before including it in its Attestation Provider Registry. To that end, a Member State SHALL define specific vetting processes and rules of acceptance for inclusion of Attestation Providers in its Registry. These processes and rules SHOULD consider any relevant differences between QEAA Providers, PuB-EAA Providers, and non-qualified EAA Providers.

Index	Requirement specification
Reg_22	A Member State SHALL identify Attestation Providers (i.e., QEAA Providers, PuB-EAA Providers and non-qualified EAA Providers) at a level of confidence proportionate to the risk arising from the potential harm a fraudulent Attestation Provider could cause to Users and other stakeholders in the EUDI Wallet ecosystem.
Reg_22a	A Registrar SHALL provide a method to suspend or cancel a registered Attestation Provider.
Reg_22b	A Registrar SHALL have a policy for the suspension or cancellation of a registered Attestation Provider, which SHALL specify that an Attestation Provider is suspended or cancelled at least on request of the Attestation Provider or of a competent national authority.

E. *Requirements for the registration of Relying Parties*

Index	Requirement specification
Reg_23	Empty
Reg_24	A Member State SHALL enable a Relying Party to register remotely, using an API or user interface.
Reg_25	A Member State SHALL identify a Relying Party at a level of confidence proportionate to the risk arising from the potential harm a fraudulent Relying Party could cause to Users and other stakeholders in the EUDI Wallet ecosystem.
Reg_26	With respect to Reg_25, a Member State SHALL consider whether a registering entity intends to act as an intermediary. *Note: According to the [European Digital Identity Regulation], an intermediary is a Relying Party.*
Reg_27	Empty

Index	Requirement specification
Reg_28	Empty
Reg_29	A Member State SHALL have a policy for the cancellation of a registered Relying Party, which SHALL specify that a Relying Party is cancelled at least on request of the Relying Party or of a competent national authority.
Reg_30	Empty

F. *Requirements for the contents of access certificates*

Index	Requirement specification
Reg_31	The common Certificate Policy mentioned in Reg_12 SHALL require that an access certificate contains a name for the PID Provider, QEAA Provider, PuB-EAA Provider, non-qualified EAA Provider, or Relying Party, in a format suitable for presenting to a User.
Reg_32	The common Certificate Policy mentioned in Reg_12 SHALL require that an access certificate contains an EU-wide unique identifier for the PID Provider, QEAA Provider, PuB-EAA Provider, non-qualified EAA Provider, or Relying Party, and SHALL specify a method for deriving such identifiers. *Notes: - The EU-wide unique identifier could, for example, be a composition of a unique identifier of the Registrar, defined in the policy, and a unique identifier for the Relying Party allocated by this Registrar. - This Relying Party identifier is identical in all access certificates issued to a given entity.*

Index	Requirement specification
Reg_33	The common Certificate Policy mentioned in Reg_12 SHALL require that an access certificate contains the URL of the online service of the Member State Registrar, which Wallet Units and other parties can use to obtain the information registered about the PID Provider, QEAA Provider, PuB-EAA Provider, non-qualified EAA Provider, or Relying Party.

A.2.3.28 Topic 28 - Wallet Unit for legal persons

Note to this Topic: Legal-person PIDs and Wallet Units for legal persons were added to the list of topics to be discussed with Member States in the future.

Description

This topic is focused on identifying high-level requirements for a legal-person Wallet Unit. All core capabilities of a Wallet Unit for a natural person are available for a legal person. There are some differences between a natural and legal person that accordingly leads to different requirements for issuing legal-person PIDs and the Wallet Units containing legal-person PIDs.

Notes:

- A legal-person PID is issued under an eID scheme.
- A legal-person PID is described in a legal-person PID Rulebook, which is different from the natural-person PID Rulebook in [PID Rulebook]. A legal-person PID has a different attestation type than a natural-person PID, and also contains different attributes. For example, date of birth or age are not relevant information for legal persons. Specifying a different Rulebook for legal-person PIDs allows Relying Parties and other Wallet Units to request these attributes.

- A legal-person Wallet Solution may be implemented in the same manner as a natural-person Wallet Solution, meaning chiefly that it is implemented on a mobile device operated by a single User, who is a natural person. However, a legal-person Wallet Solution may also be implemented as a server-based (web-based) application. In the latter case, a Wallet Unit can be used either by one or more natural persons appointed by the legal person, or by information systems of the legal persons that give an Wallet Unit commands in accordance with rules defined by the legal person.

HLRs

Index	Requirement specification
LP_01	The Commission SHALL develop a Legal-person PID Rulebook to specify the attestation scheme and other technical details applicable for legal-person PIDs.
LP_02	The attestation type of a legal-person PID SHALL be different from the attestation type of a natural person PID. *Note: See [Topic 12] for an explanation of the concept of attestation type.*
LP_03	A legal-person PID SHALL comply with all requirements in the Legal-person PID Rulebook mentioned in LP_02.

A.2.3.29 Topic 29 - Representation paradigm

Description

Note: The description of this Topic, as well as the High-Level Requirements in it, were developed in the Discussion Paper for Topic I. Please see that paper for more information.

Based on the [European Digital Identity Regulation], it should be possible to issue a dedicated representation attestation for a natural person to a representative, in accordance with applicable national and European legislation. For certain use cases (e.g., parent-child relationships), the Attestation Provider of such attestations will be able to retrieve the relevant information from authentic sources at the national level. In other cases (e.g., power of attorney), the represented natural person may be required to explicitly authorize the representative.

Representation attestations for a natural person issued to a representative have a distinct attestation type. The Attestation Rulebook describing this attestation type shall specify the nature of the representation and shall clearly define the operations that the representative is authorized to perform, thereby restricting the scope of their authority.

Furthermore, this representation attestation type (like any other attestation type, see Topic 7) is either short-lived or revocable. In the case of revocable attestations, all entities that, according to applicable law, are entitled to revoke them have the capability to request the Attestation Provider to do so. It is emphasized that the high-level requirements concerning attestation revocation, as defined in Topic 7, also apply to this attestation type.

A User holding a representation attestation is able to represent another natural person when interacting with a Relying Party. The Relying Party is always aware that it is interacting with a legal representative or agent. This is ensured by the fact that the corresponding Wallet Unit presents an attestation having a distinct type, specifically for representation attestations.

HLRs

Index	Requirement specification
RP_01	The Commission SHALL create an Attestation Rulebook for representation attestations issued to a natural person representing another natural person. The Rulebook SHALL specify the unique attestation type of these representation attestations. The Rulebook SHALL also specify attributes used for defining a validity period, the nature of the representation, and the operations the representative is authorised to perform, thereby limiting the scope of its authorisation.
RP_02	An Attestation Provider issuing representation attestations to a natural person representing another natural person SHALL ensure that either the attestations are short-lived or that all entities which, according to applicable law, must have the ability to request revocation of such attestations, are able to do so.

A.2.3.30 Topic 30 - Interaction between Wallet Units

Description

A User can request another User to present an attestation, where both Users use their Wallet Unit. This can be done only when their devices are close together (that is, in physical proximity). In this context, the requesting Wallet Unit is called the Verifier Wallet Unit, and the presenting Wallet Unit is called the Holder Wallet Unit. The User of a Holder Wallet Unit is called a Holder, and the User of a Verifier Wallet Unit is called a Verifier.

This Topic lists the high-level requirements related to the interaction between two Wallet Units. These are based on the Discussion Paper for Topic J and on subsequent discussions in the context of Technical Specification 9. For a generic discussion of this topic, please refer to Section 6.4 of the ARF main document.

HLRs

Index	Requirement specification
W2W_01	A Wallet Unit SHALL be able to act as a Holder Wallet Unit, in accordance with all requirements in this Topic.
W2W_02	When acting as a Holder Wallet Unit, if there is a contradiction between a requirement for Holder Wallet Units in this Topic and any requirement for Wallet Units in other Topics in this document, the requirement in this Topic SHALL take precedence. However, when acting as a Holder Wallet Unit, a Wallet Unit SHALL comply with all requirements for Wallet Units in other Topics in this document that do not contradict any requirement in this Topic.
W2W_03	A Wallet Unit SHALL be able to act as a Verifier Wallet Unit, in accordance with all requirements in this Topic.
W2W_04	When acting as a Verifier Wallet Unit, a Wallet Unit SHALL NOT comply with any requirement for Wallet Units in other Topics in this document.

Index	Requirement specification
W2W_05	A Wallet Unit SHALL act as a Holder Wallet Unit only if the User selects a ‘Holder Wallet Unit mode’. If the User closes the Wallet Unit, or after a period of non-activity, the Wallet Unit SHALL return to ‘normal’ mode.
W2W_06	When entering the Holder Wallet Unit mode, a Wallet Unit SHALL inform its User that this mode should only be used for interactions with natural persons using a Wallet Unit, and that the User should not proceed if they are in fact interacting with a Relying Party.
W2W_07	A Wallet Unit SHALL act as a Verifier Wallet Unit only if the User selects a ‘Verifier Wallet Unit mode’. If the User closes the Wallet Unit, or after a period of non-activity, the Wallet Unit SHALL return to ‘normal’ mode.
W2W_08	A Verifier Wallet Unit and a Holder Wallet Unit SHALL support attestation presentation only in proximity, meaning they SHALL support only [ISO/IEC 18013-5] to communicate.
W2W_09	Holder Wallet Units SHALL comply with the requirements for mDLs and for mdocs in ISO/IEC 18013-5, unless specified differently in Technical Specification 9.
W2W_10	Verifier Wallet Units SHALL comply with the requirements for mDL readers and for mdoc readers in ISO/IEC 18013-5, unless specified differently in Technical Specification 9.

Index	Requirement specification
W2W_11	A Holder Wallet Unit SHOULD provide the Holder, through a user-friendly UI, with the option to inform the Verifier Wallet Unit about the attributes which the Verifier should include in the presentation request, by sending a presentation offer. If the Holder creates a presentation offer, the Holder Wallet Unit SHALL transfer it to the Verifier Wallet Unit as specified in Technical Specification 9. *Note: This will use an extension of the device engagement structure specified in ISO/IEC 18013-5.*
W2W_12	A Holder Wallet Unit SHALL recommend the Holder to create a presentation offer, as this will increase the chance of success of the use case.
W2W_13	A Verifier Wallet Unit SHALL provide the Verifier, through a user-friendly UI, with the possibility to select the attributes that will be included in the presentation request.
W2W_14	For the purposes of W2W_07, if the Verifier Wallet Unit received a presentation offer, it SHALL present this offer to the Verifier, and enable the Verifier to include one or more of the attributes in the offer into the presentation request. However, the Verifier Wallet Unit SHALL NOT allow the Verifier to include any attribute not present in the offer.
W2W_15	For the purposes of W2W_07, if the Verifier Wallet Unit did not receive a presentation offer, it SHALL present the Verifier with a list of attributes that can be included in the presentation request. The Verifier Wallet Unit MAY ask the Verifier some questions about the purpose of the use case to narrow down the list.

Index	Requirement specification
W2W_16	A Verifier Wallet Unit SHALL authenticate the Verifier according to WIAM_15 and SHALL obtain the User’s approval prior to sending a presentation request to a Holder Wallet Unit.
W2W_17	A Verifier Wallet Unit SHALL implement measures to limit the number of presentation requests it can send per unit of time, to prevent abuse of the Wallet-to-Wallet functionality by Relying Parties. The limitation strategy, for instance exponential backoff time between subsequent presentation requests or hard limits for the number of requests, SHALL be decided by the Wallet Provider, based on applicable requirements in Technical Specification 9.
W2W_18	When receiving a presentation request, a Holder Wallet Unit SHOULD verify the validity of the Verifier Wallet Unit before presenting a received request to the Holder, provided Technical Specification 9 specifies a suitable mechanism for doing so.
W2W_19	When receiving a presentation response, a Verifier Wallet SHALL verify the received attestation according to requirements OIA_12 - OIA_15 in Topic 1.
W2W_20	A Verifier Wallet Unit SHALL display all verified attributes to the Verifier.
W2W_21	A Verifier Wallet Unit SHALL NOT persistently store any attestations or attributes received. A Verifier Wallet Unit SHOULD minimize the time the received presentation is stored in memory. A Verifier Wallet Unit SHALL comply with OIA_16 in Topic 1.
W2W_22	Wallet Providers SHOULD take measures to prevent a User from taking screenshots while their Wallet Unit is acting as a Verifier Wallet Unit.

A.2.3.31 Topic 31 - Notification and publication of PID Provider, Wallet Provider, Attestation Provider, Access Certificate Authority, and Provider of registration certificates

Description

PID Providers, PuB-EAA Providers, Wallet Providers, Access Certificate Authorities, and Providers of registration certificates must be notified by a Member State to the Commission. As part of the notification process, the trust anchors of these parties must be included in a Trusted List. A trust anchor is the combination of a public key and an identifier for the associated entity. Trust anchors are required for the verification of the signatures of PIDs, attestations, WUAs, access certificates and registration certificates that are issued by these parties.

Note: Notification does not apply to QEAA Providers and (non-qualified) EAA Providers, as explained in Sections D and F below, respectively.

This Topic contains High-Level Requirements for the notification of these parties by Member States, and for the publication of the notified information by the Commission.

HLRs

A. Generic requirements for notification

Index	Requirement specification
GenNot_01	Member States SHALL notify all PID Providers, PuB-EAA Providers, Wallet Providers, Access Certificate Authorities, and Providers of registration certificates to the European Commission, according all relevant requirements in Technical Specification 2.

Index	Requirement specification
GenNot_02	As part of [Technical Specification 2] referred to in GenNot_01, the European Commission SHALL establish standard operating procedures for the notification of a PID Provider, PuB-EAA Provider, Wallet Provider, Access Certificate Authority, or Provider of registration certificates to the Commission. *Note: The outcome of the notification procedure is the publication of the information notified by the Member State according to Article 5a (18) in a machine and human readable manner using the common system mentioned in Section H, TLPub_01.*
GenNot_03	The common system mentioned in GenNot_01 SHALL enable: - A secure notification channel between Member States and the Commission for all notifications. - A notification, verification, and publication process and associated validation steps (with follow-up and monitoring) at the Commission side. - Collected data to be processed, consolidated, signed or sealed, and published in both a machine-processable Trusted List and in a human-readable format, manually and/or automatically using e.g. a web service and/or API.
GenNot_04	As regard to GenNot_03, second bullet, the Commission SHALL verify whether the notified data is complete and meets the technical specifications, while the Member States SHALL be responsible for the correctness of the notified information.

Index	Requirement specification
GenNot_05	As part of the specifications referred to in GenNot_01, the European Commission SHALL establish standard operating procedures for the suspension or cancellation of a PID Provider, PuB-EAA Provider, Wallet Provider, Access Certificate Authority, or Provider of registration certificates. These operating procedures SHALL include unambiguous conditions for suspension or cancellation. As an outcome of the suspension or cancellation procedure, the status of the suspended or cancelled PID Provider, PuB-EAA Provider, Wallet Provider, Access Certificate Authority or Provider of registration certificates in the Trusted List SHALL be changed to Invalid.

B. Requirements for the notification of PID Providers

Index	Requirement specification
PPNot_01	The European Commission SHALL establish technical specifications for the common set of information to be notified about PID Providers.

Index	Requirement specification
PPNot_02	The common set of information to be notified about a PID Provider SHALL include at least: 1. Identification data: i. MS/Country of establishment, ii. Name as registered in an official record, iii. Where applicable: a. A business registration number from an official record, b. Identification data from that official record. 2. PID Provider trust anchors, i.e., public keys and name as per point 1) ii) above, supporting the authentication of PIDs issued by the PID Provider, 3. Trust anchors of Access Certificate Authorities for PID Providers, i.e., public keys and CA name, supporting the authentication of the PID Provider by Wallet Units at the service supply point(s) listed per point 4. below. 4. Service supply point(s), i.e., the URL(s) at which a Wallet Unit can start the process of requesting and obtaining a PID. *Notes: - Relating to point 3. above: PID Provider Access Certificate Authority trust anchors are notified separately from the Access Certificate Authority for Relying Parties (see Section G below), since PID Providers are -legally speaking- not Relying Parties. - For the concept of an Access Certificate Authority, see also [Topic 27] and Section 6.3.2 of the ARF main document.*
PPNot_03	PID Providers SHALL ensure that all PIDs they issue can be authenticated using the PID Provider trust anchors notified to the Commission.
PPNot_04	PID Providers SHALL ensure that their PID Provider access certificates can be authenticated using the applicable Access Certificate Authority trust anchors notified to the Commission. *Note: [Topic 6] describes how access certificates will be used.*

Index	Requirement specification
PPNot_05	PID Provider trust anchors SHALL be accepted because of their secure notification by the Member States to the Commission and by their publication in the corresponding Commission-compiled PID Provider Trusted List which is sealed by the Commission.
PPNot_06	Access Certificate Authority trust anchors SHALL be accepted because of their secure notification by the Member States to the Commission and by their publication in the corresponding Commission-compiled Access Certificate Authority Trusted List which is signed or sealed by the Commission.
PPNot_07	The format of the PID Provider Trusted List SHALL comply with ETSI TS 119 612 v2.1.1 or with a suitable profile similarly derived from ETSI TS 102 231.

C. Requirements for the notification of Wallet Providers

Index	Requirement specification
WPNot_01	The European Commission SHALL establish technical specifications for the common set of information to be notified about Wallet Providers.

Index	Requirement specification
WPNot_02	The common set of information to be notified about a Wallet Provider SHALL include: 1. Identification data: i. MS/Country of establishment, ii. Name as registered in an official record, iii. Where applicable: a. Business registration number from an official record, and b. Identification data from the official record. 2. Wallet Provider trust anchors, i.e., public keys and name as per point 1. b. above, supporting the authentication of Wallet Unit Attestations issued by the Wallet Provider. *Notes: - See [Topic 9] and [Topic 38] for the definition of the WUA. - A Wallet Provider does not need an access certificate to interact with Wallet Units.*
WPNot_03	Wallet Providers SHALL ensure that all WUAs they issue can be authenticated using the trust anchors notified to the Commission.
WPNot_04	Wallet Provider trust anchors SHALL be accepted because of their secure notification by the Member States to the Commission and by their publication in the corresponding Commission-compiled Wallet Provider Trusted List which is sealed by the Commission.
WPNot_05	The format of the Wallet Provider Trusted List SHALL comply with ETSI TS 119 612 v2.1.1 or with a suitable profile similarly derived from ETSI TS 102 231.
WPNot_06	If a Wallet Provider is cancelled (see requirement GenNot_05 above), that Wallet Provider SHALL immediately revoke all of its valid WUAs, in accordance with the requirements in Topic 38. If a Wallet Provider is suspended, that Wallet Provider and the Member State SHALL agree on the necessary precautionary measures that need to be taken, which MAY include the immediate revocation of all or some of its valid WUAs.

D. Requirements for the notification of QEAA Providers

There is no notification of QEAA Provider foreseen by the [European Digital Identity Regulation], except for establishing the Art. 22 Trusted List once a qualified status is granted. QTSPs issuing QEAAs to Wallet Units SHALL abide by the Implementing Act to be adopted under Art. 45d(5).

E. Requirements for the notification of PuB-EAA Providers

This notification is pursuant to Art.45f(3) and to the implementing acts to be adopted pursuant to Art.45f(7). It should be noted that the purpose of this notification is mainly to the attention of QTSPs issuing qualified certificates for electronic signatures or seals to those public sector bodies referred to in Article 3, point (46), and identified as the issuer in the PuB-EAA. The Trusted List compiled by the Commission is deemed to be a constitutive list of such Art.3(46) bodies recognised for issuing PUB-EAAs. Consequently, QTSPs are expected to verify such lists prior to issuing a qualified certificate to any entity claiming to be a Art.3(46) body.

Index	**Requirement specification**
PuBPNot_01	The European Commission SHALL establish technical specifications for the common set of information to be notified about PuB-EAA Providers.

Index	Requirement specification
PuBPNot_02	The common set of information to be notified by Member States about PuB-EAA Providers SHALL include at least: 1. Identification data: i. MS/Country of establishment, ii. Name as registered in an official record, iii. Where applicable: a. Registration number as in official record, and b. Official record identification data. iv. Identification data of the Union or national law under which a. Either the PuB-EAA Provider is established as the responsible body for the Authentic Source based on which the electronic attestation of attributes is issued, or b. The PuB-EAA Provider is the body designated to act on behalf of the responsible body referred to in point 1. iv. a. v.The conformity assessment report issued by a conformity assessment body, confirming that the requirements set out in paragraphs 1, 2 and 6 of Article 45f are met. 2. Service supply point(s), i.e., the URL(s) at which a Wallet Unit can start the process of requesting and obtaining a PuB-EAA from the PuB-EAA Provider.
PuBPNot_03	The format of the PuB-EAA Provider Trusted List SHALL comply with ETSI TS 119 612 v2.1.1 or with a suitable profile similarly derived from ETSI TS 102 231.

F. Requirements for the notification of non-qualified EAA Providers

There is no notification of non-qualified EAA Providers foreseen by the [European Digital Identity Regulation]. As stated in [Topic 12], the Schema Provider for an Attestation Rulebook describing a type of attestation that is an EAA defines in the Rulebook the mechanisms allowing a Relying Party to obtain, in a trustworthy manner, the trust anchor(s) of EAA Providers issuing this type of EAA.

G. Requirements for the notification of Access Certificate Authorities and Providers of registration certificates

Access Certificate Authorities (CA) are responsible for signing access certificates they issue to PID Providers, QEAA Providers, PuB-EAA Providers, and non-qualified EAA Providers, as well as to Relying Parties. For more information about Access Certificate Authorities, see [Topic 27].

Providers of registration certificates are responsible for signing registration certificates they issue to PID Providers, QEAA Providers, PuB-EAA Providers, and non-qualified EAA Providers, as well as to Relying Parties. For more information about Access Certificate Authorities, see [Topic 44].

Index	**Requirement specification**
RPACANot_01	The European Commission SHALL establish technical specifications for the common set of information to be notified about Access Certificate Authorities and Providers of registration certificates.
RPACANot_02	The common set of information to be notified about an Access Certificate Authority or a Provider of registration certificates SHALL include: 1. Identification data: i) Member State or country of establishment, ii) Name as registered in an official record, iii) Where applicable: - A business registration number from an official record, - Identification data from that official record. 2. Trust anchors of the Access Certificate Authority or Provider of registration certificates, i.e., public keys and name as per point 1) ii), supporting the authentication of Relying Parties, PID Providers, QEAA Providers, PuB-EAA Providers, and non-qualified EAA Providers by Wallet Units.
RPACANot_03	Relying Parties, PID Providers, QEAA Providers, PuB-EAA Providers, and non-qualified EAA Providers SHALL ensure that their access certificates can be authenticated using the trust anchors of an Access Certificate Authority notified to the Commission.

