TLP - CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Wallet-Related Service Provider Security Requirements

Based on EN 319 401

MARCH 2026

Document History

//DRAFT ONLY - DELETE THIS SECTION AND PAGE UPON FINAL PUBLICATION

Date	Version	Modification
18/11/2025	0.1	Creation
28/11/2025	0.2	Restructuration after exchanges with Member States
09/12/2025	0.3	Addition of annexes and various updates after proofreading
27/01/2026	0.4.605	Reorganisation of content and clarifications
27/02/2026	0.4.609	Reorganisation, extension, alignment to ARF 2.8.0
31/03/2026	0.5.614	Update after the EUDIW AHWG for ECCG opinion and public review

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use certification@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN Number, DOI Number (IF APPLICABLE)

Table of Contents

Executive Summary

Security requirements are the cybersecurity criteria against which EUDI Wallets and the eID schemes under which they are provided need to be evaluated in the EUDIW European cybersecurity certification scheme. These requirements depend greatly on the functional requirements provided in the standards and technical specifications for the EUDI wallet. Since the implementing acts that define these standards and technical specifications are currently being revised, this aspect of the work is preliminary.

In an initial approach that remains to be consolidated, ENISA has worked to identify some requirements, starting from various sources, in particular from the Architecture Reference Framework's (ARF) [i.8] high-level requirements, but also legal sources like Commission Implementing Regulations (CIR) (EU)2015/1502 [i.2] (on the definition of levels of assurance for electronic identification (eID) means) and CIR (EU) 2024/2981 [i.3] (on the certification of EUDI Wallets), combined with several existing schemes, standards and technical specifications.

In the eIDAS [i.1] domain, EN 319 401 [1] is one of the essential standards, which defines general policy requirements for Trust Service Providers (TSPs). Although Wallet providers are not considered in the Regulation as TSPs, there are many similarities and Article 5a(20) states that several requirements applicable to qualified trust service providers also apply to Wallet providers. Therefore, the requirements from EN 319 401 [1] are a very reasonable starting point, both because this standard is widely known and applied throughout the eIDAS [i.1] community and because it defines a baseline of requirements that forms the foundations of any certification of the provision of a complex service.

The document does not only cover the services from wallet providers, but also the relevant services from the PID provider, since a PID is required to complement a wallet solution and providing a valid eID means. Other service providers that may be involved in the process are covered as well, such as the providers of wallet and relying party validation services.

The main intent from the document mainly consists in complementing the EN 319 401 [1] standard, in a way similar to standards defined for specific categories of Trusted Services. The additional requirements often come from the ARF, adding wallet-specific requirements to the generic requirements of the EN 319 401 [1] standard.

The annexes provide mappings of the requirements to the Commission's ARF [i.8] and to a few standards.

The present version of the document only covers a part of the wallet features, centred around the issuance, management and presentation of PID and attestations.

SECTION 1

Introduction

1. Scope

1.1 About this document

1.1.1 Specification-driven requirements

The present document defines security requirements for the stakeholders involved in the provision and operation of EUDI Wallets. These requirements are expected to be eventually laid down in standards and technical specifications, but most of these documents remain under development at this time. The present document therefore intended to provide an overview of the requirements to be considered for the cybersecurity certification of EUDI Wallets. The document may apply equally to the European Cybersecurity Certification scheme under development and to the national certification schemes under development by Member States.

The requirements in this document come from various origins; the main sources have been EN 319 401 [1] and the ARF [i.8], but other documents have been used, which are listed in the bibliography.

1.1.2 Expression of the requirements

1.1.2.1 Focusing on security requirements

Most of the risks and threats identified in the risk register (Annex 1 of CIR (EU) 2024/2981 [i.3]) are actually addressed by the standards and technical specifications that are mentioned in eIDAS Implementing Acts, as follows:

Standards mentioned in CIR (EU) 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:

- SAM.01 Secured Applications for Mobile – Requirements for supporting 3rd party Applets on eSIM and eSE via SAM. v1.1 2023, GSMA;
- GPC_GUI_ 217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM v1.0 2024-04;
- GPC_SPE_0 34 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03;
- GPC_SPE_0 07 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07;
- GPC_SPE_0 13 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04;
- GPC_SPE_0 93 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03;
- GPD_SPE_0 75 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.
- ISO/IEC 18013-5:2021
- ‘Verifiable Credentials Data Model 1.1’, W3C Recommendation, 3 March 2022

Standards mentioned in CIR (EU) 2024/2977 of 28 November 2024:

- ISO/IEC 18013-5:2021

Standards mentioned in CIR (EU) 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:

- ISO/IEC 18013-5:2021
- ISO/IEC TS 18013-7:2024

These implementing acts are in the process of getting revised in order to mention more standards and technical specifications, which could include the following:

- ISO/IEC 18013-5:2021 - Mobile Driving Licence (mDL) Application
- ISO/IEC 18013-7:2025 - mDL Add-On Functions (Annex A & C)
- OpenID for Verifiable Credential Issuance 1.0
- OpenID for Verifiable Presentations 1.0
- OpenID4VC High Assurance Interoperability Profile (HAIP) 1.0, including:
- IETF RFC 9126
- IETF RFC 7636
- IETF RFC 9449
- Recommended TLS requirements
- IETF RFC 9901 - Selective Disclosure for JSON Web Tokens (SD-JWT)
- SD-JWT-based Verifiable Credentials (draft-ietf-oauth-sd-jwt-vc)
- Token Status List (draft-ietf-oauth-status-list)
- CSC API Data Model for Remote Signature Applications
- EC TS01 - EUDI Wallet Trust Mark (currently referenced in the amended IA)
- EC TS03 - Wallet Unit Attestations (WUA) (currently referenced in the amended IA)
- ETSI TS 119 412-6 - Certificate Profiles for PID, Wallet, EAA, QEAA, PSBEAA Providers
- ETSI TS 119 411-8 - Access Certificates
- ETSI TS 119 431-1 - Policy and Security Requirements for Remote QSCD / SCDev
- ETSI TS 119 432 - Protocols for Remote Digital Signature Creation
- ETSI TS 119 472-1 - EAA Profiles: General Requirements
- ETSI TS 119 472-2 - Profiles for EAA/PID Presentations
- ETSI TS 119 472-3 - Profiles for EAA/PID Issuance
- ETSI TS 119 475 - Relying-Party Attributes Supporting Wallet User Authorisation
- ETSI TS 119 602 - Lists of Trusted Entities (Data Model)
- ETSI TS 119 612 - Trusted Lists
- ETSI EN 319 142-1 - PAdES Digital Signatures SC API v2 – Architectures and Protocols for Remote Signature Applications

Since the implementing acts listing the functional standards and technical specification are under revision, the requirements listed in the present document can only be temporary; so this is why the document focuses on the core functions.

Nevertheless, the objective is that these standards and technical specifications are expected to define the functional interfaces required in Article 5c(5) of eIDAS to implement the core functions of the wallet, as defined in Article 5c(4) of eIDAS. These functional interfaces include many security features, addressing a large part of the risks and threats identified in the risk register. Therefore, security starts with adequate functional testing, including functional conformance with the requirements in these standards.

Since the EUDI wallet is mostly centred around security functions like identification and authentication, so the functional standards actually define technical security controls that address many risks from the risk register at a functional level. For instance, risks related to man-in-the-middle attacks should be mostly covered by the adoption of adequate communication protocols, and functional conformance testing could be sufficient. On the opposite, risks related to breaches of confidentiality are at least in part related to attacks on the implementation itself, and they cannot be fully covered by conformance testing of functional requirements.