Index	Requirement specification
RPACANot_03a	Relying Parties, PID Providers, QEAA Providers, PuB-EAA Providers, and non-qualified EAA Providers SHALL ensure that their registration certificates, if issued to them, can be authenticated using the trust anchors of a Provider of registration certificates notified to the Commission.
RPACANot_04	The trust anchors of Access Certificate Authorities and Providers of registration certificates SHALL be accepted because of their secure notification by the Member States to the Commission and by their publication in the corresponding Commission-compiled Trusted Lists, which are signed or sealed by the Commission.
RPACANot_05	The format of the Trusted Lists mentioned in RPACANot_04 SHALL comply with ETSI TS 119 612 v2.1.1 or with a suitable profile similarly derived from ETSI TS 102 231.

Index	Requirement specification
RPACANot_06	If an Access Certificate Authority is suspended or cancelled (see requirement GenNot_05 above), that Access Certificate Authority SHALL immediately revoke all of its temporally valid access certificates. *Note: This implies that if an intermediary obtained its access certificates from an Access Certificate Authority that is suspended or cancelled, any intermediated Relying Parties depending on that intermediary will not be able to request attributes from Wallet Units, even though it has valid registration certificates. Such an intermediated Relying Party will either have to transit to another intermediary (which has access certificates issued by an active Access Certification Authority) or wait until the original intermediary obtains new access certificates either from another Access CA or from the original one, once that CA can continue its operations.*
RPACANot_07	If a Provider of registration certificates is suspended or cancelled (see requirement GenNot_05 above), that Provider SHALL immediately revoke all of its valid registration certificates (if any). Moreover, the corresponding Registrar SHALL prohibit all access to the registry entries published online per Reg_03 and Reg_04.

H. Requirements for the publication of Trusted Lists compiled by the Commission

Index	Requirement specification
TLPub_01	The European Commission SHALL establish technical specifications for the system enabling the publication by the Commission of the information notified by the Member States regarding PID Providers, Wallet Providers, PuB-EAA Providers, Access Certificate Authorities, and Providers of registration certificates.
TLPub_02	The European Commission SHALL establish technical specifications for the set of information to be published about PID Providers, Wallet Providers, PuB-EAA Providers, Access Certificate Authorities and Providers of registration certificates, based on the information notified by the Member States. *Note: The information to be published MAY be different from the information to be notified per requirements PPNot_01, WPNot_01, PuBPNot_01, and RPACANot_01 above, respectively.*
TLPub_03	The publication of the information referred to in TLPub_01 SHALL take place over a secure channel protecting the authenticity and integrity of the published information.
TLPub_04	The technical system mentioned in TLPub_01 SHALL NOT require authentication or prior registration and authorisation of any entity wishing to retrieve the published information.
TLPub_05	The information referred to in TLPub_01 SHALL be published in an electronically signed or sealed form that is suitable for automated processing, and in a human-readable format, e.g., through introspection and display facilities, over an authenticated channel.

Index	Requirement specification
TLPub_06	The Commission SHALL publish in the OJEU the locations of the Trusted Lists for PID Providers, Wallet Providers, PuB-EAA Providers, Access Certificate Authorities, and Providers of registration certificates.
TLPub_07	The Commission SHALL publish in the OJEU the trust anchors to be used for verifying the signature or seal mentioned in TLPub_05.
TLPub_08	As part of the specifications referred to in TLPub_01, the European Commission SHALL establish technical specifications for ensuring the availability and authenticity of the full history regarding the information notified about PID Providers, Wallet Providers, PuB-EAA Providers, Access Certificate Authorities, and Providers of registration certificates.

A.2.3.32 Topic 32 - PID interoperability

See Topic 12.

A.2.3.33 Topic 33 - Wallet Unit backup and restore

Description

Backup and restore functionality is needed in case the User has lost access to their current Wallet Unit, for example in case of loss, theft, or breakdown. It is also needed if the User wants to start using another Wallet Unit, for example because they have bought a new device, need to factory-reset their existing device, or want to migrate to another Wallet Solution. In all of these cases, the User wants to restore the PIDs and attestations in their existing Wallet Unit on their new Wallet Unit, with as minimal an effort as possible.

The [European Digital Identity Regulation] does not contain a requirement mandating backup and restore functionality in the Wallet. However, Wallet Providers should implement backup and restore functionality nevertheless, because it will be expected by Users. In fact, the requirements in Topic 34 also ensure the possibility of backup and restore.

HLRs

There are no specific requirements in this Topic.

A.2.3.34 Topic 34 - Migrate to a different Wallet Solution

Description

Article 5a 4 (g) of the [European Digital Identity Regulation] ensures the User's rights to data portability. Data portability means that a User can migrate to a different Wallet Solution. The User installs an instance of the new Wallet Solution, and then wants to restore the PIDs and attestations in their existing Wallet Unit to their new Wallet Unit. This should be possible with as minimal an effort as possible, and independent of whether the User still has access to their existing Wallet Unit.

The solution described in this Topic is to introduce a Migration Object in each Wallet Unit. This object is a list of PIDs and attestations contained in the Wallet Unit, together with the information needed to request (re-)issuance of that PID or attestation. In addition, the Migration Object also contains the transaction log kept by the Wallet Unit, see Topic 19. Note that the Migration Object does not contain any private keys of PIDs or device-bound attestations. In most security architectures for a Wallet Solution described in Section 4.5 of the ARF main document, this is impossible, since the WSCA/WSCD that contains these private keys does not allow their extraction under any circumstances. An exception may be architectures in which attestation private keys are managed in a remote HSM and the migration is to a new Wallet Unit of the same Wallet Provider. However, in such cases, restoring functionality of the PIDs and device-bound attestations in a new Wallet Unit does not necessitate that private keys must be exported to another HSM. Rather, it implies the User must be able to authenticate towards the existing HSM from the new Wallet Unit, and be recognised as an existing User.

The fact that the Migration Object does not contain private keys means that PIDs and device-bound attestations cannot be backed up and restored from the object in such a way that they are usable in a new Wallet Unit without involvement of the PID Provider or Attestation Provider. Instead, the User must ask the respective PID Provider(s) or Attestation Provider(s) to issue the PID(s) or device-bound attestation(s) existing on the User's old Wallet Unit once again to the new Wallet Unit. The only function of the Migration Object is to simplify this process by listing the PIDs and attestations present in the existing Wallet Unit, together with the information needed by the new Wallet Unit to start the issuance process. For PIDs and device-bound attestations, the Migration Object does not contain attribute values or attribute identifiers, as that data is considered sensitive and is not useful anyway because of the limitations explained above. Instead, the object contains a list of attestation types and the related Attestation Providers.

For a non device-bound attestation, there are no private keys stored in the WSCD and hence it is in principle possible to back up such an attestation and restore it in a different Wallet Unit without involvement of the Attestation Provider. For non device-bound attestations, the Migration Object therefore either contains the same data as for device-bound attestations, or it contains all data including attribute identifiers

The Migration Object is stored in such a way that its confidentiality is ensured and that it can be used only by the User.

HLRs

A. Back-up requirements

Index	**Requirement specification**
Mig_01	A Wallet Unit SHALL include and keep up-to-date a Migration Object, containing the following information: - The contents of the log for all transactions executed through the Wallet Unit, as listed in requirement DASH_02. - A list of PIDs and attestations, except Wallet Unit Attestations, present in the Wallet Unit, according to the requirements in this Topic.
Mig_02	The Migration Object SHALL comply with all requirements in Technical Specification 10.

Index	Requirement specification
Mig_03	For each PID or device-bound attestation that is issued to it, a Wallet Unit SHALL add to the Migration Object all data necessary to request issuance of that PID or attestation once again. This SHALL include at least the attestation type and the PID Provider or Attestation Provider that issued the PID or attestation, as well as their service supply points. However, the Migration Object SHALL NOT contain attribute identifiers or attribute values, and SHALL NOT contain any private keys of the PID or device-bound attestation.
Mig_03a	For each non-device bound attestation that is issued to it, a Wallet Unit SHALL add to the Migration Object one of the following: either all data necessary to request issuance of that attestation once again, as listed in Mig_03, or all data necessary to transfer the attestation to a new device without involvement of the Attestation Provider, including attribute identifiers and attribute values. The Wallet Unit SHALL enable the User to indicate if they want to store attribute identifiers and values in the Migration Object.
Mig_03b	If the User deletes a PID or attestation from their Wallet Unit, the Wallet Unit SHALL delete the corresponding entry from the Migration Object.

Index	Requirement specification
Mig_04	The Wallet Unit SHALL store the Migration Object in an external storage or remote storage location of the User's choice, from among the storage options supported by the Wallet Unit, in such a way that the User can still retrieve the object from a new Wallet Unit in case the existing Wallet Unit becomes unavailable. *Notes: - It is up to the Wallet Provider to decide which external storage options or remote storage locations the Wallet Unit supports for storing the Migration Object. - The new Wallet Unit may be either an instance of the same Wallet Solution as the old one, or an instance of a different Wallet Solution.*
Mig_05	The Wallet Unit SHALL store the Migration Object in such a way that its confidentiality, integrity, and authenticity is protected and that it is protected against use by others than the User. *Note: This could be done, for example, by using password-based cryptography to encrypt the object.*

B. Restore Requirements

Index	Requirement specification
Mig_06	Directly after installation of a new Wallet Instance, the Wallet Instance SHALL enable the User to import a Migration Object from an external storage or remote storage location indicated by the User, from among the storage options supported by the Wallet Unit.

Index	Requirement specification
Mig_07	When importing a Migration Object, for each PID and device-bound attestation listed in the Migration Object, the Wallet Unit SHALL enable the User to select that PID or attestation. When a PID or device-bound attestation is selected, the Wallet Unit SHALL request the respective PID Provider or Attestation Provider to re-issue that PID or attestation. If the User selects a PID, the PID SHALL be the first to be restored.
Mig_07a	When importing a Migration Object, for each non device-bound attestation listed in the Migration Object, the Wallet Unit SHALL enable the User to select that attestation. When an attestation is selected, the Wallet Unit SHALL, depending on whether the Migration Object contains attribute identifiers and attribute values (see Mig_03a), either restore the attestation or request the respective Attestation Provider to re-issue it.
Mig_07b	When importing a Migration Object, the Wallet Unit SHALL ask the User whether they want to restore the log from the Migration Object. When the User agrees, the Wallet Unit SHALL restore the log, and SHALL append future transactions to this log according to the requirements in Topic 19.
Mig_08	Empty
Mig_09	Empty
Mig_10	Empty
Mig_11	The processes and interfaces used for issuance of a PID or attestation as part of a migration process SHALL be the same as those used for a ‘normal’ issuance process, as specified in Topic 10.
Mig_12	Empty

Index	Requirement specification
Mig_13	Empty
Mig_14	Empty
Mig_15	Empty
Mig_16	Empty

A.2.3.35 Topic 35 - PID issuance service blueprint

Description

This Topic analyses the User journeys for PID issuance to a Wallet Unit. This Topic focuses on natural persons only.

HLRs

No HLRs are present for this Topic. Note that issuance of PID is discussed in Topic 10; relevant HLRs can be found there.

A.2.3.36 Topic 36 - Risk Analysis of the Wallet usage

There are no HLRs for this Topic.

A.2.3.37 Topic 37 - QES – Remote Signing - Technical Requirements

See Topic 16.

A.2.3.38 Topic 38 - Wallet Unit revocation

Description

This Topic discusses Wallet Unit revocation. In particular, it answers the following questions: - How can a Wallet Provider revoke a Wallet Unit? - During issuance of an attestation, how can an Attestation Provider verify whether a Wallet Unit has been revoked? - When requesting attributes from an attestation, how can a Relying Party verify whether a Wallet Unit has been revoked?

Related to the last question, [CIR 2024/2977], Article 5, 4.(b) says "Where providers of person identification data revoke person identification data issued to wallet units, they shall do so (…) where the wallet unit attestation to which the person identification data was issued to has been revoked". This implies that if a Relying Party verifies that a PID it obtained from a Wallet Unit is valid (i.e., not revoked), it can trust that the Wallet Unit is also valid. Consequently, there is no need for a separate mechanism that would allow the Relying Party to verify the revocation status of a Wallet Unit directly with the Wallet Provider. Although the CIR requires this mechanism only for PIDs, other Attestation Providers may similarly revoke an attestation if the Wallet Unit on which it resides is revoked. Note that if an Attestation Provider does not support this, a Relying Party obtaining an attestation from a Wallet Unit has no way of knowing whether the Wallet Unit is revoked. Depending on the value of the attestation, this risk may be acceptable for the Relying Party.

In case of a security issue, Article 5e of the [European Digital Identity Regulation] requires Wallet Providers to first suspend a Wallet Unit and to revoke it only if the issue cannot be solved within three months. However, the suspension of a Wallet Unit is an administrative process, which does not imply that the WUAs of that Wallet Unit need to be suspended, as opposed to being revoked. Instead, if the Wallet Provider administratively suspends a Wallet Unit, it will immediate revoke all corresponding WUAs. If (within three months) the situation is remedied and the Wallet Unit can be re-instated, the Wallet Provider will issue one or more new WUAs to the Wallet Unit.

HLRs

A. Issuing a Wallet Unit Attestation

Index	Requirement specification
WURevocation_01	To enable a PID Provider or an Attestation Provider to verify the authenticity and the revocation status of a Wallet Unit it is interacting with, a Wallet Provider SHALL issue one or more Wallet Unit Attestations to the Wallet Unit, as specified in Topic 9. *Note: The first of these WUAs will be issued during the activation phase of a Wallet Unit. During the lifetime of the Wallet Unit, the Wallet Provider will re-issue WUAs as needed.*
WURevocation_02	During the lifetime of the Wallet Unit, the Wallet Provider SHALL ensure that the Wallet Unit at all times is in possession of at least one valid WUA.
WURevocation_03	Empty
WURevocation_04	Empty
WURevocation_05	Empty

A. Revoking a Wallet Unit

Index	Requirement specification
WURevocation_06	Empty
WURevocation_07	A Wallet Provider SHALL be able to revoke a Wallet Unit by revoking its WUA(s), as specified in [Topic 7].*
WURevocation_08	Empty

Index	Requirement specification
WURevocation_09	During the lifetime of a Wallet Unit, the Wallet Provider SHALL regularly verify that the security of the Wallet Unit is not breached or compromised. If the Wallet Provider detects a security breach or compromise, the Wallet Provider SHALL analyse its cause(s) and impact(s). If the breach or compromise affects the trustworthiness or reliability of the Wallet Unit, the Wallet Provider SHALL administratively revoke or suspend the Wallet Unit and SHALL immediately revoke the corresponding WUA(s). The Wallet Provider SHALL do so at least in the following circumstances: - If the security of the Wallet Unit, or the security of the mobile device and OS on which the corresponding Wallet Instance is installed, or the security of a WSCA/WSCD it uses for managing cryptographic keys and sensitive data, is breached or compromised in a manner that affects its trustworthiness or reliability. - If the security of the Wallet Solution is breached or compromised in a manner that affects the trustworthiness or reliability of all corresponding Wallet Units. - If the security of the common authentication and data protection mechanisms used by the Wallet Unit is breached or compromised in a manner that affects their trustworthiness or reliability. - If the security of the electronic identification scheme under which the Wallet Unit is provided is breached or compromised in a manner that affects its trustworthiness or reliability.

Index	Requirement specification
WURevocation_9b	If within three months from an administrative suspension of a Wallet Unit the security breach or compromise is remedied, the Wallet Provider SHALL issue one or more WUAs to the Wallet Unit, such that the User can again use it.
WURevocation_10	A Wallet Provider SHALL revoke a Wallet Unit upon the explicit request of the User registered during the Wallet Unit activation process, see Topic 40. To do so, the Wallet Provider SHALL revoke all valid WUA(s) for that Wallet Unit. The Wallet Provider SHALL authenticate the User before accepting a request to revoke the Wallet Unit.
WURevocation_11	A Wallet Provider SHALL revoke a Wallet Unit upon the explicit request of a PID Provider, in case the natural person using the Wallet Unit has died or the legal person using the Wallet Unit has ceased operations. To do so, the Wallet Provider SHALL revoke all valid WUA(s) for that Wallet Unit. To identify the Wallet Unit that is to be revoked, the PID Provider SHALL use a Wallet Unit identifier provided by the Wallet Provider in the WUA during PID issuance. *Note: See the notes to WUA_08.*
WURevocation_12	Before revoking a Wallet Unit per WURevocation_11, the Wallet Provider SHALL verify that the party requesting revocation is indeed a valid PID Provider listed in the Trusted List of PID Providers.
WURevocation_13	Before requesting a Wallet Provider to revoke a Wallet Unit per WURevocation_11, the PID Provider SHALL ensure that the revocation does not harm the interests of any of the stakeholders. The PID Provider SHALL have (and follow) a documented policy to ensure that this is the case.

B. Informing the User

Index	Requirement specification
WURevocation_14	A Wallet Provider SHALL inform a User without delay, and within 24 hours at most, in case the Wallet Provider decided to revoke the User’s Wallet Unit. The Wallet Provider SHALL also inform the User about the reason(s) for the revocation. This information SHALL be understandable for the general public. It SHALL include (a reference to) technical details about any security breach if applicable.
WURevocation_15	Empty
WURevocation_16	To inform a User about the revocation of their Wallet Unit, the Wallet Provider SHALL use a communication channel that is independent of the Wallet Unit. In addition, the Wallet Provider MAY use the Wallet Unit itself to inform the User.

C. Verifying the revocation status of a Wallet Unit

Index	Requirement specification
WURevocation_17	Empty

Index	Requirement specification
WURevocation_18	A PID Provider issuing revocable PIDs SHALL, for each of its valid PIDs, regularly verify whether the Wallet Provider revoked the Wallet Unit on which that PID is residing, using the revocation information in the WUA it received during issuance of that PID. If it turns out that the Wallet Unit is revoked, the PID Provider SHALL immediately revoke the respective PID in accordance with all requirements in [Topic 7]. *Notes: - This is a consequence of the legal requirement in [CIR 2024/2977], Article 5, 4.(b). - See Technical Specification 3 for how the PID Provider can do this verification. - The reverse is not true: When a PID is revoked, this does not imply that the Wallet Unit on which it is residing should also be revoked. Instead, the Wallet Unit moves to the Operational state. See ARF main document Section 4.6.3.*
WURevocation_19	An Attestation Provider issuing revocable attestations MAY decide to revoke an attestation if the Wallet Provider revoked the Wallet Unit on which that attestation is residing, in the same manner as described in WURevocation_18. An Attestation Provider SHALL publish its policy in this regard. *Note: Publishing its policy regarding revocation allows a Relying Party to decide if it can put sufficient trust in the attestations issued by that Attestation Provider.*
WURevocation_19a	Empty
WURevocation_19b	Empty
WURevocation_20	Empty
WURevocation_21	Empty

A.2.3.39 Topic 39 - Wallet to wallet technical Topic

See Topic 30.

A.2.3.40 Topic 40 - Wallet Instance installation and Wallet Unit activation and management

Description

This Topic discusses requirements related to the installation of a Wallet Instance by the User, the subsequent activation of the Wallet Unit by the User and the Wallet Provider, and the management of the Wallet Unit throughout its lifetime.

A - HLRs for Wallet Instance installation

Index	Requirement specification
WIAM_01	To ensure that the User can trust the Wallet Solution, a Wallet Provider SHOULD make its certified Wallet Solution available for installation only via the official app store of the relevant operating system (e.g., Android, iOS). *Note: This allows the operating system of the device to perform relevant checks regarding the authenticity of the Wallet Unit.*

Index	Requirement specification
WIAM_02	If a Wallet Provider makes its certified Wallet Solution available for installation through other means than the official OS app store, it SHALL implement a mechanism allowing the User to verify the authenticity of the Wallet Unit. Moreover, it SHALL provide clear instructions to the User on how to install the Wallet Instance, including at least: - instructions on the verification of the authenticity of the Wallet Instance to be installed, - instructions on bypassing of any operating system limitations on side-loading of apps, if applicable, and ensuring that these limitations are restored after the Wallet Instance has been installed. *Note: This requirement also applies for the installation of a Wallet Instance on a User device that is not a mobile device, and for which no official operating system app store may exist.*

B - HLRs for Wallet Unit activation

Index	Requirement specification
WIAM_03	A Wallet Provider SHALL ensure that a Wallet Instance starts a process to activate the new Wallet Unit with the Wallet Provider immediately after installation or when the User first opens the Wallet Instance. The Wallet Provider SHALL ensure that the Wallet Instance starts this process only with a secure backend of the Wallet Provider.
WIAM_04	During the activation process of a new Wallet Unit, the Wallet Provider SHALL verify that the new Wallet Instance is a genuine instance of its Wallet Solution.

Index	Requirement specification
WIAM_05	During the activation process of a new Wallet Unit, the Wallet Provider SHALL process information about the User device and the available WSCAs and WSCDs, as far as necessary to issue a Wallet Unit Attestation to the Wallet Unit conform all requirements in Topic 9 section A. The Wallet Provider MAY process additional information necessary for managing the Wallet Unit, but it SHALL NOT process more information than it reasonably needs for legitimate purposes. The Wallet Provider SHALL request User consent (through the Wallet Instance) for all information and data it will process, both during activation and throughout the lifetime of the Wallet Unit. The Wallet Provider SHALL inform the User about the purposes of data processing, in accordance with the General Data Protection Regulation.
WIAM_06	The Wallet Provider SHALL request the User, through the new Wallet Instance, to set up a User account at the Wallet Provider. The Wallet Provider SHALL explain to the User that this is necessary to enable the User to request revocation of the Wallet Unit in case of theft or loss. The Wallet Provider SHALL register one or more User authentication methods that the Wallet Provider will use to authenticate the User in the future. These methods SHALL be independent of the Wallet Unit and the User device. The Wallet Provider SHALL allow the User to register using an alias instead of true identity data. The Wallet Provider SHALL NOT use any registered User data for purposes other than User authentication, unless the User gives explicit consent to do so. The Wallet Provider SHALL register the relationship between the Wallet Unit and the corresponding User account.

Index	Requirement specification
WIAM_07	A Wallet Provider SHALL activate a new Wallet Unit before a User can use it to have issued an PID or attestation. *Note: The WUA is issued as part of the activation.*
WIAM_08	A Wallet Provider SHALL only activate a new Wallet Unit if it has verified that: - The Wallet Unit includes at least one WSCA/WSCD that is certified to be compliant with applicable requirements in this Topic, for Level of Assurance High in Commission Implementing Regulation (EU) 2015/1502 section 2.2.1. In addition, the Wallet Unit MAY include one or more other WSCAs, which SHALL be certified to be compliant with applicable requirements for Level of Assurance Substantial or High. - The private key corresponding to the public key in the WUA (see WUA_09) is protected by the respective WSCA/WSCD under control of the User.
WIAM_09	If a WSCA/WSCD contains cryptographic keys related to multiple Wallet Units, the Wallet Provider SHALL ensure that a Wallet Unit can only access keys that are related to that Wallet Unit.
WIAM_10	During the activation process of a new Wallet Unit, a Wallet Provider SHALL create and sign at least one Wallet Unit Attestation, and issue them to the Wallet Unit.
WIAM_10a	During the activation process of a new Wallet Unit, the Wallet Provider SHALL offer the User a means to verify the formal certification information of their Wallet Solution.