The focus of the cybersecurity conformity assessment should therefore be the requirements for which conformance testing is not sufficient, and those should be the security requirements of the scheme.

1.1.2.2 Types of requirements

This document uses EN 319 401 [1] as a basis. A first set of requirements are added to complement the standard's requirements in Chapters 4 to 7.

Most of the requirements, however, are added in specific chapters, while requirements related to the provision and operation of a wallet solution are defined in Chapters 8 and 9, and requirements related to the provision of PID are defined in Chapter 10. Most requirements are implementation security requirements (*i.e.* requirements that refer to the safe implementation of the functions and to the protection of sensitive assets needed to perform these functions), and a few are additional functional security requirements (*i.e.* complements to the EUDI Wallet functional specifications that matter for security).

The requirements that are specific to EUDI Wallets are mostly derived from the "common protocols and interfaces" that are being defined by the Commission to satisfy Article 5a(5)(a) of eIDAS, based on standards and technical specifications, a few of which are issued by the Commission themselves.

1.1.2.3 Evaluation methods

As a general rule, conformity to functional security requirements can usually be evaluated through testing, whereas conformity to implementation security requirements needs to rely on audit or inspection. There are exceptions, in particular for functional security requirements, that apply to the parts of the EUDI Wallet that are less strictly standardised, for which inspection may be more practical than testing. Similarly, when interactions are required, automated testing is not always possible.

As mentioned above, a key assumption is that functional compliance to these common protocols and interfaces will mitigate most of the identified threats at the functional level. The cybersecurity certification therefore needs to focus mostly on three aspects:

- conformity to non-functional requirements, i.e. to the requirements whose conformity cannot be assessed solely by conformance testing;
- resistance of the implementation of common protocols and interfaces to secondary threats, i.e. threats on the implementation of protocols rather than directly on the wallet's assets.
- overall resistance of the implementation to the threats on the wallet's assets as identified in the risk register defined in Annex I of CIR (EU) 2024/2981.

The last aspect is addressed by the mapping proposed in Annex B, and also by the overall evaluation, which needs to ensure that the different components of the wallet solution and the eID scheme used to provide it provide sufficient coverage of these risks and threats.

In a first approximation and before the availability of a final list of standards and technical specifications to be considered, the high-level requirements (HLRs) defined in Annex 2 of the ARF have been used as basis instead of the different specifications referred in the Implementing Acts, and the requirements for which compliance testing is not sufficient, requiring at least some form of inspection, audit, or even specific testing (e.g. testing a no-standard feature or even interactive testing) have been considered as of potential interest for the cybersecurity certification, as a complement to the functional compliance certification.

> NOTE: This list therefore needs to be consolidated once the revised implementing acts will be adopted, and the requirements in this document will also need to be updated.

In addition, most requirements, and in particular those inspired from the ARF, come with notes on conformity assessment, which suggest evaluation activities at a very high level, and give an indication why the requirement was included. These notes are guidance and they are not normative; alternative activities may be used instead as suitable.

For all activities, evaluators need to identify potential vulnerabilities in the implementation, and if they deem it necessary, need to design potential attack paths and perform penetration testing in order to assess the resistance of the EUDI Wallet to attackers. Specific guidance is included on a few requirements related to sensitive features, but this is not an objective of the present document.

ENISA and other EUDI Wallet stakeholders are also working on the definition of additional methods for the evaluation of specific components of the EUDI Wallet, such as an EUCC [i.6] Protection Profile for Wallet Secure Cryptographic Applications (WSCA) being developed by CEN/TC 224/WG 17, or an EN 17640 [i.7] Protection Profile for mobile wallet user interface applications, currently under development with the support of ENISA's Ad Hoc Working Group on the certification of EUDI Wallets (EUDIW AHWG). Several protection profiles also already exist for the certification of Wallet Secure Cryptographic Devices (WSCD) using EUCC [i.6].

However, because the split of functions and assets between the various components depends on the architecture selected by each EUDI Wallet provider, it is not possible in the present document to go below the granularity of the wallet unit in most cases, with few exceptions such as the operations on critical assets (assigned by definition to the WSCA/WSCD) and the user interface (assigned by definition to the wallet instance).

1.1.3 Current status

1.1.3.1 Versions of documents

The present document was developed on the basis of the latest release of EN 319 401 [1], v3.2.1 as published in January 2026, and on v2.8.0 of the ARF, with some alignments with the upcoming version of the ARF.

1.1.3.2 Simplifying assumptions

For the purpose of this document, we only consider wallet solutions in which wallet units satisfy the following conditions:

- Each wallet unit contains a single WSCA and a single WSCD.
- Each wallet unit contains a single wallet instance.

The reason for these conditions is that the use of multiple WSCAs and WSCDs, or of multiple wallet instances, although included in the definition of a wallet unit, is not well supported by the ARF [i.8] and by standards, both existing and under development.

Although it is not easy to define rules for the use of multiple WSCAs, WSCDs or wallet instances that would work for all architectures and configurations, the absence of rules does not preclude their use in certified wallet solutions. However, it means that specific requirements may need to be added, while tailored to the solution, to ensure that the wallet solution complies with the regulatory requirements. Such specific rules should be much easier to define than the generic rules mentioned above.

1.1.3.3 Coverage of requirements

The current version of the requirements does not cover all the requirements for the EUDI Wallet. It focuses on the security of the essential functions of the wallet, *i.e.*, the management of wallet units, the management of PID and of device-bound attestations and their presentation to relying parties.

Other important topics such as support of the DC API, pseudonyms, qualified electronic signatures, embedded disclosure policies, wallet to wallet interactions, transaction logs are not covered in this version of the document and will be added in a future update.

Finally, the Implementing Acts that define the common protocols and interfaces are currently being revised, so some of the requirements included in the present document may not be relevant for the final version of the Implementing Acts.

1.2 Wallet requirements, scope and security objectives

1.2.1 Feature-related requirements on wallet units

These requirements are related to the lifecycle of wallet units, to the management of wallet unit attestations (issuance, management, revocation), and to the management of PID and device-bound attestations (issuance, management, presentation, revocation).

> NOTE: These requirements will be enriched as the present document will cover more features of EUDI Wallets.

1.2.2 Horizontal requirements on wallet units

These requirements apply horizontally to the different components of the wallet unit, and they are not related to a given feature of the wallet.

1.2.2.1 User authentication

User authentication is essential for the EUDI Wallet, in order to ensure that the person authorising the management and presentations of identity-related information is indeed the legitimate holder of the wallet.

In the EUDI Wallet, there are several kinds of authentication with different purposes, including the following two:

- Application-level authentication, which is required to perform any operation on the EUDI Wallet.
- WSCA/WSCD authentication, which is required prior performing a sensitive action (most often, before using a private key protected by a WSCD).

NOTE: Further discussions need to be held in the EUDIW AHWG about the exact requirements on different aspects of authentication. We have here included a baseline of requirements that may be extended or made stricter in the future.

NOTE (application-level): Application-level authentication is the main access control measure for the EUDI Wallet, allowing all operations to be performed, except those that require WSCA/WSCD authentication.