C - HLRs for Wallet Unit management

Index	Requirement specification
WIAM_11	During the lifetime of the Wallet Unit, the Wallet Provider SHALL update the Wallet Unit as necessary to ensure its continued security and functionality.
WIAM_12	All communication between the Wallet Provider and the Wallet Unit SHALL be mutually authenticated and SHOULD be encrypted.
WIAM_12a	The Wallet Unit SHALL ensure that the Wallet Provider cannot access the contents of the Wallet Unit, in particular to learn a) which attestations are present on the Wallet Unit, b) the status of these attestations, c) the value of attributes in these attestations, and d) the contents of the Wallet Unit log meant in DASH_02.
WIAM_13	If the User uninstalls the Wallet Unit, the Wallet Unit SHALL ensure that all cryptographic key material in the WSCA(s) related to the Wallet Unit is securely destroyed. This includes all keys of the WUAs, PIDs, and device-bound attestations stored in the Wallet Unit. *Note: Key deletion is a cryptographic key operation and requires User authentication, as specified in requirement WIAM_14.*
WIAM_13a	If a Wallet Unit supports the [W3C Digital Credentials API] and the User uninstalls the Wallet Unit, the Wallet Unit SHALL disclose the fact that it no longer stores any PID(s) or attestation(s) to the Digital Credentials API framework.

Index	Requirement specification
WIAM_14	A WSCA/WSCD SHALL authenticate the User before performing any cryptographic operation involving a private or secret key of a Wallet Unit (i.e., a WUA key) or a private or secret key of a PID or a device-bound attestation stored in a Wallet Unit. For a PID key (which is part of the EUDI Wallet eID means), this WSCA/WSCD SHALL be certified to be compliant with applicable requirements for Level of Assurance High in Commission Implementing Regulation (EU) 2015/1502 section 2.2.1. *Note: Many actions of the Wallet Unit, such as processing a Relying Party presentation request and presenting an attestation, require multiple cryptographic operations, for example ephemeral key generation followed by key agreement and presentation signing and encryption. This requirement does not imply that a separate User authentication is necessary before each of these operations. Rather, a successful User authentication will be valid for all cryptographic operations necessary for a Wallet Unit action. It is up to the Wallet Provider to determine what constitutes a 'Wallet Unit action', finding a balance between security (more User authentications) and User convenience (fewer User authentications). During certification of the Wallet Solution, it will be verified that the solution provides an adequate level of security.*
WIAM_15	Before performing any operation, a Wallet Unit SHALL authenticate the User. The Wallet Unit SHALL use the OS-level authentication mechanism according to WIAM_15a, unless this is technically impossible (for instance on some legacy devices), or the User prefers to use a Wallet Unit-specific PIN implemented by the Wallet Unit itself, as specified in WIAM_15b.

Index	Requirement specification
WIAM_15a	In order to ensure that operating system-level authentication can be used and is sufficiently secure, during installation of the Wallet Unit, the Wallet Unit SHALL enforce the activation of an OS-level User authentication mechanism with adequate security policies.
WIAM_15b	During installation of the Wallet Unit, the Wallet Unit SHALL enable the User to indicate if they want to use a Wallet Unit-specific PIN for User authentication, or use the OS-level User authentication mechanism. The Wallet Unit SHALL enable the User to change this preference during the lifetime of the Wallet Unit.
WIAM_16	For User authentication according to WIAM_15, a Wallet Unit SHALL implement an idle timeout, after which User authentication SHALL again be required. The Wallet Unit SHOULD provide the User with the option to set the idle timeout to a duration shorter than the default timeout.
WIAM_17	A WSCA/WSCD SHALL be able to authenticate a User in accordance with the requirements in Commission Implementing Regulation (EU) 2015/1502 section 2.2.1.
WIAM_18	A WSCA/WSCD SHALL be able to generate a new key pair on request of the Wallet Provider via the Wallet Instance.
WIAM_19	A WSCA/WSCD SHALL be able to prove possession of the private key corresponding to a public key on request of a Wallet Instance, for example by signing a challenge with that private key.

Index	Requirement specification
WIAM_20	A WSCA/WSCD SHALL protect a private key it generated during the entire lifetime of the key. This protection SHALL at least imply that the WSCA/WSCD prevents the private key from being extracted in the clear. If a WSCA/WSCD is able to export a private key in encrypted format, the resulting level of protection SHALL be equivalent to the protection level of the private key when stored in the WSCA.
WIAM_21	Whenever the WSCA/WSCD successfully authenticated the User according to WIAM_14, the Wallet Unit SHOULD check if there are any PIDs or device-bound attestations on the Wallet Unit that cannot be presented any longer to Relying Parties, for example because they have expired or because a once-only attestation (see Topic 10, section D, method A) was presented to a Relying Party already. The Wallet Unit SHOULD then request the WSCA/WSCD to destroy all cryptographic key material related to these PIDs or attestations. *Note: The reason for this recommendation is that probably, Wallet Providers will want to prevent an accumulation of unused private keys in the WSCA/WSCD, given that such devices typically do not have much storage space. However, deletion of private keys (and potentially other key material) is a cryptographic key operation and cannot be done without User authentication; see WIAM_14. At the same time, for usability reasons the User must not be involved in such 'cleaning up' processes, see also ISSU_42. The recommended solution is to take advantage of a User authentication event to also carry out any necessary cleaning operations.*

A.2.3.41 Topic 41 - Minimum requirements on PuB-EAAs rulebooks

See Topic 12.

A.2.3.42 Topic 42 - Requirements for QTSPs to access Authentic Sources

Description

This Topic discusses the ability of QTSPs issuing electronic attestations of attributes to verify those attributes by electronic means at the request of the User, wherever those attributes rely on Authentic Sources within the public sector.

HLRs

Index	Requirement specification
QTSPAS_01	In accordance with technical specifications referred to in QTSPAS_07, Member States SHALL define: - discovery mechanisms that enable QTSPs to request information about Authentic Sources or designated intermediaries recognised at the national level. This includes information regarding the attributes of a natural or legal person for which the Authentic Source or designated intermediary is considered a primary source, or for which it is recognised as authentic in accordance with Union law or national law, including administrative practices. - procedures for QTSPs to request the verification of attributes from Authentic Sources.

Index	Requirement specification
QTSPAS_02	An Authentic Source in the public sector, or its designated intermediary, SHALL implement an interface complying with the technical specification mentioned in QTSPAS_07 for receiving verification requests and sending responses. For each received request, the Authentic Source SHALL - identify and authenticate the requestor in such a way that it can subsequently determine whether the requestor is a QTSP issuing qualified electronic attestation of attributes, for example by means of a lookup in the QTSP Trusted List. - authenticate the User and obtain their approval, if it is legally obliged to do so, in addition to the User authentication and approval already performed by the QTSP according to QTSPAS_08. - verify whether the attribute values claimed by the QTSP match the values held by the Authentic Source; and, finally, - respond with one of the following for each attribute: +'match', if the attribute value held for this User by the Authentic Source is identical to the value claimed by the QTSP, + 'no match', if the attribute value held for this User by the Authentic Source is not identical to the value claimed by the QTSP, including if the Authentic Source is the authentic source for this attribute but does not hold a value for this User, +'unknown', if the Authentic Source is not the authentic source for this attribute.
QTSPAS_03	An Authentic Source or designated intermediary SHALL respond to a verification request for attributes by any QTSP issuing qualified electronic attestation of attributes.

Index	Requirement specification
QTSPAS_04	An Authentic Source or designated intermediary SHALL implement the technical specifications mentioned in QTSPAS_01, so that the QTSP will receive the result of the verification of the requested attributes as described in QTSPAS_02. If the verification is deferred, the response to the QTSP SHALL include the maximum time that it will take to verify the requested attributes, and a unique identifier that the QTSP SHALL use to obtain the result of the verification.
QTSPAS_05	A QTSP SHALL send an attribute verification request directly to the Authentic Source or designated intermediary recognised at national level, after discovering it using the mechanisms mentioned in QTSPAS_01.
QTSPAS_06	Member States SHALL specify the processes and mechanisms to designate the Authentic Sources or intermediaries recognised at national level in accordance with Union or national law, allowing these Authentic Sources or intermediaries to verify the attributes presented to them by QTSPs.
QTSPAS_07	The Commission SHALL publish, in cooperation with the European Digital Identity Cooperation Group, a technical specification, referring to applicable standards, specifications and procedures, that will cover at least the attributes specified in Annex VI, wherever those attributes rely on Authentic Sources within the public sector, for which Member States must ensure that measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means, at the request of the User, their authenticity against the relevant authentic source.

Index	Requirement specification
QTSPAS_07a	The standards and procedures mentioned in QTSPAS_07 SHOULD, whenever possible, be aligned and compatible with those used for the platforms implementing the Once Only Technical System (OOTS). *Note: There is a clear synergy of both of these data exchange approaches. In fact, the national OOTS node would be a candidate for acting as an intermediary between QTSPs issuing QEAAs and the Authentic Sources.*
QTSPAS_08	A QTSP SHALL obtain approval from the User to verify the authenticity of the attributes, before requesting the verification of those attributes by the relevant Authentic Source or designated intermediary.

A.2.3.43 Topic 43 - Embedded disclosure policies

Description

This topic is focused on identifying high-level requirements for disclosure policies which may be embedded in an attestation. Such a policy may be created by the Attestation Provider, and allows the Wallet Unit, using data obtained from the Relying Party, to determine whether the Attestation Provider agrees with releasing attributes from the attestation to the Relying Party. Note that an embedded disclosure policy, if present, is applicable for any attribute in the attestation.

Note that embedded disclosure policies do not apply to Wallet-to-Wallet interactions as described in Topic 30, because a requesting Wallet Unit is not registered and therefore no authenticated information is available to evaluate an embedded disclosure policy.

HLRs

Index	Requirement specification
EDP_01	A Wallet Unit SHALL enable an Attestation Provider to optionally express an embedded disclosure policy for a QEAA, PuB-EAA, or non-qualified EAA. *Note: The [European Digital Identity Regulation] does not contain a requirement for PIDs to be able to contain an embedded disclosure policy.*
EDP_02	A Wallet Unit SHALL support embedded disclosure policies implementing the ‘Authorised relying parties only policy’ described in Annex III of Implementing Regulation (EU) 2024/2979. If present, such an embedded disclosure policy SHALL contain a list of EU-wide unique identifiers of Relying Parties, as specified in Reg_32. The Wallet Unit SHALL retrieve the Relying Party identifier from the access certificate presented by the Relying Party, and compare it to the list of authorised identifiers in the policy, unless the Relying Party is an intermediary. If the Relying Party is an intermediary, the Wallet Unit SHALL retrieve the unique identifier of the intermediated Relying Party from the presentation request or from the registration certificate of the intermediated Relying Party and compare this identifier to the list of authorised identifiers in the policy. *Note: See RPI_07 for how the Wallet Unit can see if the Relying Party is an intermediary.*

Index	Requirement specification
EDP_03	A Wallet Unit SHALL support embedded disclosure policies implementing the 'Specific root of trust' policy described in Annex III of Implementing Regulation (EU) 2024/2979. If present, such an embedded disclosure policy SHALL contain a list of root or intermediate certificates used for signing Relying Party access certificates. The Wallet Unit SHALL compare the certificate chain that was used to sign the access certificate provided by the Relying Party to the list of authorised root or intermediate certificates in the policy, unless the Relying Party is an intermediary. If the Relying Party is an intermediary, the Wallet Unit SHALL retrieve the root certificate of the Provider of registration certificates of the intermediated Relying Party from the presentation request or from the Registrar's online service (as applicable) and compare this certificate to the list of authorised certificates in the policy. *Note: See RPI_07 for how the Wallet Unit can see if the Relying Party is an intermediary.*
EDP_04	Empty
EDP_05	An embedded disclosure policy SHOULD contain a link to a website of the Attestation Provider explaining the disclosure policy in layman's terms. If this is the case, the Wallet Unit SHALL display the link to the User and allow them to navigate to that website.
EDP_06	The Wallet Unit SHALL evaluate an embedded disclosure policy in conjunction with the information received from the requesting Relying Party, in order to determine if the Relying Party has permission from the Attestation Provider to access the requested attestation.

Index	Requirement specification
EDP_07	The Wallet Unit SHALL enable the User, based on the outcome of the evaluation of the applicable embedded disclosure policy(s), to deny or allow the presentation of the requested attestation to the Relying Party.
EDP_08	The Commission SHALL take measures to ensure a technical specification is created establishing common mechanisms for the specification of embedded disclosure policies by Attestation Providers, and for the evaluation of such policies by Wallet Units.
EDP_09	An Attestation Provider SHALL include an embedded disclosure policy (if any) by value in the Issuer metadata related to the attestation, in compliance with the [OpenID4VCI] issuance protocol or an extension thereof specified in the technical specification mentioned in EDP_08.
EDP_10	During attestation issuance, a Wallet Unit SHALL retrieve and store locally the corresponding embedded disclosure policy, if any.
EDP_11	An Attestation Provider SHALL revoke an attestation if a corresponding embedded disclosure policy is added, changed, or deleted.

A.2.3.44 Topic 44 - Registration certificates for PID Providers, Providers of QEAAs, PuB-EAAs, and non-qualified EAAs, and Relying Parties

Description

This topic identifies high-level requirements for registration certificates, which were introduced in Commission Implementing Regulation 2024/2982 [2024/2982]. A registration certificate may be issued by a Provider of registration certificates to a PID Provider, a QEAA Provider, a PuB-EAA Provider, a non-qualified EAA Provider, or a Relying Party during the registration process described in Topic 27. However, although registration of these entities is mandatory, issuance of a registration certificate is optional.

Registration certificates contain generic information regarding its subject, such as name, unique identifier, role (Relying Party, PID Provider, QEAA Provider, etc.), service description, etc. Apart from this generic information, the contents and use of registration certificates differs between Relying Parties on the one hand and PID Providers, QEAA Providers, PuB-EAA Providers, and non-qualified EAA Providers on the other:

- A registration certificate for a Relying Party contains the list of attributes registered by the Relying Party according to Article 5b 2 (c) of the [European Digital Identity Regulation]. As a Relying Party is obliged to register for each purpose ("intended use") separately, multiple registration certificates may be issued to a single Relying Party, where each certificate is related to one specific intended use. As specified in Technical Specification 5, the Registrar assigns an identifier to each registered intended use of a Relying Party. A registration certificate als contains information about the intermediary used by this Relying Party, if applicable.
- A registration certificate for a PID Provider, a QEAA Provider, a PuB-EAA Provider, a non-qualified EAA Provider contains information on the attestation type(s) it intends to issue.

Note that the above types of registration certificate can be combined in a single certificate, for instance in case an Attestation Providers intends to request data from the User's PID during issuance of an attestation. Such an Attestation Provider would then register both as a Relying Party (which is called a Service Provider in Technical Specification 5) and as a PID Provider, QEAA Provider, PuB-EAA Provider, or non-qualified EAA Provider.

A registration certificate is signed by the Provider of registration certificates that issued it. Commission Implementing Regulation 2024/2982 requires a Wallet Unit to authenticate and validate the registration certificate, if available. If no registration certificate is available, the same information can also be retrieved from the Registrar's online service. This enables Users

- for a Relying Party they are interacting with, to verify that the attributes being requested by the Relying Party are within the scope of their registered attributes. This provides assurance that the request is legitimate and trustworthy.
- for a PID Provider or Attestation Provider they are interacting with, to verify that the issued attestation is within the scope of their registered attestations. This provides

assurance that the attestation is legitimate and trustworthy.

HLRs

A. Generic requirements on the specification and contents of registration certificates

Index	**Requirement specification**
RPRC_01	The Commission SHALL provide a technical specification establishing a common Certificate Policy for registration certificates, covering at least management and selection of signing keys, revocation and lifecycle management of registration certificates on individual intended use level. *Note: The technical specification may require the Provider of registration certificates to follow applicable parts of technical standards such as EN 319 401 (for General Policy Requirements for TSPs) and TS 119 461 (for identity proofing of Relying Party representatives).*

Index	Requirement specification
RPRC_02	The Commission SHALL ensure that a technical specification is created, describing at least 1. the contents and format of registration certificates for Relying Parties, see the other requirements in this section below. 2. the signing method(s) used to ensure the authenticity of the registration certificate. 3. the trust infrastructure necessary for signing registration certificates and for verifying these signatures, including the use of Trusted Lists to establish trust in Providers of registration certificates and to distribute their trust anchors to Wallet Units. 4. the method used for binding each registration certificate to the access certificate that will be used in the same presentation request. This binding method SHALL enable a Wallet Unit to verify that the registration certificate is bound to the entity that authenticated itself using the access certificate. The binding method SHALL consider situations in which a Relying Party uses the services of an intermediary (see Topic 52) to connect to the Wallet Unit. 5. whether or not a registration certificate must have a validity period. 6. the method to be used for revocation of registration certificates. Moreover, the technical specification SHALL describe the impact of revocation, especially compared to the impact of revocation of the access certificate(s) of the same entity.
RPRC_03	The contents of a registration certificate SHALL include at least the information required in Annex V of the CIR 2025/848 regarding registration of wallet-relying parties.

Index	Requirement specification
RPRC_04	If the subject of the registration certificate uses the services of an intermediary (see Topic 52), the ‘association to the intermediary’ mentioned in Annex I (15) of [CIR 2025/848] SHALL consist of the user-friendly name and unique identifier of this intermediary, as meant in requirements Reg_31 and Reg_32. *Note: this name and identifier are identical to those in the access certificate of the intermediary.*
RPRC_04a	If the subject of the registration certificate uses the services of an intermediary (see Topic 52), the contents of a registration certificate SHALL include the URL of the online service of the Registrar of the Relying Party. *Note: this is needed because an intermediary will send it own access certificate to a Wallet Unit (see RPI_06), which contains the URL of its own registrar (see Reg_33), and not the URL of the Registrar of the intermediated Relying Party.*
RPRC_05	If the subject of the registration certificate is not a Relying Party (i.e. in the terms of CIR 2025/848, a Service Provider), the certificate SHALL NOT contain the intended use as meant in Annex I (9) and (10) of CIR 2025/848. *Note: A PID Provider or Attestation Provider may request attributes from the Wallet Unit during issuance. If so, it registers as both a Service Provider and an Attestation Provider, and consequently its registration certificate contains its intended use.*
RPRC_06	The contents of a registration certificate SHALL include a name for the subject of the certificate, in a format suitable for presenting to a User. *Note: A Wallet Unit needs the name of a Relying Party at least when requesting User approval according to [Topic 6]*

Index	Requirement specification
RPRC_07	The contents of a registration certificate SHALL include an EU-wide unique identifier for the subject of the certificate, and SHALL specify a method for deriving such identifiers. *Notes: - A Wallet Unit needs an identifier for a Relying Party at least to allow the User to send a report of suspicious Relying Party presentation requests to a data protection authority according to Topic 50. - The EU-wide unique identifier could, for example, be a concatenated list of one or more registered official Relying Party identifiers listed in Annex I(3) of the CIR 2025/848 regarding registration of Wallet Relying Parties, expressed in the semantic form defined in [ETSI EN 319 412-1] sections 5.1.4 or 5.1.5. The exact specification is left for the technical specifications to be developed by the European Commission.*
RPRC_08	The EU-wide unique identifier meant in RPRC_07 SHALL be identical in all registration certificates issued for a given entity. *Note: In case the registration certificates issued to an intermediated Relying Party are held and presented by an intermediary, the entity meant in this requirement is the intermediated Relying Party. An intermediary may obtain and hold registration certificates with a different unique identifier for other intermediated Relying Parties.*

B Requirements on the issuance of registration certificates to Relying Parties

Index	Requirement specification
RPRC_09	A Member State Registrar MAY decide that, during the registration process for Relying Parties, as specified in Topic 27, a Provider of registration certificates associated to the Registrar must create and sign or seal one or more registration certificates. If the Registrar decides to do so, the Provider of registration certificates SHALL create and sign or seal a separate registration certificate for each intended use registered by each Relying Party, and issue it to the Relying Party. Each registration certificate SHALL comply with the requirements in the technical specification mentioned in RPRC_02. *Note: See also Topic 52.*
RPRC_10	If, during registration, a Relying Party received one or more registration certificates, it SHALL distribute these to all its Relying Party Instances.
RPRC_11	The contents of a registration certificate issued to a Relying Party SHALL at least one of the following: a) the URL of a web form provided by the Relying Party, which Users can use to send data deletion requests, b) an e-mail address of the Relying Party, on which the Relying Party is prepared to receive data deletion requests from Users, c) a telephone number of the Relying Party, on which the Relying Party is prepared to receive data deletion requests from Users. *Note: See Topic 48 for more information about data deletion requests.*

Index	Requirement specification
RPRC_12	The contents of a registration certificate issued to a Relying Party SHALL contain the name and country of the Data Protection Authority supervising the Relying Party. In addition, the registration certificate SHALL contain at least one of the following: a) the URL of a web form provided by the DPA, which Users can use to report suspicious attribute presentation requests. c) an e-mail address of the DPA, on which the DPA is prepared to receive reports about suspicious attribute presentation requests from Users, c) a telephone number of the DPA, on which the DPA is prepared to receive reports about suspicious attribute presentation requests from Users. *Note: See Topic 50 for more information about reporting suspicious attribute presentation requests.*

C. Requirements on the issuance of registration certificates to PID Providers and Attestation Providers

Index	Requirement specification
RPRC_13	A Registrar MAY decide that, during the registration process for PID Providers, QEAA Providers, PuB-EAA Provider, or non-qualified EAA Providers, as specified in Topic 27, a Provider of registration certificates associated to the Member State Registrar must create and sign or seal a registration certificate and issue it to the registering party. If so, that registration certificate SHALL comply with the requirements in the technical specification mentioned in RPRC_02.

Index	Requirement specification
RPRC_14	If, during registration, a PID Provider, QEAA Provider, PuB-EAA Provider, or non-qualified EAA Provider received a registration certificate, it SHALL distribute it to all its service supply points. *Note: a service supply point is a system at which a Wallet Unit can start the process of requesting and obtaining a PID or attestation.*
RPRC_15	The contents of a registration certificate issued to a PID Provider, a QEAA Provider, a PuB-EAA Provider, or a non-qualified EAA Provider SHALL contain the type(s) of attestation that this entity intends to issue to Wallet Units.

D. Requirements on the presentation and verification of registration certificates of Relying Parties

Index	Requirement specification
RPRC_16	Either after receiving a presentation request or as a general User setting, a Wallet Unit SHALL offer the User the possibility to indicate whether the User wants to verify the information registered by the competent Registrar about the Relying Party the User is interacting with.
RPRC_17	If the User indicated that they want to verify the information registered about the Relying Party and the Relying Party sent a registration certificate to the Wallet Unit, the Wallet Unit SHALL verify the authenticity and validity of the registration certificate according to the technical specification meant in RPRC_02. If the outcome of the verification is negative, the Wallet Unit SHALL, when asking for User approval according to RPA_07, notify the User that it could not obtain the information registered about the entity.