NOTE (WSCA/WSCD): There is a strong link between WSCA/WSCD authentication and authorisation, in particular because the access to the WSCA/WSCD is only allowed after successful WSCA/WSCD authentication. However, because of the need to renew PIDs and attestations, to manage the “expired” PIDs and attestations, and where applicable, to manage batches of PIDs and attestations, a single authentication may authorise more than one operation on the WSCD.

1.2.2.2 Orchestration

The key operations for the wallet (*e.g.* issuance, presentation) are complex operations which require many operations to be performed in a right sequence for security reasons. In particular, data coming from other stakeholders needs to be validated (including its format, integrity, authenticity) before it can be used.

It is also important to ensure that no step is skipped in a complex operation, to avoid providing an opportunity for attackers

Orchestration requirements require the developer to include measures to ensure that a sensitive operation cannot be completed without performing all required operations.

1.2.2.3 Authenticity and trust anchor checks

Similar to the orchestration mentioned above, chains of trust need to be processed completely and in the proper order in order to provide the expected protection.

Specific requirements apply to these complex processes, in particular those that start from a trust anchor that also needs to be securely retrieved and validated.

1.2.3 Requirements on wallet instances

1.2.3.1 Protection of assets in the wallet instance

The wallet instance needs to manage many assets that are not considered critical, but are nonetheless sensitive. The requirements in this section provide some guidance on the management of these assets.

1.2.3.2 User interaction

The EUDI Wallet includes an interface with users, through which they control the management and the presentation of their identification data and other attributes.

Phishing is one of the main threats on any sensitive application, where scammers convince their victims to perform or approve operations to the benefit of the scammer. Defending against phishing requires an analysis of fraud patterns and technical measures like origin binding and cryptographic challenge response mechanisms, but another essential aspect is the clarity of the interactions with a user, making it more difficult for a scammer to abuse their victims.

The user interaction requirements apply to all interactions within the wallet user interface application.

1.2.3.3 Wallet instance (mobile application)

Specific requirements apply when the wallet instance is implemented as a mobile application, mostly related to the fact that the underlying platform can usually not be trusted.

Many of the requirements are inspired from the OWASP Mobile Application Security framework [i.9], complemented by specific recommendations for sensitive applications.

1.2.3.4 Wallet instance (Web application)

Specific requirements also apply when the wallet instance is implemented as a Web application, in particular because the underlying execution platform cannot be trusted.

The current requirements refer directly to the OWASP framework [i.10] and should be enhanced.

1.2.4 Requirements on the WSCA

These are very basic requirements on the minimal features of a WSCA, inspired by the draft EUCC [i.6] protection profile currently under development in CEN/TC 224/WG 17.

1.2.5 Requirements on wallet services

These are the requirements on the wallet provider's backend, complementing the general requirements from Chapters 5 to 7 with technical requirements.

Many of these requirements are symmetrical to the requirements on wallet units, for instance on topics related to the management of wallet units and wallet unit attestations.

1.2.6 Requirements on PID provider services supporting EUDI Wallets

This last set of requirements is related to the management of PID in the wallet, which is part of the eID means.

Just like the requirements on wallet services, they complement the general requirements from Chapters 5 to 7 with technical requirements. Therefore, many of these requirements are symmetrical to the requirements on wallet units on topics related to the management of PID.

2. References and terminology

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are necessary for the application of the present document.

[1] EN 319 401 v3.2.1: “Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers”, January 2026

[2] European Cybersecurity Certification Group sub-group on Cryptography, “Agreed Cryptographic Mechanisms”, Version 2.0, April 2025

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are not necessary[1] for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[i.2] CIR (EU)2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[i.3] CIR (EU) 2024/2981 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

[i.4] CEN TS 18098: “Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets”

[i.5] EN ETSI 319 403-1: “Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers”

[1] All regulations listed in the informative references will have a clear impact, and they are the basis of the evaluation of these requirements

[i.6] CIR (EU) 2024/482 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

[i.7] EN 17640:2022, “Fixed-time cybersecurity evaluation methodology for ICT products”

[i.8] EUDI Wallet Architecture Reference Framework, v 2.8.0
https://eudi.dev/2.8.0/architecture-and-reference-framework-main/

[i.9] OWASP Mobile Application Security
https://owasp.org/www-project-mobile-app-security/

[i.10] OWASP Application Security Verification Standard
https://owasp.org/www-project-application-security-verification-standard/

[i.11] EN ISO/IEC 15408:2022, Parts 1 to 5, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security (Common Criteria)

[i.12] Regulation (EU) 2019/881 of the European parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[i.13] CIR (EU) 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

[i.14] CIR (EU) 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

[i.15] CIR (EU) 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

2.3 Terminology

2.3.1 Terms

In addition to the terms defined in the various sources, the following terms have been added or refined:

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
NOTE: The assets considered here are only data assets, and they do not include code, hardware or other assets
[SOURCE: From CIR (EU) 2024/2981, Article 2(11), note added]

user device: device under the control of the wallet user that is used to support the operation of a wallet unit
NOTE 1: A user device may be a device on which a wallet user interface application is running, as a standalone application or as a browser.
NOTE 2: A user device may be used as the basis of authentication through proof of possession.
NOTE 3: A user device supporting a wallet unit may be composed of several devices, for instance a workstation and a token used as proof of ownership.

remote user environment: part of the wallet unit that is hosted in the wallet provider's remote environment
NOTE: Although all remote user environments are part of the same remote environment, a user only has access to their own user environment

wallet instance: 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
NOTE: when focusing on the code of the wallet instance, references may be made to a "wallet instance application" in opposition to the fully installed and configured wallet instance.
[SOURCE: From CIR (EU) 2024/2981, Article 2(5), note added]

wallet provider: natural or legal person who provides wallet solutions
[SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(8)]

wallet secure cryptographic application, **WSCA**: application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device
NOTE: a wallet secure cryptographic application needs to run in a secure environment, which may be a wallet secure cryptographic device, another secure environment on the user device, or a secure environment within the wallet provider backend.
[SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(4), note added]

wallet secure cryptographic device, **WSCD**: 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
[SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(6)]

wallet solution: 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
NOTE 1: The wallet solution includes all the components of an EUDI Wallet that need to be certified, and that may be instantiated into an electronic identification means.
NOTE 2: The wallet solution is likely to include several variants of the wallet instance application, and possibly of wallet secure cryptographic applications, targeting different kinds of user devices.
[SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(1), notes added]

wallet unit: 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
NOTE 1: The wallet unit does not include the parts of the wallet solution that are not supporting directly the user, and in particular most of the services provided by the wallet provider backend.
NOTE 2: The parts of the wallet unit running on the wallet provider's backend may be referred to

as “wallet unit service”.
NOTE 3: The wallet secure cryptographic devices are not always actually provided to the user, as they can be included in the device provided by the wallet user, or the wallet provider may only provide access to a remote wallet secure cryptographic device shared with many other users.
NOTE 4: A typical wallet unit will include a single wallet instance and wallet secure cryptographic application, suitable for the wallet user’s device.
[SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(10), notes added]

2.3.2 Abbreviations

EAA	Electronic Attestation of Attributes
PID	Person Identification Data
WSCA	Wallet Secure Cryptographic Application
WSCD	Wallet Secure Cryptographic Device
WUA	Wallet Unit Attestation

SECTION 2

Wallet Architecture Considerations

3. Guidelines for wallet service architecture

3.1 Architecture

The architecture of the EUDI Wallet, as described in the ARF [i.8] has been designed to leave a lot of flexibility to designers. The diagram below, which focuses on implementation, identifies many components of the wallet solution that may be certified independently:

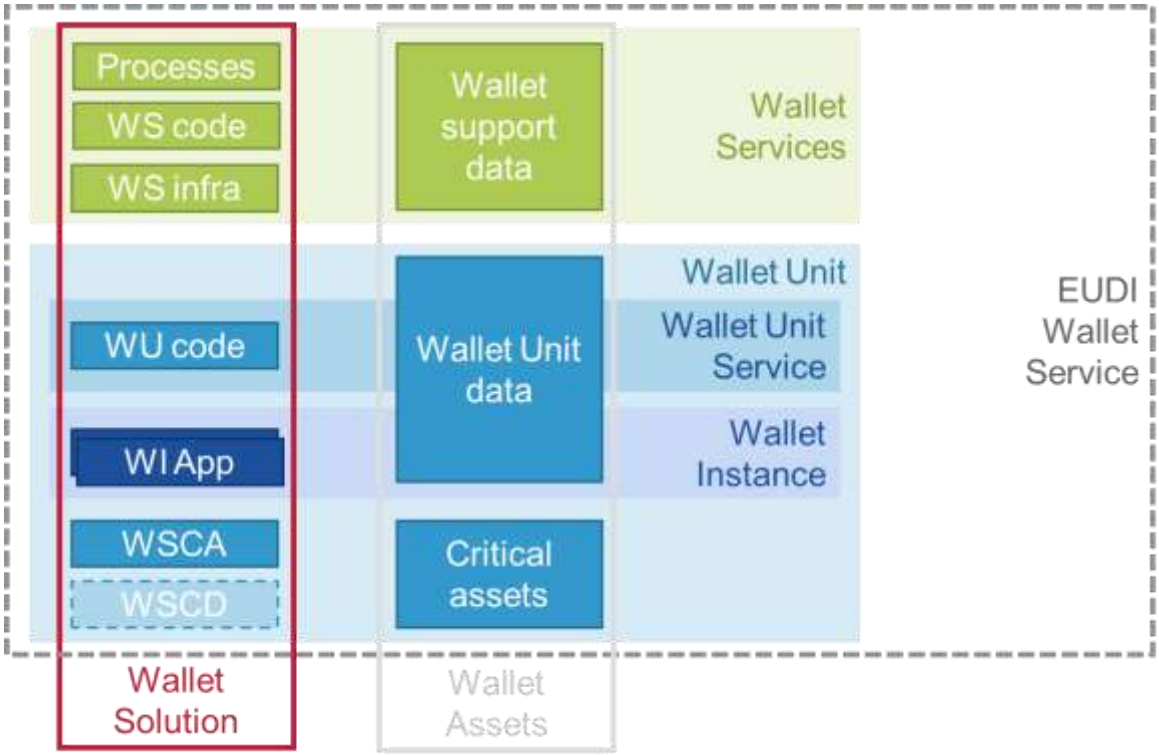

Figure 1: Implementation of the EUDI Wallet architecture

The EUDI Wallet is here considered as an ICT service, which is made of two high-level components, the wallet service in green (globally provided by the wallet service provider), and the wallet unit in blue (individually provided for each user by the service provider).

Each component manages wallet assets in grey and includes hardware, software, services, settings and configurations, which all together constitute the wallet solution in red. CIR (EU)2024/2981 [i.3] defines the notions of wallet instance, wallet unit and EUDI Wallet, which includes the assets together with the means to process them, but the certification of the EUDI Wallet focuses on the active components that perform the processing, *i.e.* the wallet solution.

The following subsections describe these in more details.

3.1.1 Wallet unit

The wallet unit includes the following low-level subcomponents:

- Wallet secure cryptographic application (WSCA). The WSCA is the software component that manages the wallet unit's critical assets. The present document defines a few assets that have to be considered critical in all implementations and processed solely by the WSCA, but some implementations may consider more assets critical. In addition, implementations may decide to process non-critical assets in the WSCA.
  It includes software, settings and configurations.
- Wallet secure cryptographic device (WSCD). The WSCD is the hardware component that performs critical operations, including in particular critical cryptographic operations, and processes the related critical assets. The WSCD can be provided by the user, for instance when it is a secure element in a mobile device, so it may not be part of the object of certification, but the wallet unit needs to include a mechanism to verify that the assumptions made on the WSCD (typically a certification) are verified in practice.
  It includes hardware, software, settings and configurations.
- Wallet instance application. The Wallet instance application is the software component that implements the user interface with the wallet user, which may typically be implemented as a local application or as a Web application. There are usually several variants of a Wallet instance application in a given wallet solution, targeting different categories of devices. The wallet instance application may rely on the Wallet unit
  It includes software, settings and configurations.
- Wallet unit code. The wallet unit service runs on the wallet provider's systems and it supports the implementation of the wallet unit, including the wallet instance. The wallet unit service relies on dedicated wallet unit code, and on an ISMS to provide a service running that code.
  It includes software, settings and configurations.

  NOTE: The "wallet unit code" that runs on the wallet provider's systems can also be considered as part of the wallet instance. The reason for separating it is that it does not run in the same environment, so its assessment may be quite different.

Overall, the organisation is only constrained as follows:

- Access to critical assets within the WSCD is managed by the WSCA.
- The user interface is implemented by the wallet instance application.

All the other features can be implemented as part of the wallet instance application, or on the user's environment in the wallet provider backend as part of the wallet unit service, or even as part of the WSCA. These are design decisions of the wallet provider.

Following the assumption that there is a single wallet instance per wallet unit, and since most functions can be implemented in several subcomponents of the wallet unit, the vast majority of technical requirements refer to the wallet unit, although in practice they will have to apply to one or more of the wallet unit's subcomponents, depending on the implementation.

As an exception to that rule, a limited number of requirements are assigned directly to the WSCA (if they relate to critical assets) and to the wallet instance (if they relate to the user interface).

Since the WSCD is sometimes not provided by the wallet provider, the requirements that apply to the WSCA are in most cases not separated from those that apply to the WSCD, and are mentioned as “WSCA/WSCD”.

3.1.2 Wallet service

The wallet service include the following low-level components:

- Wallet service infrastructure: The wallet service infrastructure is the IT infrastructure that is operated by the wallet provider to provide the wallet service.
  It includes hardware, software, settings and configurations.
- Wallet service code: The wallet service code is the code that implements the wallet service.
  It includes software, settings and configurations.
- Processes: The processes are all the processes that support the operation of the EUDI Wallet service, typically grouped in an ISMS.

3.2 Related services

The wallet service by itself does not provide a complete EUDI Wallet; it does not even constitute a full eID means, since an eID means needs to include a PID. In addition, the eIDAS Regulation requires the certification of the validation services defined in Article 5a(8).

These services are considered independently because they are likely to be provided by another entity than the Wallet provider, and it is therefore desirable to isolate their requirements, in order to allow them to be evaluated or even certified independently.

3.2.1 PID provider services supporting an EUDI Wallet

A PID provider typically provides several services that are required for an eID means, and in particular the user on-boarding as defined in CIR (EU) 2015/1502 [i.2]. They also typically generate the PID and provision them into each wallet unit to make them a full eID means.

The objective here is only to consider the services that could support the EUDI Wallet, and not all the other services that the PID provider may provide.

3.2.2 Validation services

The objective of these services is to allow different stakeholders to confirm the validity of EUDI Wallets and of relying parties. These are rather simple services that serve as a repository for reference information. They are required in eIDAS Article 5a(8), under the responsibility of Member States.

These validation services do not include the registration process for relying parties, which is out of the scope of required certification; they are only intended to make available limited information about previously registered relying parties. The validation function itself only covers the provision of lists of trusted entities that will support the verification of the authenticity and validity of the EUDI wallets and of the relying parties.

3.3 Ongoing discussions

3.3.1 Scope of the WSCA

The WSCA is defined as the “application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device”. It is therefore strongly linked to the management of critical assets in the WSCD.

The definition of critical assets is rather wide, mentioning all assets whose compromise has a “serious, debilitating effect on the ability to rely on the wallet unit”. These critical assets include at least:

- The private keys used to authenticate all PIDs and some attestations, related WUAs, and their processing.
- The WSCA/WSCD user authentication verification data and the verification itself.

The requirements for user control on their data also requires the WSCA to include a link between the verification of the user’s authentication factors and the user of the private keys used to authenticate WUAs, PID and attestations managed by the WSCA (i.e. at least those that require binding to a WSCA/WSCD). On the other hand, the wallet provider has more freedom in the choices regarding the management of the confidentiality and integrity of the WUAs, PID and attestations.

There have been discussions about the protection of some of the assets on the user device, in particular the assets used as an ownership authentication factor, typically cryptographic keys. Although these assets are important, they ultimately are under the responsibility of the user being authenticated (*e.g.* keeping a key confidential, just like the user has to keep a PIN code or password confidential). The wallet provider may require the use of specific measures to protect these assets, or even decide that the protection offered by the user device is not sufficient, this does not necessarily make this asset a critical asset to be protected by the WSCA.

Similarly, there are many other cryptographic keys that are used by the wallet unit and the wallet service, for instance to establish communication between the various components of the wallet solution. Although these keys are sensitive assets, but they are not considered critical. The proposal therefore is to limit the minimum role of the WSCA to the protection of the critical assets described above.

Nevertheless, the wallet provider may decide to manage more assets on the WSCA, for instance to protect the integrity and confidentiality of the attestations, or keys that are not critical assets:

- The data used to protect the integrity and, if needed, the confidentiality of WSCA WUAs, of PID and of attestations requiring protection from attackers with a high attack potential.
- The WUAs, PIDs and attestations, may be stored locally in the WSCA instead of only managing their integrity and confidentiality.
- The wallet provider may decide to store keys related to attestations that do not require protection from attackers with a high attack potential in the WSCA.

Finally, one of the essential roles of the WSCA is to ensure that all operations are authorised by the user. When PID and attestations are issued in batches and re-issued, this may create some difficulty that would also make it easier to manage some assets on the WSCA, such as re-

issuance tokens. Such a decision is left to the wallet provider in the design of the wallet unit, but it impacts significantly the role of the WSCA.

Assumptions about the WSCA
In this document, the assumption is that the WSCA manages at least the following critical assets: • The private keys used to authenticate all PIDs and some attestations, related WUAs, and their processing; • The WSCA/WSCD user authentication verification data and the verification itself; • The WSCA also needs to ensure that all operations performed on the WSCD have been explicitly or implicitly authorised by the user. Implicit authorisation may apply to batch issuance, re-issuance and to deletion of WUAs, PID and attestations that cannot be presented. In some cases, additional assets, like re-issuance tokens, may therefore need to be managed by the WSCA.

3.3.2 Keystores and level of assurance

Recent versions of the ARF have introduced the notion of keystores, which complement the WSCA/WSCD to store assets that are sensitive but not critical. The ARF does not specify a minimum level of assurance for such keystores.

The WSCA/WSCD is associated in CIR (EU) 2024/2981 with the AVA_VAN.5 assurance level in EN ISO/IEC 15408 [i.11], so since keystores are not intended to process the assets as critical as those processed by the WSCA/WSCD, it is safe to assume that the requirement for keystores is lower than that.

The OpenId4VCI defines four levels of assurance that may be requested for the management of attestations in keystores. Keystores may be evaluated at levels AVA_VAN.2 to AVA_VAN.5, and there are at least five ways to evaluate their resistance to attacks:

- Evaluate the keystore as a part of the wallet instance at the same level as the wallet instance.
- Evaluate the keystore separately at level AVA_VAN.2, and include in the evaluation of the wallet instance the verification of an assumption that the keystore has been certified at that level.
- Evaluate the keystore separately at level AVA_VAN.3, and include in the evaluation of the wallet instance the verification of an assumption that the keystore has been certified at that level.
- Evaluate the keystore separately at level AVA_VAN.4, and include in the evaluation of the wallet instance the verification of an assumption that the keystore has been certified at that level.
- Evaluate the keystore separately at level AVA_VAN.5, and include in the evaluation of the wallet instance the verification of an assumption that the keystore has been certified at that level.

In the case of a separate evaluation, some aspects still need to be clarified. In particular, there may be a need to establish a distinction between the storage and processing of keys (similar to a WSCD) and their coordination, in particular related to user authorisation (similar to a WSCA). In

addition, the use of the keystore will need to be foreseen in the evaluation of the corresponding wallet instance.

Assumptions on keystores
In the rest of this document, the assumption is that the keystores are either evaluated as part of the evaluation of the wallet instance, or that a mechanism exists to verify that some assurance information is available to justify their status. An additional assumption is that a request for an AVA_VAN.5 keystore would be a request to have an attestation managed by the WSCA/WSCD, and therefore to benefit from the additional protections required for the WSCA/WSCD.

3.3.3 Assurance level of user authentication

User authentication is essential for the security of the EUDI Wallet. In the present document, two distinct authentication types are used:

- Application-level authentication is used to get access to the wallet unit's basic functions.
- WSCA/WSCD authentication is used to get access to the wallet unit's functions that require the use of a private key stored in the WSCD.

CIR (EU)2015/1502 defines in section 2.3 some requirements for authentication mechanisms at assurance level high of eIDAS:

1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication.
2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.
3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

Although the notion of "high attack potential" mentioned here is not directly linked to Common Criteria [i.11], CIR (EU)2024/2981 on the certification of EUDI Wallets requires this mechanism to be certified with the Common Criteria methodology (or equivalent), including an AVA_VAN.5 vulnerability assessment (or equivalent).

However, these requirements pre-exist the EUDI Wallet, so there are different interpretations of how this applies to the EUDI Wallet:

- The requirements for assurance level high apply to every authentication type (application-level and WSCA/WSCD).
- The requirements for assurance level high apply only to WSCA/WSCD authentication.

The first interpretation is disputable, because application-level authentication does not allow the "release of person identification data", which requires WSCA/WSCD authentication. Of course, if one of the authentication factors of application-level authentication is considered as being one of the authentication factors required for WSCA/WSCD authentication, it would then need to be

considered when checking that the overall authentication mechanism meets the requirements of assurance level high of eIDAS.

In the present document it is therefore preferable to consider the application of requirements for assurance level high of eIDAS to WSCA/WSCD-related authentication, which needs to include two authentication factors (typically, knowledge-based and possession-based).

The certification of WSCA/WSCD authentication as part of the WSCA, as required by Article 5(1)(b) of CIR (EU) 2024/2979 [i.14] should not present any issue.