Index	Requirement specification
RPRC_18	If the User indicated that they want to verify the information registered about the Relying Party, but the Relying Party did not send a registration certificate to the Wallet Unit, the Wallet Unit SHALL connect to the URL of the online service of the Registrar to obtain this information. If the Wallet Unit cannot connect to this URL or if it cannot verify the authenticity and validity of the registered information, it SHALL, when asking for User approval according to RPA_07, notify the User that it could not obtain the information registered about the Relying Party. *Note: If the Relying Party does not use the services of an intermediary, the URL of the Registrar is included in the access certificate received by the Wallet Unit, see Reg_33. If the Relying Party uses an intermediary, this URL is included in the received registration certificate if available (see RPRC_04a) or directly in the presentation request if no registration certificate is available (see RPI_06).*
RPRC_19	If a Relying Party Instance received one or more registration certificates (see RPRC_10), it SHALL include a single registration certificate applicable for its current intended use in each presentation request to a Wallet Unit, according to the applicable standard's extension mentioned in RPRC_20. The registration certificate SHALL be included in the request by value, not by reference. The Relying Party Instance SHALL do so both in proximity and remote presentation flows. *Note: - This ensures that no external requests are necessary to validate the Relying Party, and that presentation transactions are atomic and self-contained.*

Index	Requirement specification
RPRC_19a	If a Relying Party Instance did not receive a registration certificate, it SHALL include in each presentation request a) a User-friendly description of the Relying Party's intended use, b) the URL of its Registrar, and c) the identifier of the intended use. *Note: including a) enables the Wallet Unit to inform the User about the intended use even in case there is no registration certificate. Including b) and c) enables the Wallet Unit, if desired by the User, to request from the Registrar the attributes registered by the Relying Party for this intended use, as well as the corresponding privacy policy and other registered information. See Technical Specification 5 for the definition of this information.*
RPRC_20	The Commission SHALL ensure that extensions are specified for [ISO/IEC 18013-5] and for [OpenID4VP], allowing a Relying Party to transfer a single Relying Party registration certificate to a Wallet Unit in a presentation request. These extensions SHALL comply with applicable requirements in these standards. *Note: It must not be possible to include multiple registration certificates in a single presentation request.*

Index	Requirement specification
RPRC_21	If the User indicated that they want to verify the information registered about a Relying Party and the Wallet Unit retrieved this information either from the registration certificate or from the online service of the Registrar (see RPRC_16 - RPRC_18), it SHALL verify that all attributes requested in the presentation request are included in the list of attributes registered by the Registrar. If the outcome of the verification is negative, the Wallet Unit SHALL, when asking for User approval according to RPA_07, notify the User about the requested attributes that the Relying Party did not register.

F. Requirements on the presentation and verification of registration certificates of PID Providers and Attestation Providers

Index	Requirement specification
RPRC_22	If a PID Provider or Attestation Provider received a registration certificate (see RPRC_14), it SHALL include the registration certificate in its Issuer metadata used in the common OpenID4VCI protocol referenced in ISSU_01. The registration certificate SHALL be included in the metadata by value, not by reference. *Notes: - This ensures that no external requests are necessary to validate the PID Provider or Attestation Provider, and that issuance transactions are atomic and self-contained. - See also ISSU_22 - ISSU_22b and ISSU_32 - ISSU_32b.*

Index	Requirement specification
RPRC_23	A Wallet Unit SHALL verify that the type of attestation it wants to request from the PID Provider or Attestation Provider is registered by the Registrar, according to ISSU_24a for PID Providers and ISSU_34a for Attestation Providers. *Note: Unlike for Relying Parties, see RPRC_21, the Wallet Unit always carries out this verification, regardless of the preference of the User set as per RPRC_16.*

A.2.3.45 Topic 45 - QEAA Rulebook

See Topic 12.

A.2.3.46 Topic 46 - Protocols and interfaces for Presentation of PID and (Q)EAA with Relying Parties

See Topic 1 and Topic 12.

A.2.3.47 Topic 47 - Protocols and interfaces for PID and (Q)EAA issuance, and (non-)qualified certificates issuance

See Topic 10/23.

A.2.3.48 Topic 48 - Blueprint for requesting data deletion to Relying Parties

Description

In this use case, a User requests the deletion of their personal attributes from Relying Parties with which they have interacted through their Wallet Unit.

Users are concerned about having control over their personal data, thus the function of requesting data deletion ensures a higher degree of transparency, privacy and control of the Users over their personal data.

This Topic lists high-level requirements related to the function of Users requesting the deletion of their personal data from Relying Parties through their Wallet Unit.

Note: A Relying Party may use the services of an intermediary to request data from a Wallet Unit, see Topic 52. However, such intermediaries are required to delete any data they obtain from a Wallet Unit immediately after sending it to the Relying Party. Data deletion requests are therefore always sent to the Relying Party, not the intermediary.

HLRs

Index	Requirement specification
DATA_DLT_01	A Wallet Provider SHALL ensure that its Wallet Units support the possibilities mentioned in DATA_DLT_02, allowing a User to request from a Relying Party the erasure of their attributes that were presented by that Wallet Unit to that Relying Party, in accordance with Article 17 of Regulation (EU) 2016/679.
DATA_DLT_02	A Wallet Unit SHALL support at least the following possibilities to send a data erasure request to a Relying Party: a) Open a URL in an external browser to ask for the deletion of data in a web form provided by the Relying Party, b) Open an external mail client and start a draft e-mail to the Relying Party, with a suitable template text, c) open an external phone client and start a phone call. Depending on whether a Relying Party URL, e-mail address, and/or phone number was logged for the relevant attestation presentation transaction (see requirement DASH_03 in Topic 19), the Wallet Unit SHALL offer the User to use one or more of these possibilities.

Index	Requirement specification
DATA_DLT_02a	If the User initiates sending a data erasure request for a particular attestation presentation transaction, but no Relying Party URL, e-mail address, or telephone number is available in the log for that transaction, the Wallet Unit SHALL connect to the URL of the online service of the Registrar indicated in the log to obtain this information. The Wallet Unit SHALL inform the User that it must connect to the Registrar to look up the contact information it needs to send a data deletion request. *Note: this situation may occur if there was no registration certificate in the presentation request and the User did not request the Wallet Unit to obtain the information registered about the Relying Party from the Registrar. See RPRC_16 - RPRC_18 in Topic 44.*
DATA_DLT_03	A Wallet Instance SHALL provide a function where the User may select one Relying Party to which a data deletion request must be submitted.
DATA_DLT_04	Empty
DATA_DLT_05	A Wallet Unit SHALL include the initiation of a data deletion request in a log, so it can be displayed to the User via the dashboard as specified in Topic 19. *Note: Because the request is sent by an external web browser, e-mail client, or phone client (see DATA_DLT_02), the Wallet Unit can only log the initiation of the request.*
DATA_DLT_06	For the initiation of a data deletion request, the log SHALL contain at least: - Date and time of the initiation of the request, - Name and unique identifier of the Relying Party to which the request was made, - Attributes requested to be deleted.

Index	Requirement specification
DATA_DLT_07	Before executing a data deletion request, a Relying Party SHALL authenticate the requesting User (or the request itself), using appropriate authentication mechanisms of its own choosing. The Relying Party SHOULD use the authentication or signature facilities offered by the User's Wallet Unit for this purpose.
DATA_DLT_08	Wallet Units, Relying Parties, and Registrars SHALL comply with the relevant requirements in Technical Specification 7.

A.2.3.49 Topic 49 - Protocol and interfaces for requesting data deletion to relying parties

Deleted.

A.2.3.50 Topic 50 - Blueprint to report unlawful or suspicious request of data

Description

In this use case, a User reports a Relying Party to the competent national data protection authority, because the User claims that this Relying Party sent an unlawful or inappropriate request for attribute to the Wallet Unit. Users are concerned about having control over their personal data, and specifically about a Relying Party over-asking for personal information, thus the function of reporting suspicious or inappropriate requests ensures a higher degree of transparency, privacy and control of the Users over their personal data.

This topic lists high-level requirements related to the function of Users reporting unlawful or inappropriate attribute requests from Relying Parties.

HLRs

Index	Requirement specification
RPT_DPA_01	A Wallet Unit SHALL enable the User to start the process of reporting a suspicious presentation request to a DPA. When prompted by the User, a Wallet Unit SHALL provide the contact details of the DPA which supervises the Relying Party that made the suspicious request, if available in the log for that request (see DASH_03). If the contact details of the supervising DPA are not available in the log, the Wallet Unit SHALL provide the contact details of the DPA of the region in which the Wallet Provider is residing. In addition, the Wallet Unit MAY also provide the contact details of other DPAs, taken from the “European Data Protection Board” website (https://www.edpb.europa.eu/about-edpb/about-edpb/members_en). *Note: The DPA contact details may be unavailable in the log if there was no registration certificate in the presentation request and the User did not request the Wallet Unit to obtain the information registered about the Relying Party from the Registrar. See RPRC_16 - RPRC_18 in Topic 44.*
RPT_DPA_02	The Wallet Unit SHALL offer the User the option to report a suspicious request to a DPA via the transaction log presented in the dashboard, see Topic 19.
RPT_DPA_02a	A Wallet Unit SHALL support at least the following possibilities to report a suspicious presentation request to a DPA, depending on what contact details are available for the DPA: a) Open a URL in an external browser to report the request in a web form provided by the DPA. b) Open an external e-mail client and start a draft e-mail to the DPA, with a suitable template text, c) open an external phone client and start a phone call.
RPT_DPA_03	Empty

Index	Requirement specification
RPT_DPA_04	A Wallet Provider SHALL ensure that a Wallet Unit allows its User to substantiate a report sent to a DPA, including by attaching relevant information to identify the Relying Party and the Users' claims in a machine-readable format. *Note: The log kept by the Wallet Unit will be standardized and is machine-readable in order to enable data portability. An excerpt from this log therefore can be used to substantiate the report.*
RPT_DPA_05	A Wallet Unit SHALL log the fact that it initiated the sending of a report to a DPA (see RPT_DPA_02a), as specified in Topic 19.
RPT_DPA_05a	For a report sent to a DPA, the log SHALL contain at least: a) the date and time when the report was sent, b) the name and country of the DPA, and c) the channel and contact information used for initiating sending the report, i.e., the URL, e-mail address, or phone number of the DPA.
RPT_DPA_06	Wallet Units, Data Protection Authorities, and Registrars SHALL comply with the relevant requirements in Technical Specification 8.

A.2.3.51 Topic 51 - PID or attestation deletion

Description

This topic lists high-level requirements related to a User deleting a PID or attestation from their Wallet Unit.

HLRs

Index	Requirement specification
PAD_01	A Wallet Unit SHALL at any time enable the User to delete any PID or attestation from their Wallet Unit.
PAD_02	If the User indicates that a PID or attestation must be deleted, and the Wallet Unit contains multiple PIDs or attestation having the corresponding attestation type and Provider, a Wallet Unit SHALL delete all of these PIDs and attestations simultaneously. *Note: This situation may occur if the PID Provider or Attestation Provider issued a batch of attestations to the Wallet Unit, rather than a single one.*
PAD_03	If the Wallet Unit deletes a PID or attestation on the User's request, the Wallet Unit SHALL NOT notify the respective PID Provider or Attestation Provider. *Note: This is a matter of User privacy.*
PAD_04	If the Wallet Unit deletes a PID or device-bound attestation on the User's request, the Wallet Unit SHALL ensure that all cryptographic key material in the WSCA/WSCD related to this PID or attestation is securely destroyed. *Note: Key deletion is a cryptographic key operation and requires User authentication, as specified in requirement WIAM_14.*
PAD_05	If a Wallet Unit supports the [W3C Digital Credentials API] and it deletes a PID or attestation on the User's request, the Wallet Instance SHALL disclose the fact that it no longer stores this PID or attestation to the Digital Credentials API framework.

Index	Requirement specification
PAD_06	If the User uninstalls the Wallet Instance, the Wallet Instance SHALL request the associated WSCA(s) to delete all sensitive data and cryptographic keys related to the Wallet Unit and to all PIDs and device-bound attestations on the Wallet Unit, if the WSCA(s) are connected to the User device at the moment the Wallet Instance is uninstalled. *Note: It may happen there is no connection to the WSCA at the moment the User uninstalls the Wallet Instance; for instance, in case the WSCD is an external smart card and the User does not present that card to the User device. Another example occurs when the WSCD is a remote HSM and the User device is offline at the moment the User uninstalls the Wallet Instance. In such cases, the cryptographic keys will probably remain present on the WSCD, even though they will never be used again. If needed, it is up to the Wallet Provider to define how the Wallet Unit should handle such situations. For example, an HSM manager could address such cases by deciding to delete cryptographic keys in the HSM that are too old or haven't been used for too long, while being aware of the risks in doing so.*

A.2.3.52 Topic 52 Relying Party intermediaries

Description

This topic lists high-level requirements regarding so-called intermediaries, which form a special class of Relying Party. Article 5b (10) of the [European Digital Identity Regulation] states “Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction”. Such an intermediary is a party that offers services to Relying Parties to, on their behalf, connect to Wallet Units and request the User attributes that these Relying Parties need. The intermediary then performs all necessary verifications, and, if successful, sends the presented attributes to the intermediated Relying Party. This implies that an intermediary performs all tasks assigned to a Relying Party in this ARF on behalf of the intermediated Relying Party.

HLRs

Index	Requirement specification
RPI_01	An intermediary SHALL register as a Relying Party, in accordance with all requirements in Topic 27, while indicating it intends to act as an intermediary. *Notes: - This implies that an intermediary obtains an access certificate containing its own name and unique Relying Party identifier. - An intermediary may also obtain a registration certificate according to Topic 44, but this certificate will not be used for intermediated transactions. - An entity that registered as an intermediary may also register as a Relying Party in its own capacity. In such a case, it will receive one or more registration certificates for its intended use(s), and will use one of these certificates when interacting with a Wallet Unit.*
RPI_02	Empty
RPI_03	An intermediary SHALL register each intermediated Relying Party it is acting on behalf of at a Registrar in the Member State where the intermediated Relying Party is established, according all requirements in Topic 44. If a Provider of registration certificates associated with the Registrar issues registration certificates, the intermediary SHALL receive a registration certificate for each of the registered intended uses of the intermediated Relying Party.

Index	Requirement specification
RPI_04	When registering an intermediated Relying Party, an intermediary SHALL provide legally valid evidence that this Relying Party will indeed use the services of this intermediary to interact with Wallet Units. The Registrar SHALL verify this evidence, and, if it is found to be correct, SHALL register the relationship between the intermediary and the intermediated Relying Party. *Note: Such evidence may, for instance, be a contract between the intermediary and the intermediated Relying Party.*
RPI_05	When an intermediated Relying Party asks its intermediary to request some attributes from a Wallet Unit, it SHALL specify which registration certificate the intermediary must include in the presentation request. If the intermediated Relying Party does not have any registration certificates, it SHALL specify instead a) its user-friendly name, b) its unique identifier, c) the URL of its Registrar. d) the identifier of its intended use, e) a User-friendly description of its intended use. *Notes: - See RPI_06 for why this information is needed. - Since a), b) and c) will not change for each request, specification of this information can be done once. The same is true for d) and e) if the intermediated Relying Party has only one registered intended use.*

Index	Requirement specification
RPI_06	When requested by an intermediated Relying Party, an intermediary SHALL request a presentation of attributes from a specific Wallet Unit, using the intermediary's access certificate meant in requirement RPI_01 and the registration certificate of the Relying Party, as meant in RPI_03, if available. If no registration certificate is available, the intermediary SHALL include the following information about the intermediated Relying Party in an extension of the presentation request, according to RPI_06a: a) its user-friendly name, b) its unique identifier, c) a User-friendly description of its intended use, d) the URL of its Registrar, and e) the identifier of its intended use. *Note: Including a) and b) enables the Wallet Unit to show to the User the name of the intermediated Relying Party. Including c) enables the Wallet Unit to inform the User about the intended use.Including c) and d) enables the Wallet Unit, if desired by the User, to request from the Registrar the attributes registered by the Relying Party for this intended use, as well as the corresponding privacy policy and other registered information. See Technical Specification 5 for the definition of this information.*
RPI_06a	The Commission SHALL ensure that extensions are specified for [ISO/IEC 18013-5] and for [OpenID4VP], allowing a Relying Party to transfer the information listed in RPI_06 to a Wallet Unit. These extensions SHALL comply with applicable requirements in these standards.

Index	Requirement specification
RPI_07	In case a Wallet Unit receives a presentation request from an intermediary on behalf of an intermediated Relying Party, during the Relying Party authentication process it SHALL display the names and identifiers of both the intermediary and the intermediated Relying Party to the User when asking for User consent, as described in RPA_07. *Note: The Wallet Unit can see that a presentation request is from an intermediary either because this is indicated in the registration certificate or because the extension meant in RPI_06 and RPI_06a is present.*
RPI_07a	In case a Wallet Unit receives a presentation request from an intermediary on behalf of an intermediated Relying Party, and if the User indicated that they want to verify the information registered about this Relying Party (according to RPRC_16), and if a registration certificate is available, the Wallet Unit SHALL verify that the name and the unique identifier of the intermediary, as included in the registration certificate of the intermediated Relying Party (see RPI_05), are identical to the name and unique identifier in the access certificate. If this verification fails, the Wallet Unit SHALL notify the User when asking for User consent.

Index	Requirement specification
RPI_07b	In case a Wallet Unit receives a presentation request from an intermediary on behalf of an intermediated Relying Party, and if the User indicated that they want to verify the information registered about this Relying Party (according to RPRC_16), and if no registration certificate is available, the Wallet Unit SHALL connect to the URL of the online service of the Registrar of the intermediated Relying Party (as included in the request, see RPI_06) to obtain this information, using the unique identifier of the intermediated Relying Party. The Wallet Unit SHALL verify that the name and the unique identifier of the intermediary for this intermediated Relying Party, as registered by the Registrar, are identical to the name and unique identifier included in the access certificate. If this verification fails, the Wallet Unit SHALL notify the User when asking for User consent.
RPI_08	When a Wallet Unit presents to an intermediary any User attributes from a PID or attestation, the intermediary SHALL, after successfully carrying out the verifications in RPI_09, forward these attributes (only) to the Relying Party on behalf of which the presentation request was made. If any of the verifications in RPI_09 fail, the intermediary SHALL NOT forward any attributes to the Relying Party.

Index	Requirement specification
RPI_09	When a Wallet Unit presents to an intermediary any attributes from a PID or attestation, the intermediary SHALL verify the authenticity of the PID or attestation, its revocation status, device binding, and User binding, as well as any combined presentation of attributes, if applicable, as specified in this ARF and if agreed with the Relying Party. Furthermore, the intermediary SHALL verify the authenticity of the Wallet Unit and its revocation status, as specified in this ARF, if agreed with the Relying Party. *Note: This ARF does not mandate that a Relying Party must carry out all of these verifications. Therefore, the intermediary and any Relying Party using its services must agree on what verifications the intermediary will carry out.*
RPI_10	The intermediary SHALL delete any PIDs or attestations it obtained from the Wallet Unit, including any User attributes, completely and immediately after it has sent the User attributes to the intermediated Relying Party. If the intermediary does not send any User attributes to the intermediated Relying Party, for example because one of the verifications in the previous step failed, the intermediary SHALL delete the PIDs, attestations, or WUAs completely and immediately as soon as it has completed all necessary verifications.

A.2.3.53 Topic 53 Zero-Knowledge Proofs

Description

NOTE: Discussions on Zero-Knowledge Proofs are ongoing. No specific ZKP has been selected to be supported by components in the EUDI Wallet ecosystem. For an up-to-date discussion, see Technical Specification 4.

This topic lists high-level requirements for a Zero-Knowledge Proof scheme to be used within the EUDI Wallet ecosystem as a proof mechanism for PIDs and attestations. A Zero-Knowledge Proof (ZKP) is a cryptographic protocol that allows one party (the prover) to convince another party (the verifier) that a given statement is true without revealing any additional information beyond the validity of the statement itself. This ensures that the verifier gains no knowledge about how the prover knows the statement to be true, preserving privacy while enabling trust.

The topic of ZKPs for the EUDI Wallet ecosystem was introduced in the Discussion Paper for Topic G. The high-level requirements in this Topic were taken from that discussion paper.

HLRs

Index	Requirement specification
ZKP_01	A ZKP scheme SHALL provide support for the following generic functions, while hiding all attributes of PIDs or attestations: (i) generation of a proof that an (some) attribute(s) having a specific value is (are) included in a PID or attestation, (ii) generation of a proof that a PID or attestation is within its validity period, (iii) generation of a proof that a PID or attestation has not been revoked, and (iv) generation of a proof that a PID or a device-bound attestation is bound to a key stored in the WSCA/WSCD of the Wallet Unit. Additionally, a ZKP scheme SHOULD provide support for the following function, which SHOULD be used only when hiding the PID Provider or Attestation Provider is necessary: (v) generation of a proof that a PID or attestation has been issued by a trusted PID Provider or Attestation Provider, without revealing the PID Provider or Attestation Provider. *Note: See section 4.1.1 of the Discussion Paper for Topic G.*
ZKP_02	A ZKP scheme SHALL support proving possession of attestation of a given type. *Note: See section 4.1.2 and 4.1.3 of the Discussion Paper for Topic G.*

Index	Requirement specification
ZKP_03	A ZKP scheme SHOULD support the privacy-preserving binding of an attestation to a PID. In addition to the generic functions defined in ZKP_01, for this use case, a ZKP scheme SHALL provide support for the following functions: (i) generation of a proof that the Wallet Unit stores an attestation and a PID and that the attestation includes a specific attribute, having a specific value, which is also present in the PID. *Note: See section 4.1.4 of the Discussion Paper for Topic G.*
ZKP_04	A ZKP scheme SHOULD support the derivation of a verifiable User pseudonym, by combining an attribute value that is unique for the User with Relying Party-specific context (e.g., the Relying Party identifier) In addition to the generic functions defined in ZKP_01, for this use case, a ZKP scheme SHALL provide support for the following functions: (i) generation of a request for the issuance of an attestation that includes a secret attribute unique to the User, without revealing this attribute to the Attestation Provider, (ii) generation of an attestation presentation that includes a verifiable pseudonym derived from the secret attribute, a Relying Party identifier, and context-related information. *Note: See section 4.1.5 of the Discussion Paper for Topic G.*
ZKP_05	A ZKP scheme SHALL be usable in both remote and proximity presentation flows. While the inclusion of ZKP will introduce computational and verification delays, these delays SHALL NOT critically undermine or defeat the purpose of the Relying Party service (e.g. because of a critical impact on the User experience of the Wallet Unit).
ZKP_06	A ZKP scheme SHOULD be able to generate proofs for already issued PIDs and attestations in the formats specified in [ISO/IEC 18013-5] or [SD-JWT VC].

Index	Requirement specification
ZKP_07	A ZKP scheme SHALL NOT introduce any additional communication or information that could be used to track or link User activity during, before, or after proof generation.
ZKP_08	A ZKP scheme SHALL rely solely on algorithms standardised by a standardisation organisation recognised by the Commission or in a standard recognised by the Commission.
ZKP_09	Use of a ZKP scheme SHALL NOT prevent the Wallet Unit’s ability to provide User authentication with Level of Assurance High.

A.2.3.54 Topic 54 - Accessibility

Description

It is essential to ensure that Wallet Units are inclusive by design and fully aligned with the applicable European legal and technical frameworks on accessibility. This is not only a matter of legal compliance but also a fundamental component of ensuring equal access, User trust, and widespread adoption across all segments of the population, including persons with disabilities. For further discussion, please refer to Section 4.2.2 and Chapter 8 of the ARF main document.

HLRs

Index	Requirement specification
ACC_01	Wallet Providers SHALL ensure that their Wallet Units comply with applicable requirements and standards in Directive 2016/2012 on the accessibility of websites and mobile applications of public sector bodies, including European Standard ETSI EN 301 549 V1.1.2.
ACC_02	Wallet Providers SHALL ensure that their Wallet Units comply with accessibility requirements for products and services established under Directive (EU) 2019/882.

ANNEX 3.01 - PID Rulebook

The **PID rulebook** has been moved to a dedicated repository and is now available in the attestation rulebooks catalog on GitHub.

ANNEX 3.02 - mDL Rulebook

The **mDL rulebook** has been moved to a dedicated repository and is now available in the attestation rulebooks catalog on GitHub.

EUDI Wallet - Design Guide

For the EUDI Wallet ecosystem

November 2024 v1.1.0

This is a working document that holds no legal value and does not reflect any common agreement or position of the co-legislators. It presents a state-of-play of ongoing work of the eIDAS Expert Group. This document is being continuously updated and should not be considered final.

1 Introduction

1.1 Purpose of the design guide

This design guide outlines the principles, guidelines, and best practices for creating consistent and effective design solutions for the EUDI wallet. The purpose of a design guide is to ensure that all design work produced by a team or across different teams is consistent, coherent, adheres to certain standards and aligns with the overall goals and values of the project.

As many sections will be subject to national implementation this document includes guidelines to assist in creating a user interface that is useful, usable, and enjoyable to use. It also provides specific instructions and tips for creating accessible and inclusive designs.

1.2 Boundaries of the design guide

It shall be highlighted that this design guide does not aim to provide detailed design elements to be adopted by national EUDI Wallet implementations. Overall, the objective of the EUDI Wallet Design Guide is to:

- Identify key design principles and provide guidelines against these design principles;
- Identify specific areas of the EUDI Wallet for which design principles are considered important and expand on those in future iterations of the EUDI Wallet Design Guide.

The design guidelines listed in this document shall not be considered as mandatory towards the implementations of the EUDI Wallet, but rather stand as recommendations to ensure a common user experience across the different national implementations.

1.3 Importance of design consistency

UI (User Interface) consistency is important because it provides a better user experience and helps users navigate a mobile application more easily. When elements such as icons, colours, and fonts are consistent throughout an application, users can quickly learn how to use it and understand the application’s intention.

Familiarity

Consistent UI elements give users a sense of familiarity and they can feel more comfortable using the application. If the user interface changes too often, it can cause confusion and frustration.

Efficiency

Consistency in the user interface can make navigation easier and more efficient. Users will know where to find the features they need, and they reduce cognitive load.

Accessibility

Consistent UI elements make it easier for users with disabilities to navigate the application. Users with visual impairments, for example, can more easily use screen readers when consistent UI elements are used.

Overall, UI consistency is an essential aspect of good user interface design. It makes the application more user-friendly, efficient, and accessible.

1.4 Overview of design criteria

Twelve design criteria have been selected which we go over in details in 'Section 2'. The first 10 are the usability heuristics from the Nielsen Norman group. They are called "heuristics" because they are broad rules of thumb and not specific usability guidelines. These are used to evaluate a User Interface, so it is good to have them as guiding principles during the design phase as well. These 10 principles are:

- Visibility of system status
- Match between system and the real world
- User control and freedom
- Consistency and standards
- Error prevention
- Recognition rather than recall
- Flexibility and efficiency of use

- Aesthetic and minimalist design
- Help users recognize, diagnose, and recover from errors
- Help and documentation

An additional 2 were added to address these important areas:

- Accessibility
- Writing

---

2 Design criteria

```
Disclaimer: The design guidelines listed in this document shall not be
considered as mandatory towards the implementations of the EUDI Wallet, but
rather stand as recommendations to ensure a common user experience across the
different national implementations. Any design elements included in the
following chapter are indicative and are only used to better illustrate the
corresponding design criteria.
```

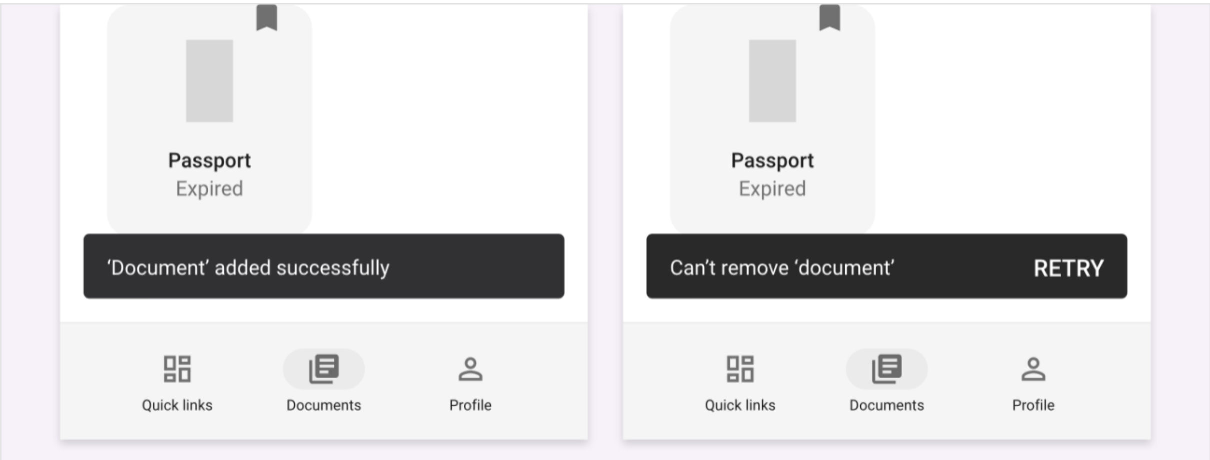
2.1 Visibility of system status

```
The design should always keep users informed about what is going on through
appropriate feedback within a reasonable amount of time.
```

2.1.1 Indicative examples

Document management

When adding or removing a document the application should let the user know whether the process was completed successfully of not.



'Document' added successfully

Can't remove 'document'

Figure 1: Document Management example

Interactive elements

Interactive elements such as buttons must have a pressed and focused state.

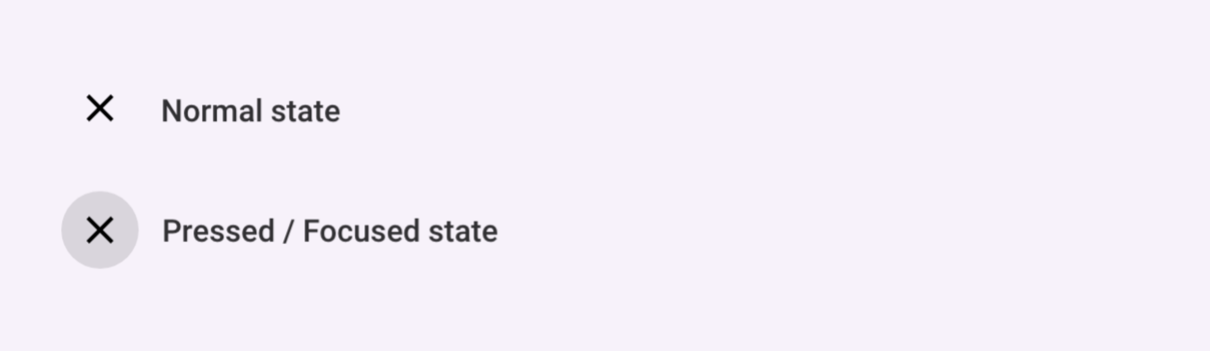


Figure 2: Interactive Elements example

2.2 Match between system and the real world

```
The design should speak the users' language. Use words, phrases, and concepts
familiar to the user, rather than internal jargon. Follow real-world
conventions, making information appear in a natural and logical order.
```

2.2.1 Indicative examples

Document representation

Documents should be (where possible) represented in the UI by what is familiar to the user instead of generic / ambiguous icons.

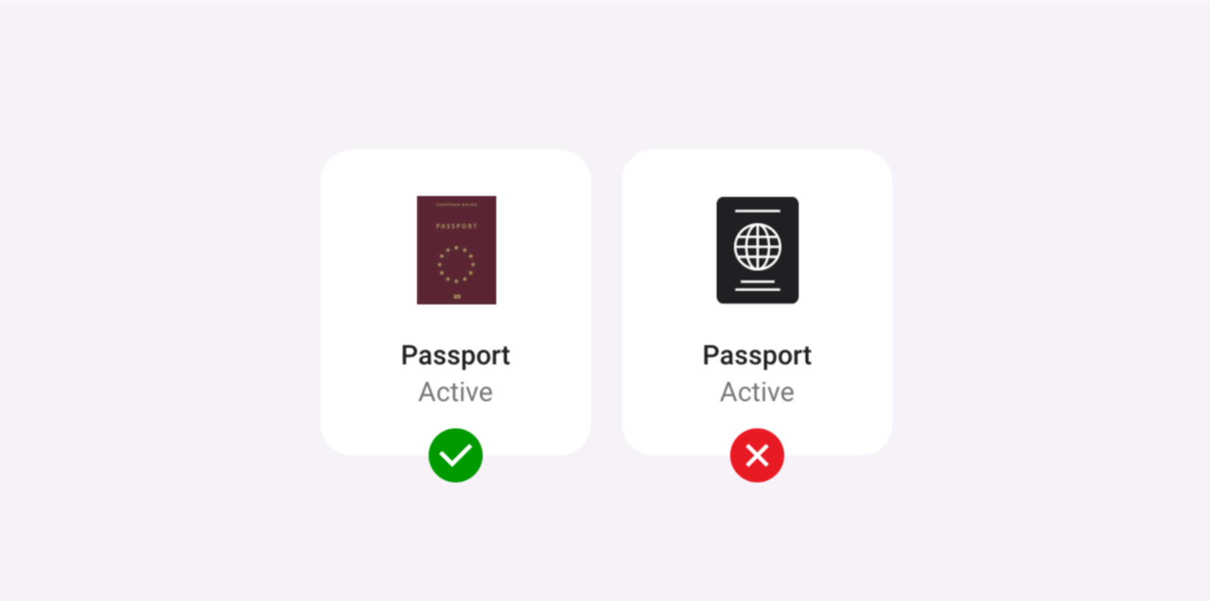


Figure 3: Document Presentation Example

Labels

Stay away from technical terms and jargon. Use labels that people use in their everyday life.

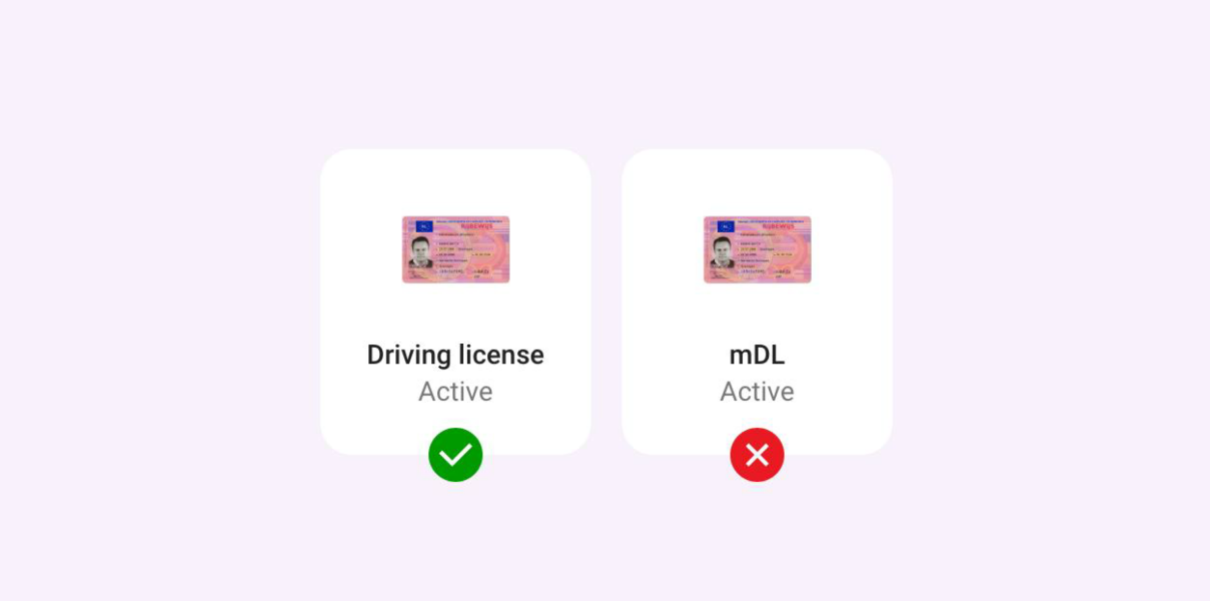


Figure 4: Labels example

Icons

People spend most of their time in other apps/websites. Use icons that are familiar and clear to them instead on ambiguous ones.

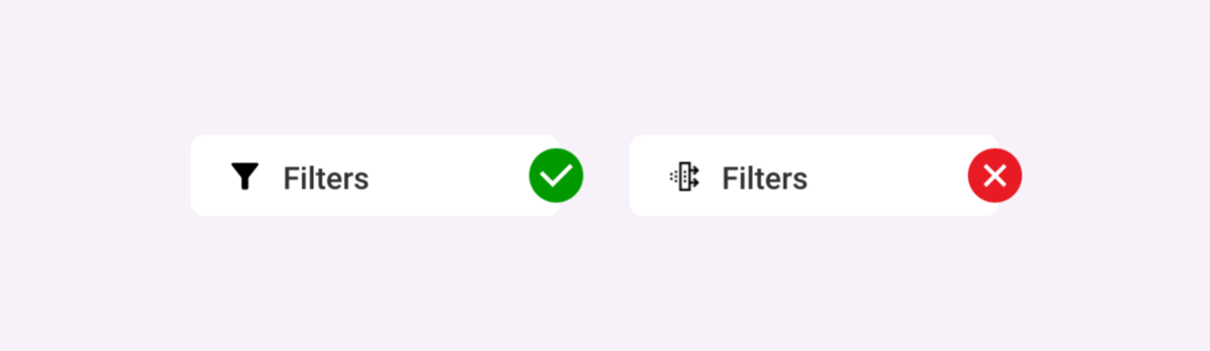


Figure 5: Icons Example

2.3 User control and freedom

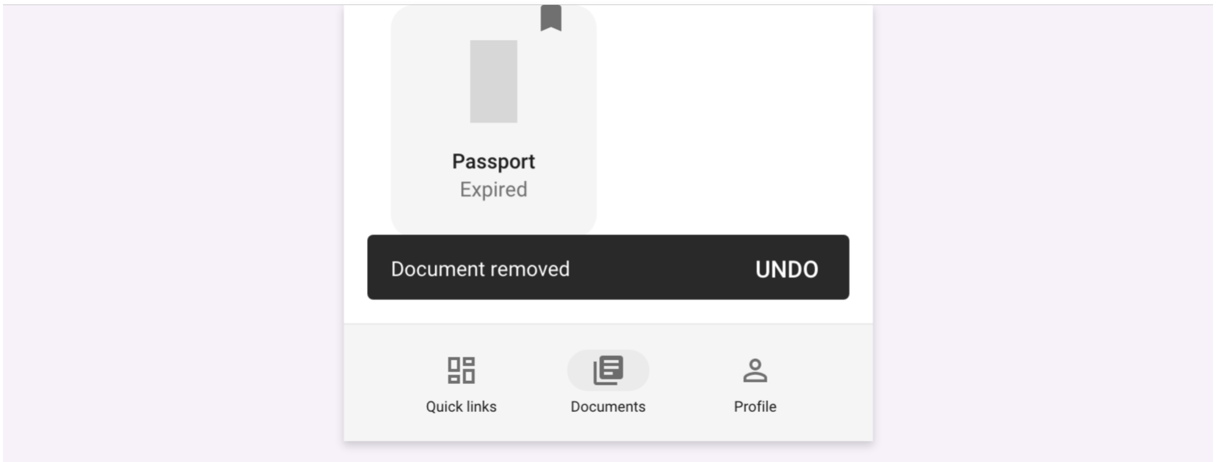
```
Users often perform actions by mistake. They need a clearly marked "emergency
exit" to leave the unwanted action without having to go through an extended
process.
```

2.3.1 Indicative examples

Undo & Redo

The third principle talks about giving the freedom to the user to navigate and perform actions

- for instance, the freedom to undo or redo any accidental moves



Document removed

Figure 6: Undo and Redo Example

2.4 Consistency and standards

```
Users should not have to wonder whether different words, situations, or actions
mean the same thing. Follow platform and industry conventions.
```

App should follow interface standards and platform conventions. Conventions have been established that users are familiar with. This knowledge should be capitalised upon to make the app have a higher level of intuitiveness.

E.g. Position of menu, Navigation bar, Search location

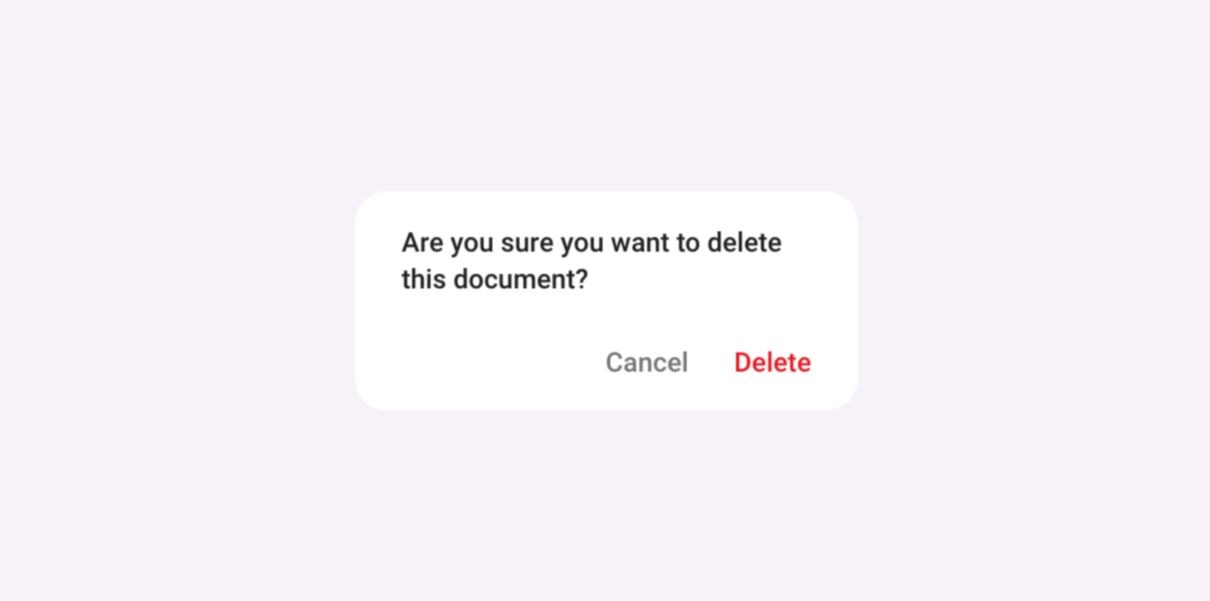
2.5 Error prevention

```
Good error messages are important, but the best designs carefully prevent
problems from occurring in the first place. Either eliminate error-prone
conditions or check for them and present users with a confirmation option before
they commit to the action.
```

2.5.1 Indicative examples

Confirmation dialogue

For accidental actions such as miss-clicks

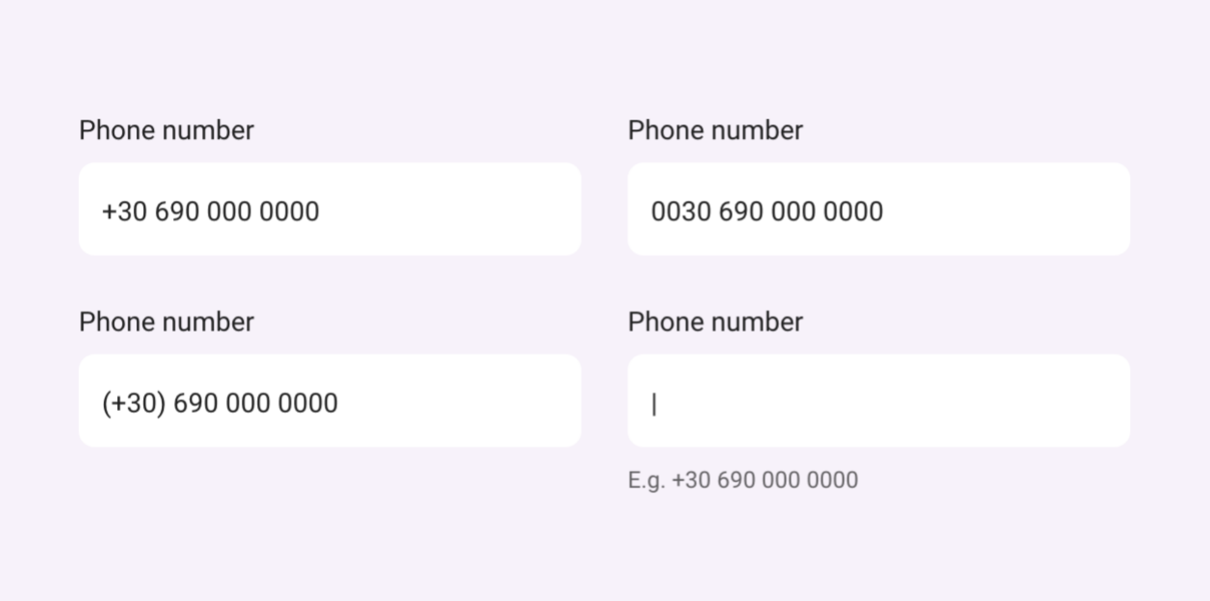


Are you sure you want to delete this document?