Regarding the part of the authentication mechanism that is implemented on the user device, this level of assurance may be difficult to reach solely from the protection of the authentication mechanisms themselves, but the requirements include additional mechanisms to strengthen this mechanism, including in particular requirements on user interactions intended to increase the likelihood that users will follow the user guidance, and requirements on fraud management, which are specifically intended to address threats related to social engineering.

Finally, there are some debates about the use of mechanisms provided by the user device (with which the user is familiar, but for which no assurance is available in most cases), or to favour mechanisms implemented in the wallet unit itself (less user-friendly, but which can be evaluated during the certification process).

Proposal on authentication
The proposal on authentication would be as follows (loosely based on ARF requirements WIAM_15 and following): • Multi-factor authentication is required before performing any operation (i.e. on startup) • It should include at least one OS-level mechanism • It may be complemented by a wallet unit-specific authentication mechanism (e.g. PIN) • The wallet unit-specific mechanism may be mandatory or offered as option to the user. • The mandatory mechanisms taken together are expected to provide an acceptable level of security for normal operations • For operations requiring eIDAS LoA high (including at least Issuance and presentation of PID and some EAAs), a specific authentication of the user by the WSCA/WSCD is required (for each user-triggered operation).

SECTION 3

Requirements

4. Overview

4.1 General

The requirements defined in EN 319 401 [1] are general requirements that apply to all trusted service providers. Although the provision of EUDI Wallets is separated from trust service providers, these requirements are very similar, and in some cases identical (as per Article 5a(20) of Regulation (EU) No 910/2014 [i.1]).

In addition, the object of certification required in article 5c(1) of eIDAS [i.1] is the “EUDI Wallet and the eID scheme under which it is provided”, not a service provider. However, the EUDI Wallet is considered as an ICT service, and the secure operation of this service includes many requirements on the provider’s processes. In addition, EN 319 403-1, which specifies the requirement for CABs assessing TSPs and their services, is based on ISO/IEC 17065, so its main focus is the service provided rather than the TSP itself. Therefore, the requirements in chapters 4 to 8, inherited from EN 319 401 [1], should be understood as applying to the entity who provides the EUDI Wallet service, not necessarily as the entire organisation of the wallet provider.

Unless specified otherwise, the requirements in Chapters 4 to 7 can apply to all service providers involved in the provision of the EUDI Wallet and the eID scheme under which it is provided, including at least the wallet provider, the PID provider or the validation service provider. When mentioned collectively, they are referred as EUDI service providers.

> NOTE: As of today, the present document does not contain any requirements that are specific to providers of validation services.

Also, in the requirements in Chapters 4 to 7, whenever the requirements in EN 319 401 [1] mention “trust service” or related terms, they should be understood as described below.

- “trust service” should be understood as “EUDI service”
- “trust service component” should be understood as “EUDI service component”
- “trust service policy” should be understood as “EUDI service policy”
- “trust service practice statement” should be understood as “EUDI service practice statement”
- “Trust Service Provider” should be understood as “EUDI service provider”

In addition, EUDI service components are not limited to services, but they also include product or process components, in particular those that may be subject to a specific evaluation, such as the WSCA and the wallet instance.

4.2 Applicability of Conditional Requirements

GEN-4.2-01: The requirements specified in EN 319 401 [1], clause 4.2 shall NOT apply, and the [PRO] indication shall not be used.

> NOTE: The proposal is to not apply proportionality to the EUDI wallet security requirements and to rather define the expected assurance level where required.

GEN-4.2-02: The requirements indicated by “[PRIVACY]” are optional.

NOTE: These requirements are related to privacy, so they are not directly in scope of the cybersecurity certification, but they may be considered in the evaluation in order to optimise the overall evaluation activities (e.g. by performing a single audit). In addition, the controls used to meet these requirements are usually relevant to cybersecurity, so they are already in scope of the cybersecurity certification.

5. Risk Management Framework and Risk Assessment

GEN-5-01: The requirements specified in EN 319 401 [1], clause 5 shall apply.

NOTE: These requirements define an extensive risk management framework, taking into account the specific risks associated to the service's definition and architecture, so it covers the obligation to include risks that are specific to the wallet's architecture.

GEN-5-02: The risk assessment shall consider as input the risk register defined in Annex 1 of CIR (EU) 2024/2981 [i.3].

NOTE: A mapping of the requirements defined in the present document to the risks and threats identified in the risk register is included in Annex B.

6. Policies and Practices

6.1 Wallet Service Practice statement

GEN-6.1-01: The requirements specified in EN 319 401 [1], clause 6.1 shall apply.

NOTE: There are requirements to make documentation about the service available to its users, so the provisions in this section support both this aspect and the description of the service that is anyway required for certification.

6.2 Terms and Conditions

GEN-6.2-01: The requirements specified in EN 319 401 [1], clause 6.2 shall apply.

NOTE: The requirements on information to users are defined in CIR (EU) 2015/1502, sections 2.1.1 and 2.4.2.

GEN-6.2-02: The published terms and conditions shall include a privacy policy.

NOTE: This is from CIR (EU) 2015/1502 [i.2], section 2.4.2, point 1.

GEN-6.2-03: The wallet provider shall define and implement policies and procedures to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service.

NOTE: This is from CIR (EU) 2015/1502 [i.2], section 2.4.2, point 2.

GEN-6.2-04: The wallet provider shall define and implement policies and procedures that provide for full and correct responses to requests for information.

NOTE: This is from CIR (EU) 2015/1502 [i.2], section 2.4.2, point 3.

GEN-6.2-05: The terms and conditions shall list the services that are provided free of charge, which shall include at least the issuance, use and revocation of EUDI Wallets to natural persons and the ability for natural persons to sign by means of qualified signatures for non-professional purposes.

NOTE: This is a requirement from Article 5a(5)(g) and Article 5a(13) of eIDAS [i.1].

6.3 Information and Network Security Policy

GEN-6.3-01: The requirements specified in EN 319 401 [1], clause 6.3 shall apply, except for requirement REQ-6.3-04.

NOTE: Requirement REQ-6.3-04 has been removed because it mentions notification of changes to the supervisory body. In the case of a certified EUDI Wallet service, notification obligations exist, but they are defined in the certification scheme as a scheme rule rather than as a requirement, with a notification to the certification body, which under specific circumstances has to notify the supervisory body.

7. Wallet provider management and operation

7.1 Internal organisation

7.1.1 General

GEN-7.1.1-01: The requirements specified in EN 319 401 [1], clause 7.1.1 shall apply.

GEN-7.1.1-02: The wallet provider shall operate effectively an information security management system based on proven standards or principles for the management and control of information security risks.

NOTE: This is a requirement from the Annex to CIR (EU) 2015/1502 [i.2], section 2.4.3. Adherence to EN 319 401 [1] would satisfy the requirement on “proven standards and principles” (from levels of assurance Substantial and High), but it lacks the explicit reference to an ISMS.

7.1.2 Organization reliability

GEN-7.1.2-01: The requirements specified in EN 319 401 [1], clause 7.1.2 shall apply.

NOTE: Article 5a(19) and Article 11 of eIDAS [i.1] define the rules for liability for the EUDI Wallet.

7.1.3 Segregation of duties

GEN-7.1.3-01: The requirements specified in EN 319 401 [1], clause 7.1.3 shall apply.

NOTE: In the context of EUDI Wallets, the segregation of duties should specifically consider potential issues when the same stakeholder has two roles in the wallet ecosystem (e.g., wallet provider and PID provider, or wallet provider and relying party).

7.2 Human resources

GEN-7.2-01: The requirements specified in EN 319 401 [1], clause 7.2 shall apply.

7.3 Asset management

7.3.1 General requirements

GEN-7.3.1-01: The requirements specified in EN 319 401 [1], clause 7.3.1 shall apply.

7.3.2 Assets classification

GEN-7.3.2-01: The requirements specified in EN 319 401 [1], clause 7.3.2 shall apply.

NOTE: There are no specific requirements for every category, but the classification of assets such as personal data, cryptographic data or authentication data should be considered with great care, regardless of their level of criticality.

GEN-7.3.2-02: At least one of the classification levels shall correspond to the critical assets that are protected in the WSCA/WSCD.

NOTE 1: Beyond the wallet unit, if some of these critical assets are identified on the wallet provider's backend, they will also need to be adequately protected.

NOTE 2: Further requirements applying to critical assets are defined in the present document.

GEN-7.3.2-03: The wallet provider should define a classification level that correspond to the assets that are processed on the user device, which are subject to specific risks.

NOTE 1: This is only a recommendation, intended to outline that the classification of assets for wallets is likely to be more complex than for a simple TSP.

GEN-7.3.2-04: The wallet provider shall define one or more levels of protection suitable for the assets related to the device binding of attestations, including at least one that enables binding to the WSCA/WSCD.

NOTE: Since there is an assumption in the present document that a single WSCA is being used, the mandatory level of protection, which is the highest level, should be implemented on the WSCA.

7.3.3 Storage media and asset handling

GEN-7.3.3-01: The requirements specified in EN 319 401 [1], clause 7.3.3 shall apply.

7.4 Access control

7.4.1 General

GEN-7.4.1-01: The requirements specified in EN 319 401 [1], clause 7.4.1 shall apply.

7.4.2 Privileged and system administration accounts

GEN-7.4.2-01: The requirements specified in EN 319 401 [1], clause 7.4.2 shall apply.

7.4.3 Administration systems

GEN-7.4.3-01: The requirements specified in EN 319 401 [1], clause 7.4.3 shall apply.

7.4.4 Identification

GEN-7.4.4-01: The requirements specified in EN 319 401 [1], clause 7.4.4 shall apply.

7.4.5 Authentication

GEN-7.4.5-01: The requirements specified in EN 319 401 [1], clause 7.4.5 shall apply.

NOTE: More requirements related to authentication are defined throughout the specific requirements in Chapters 8 and 9. In particular, see section 8.3.1 for horizontal requirements related to authentication.

7.4.6 Multi-factor authentication

GEN-7.4.6-01: The requirements specified in EN 319 401 [1], clause 7.4.6 shall apply.

NOTE: These requirements apply to the wallet provider's infrastructure.

7.5 Cryptographic controls

GEN-7.5-01: The requirements specified in EN 319 401 [1], clause 7.5 shall apply.

GEN-7.5-02: The cryptography used in the implementation of wallet solutions shall implement the recommended mechanisms referred in the ECCG Agreed Cryptography Mechanisms [2], considering the relevant implementation guidance.

NOTE: The most sensitive cryptographic algorithms are expected to be implemented in the WSCD and used directly only from the WSCA, both of which are expected to be evaluated at a level including a vulnerability assessment at level AVA_VAN.5, or equivalent activities.

GEN-7.5-03: Beyond the wallet unit and the WSCA/WSCD, critical cryptographic assets that are processed on the provider's systems shall be protected with a level of resistance to attacks similar to that of the WSCA and WSCD.

NOTE: This implies that HSMs should be used for such assets (similar to a WSCD), and that the way in which they are accessed should also be adequately protected against misuse (similar to a WSCA, but with different requirements).

7.6 Physical and environmental security

GEN-7.6-01: The requirements specified in EN 319 401 [1], clause 7.6 shall apply.

GEN-7.6-02: For components that are critical to the secure operation of the service, and in particular if they have been certified separately, the protection of their physical environment shall meet the requirements of these components' security guidance to the expected level of security.

NOTE: This complements the several mentions in EN 319 401 [1], clause 7.6 to components whose security is critical, reminding what requirements have to be met. This should cover at least the WSCD and the WSCA when they are operating on the wallet provider's facilities, and even more specifically the WSCA in cases where it runs outside of the WSCD.

7.7 Operation security

GEN-7.7-01: The requirements specified in EN 319 401 [1], clause 7.7 shall apply.

7.8 Network security

GEN-7.8-01: The requirements specified in EN 319 401 [1], clause 7.8 shall apply.

7.9 Vulnerabilities and Incident management

7.9.1 Monitoring and logging

GEN-7.9.1-01: The requirements specified in EN 319 401 [1], clause 7.9.1 shall apply.

7.9.2 Incident response

GEN-7.9.2-01: The requirements specified in EN 319 401 [1], clause 7.9.2 shall apply.

7.9.3 Reporting

GEN-7.9.3-01: The requirements specified in EN 319 401 [1], clause 7.9.3 shall apply.

NOTE: eIDAS [i.1], in Article 5a(20), defines specific notification requirements.

7.9.4 Event assessment and classification

GEN-7.9.4-01: The requirements specified in EN 319 401 [1], clause 7.9.4 shall apply.

7.9.5 Post-incident reviews

GEN-7.9.5-01: The requirements specified in EN 319 401 [1], clause 7.9.5 shall apply.

NOTE: eIDAS [i.1], in Article 5a(10), defines specific requirements about notification of technical problems and incidents by users.

7.9.6 Fraud management

GEN-7.9.6-01: The EUDI provider shall keep itself informed about fraud and fraud attempts on the services it provides.

NOTE 1: Here, fraud is to be understood as social engineering or exploitation of a user device issue or vulnerability.
Social engineering is a successful attempt by a malicious agent to make a user of the EUDI Wallet perform an operation on their behalf, hence allowing them to misuse the user's identity or attributes, without exploiting a specific vulnerability.

NOTE 2: The main characteristic of fraud is that it does not rely on a vulnerability of the certified ICT service, but either on abusing the user or on exploiting a vulnerability or issue on the user device.

GEN-7.9.6-02: The EUDI provider shall analyse the fraud or fraud attempt, and identify, where possible, the opportunity exploited by the malicious agent and the root cause in the implementation of their service.

NOTE: The objective is here to identify whether a specific feature of the EUDI Wallet, for instance in its user interface, has provided an opportunity to the malicious agent to convince their victim of performing the operation on their behalf. There is not always such an issue, as the malicious agent may use other means (e.g., constraint, general confusion of the user).

GEN-7.9.6-03 [CONDITIONAL]: If a root cause has been identified that creates an opportunity for fraud, it shall then be managed as a vulnerability.

NOTE: The objective is here to reduce the opportunity for malicious agents, by treating the specific feature that helped them perform fraud as a vulnerability, requiring some mitigation.

NOTE: Another objective is here to allow the information about fraud to be distributed to NCCAs in application of the vulnerability management and disclosure obligations.

GEN-7.9.6-04 [CONDITIONAL]: If a fraud or fraud attempt is managed as a vulnerability, the EUDI provider shall share the resulting impact assessment report and proposed mitigation with the certification body, regardless of the materiality of the impact.

NOTE: The objective is here to share the information as widely. The scheme shall then require the certification body to share the information further if they think it should.

7.10 Collection of evidence

GEN-7.10-01: The requirements specified in EN 319 401 [1], clause 7.10 shall apply.