Figure 7: Confirmation Dialogues Example

Flexible inputs

Flexible inputs allow people to answer questions the way they want instead of the way a database requires them to. But these input fields come with a promise to users: “whatever format you choose, we’ll take it.” For example, a phone number can be entered in various ways by different people. The field can either format it accordingly on each own or provide a hint of the expected format instead of producing in-line errors or result in guesswork.



Phone number: +30 690 000 0000

Phone number: 0030 690 000 0000

Phone number: (+30) 690 000 0000

Phone number: |

E.g. +30 690 000 0000

Figure 8: Flexible Inputs Example

2.6 Recognition rather than recall

```
Minimize the user's memory load by making elements, actions, and options
visible. The user should not have to remember information from one part of the
interface to another. Information required to use the design (e.g. field labels
or menu items) should be visible or easily retrievable when needed.
```

2.7 Flexibility and efficiency of use

```
Offer shortcuts quick ways to get one or more tasks done with your apps. They
should speed up the interaction with an app for the expert user
```

2.7.1 Indicative examples

It's possible to improve the efficiency of interaction with an app for experienced users with ways that will allow them to complete frequent actions faster.

Bookmarked or Recently used documents on homepage

Users can customise their home screens with the documents most relevant for them.

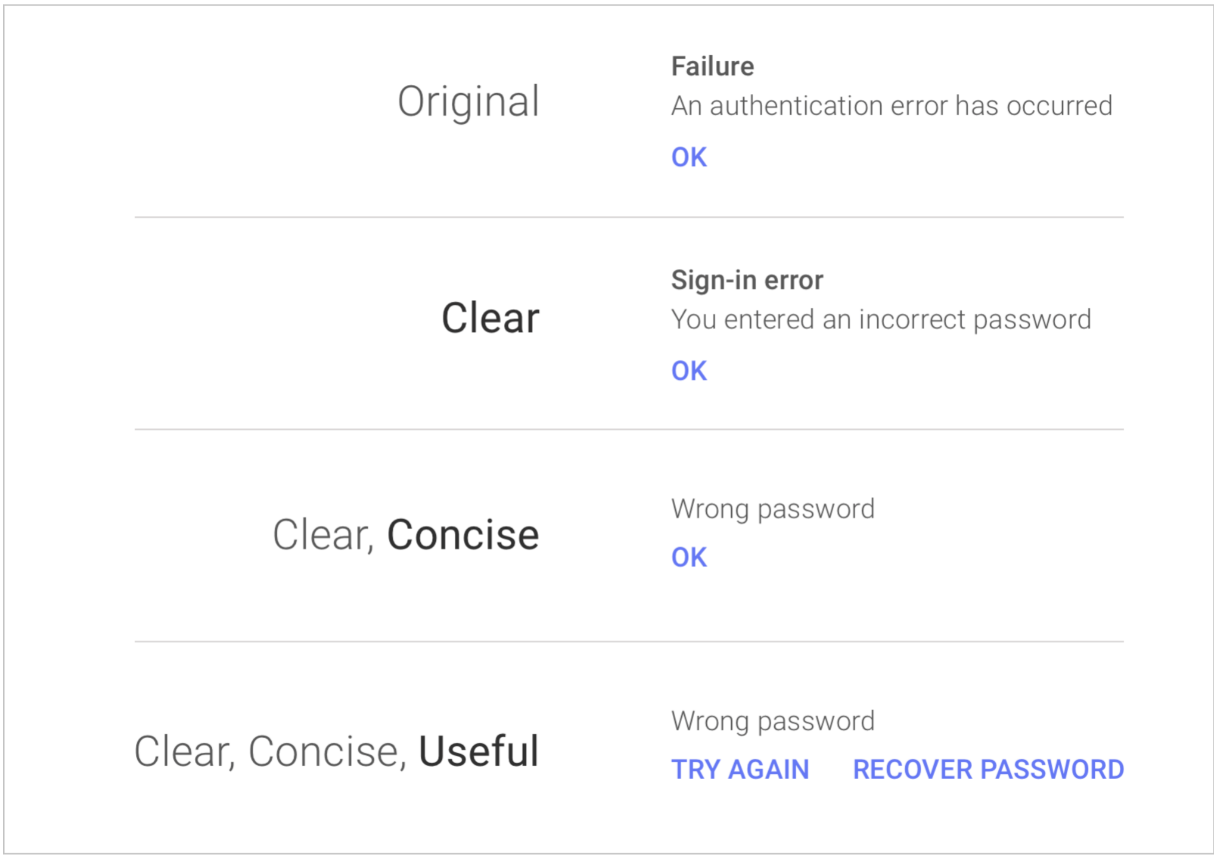
2.8 Aesthetic and minimalist design

```
Interfaces should not contain information which is irrelevant or rarely needed.
Every extra unit of information in an interface competes with the relevant units
of information and diminishes their relative visibility. Use whitespace in
harmony with your content.
```

2.9 Help users recognize, diagnose, and recover from errors

```
Error messages should be expressed in plain language (no error codes), precisely
indicate the problem, and constructively suggest a solution.
```

2.9.1 Indicative examples



Failure
An authentication error has occurred

Sign-in error
You entered an incorrect password

Wrong password

Wrong password

Figure 9: Error Messages Examples

2.10 Help and documentation

```
It's best if the system doesn't need any additional explanation. However, it may
be necessary to provide documentation to help users understand how to complete
their tasks.
```

2.10.1 Indicative examples

This can come in the form of App-onboarding, tutorials, F.A.Q.s or a Help section.

2.11 Accessibility

An estimated 100 million people in the EU have some form of disability, and so represent an important segment of its population and a large user group.

With Europe's ageing population this number is only going to rise. Keeping this in mind, it is important to distinguish accessibility from disabilities. Accessibility in this case, refers to making a website accessible to users who due to their temporary or permanent condition, their age, or their situation may face issues with accessing website content. For example, individuals with reduced manual dexterity due to injury or neurological conditions (permanent), or with an injured arm (temporary), or a new parent holding a baby (situational) all experience difficulties that may impede movement, coordination, or sensation or what is most commonly referred to as motor disability. Therefore, it concerns a much wider audience that one may initially think. The definition of disability differs as the term disability refers to 'long- term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder a person's full and effective participation in society on an equal basis with others. By delivering the user experience in a way that is accessible to people with the aforementioned needs, we are providing equal access to information for all citizens regardless of their situation or condition.

2.11.1 Layout

Aim to have at least the main controls for the app at the bottom half of the screen when they are easily reachable with the thumb when operating the phone with one hand. The top half should be used for displaying information, documents, QR codes etc.

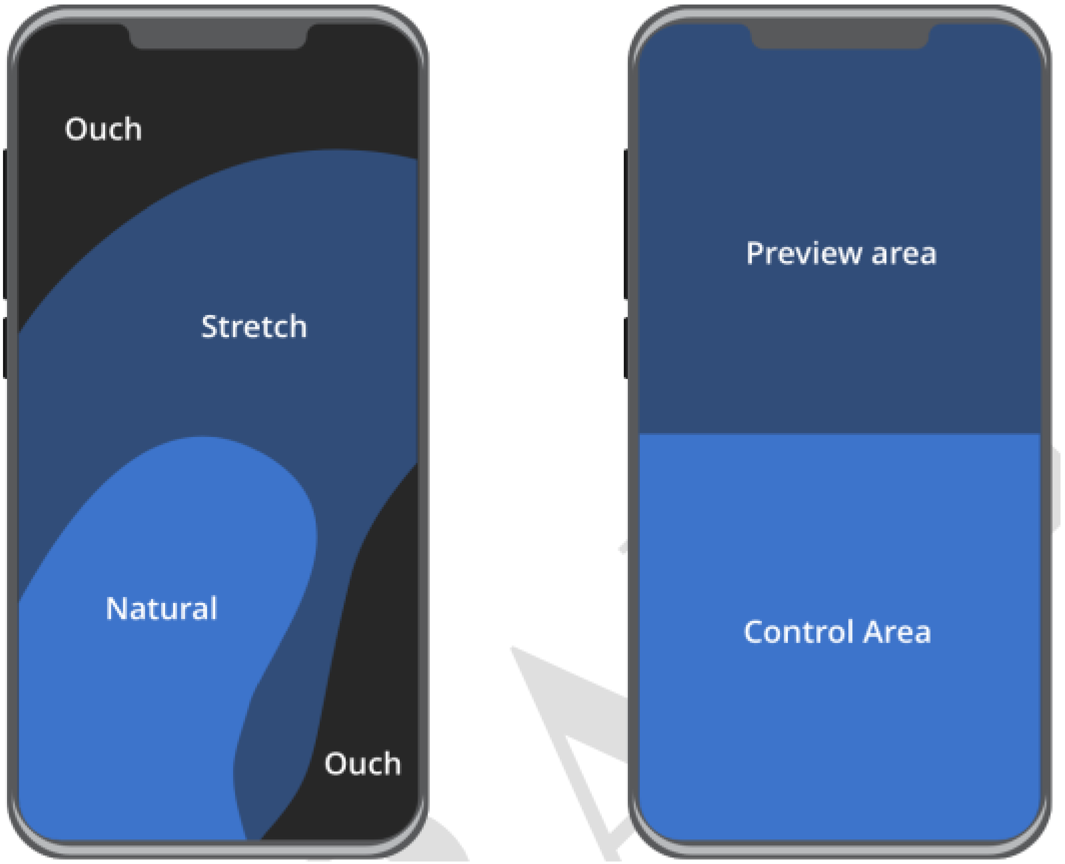


Figure 10: Layout

2.11.2 Target sizes

A target size is the area that can be activated in order to interact with an element. Individuals with dexterity challenges may find it more challenging to utilize a website if the target size is smaller. In this section, we'll examine methods (Apple's HIG and Google's Material) for generating target sizes that are user-friendly, uniform, and properly spaced. A person's ability to interact with smaller controls may be impacted by a disability or a combination of disabilities that affect their motor movements and dexterity, as well as by the act of using a website while on the move, such as while walking or commuting.

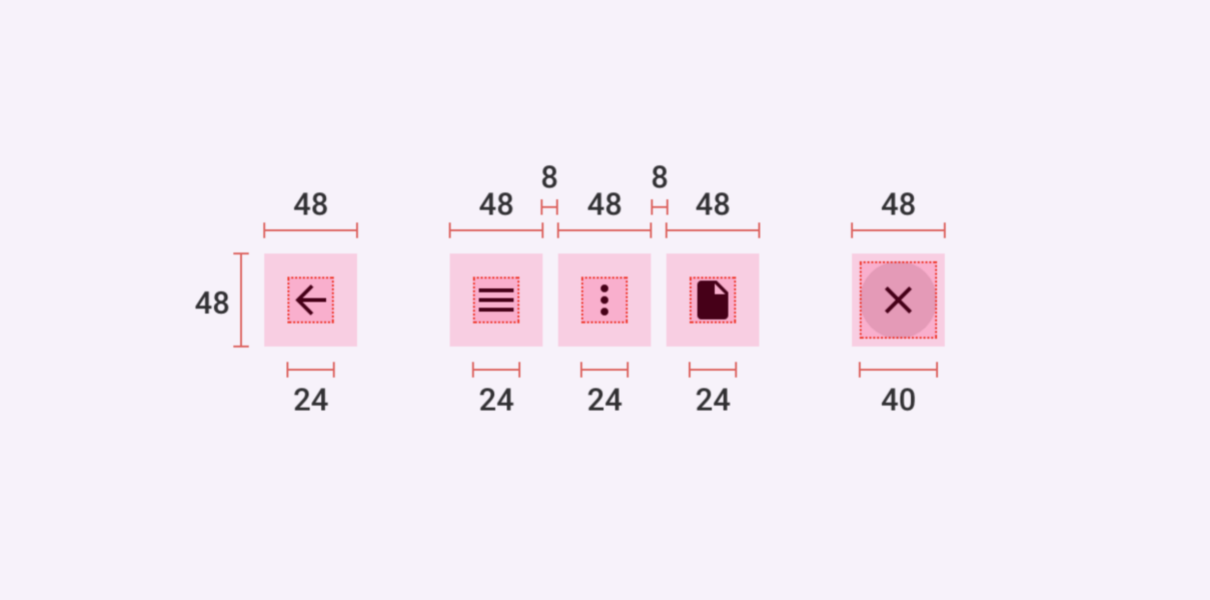


Figure 11 : Target Sizes

2.11.3 Colour contrast guidelines

Text to background colour contrast should meet a 4.5:1 ratio.

How to check: enter the hex codes for the foreground and background colours using: https://whocanuse.com/

2.11.4 Font size guidelines

The UI should be designed to support up to x 2 the text size without breaking.

2.11.5 Animations

Avoid adding flashing, blinking, and rotating animations on the background. Excessive screen movement with no mechanism to control can make it difficult for users to gather information.

Animations and transitions should be:

- **Informative** (Motion design informs users by highlighting relationships between elements, action availability, and action outcomes.)
- **Focused** (Motion focuses attention on what's important, without creating unnecessary distraction.)
- **Expressive** (Motion celebrates moments in user journeys, adds character to common interactions, and can express a brand's style.)

2.11.6 Screen readers

Make sure you provide the relative support for screen readers. Consider how the reader is going to read the screen and place items accordingly for convenience. In case of having to read through a lot of content to get to the main controls, consider providing a skip button.

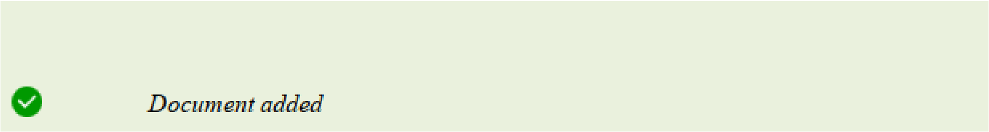
2.12 Writing

Text should be understandable by anyone, anywhere, regardless of their culture or language. UI text can make interfaces more usable and build trust. Text should be clear, accurate, and concise.

2.12.1 Write in the present tense

Use the present tense to describe product behaviour. Avoid using the future tense as this usually requires later updates.

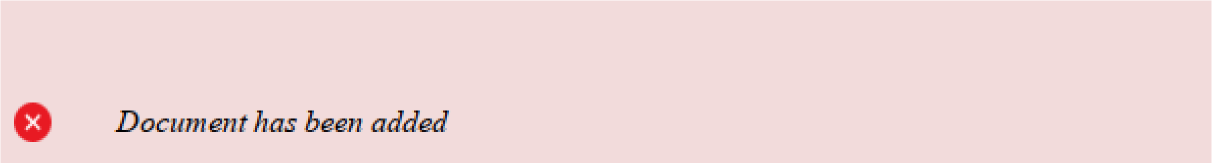
Use the present tense to describe product behaviour. Avoid using the future tense to describe the way a product always acts. When you need to write in the past or future tenses, use simple verb forms. This may not be applicable to all languages; the overall goal is to be as concise as possible without compromising clarity.



✓ *Document added*

Figure 8: Example showing “Document added” text

Write in the present tense.



✕ *Document has been added*

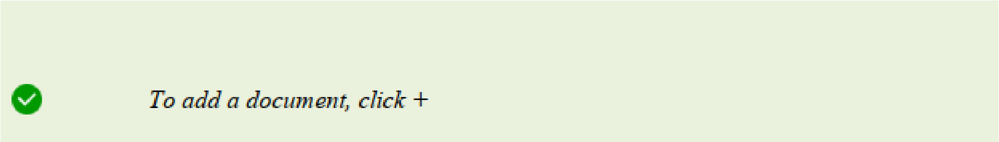
Figure 9: Example showing “Document has been added” text

Don’t write in different variations of the present tense, such as the present perfect tense.

2.12.2 Begin with the objective

When a phrase describes a goal and the action needed to achieve it, start the sentence with the goal.

```
To add a document, click +
```

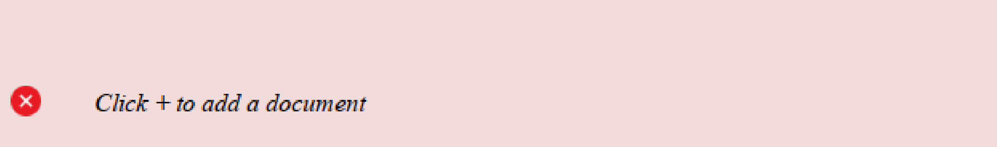


✓ *To add a document, click +*

Figure 10: Example showing “To add a document, click +” text

Start a statement with the objective (“to add a document”) and end it with the user action (“click +”).

```
Click + to add a document
```



✗ *Click + to add a document*

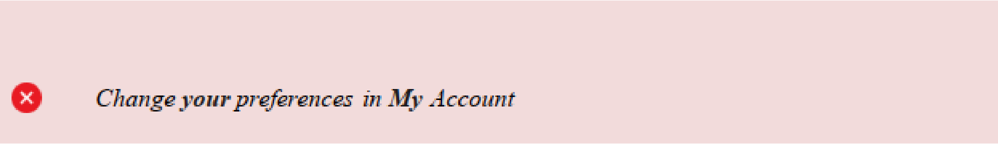
Figure 11: Example showing “Click + to add a document” text

Don’t state the action the user takes (“Click +”) before the objective (“to add a document”).

2.12.3 Avoid combining first and second person

To avoid confusing the user, avoid using “me” or “my,” and “you” or “your,” in the same phrase.

```
Change your preferences in My Account
```

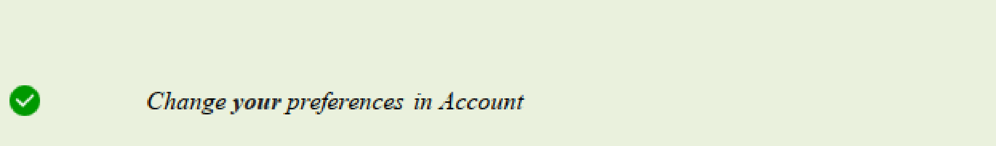


✗ *Change your preferences in My Account*

Figure 12: Example showing “Change your preferences in My Account” text

Don’t refer to the user in both the second person and the first person within the same phrase.

```
Change your preferences in Account
```



✓ *Change your preferences in Account*

Figure 13: Example showing “Change your preferences in Account” text

---

3 EUDI Wallet - Design Considerations

This section lists specific areas/features on which design considerations are deemed important to ensure a common user experience across the national implementations of the EUDI Wallets. It shall be noted that this list highlights specific areas which are prioritised as important but does not aim to be an exhaustive list.

3.1 User authentication

- Covering common user authentication aspects, e.g. PIN, biometrics etc.
- Exploring the balance between the corresponding security aspects comparing to the user friction points throughout the entire user flow (e.g. required only at the point of sharing data? Or at login as well?)
- *Guidelines around 'user consent'* in data sharing scenarios (e.g. requesting user consent, enforcing trust)

3.2 Browsing credentials/documents

- Guidelines in relation to displaying a list of credentials/attestations in the EUDI Wallet

---

3.3 QR code presentation

- Guidelines in relation to presenting the QR code for the corresponding proximity use cases

---

3.4 Confirmation/Summary/Authentication results

- Guidelines in relation to the authentication results presentation, i.e. successful/unsuccessful identification and authentication
- Guidelines in relation to data transfer results for proximity sharing use cases, i.e. successful/unsuccessful data transfer)
- Covering guidelines related to the confirmation/summary results presented to the user

---

3.5 Error Messages

- Handling/Display of error messages in different scenarios
  - Erroneous user credentials
  - User is not authenticated.
  - Document is considered invalid.
  - Relying party is not considered trusted.
- Principles/guidelines on how these shall be presented/structured etc.

3.6 Privacy/Security by Design

- Covering applicability of privacy/security aspects in the data sharing process (e.g. visual representation _of 'password' field)

3.7 Trust Mark

- Establish trust through the use of the EUDI Wallet Trust Mark
- Applicability and placement in the corresponding sharing processes

---

3.8 Notification guidelines

- Guidelines in relation to displaying user notifications (where applicable) in the EUDI Wallet

4 Conclusion

In conclusion, this EUDI Wallet Design Guide document represents the first iteration of what intends to be a 'living' document, which will be further elaborated for the specificities of the EUDI Wallet functionalities, as listed in section 3 of the document. As such, it is recognized that there may be areas for further elaboration and analysis on which feedback and improvement suggestions from stakeholders is anticipated.

Taking into consideration that the EUDI Wallet Design Guide shall be applicable for the national implementations of the EUDI Wallet, the boundaries of this document are set to common principles that shall be applicable to all national implementations. These shall be considered as recommendations to ensure a similar user experience across the different national implementations. By taking a collaborative approach and continuously improving upon this document, the aim is to create a EUDI Wallet Design Guide that assists in the national implementations, while at the same time meets the user expectations. We encourage stakeholders to review this EUDI Wallet Design Guide document thoroughly and kindly provide feedback that will assist if further shaping this design guide.

EUDI WALLET DESIGN GUIDE - DATA SHARING SCENARIOS

v1.11.0

1 Situations for Identification/Authorization

In alignment with section '6.4' of the Architecture Reference Framework (ARF), there are four main types of flows that the EUDI Wallet must support. These main flows are as follows:

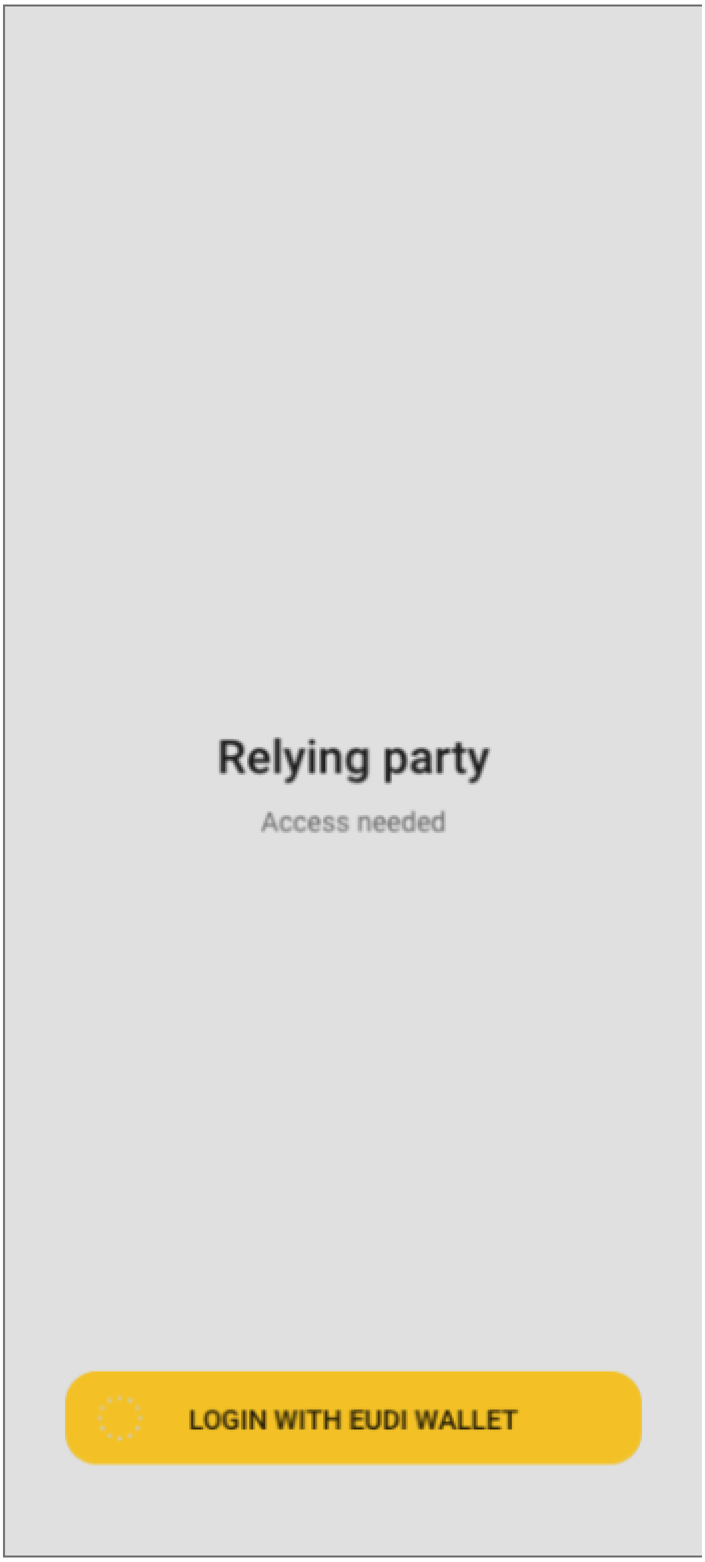
- Remote same-device flow

- Remote cross-device flow
- Proximity supervised flow
- Proximity unsupervised flow

It shall be noted that remote supervised cases are also considered as possible in some use cases, but the document focuses mainly on the types of flows detailed in the ARF, as listed in the above list.

The 'EUDI Wallet Design Guide' aims to expand on the defined 'Service Blueprints' (published in 'ARF v1.1.0' where the focus is on the 'remote same-device' and 'proximity' flows. However, design interactions applicable for the 'remote cross-device' flow will also be analysed at a high-level.

In relation to the remote flows, it shall be noted that the data exchange occurs over the Internet, but the key differentiator is related to the devices being utilized in the flows. In the 'remote same-device' flow, the EUDI Wallet User is on a mobile device, requesting access to a Relying Party's service (i.e. app or browser) and authorizes by using the EUDI Wallet app, which is also installed on the same device.



Relying party

Access needed

Figure 14: Login interface showing EUDI Wallet login button on mobile device

In contrast, in the ‘remote cross-device’ flow, the EUDI Wallet user consumes information from a Relying Party service on another device than the EUDI Wallet device, e.g. user visits the relying party’s service on their web browser on a PC and uses the EUDI Wallet app to scan a QR Code on a login page in order to get access to a service provided by the Relying Party.

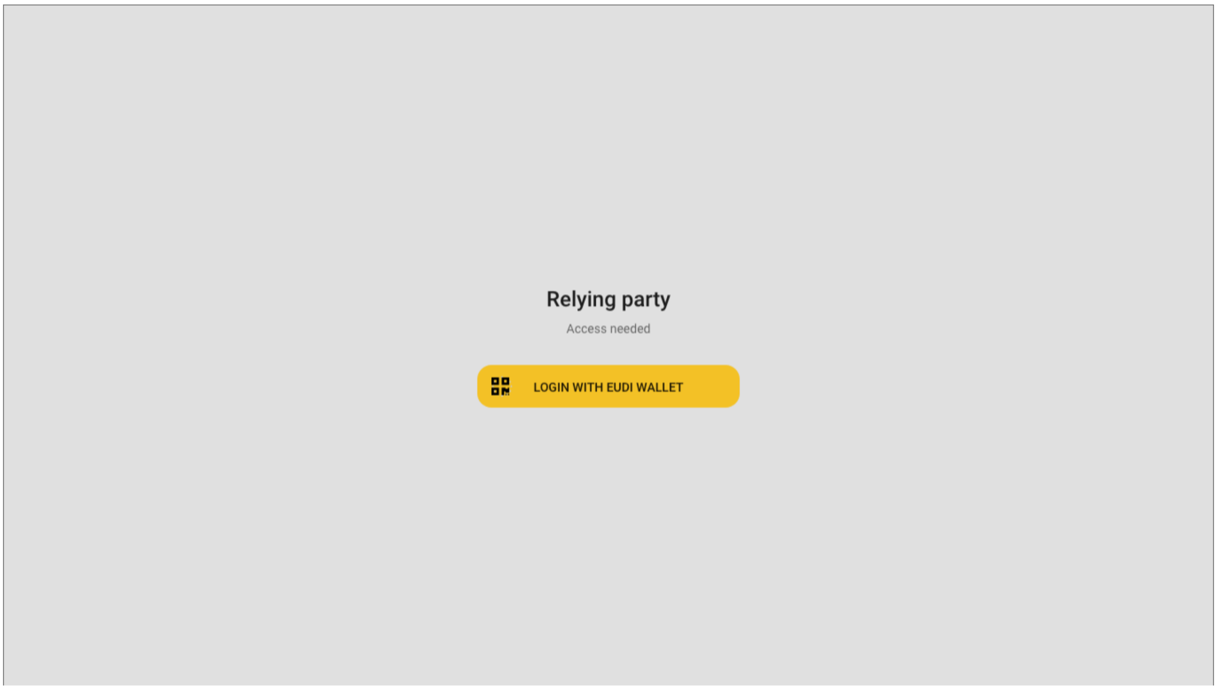
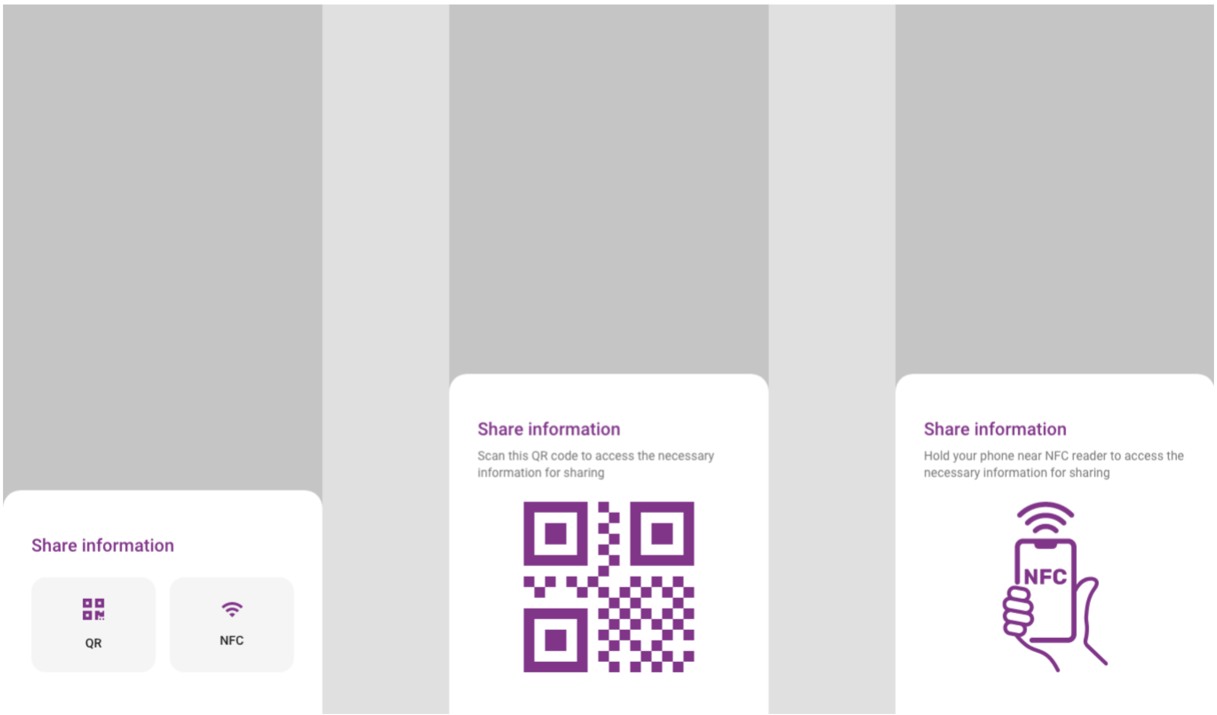


Figure 15: Login screen with EUDI Wallet login option on desktop browser

In relation to the ‘proximity’ flows, both flows are related to scenarios where the EUDI Wallet User is physically close to a Relying Party, the user does not necessarily have internet connectivity and the data presentation occurs using proximity protocols (NFC, Bluetooth, QR- Code, etc.). The key differentiator in the two proximity flows, is that in the supervised flow, the EUDI Wallet presents data (e.g. a mobile driving license) to, or under the supervision of, a human acting as a Relying Party (who may operate a device of their own). In the unsupervised flow, the EUDI Wallet presents verifiable attributes to a machine without human supervision.



Share information

Share information

Scan this QR code to access the necessary information for sharing

Share information

Hold your phone near NFC reader to access the necessary information for sharing

Figure 16: Share information screen showing QR and NFC sharing options

2 Identifications

2.1 Identification Points

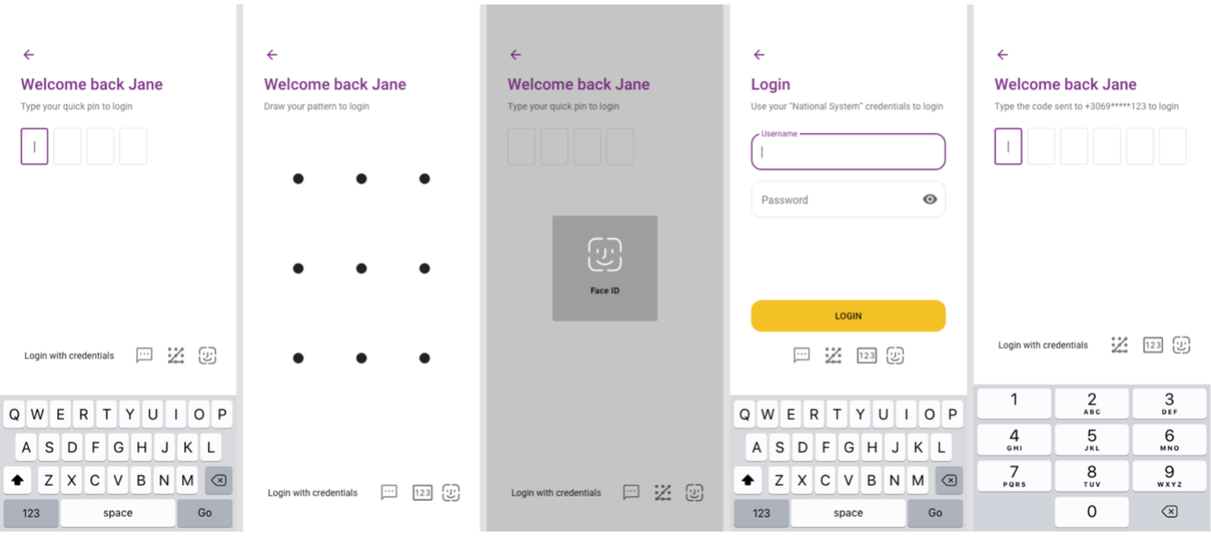
The following points are depicted as identification points within the described user flows:

- identification on application launch
- identification when authorizing disclosure of data in proximity flows (possibility to be disabled via corresponding settings) (authorization process)
- identification when presenting via deep link (authorization process)
- identification after being idle

2.2 Identification Methods

A set of 'authentication means' applicable for the EUDI Wallet are being analysed in this Design Guide. These are:

- PIN
- Pattern
- Biometrics
- Password
- OTP



Welcome back Jane

Type your quick pin to login

Welcome back Jane

Draw your pattern to login

Welcome back Jane

Type your quick pin to login

Login

Use your "National System" credentials to login

Welcome back Jane

Type the code sent to +3069*****123 to login

Figure 17: Multiple authentication method screens showing PIN, pattern, biometrics, password and OTP options

It shall be clarified that different levels of security shall be required per use case, e.g. sharing a user's 'Person Identification Data' is associated with 'High Level of Assurance', while presenting a 'loyalty card' may be associated with simpler means of authentication.

Thus, it is expected that a combination of 'authentication means' are available for the user to select and be used as per the needs of the applicable use case. However, it shall be clarified that the available authentication means are defined by the 'EUDI Wallet Provider' and the 'Device Manufacturer' and in principle shall adhere to the native way of the operating system, e.g. password and biometrics.

It shall be noted that this section reflects a preliminary analysis which is based on desk research and not on usability testing/field research and it shall further be expanded and validated with detailed research/user testing.

The analysed authentication means are being scored-in a scale of 0 to 10-against a set of design- related criteria, aiming to quantify the pros and cons of each mean.

The criteria used for the rating are:

- **Convenience**: The level of intuitiveness of each authentication method
- **Experience**: Overall user experience from a user perspective (i.e. smooth experience)
- **Speed**: Speed of use for the user's authentication process
- **Error Prevention**: Assisting users to minimize potential errors in the authentication process
- **Accessibility**: Adherence to accessibility standards/specificities

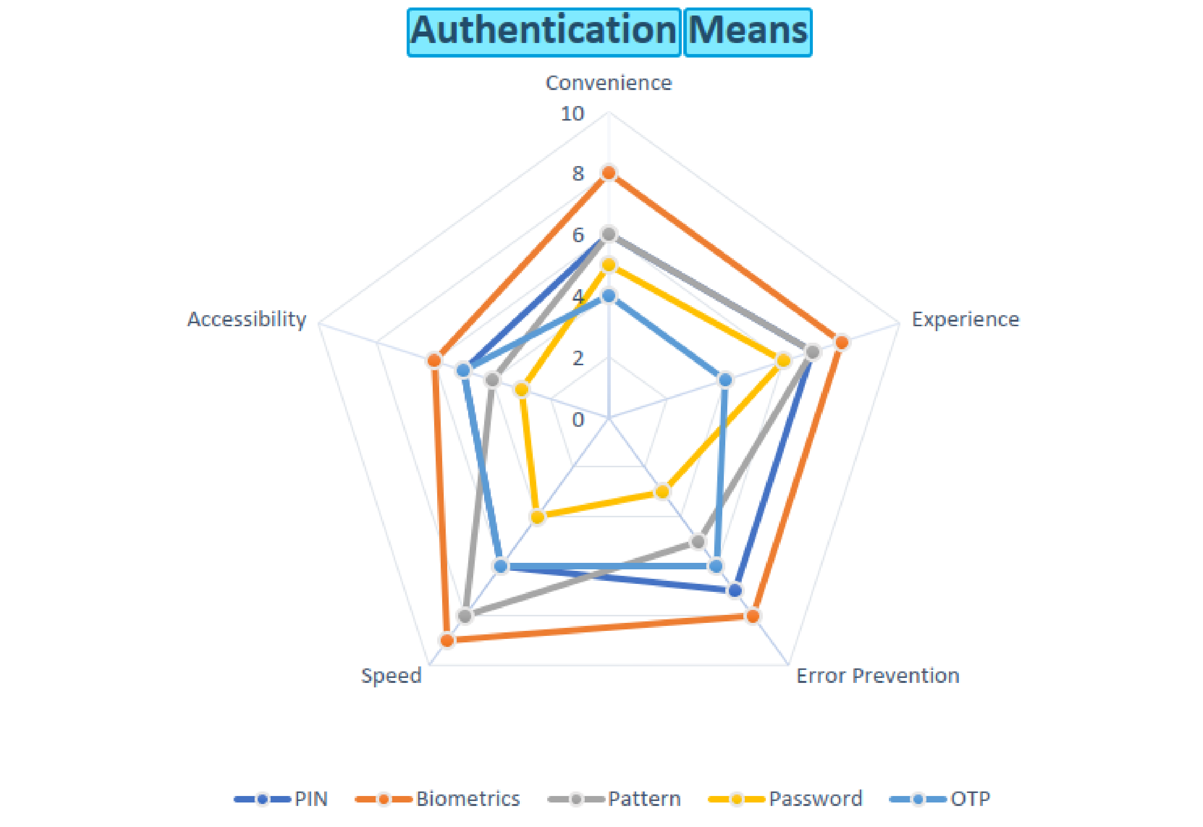


Figure 18: Radar chart comparing different authentication methods across multiple criteria

> ***NOTE:*** *Ratings have been based on a desk study and not actual first-hand testing.*

Authentication Methods Comparison

Method	Pros	Cons
PIN	Short and easy authentication method Flexibility in PIN requirements	Slower unlocking compared to other authentication methods Requires users to memorize numbers Recovery can be hard if you forget the PIN Often predictable
Pattern	Simple and intuitive to use	Many people choose simple, predictable patterns Input method is visible to those around you Belongs to a third party
Password	More secure than a PIN Flexibility in password requirements	Easy to guess Slower unlocking Password recovery can be as hard as a PIN recovery
Biometrics (fingerprint)	Fast and convenient authentication method	Fingerprints can be replicated Fingerprint distortion can cause failures Belongs to a third party

Method	Pros	Cons
Biometrics (face scan)	Fast unlocking method It doesn't require memorizing codes and passwords	Light effects and facial changes can cause failures Screen orientation and distance from the camera can impact readability The scanner can be fooled by user's photos or sometimes familial similarities Provided by a third party
One Time Password (OTP)	Alleviates the burden associated with memorizing passwords Usually utilized as 2FA on top of PIN/Passwords but may also be used as an alternative to passwords (applicable after first registration to a service) Offers a sense of advanced safety for the user	Associated with higher 'interaction cost' (i.e. users are requested to type a code) May raise confusion if OTP is not received on time - multiple attempts to receive an OTP May require clear and concise OTP text (e.g. SMS or email)

---

3 Receiving & Configuring Data Request (by the User)

The EUDI Wallet should provide a secure and user-friendly environment by empowering users with granular control over presenting their data, ensuring transparency and clarity, and enabling user control and consent.

- **Selective Disclosure**: The EUDI Wallet should empower users to have granular control over the information they present. The EUDI Wallet should provide clear options for selective disclosure, allowing users to choose between mandatory and optional information to be presented, intending to emphasize on the data points which are required to be shared by the user. It is recommended that optional data shall be grouped in collapsed sections and be unselected by default. On the other hand, it should be clearly depicted that mandatory data cannot be unselected. The app should show users a concise summary of the requested data, clearly indicating which fields are mandatory and which are optional, as per each Member State (MS) / Relying Party (RP) policy decision. This empowers users to make informed decisions about what information they want to disclose, ensuring their privacy preferences are respected, with the risk of not completing a data request in a later step (more details in section 5 Error Cases).

- **Transparency and Clarity**: Transparency is key in ensuring that users are always aware of what information is being presented. The EUDI Wallet should include clear and concise explanations about the purpose of each data request, the relying party's identity, and how the data will be used, highlighting data storage and 'intent to store' aspects to the user. Utilising plain language and avoiding technical jargon can enhance understanding and minimise user confusion.
- **User Control and Consent**: To promote a sense of trust and control, the EUDI Wallet should prioritise user consent throughout the data-sharing process. The app should provide intuitive controls to enable users to configure their preferences easily. Clear notifications should be presented when changes are made, ensuring users are always aware of their data-sharing settings and can adjust them as needed.
- **Pre-authorisation**: Pre-authorisation is a feature allowing the user to give automatic consent for releasing certain attributes, prior to any interaction. 'Pre-authorisation' as a concept may be implemented in the form of one or multiple 'profiles'. For example, if the user selects an 'age verification' profile, the EUDI Wallet will always release the corresponding attribute (e.g. age_over_NN) when requested by a Relying Party. However, if the user chooses to set a 'law enforcement' profile, the EUDI Wallet will release all attributes with a Relying Party, without giving the User the option of withholding consent during the transaction.

  It shall be highlighted that the 'pre-authorisation' concept may optionally be implemented, under the following conditions:

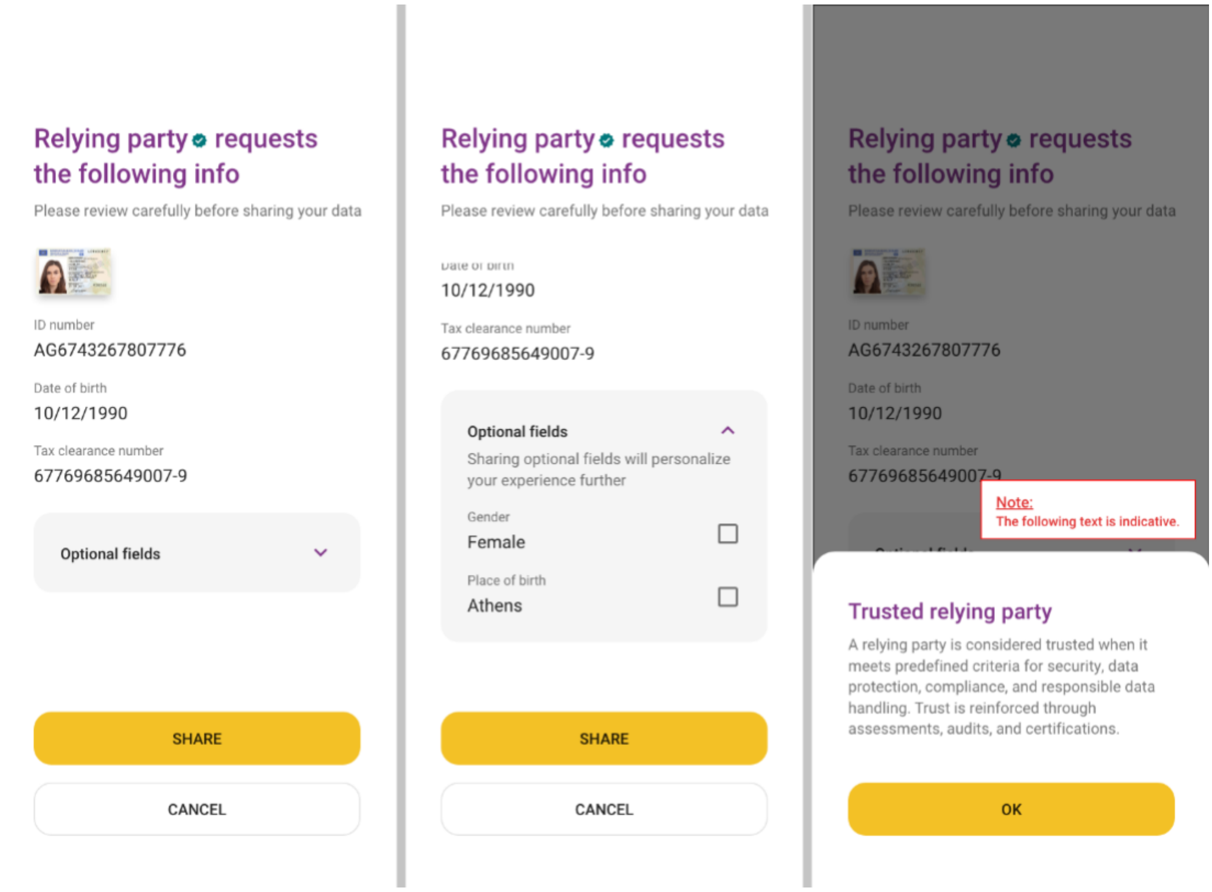
  - The pre-authorisation mechanism shall give the user the possibility to select which attribute(s) the EUDI Wallet Instance must release with which specific Relying

Parties without asking for user consent during the interaction. User consent shall never apply indiscriminately to all Relying Parties or to all attributes.

  - A Relying Party for which pre-consent is given shall have been authenticated by the EUDI Wallet at least once. This is a consequence of the previous point as it is not possible to select a Relying Party if that Relying Party is not unambiguously known to the Wallet Instance. It shall be noted that this requirement holds for both proximity use cases and remote use cases.
  - Giving pre-authorisation shall be a 'friction-full' process, meaning that it shall not be too easy and requires a considered user decision. Possibly, giving pre-authorisation should require an additional user authentication step.
  - The EUDI Wallet shall be able to present to the user a clear overview of all pre-authorisation given, with the ability to easily change or withdraw one or more of these pre-authorisations.
  - It shall be noted that pre-authorisations shall have a validity limit or the user should be regularly prompted to review any set up pre-authorisations.
  - If pre-authorisation applies for one or more requested attributes, the EUDI Wallet shall release these attributes without first notifying the user. However, immediately afterwards the EUDI Wallet shall notify the User that one or more attributes were released on the basis of pre-consent. That notification shall include an option to withdraw the applicable user consent, but also highlight 'intent to store' aspects to the user.
  - It shall be noted in the case where request also includes additional optional data request, it would be proposed pre-authorisation would prevail the potential request of optional data, since the concept of pre-authorisation would be introduced to simplify the user flow. However, further exploration and user research would be required for such flows.
  - Solution providers shall duly consider the associated security/privacy risks associated with the pre-authorisation feature in conjunction with the specific conditions listed above.

- **Relying Party Trustworthiness**: Trust in relying parties is crucial for users to feel confident sharing their personal information. The EUDI Wallet should incorporate clear information and visual indicators or badges e.g. Trust Mark could be utilised to indicate whether the Relying Party is considered trusted, based on the underpinning trust framework established. Providing users with this data helps them make informed decisions about which parties they trust and are comfortable sharing their data with. Further information must be provided upon clicking on the badge regarding what it means to be a trusted party and how you become one.

The EUDI Wallet aims to promote user confidence and foster a sense of control and privacy, thereby enhancing the overall adoption and utility of the app.



Relying party requests the following info

Please review carefully before sharing your data

ID number
AG6743267807776

Date of birth
10/12/1990

Tax clearance number
67769685649007-9

Optional fields

Relying party requests the following info

Please review carefully before sharing your data

Date of birth
10/12/1990

Tax clearance number
67769685649007-9

Optional fields

Sharing optional fields will personalize your experience further

Gender
Female □

Place of birth
Athens □

Relying party requests the following info

Please review carefully before sharing your data

ID number
AG6743267807776

Date of birth
10/12/1990

Tax clearance number
67769685649007-9

Note:
The following text is indicative.

Trusted relying party

A relying party is considered trusted when it meets predefined criteria for security, data protection, compliance, and responsible data handling. Trust is reinforced through assessments, audits, and certifications.

Figure 19: Data sharing screens showing mandatory and optional information requests from Relying Party

4 Authorization

4.1 Remote (Online) Authorization and Authentication

To enable authorization for data sharing during online processes, the following methods can be employed:

4.1.1 Same Device

- **Deep Link**: When sharing data on the same device as the wallet app, users can simply click on a deep link provided by the third-party service, such as “Log in via EUDI Wallet.” This action will instantly launch the EUDI Wallet app and present the authorization screen.

4.1.2 Cross Device

- **QR Code**: When sharing data from a different device, users can scan a QR code generated by the third-party service using their EUDI Wallet. This will seamlessly open the app and display the authorization screen.

4.2 Proximity-Based Authorization

To enable authorization for data sharing during offline processes, the following methods can be employed:

4.2.1 Cross Device (Attended)

- **QR/Bluetooth**: When presenting data to a Relying Party (attended service), users can display a QR code on their EUDI Wallet to be scanned by the Relying Party’s reader device and transmit the information via Bluetooth using their EUDI Wallet.

- **NFC/Bluetooth**: Alternatively, users can use Near Field Communication (NFC) to engage with the Relying Party's device and Bluetooth to transmit the data to the Relying Party service through their EUDI Wallet.

4.2.2 Cross Device (Unattended)

- **QR/Bluetooth**: When presenting data to a Relying Party (unattended service), users can display a QR code and present the information via Bluetooth through their EUDI Wallet.
- **NFC/Bluetooth**: Similarly, users can utilize NFC and Bluetooth to transmit the data to the Relying Party service through their EUDI Wallet.

During the authorization processes, a comprehensive screen will be presented to the citizen which shall clearly display both mandatory and optional data requested by the third-party service (as presented in 'section 3'). The citizens will have the freedom to choose which optional information they wish to share, providing them with complete control over their personal data. Additionally, a clear indication of the data transfer outcome shall be presented to the users in all scenarios described above, e.g. descriptive message regarding successful data transfer.

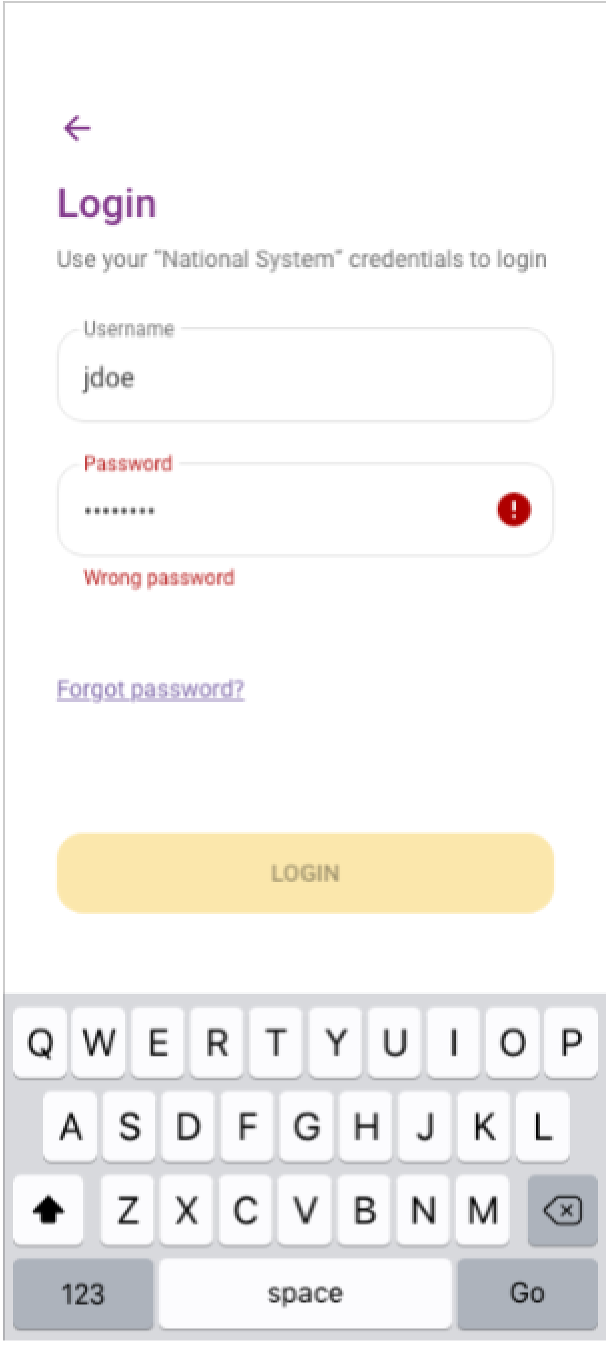
---

5 Error Cases

Handling/Display of error messages in different scenarios. (Principles/guidelines/consequences on how these shall be presented/structured etc.)

- **5.1 Erroneous user credentials**

  When the user attempts to log in to the app, expects to receive feedback indicating the success or failure of their login attempt.



Login

Use your "National System" credentials to login

Username: jdoe

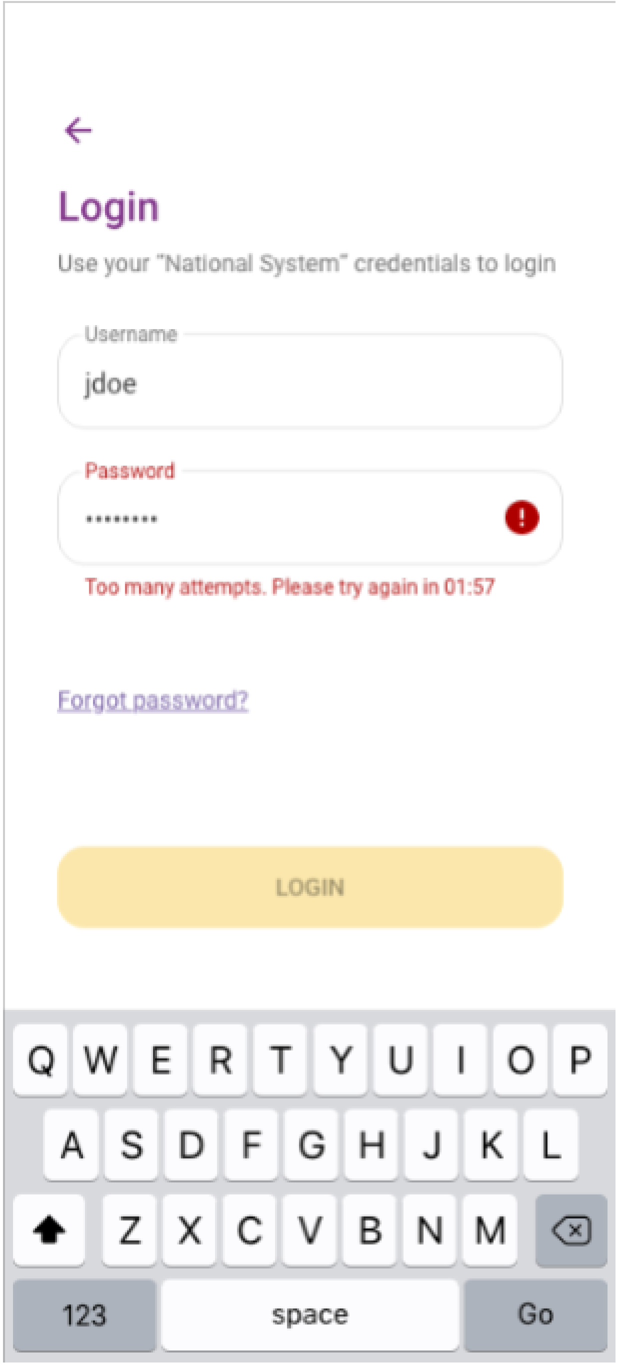
Password: ********

Wrong password

The user gets an error message indicating that his credentials were wrong:

- **5.2 Multiple failed attempts to login or present information**

  When the user is facing multiple failed attempts (e.g., 3) when trying to log in, they get an error message as feedback from the app. The error message typically indicates that the entered credentials are incorrect or that there has been a problem with the identification process. It can also guide the user in resolving the issue by reviewing the credentials or checking for typos, etc., and prompts the user to try again in 2 minutes or try to recover their password, hence the recovery functionality may be presented as a fallback option for the user in case his/her log-in attempts are not successful. By limiting the number of login attempts, the app reduces the risk of malicious factors attempting to gain unauthorized access by repeatedly guessing passwords or usernames.



Login

Use your "National System" credentials to login

Username: jdoe

Password: •••••••••

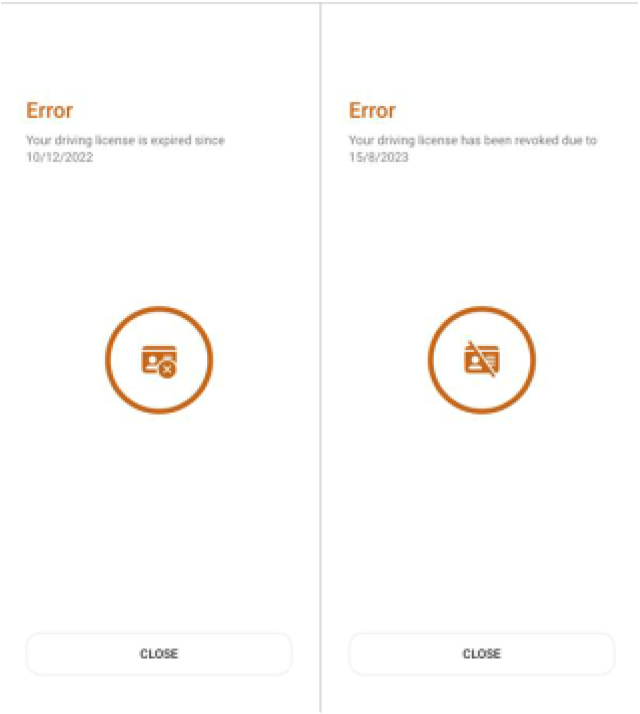
Too many attempts. Please try again in 01:57

Figure 20: Login screen showing too many attempts error with timer

The user gets an error message indicating that they must try again later:

- **5.3 The document is considered invalid (expired/revoked)**

When the user presents an invalid document through the app, (e.g., a driver's license to a police officer) the app displays an error message on the user's screen, indicating that the document could not be verified because it is expired or revoked.



Error

Your driving license is expired since 10/12/2022

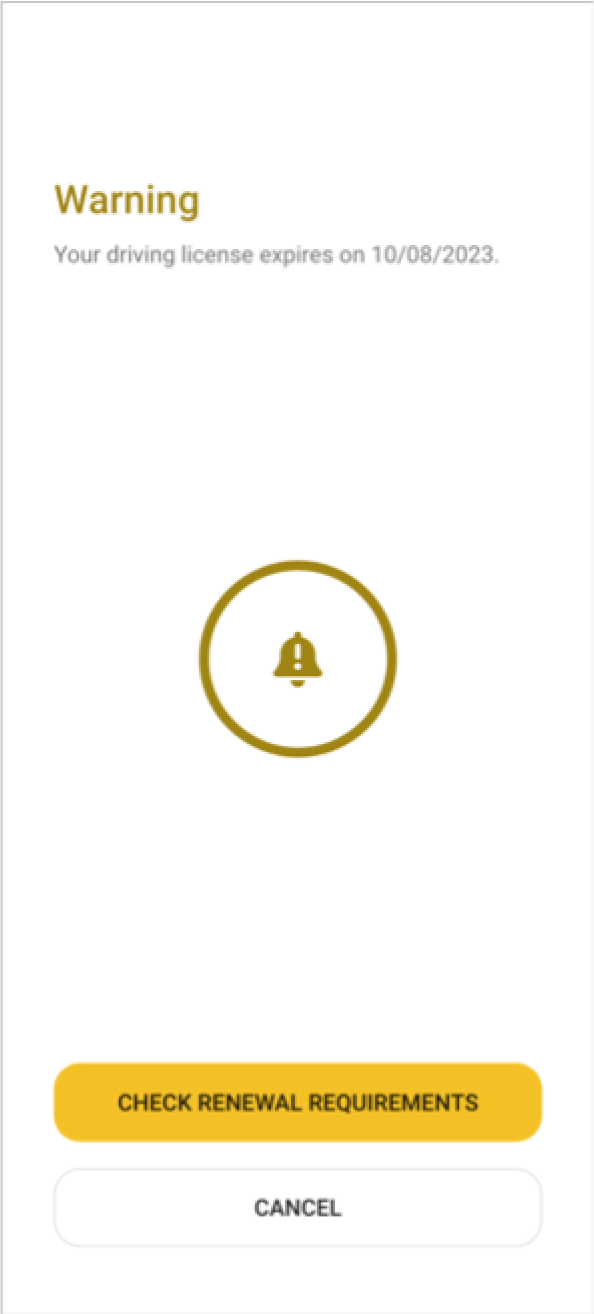
Error

Your driving license has been revoked due to 15/8/2023

Figure 21: Error message showing additional documents required

The user gets a message indicating the status of the document:

However, the user should be warned if a document they have saved within the app is expired or revoked. The warning could be presented as a notification or prompt within the app, indicating that a saved document is approaching or has already passed its expiration date. The message could include information on how to renew or update the document, directing the user to the appropriate authorities, or providing relevant instructions.



Warning

Your driving license expires on 10/08/2023.

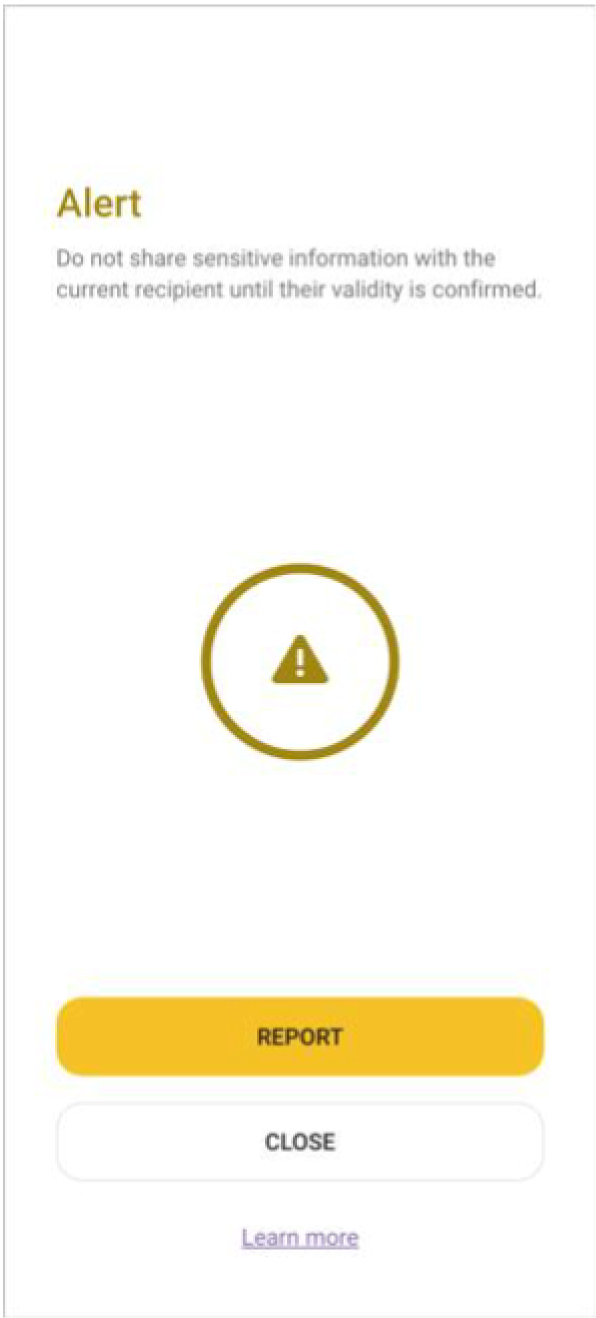
Figure 22: Warning notification about document expiration with renewal option

The user gets a message indicating that the document expires shortly:

By providing proactive reminders about expired documents, the app can contribute to a smoother user experience, help users remain compliant with regulations, and foster trust and confidence in the app’s functionality and user support.

- **5.4 The Relying party is not considered trusted. Is not verified or could not be verified (Maybe address safety)**

  When the user attempts to share information through the app with a third party -a physical person or a digital service- and it turns out that the third party is not valid or is a fraud, they must get an alert warning message.



Alert

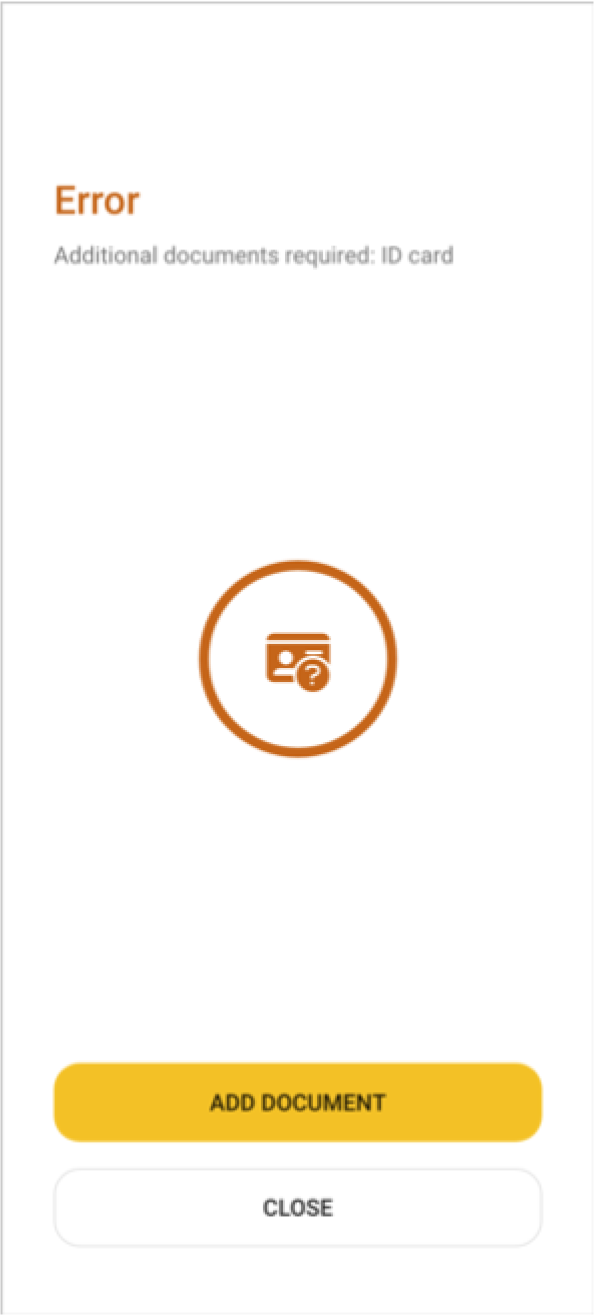
Do not share sensitive information with the current recipient until their validity is confirmed.

Figure 23: Alert warning about untrusted relying party with security options

The user gets a message indicating that they must not share information with that party. The options are to report it, to close the app, or to search for information about security:

- **5.5 The user fails to present requested document**

When a user scans their QR code using a QR code scanning device, they receive a prompt to provide additional documents, such as an ID. If the required document is not present in the user's app, an error message is displayed, notifying the user that the document is not stored in their app.



Error

Additional documents required: ID card

Figure 24: Error message showing missing ID card document with add document option

The error message then suggests adding the document from the available documents list.