NOTE: These requirements cover the requirements on record keeping defined in section 2.4.4 of the Annex to CIR (EU) 2015/1502 [i.1].

7.11 Business continuity management

7.11.1 General

GEN-7.11.1-01: The requirements specified in EN 319 401 [1], clause 7.11.1 shall apply.

7.11.2 Back up

GEN-7.11.2-01: The requirements specified in EN 319 401 [1], clause 7.11.2 shall apply.

7.11.3 Crisis management

GEN-7.11.3-01: The requirements specified in EN 319 401 [1], clause 7.11.3 shall apply.

7.12 Wallet provider termination and termination plans

GEN-7.12-01: The requirements specified in EN 319 401 [1], clause 7.12 shall apply.

7.13 Compliance

GEN-7.13-01: The requirements specified in EN 319 401 [1], clause 7.13 shall apply.

NOTE: These requirements are considered to cover the requirements from section 2.4.7 of the Annex to CIR (EU) 2015/1502 [i.2], in particular because certification of the EUDI Wallet service is required, including periodical third-party audits.

7.14 Supply chain

7.14.1 Supply chain policy

GEN-7.14.1-01: The requirements specified in EN 319 401 [1], clause 7.14.1 shall apply.

7.14.2 Supply chain procedures and processes

GEN-7.14.2-01: The requirements specified in EN 319 401 [1], clause 7.14.2 shall apply.

7.14.3 Responsibility, third parties agreements and SLA

GEN-7.14.3-01: The requirements specified in EN 319 401 [1], clause 7.14.3 shall apply.

GEN-7.14.3-02 [CONDITIONAL]: When the wallet-related service provider makes use of other parties, all relevant requirements from the present document shall be met by this other party.

NOTE: This requirement entails that the tasks performed by third-parties are fully in scope of the certification, so evidence needs to be provided that the third-party satisfies these requirements (e.g. if a cloud service is used, relevant assurance documentation must be available for that cloud service).

8. Wallet Unit requirements

IMPORTANT NOTES:
Some requirements in this section are functional requirements that could be at least partially covered by testing, but that may not be fully covered by the specifications as available today. In addition, some of these requirements are essential for the security of the EUDI Wallet, and hence, it is recommended to complement testing with inspection, to ensure that the requirement is fully covered in the implementation.

Other requirements cannot be tested, as they relate to the security of the implementation. Therefore, the evaluation needs to rely on audit and inspection. Audit is used in particular for the requirements that relate to features that are not fully specified and for which the wallet provider is expected to write policies or specifications.

In this chapter, requirements include an indication of their essential nature, using **Fun** for functional requirements and **Sec** for security requirements, inserted in the requirement identifier.

Some requirements that are stricter than the ARF [i.8] are written as recommendations, using "should", together with a note.

8.1 General and lifecycle requirements

WUG-8.1-Fun-01: [ARF WIAM_07] The wallet unit shall be activated by issuing at least one WUA bound to its WSCA/WSCD before the user can use it to have a PID issued.

NOTE 1: This is only testing, because there should not be any possibility to issue a PID without an attestation, so this is mostly about verifying that the option is not even available to the user.

NOTE 2: Since there may be WUAs on keystores, the intention is here to ensure that a wallet unit cannot be considered activated without a WUA describing the WSCA/WSCD.

NOTE ON ASSESSMENT:
Testing: Include negative use cases in which the user attempts to get a PID before activating the wallet or by only provisioning a keystore WUA (these may need to be interactive tests).

WUG-8.1-Fun-02: The wallet unit shall not support the issuance of attestations before a PID has been issued to it and activated.

NOTE: This recommendation goes beyond the ARF [i.8], as it suggests the provision of a PID before the provision of an attestation. The main reasons are here to exclude potential security issues, since some verifications of the user's identity are performed only during the installation of a PID, and also to match the formal definition of the EUDI Wallet as an eID means, which is only true after provisioning a PID. There isn't a consensus on this requirement at this stage.

NOTE ON ASSESSMENT:
Testing: Include negative use cases in which the user attempts to get a an EAA before activating a PID (these may need to be interactive tests).
Inspection: Focus on the checks performed before allowing a user to launch an operation. If an attestation can be issued before a PID, ensure that the situation cannot be exploited.

WUG-8.1-Sec-03: [ARF WUA_09] A WUA shall contain one or more public key(s), and the corresponding private key(s) shall be generated by the WSCA/WSCD or the keystore described in the WUA.

NOTE ON ASSESSMENT:
Inspection: Verify that the private keys are generated in the WSCA/WSCD or the keystore, as required.

WUG-8.1-Sec-04: [ARF WUA_10a] A Wallet Unit shall not send a WUA to an Attestation Provider when requesting a non-device-bound attestation.

NOTE ON ASSESSMENT:
Functional testing: Verify the absence of the WUA when an attestation provider indicates in its credential issuer metadata that it issues.

WUG-8.1-Sec-05 [CONDITIONAL]: [ARF WUA_16] If a WSCD is able to export private keys, the wallet provider shall specify this capability as an attribute in the WUA.

NOTE 1: This is mostly about the export of keys for the purpose of backing up the content of a remote WSCD (HSM), or to transfer data to a new one. This capability has to be considered as a potential security issue.

NOTE 2: If a WSCD offers the possibility to create keys as individually exportable, this possibility should not be used, in particular since the WSCA is explicitly forbidden from using it.

NOTE ON ASSESSMENT:
Inspection: Verify that the feature is declared if present.

WUG-8.1-Sec-06: [WIAM_09] If a WSCA/WSCD contains cryptographic keys related to multiple wallet units, a wallet unit shall only be able to access keys and other assets that are related to that wallet unit.

NOTE: This requirement applies in particular to remote WSCAs, which will handle critical assets on behalf of many wallet units. This issue may for instance be addressed by mutual authentication at the communication protocol level. In addition, on devices with the possibility of hosting multiple users, a local WSCA may also need to implement isolation measures.

NOTE ON ASSESSMENT:
Inspection: Verify that the use of a key managed by a remote WSCA is only possibly after authenticating the user to whom the key belongs. For remote WSCAs, verify that the wallet instance is authenticated before allowing access to the wallet unit services and to the WSCA.

WUG-8.1-Sec-07: [WIAM_12a] The wallet provider shall not access at any time the contents of the wallet unit that are stored outside of the wallet provider's own systems, and in particular on the user device.

NOTE ON ASSESSMENT:
Inspection: For all data stored on the user's device, ensure that the wallet provider does not have any way to get access to the data.

WUG-8.1-Sec-08: [WIAM_12a] The wallet provider shall define and implement strict controls to limit the access by the wallet provider to the contents of the wallet unit that are stored on the wallet provider's own systems, 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.

NOTE 1: This requirement will imply a strict separation between the infrastructure that supports the wallet units and the infrastructure that implements the wallet provider's own obligations, combined with strict encryption and access control policies. However, if the wallet provider hosts (part of) the wallet units in its own infrastructure, there may be exceptional circumstances where such an access may occur, with strict controls.

NOTE 2: This requirement is slightly weaker than that from the ARF, which totally forbids access by the wallet provider, and may be difficult to meet on implementations where the wallet unit is totally or partially hosted by the wallet provider.

NOTE ON ASSESSMENT:
Inspection: Verify that the wallet unit service is clearly separated from the other services provided by the wallet provider from its backend. Furthermore, for all wallet unit data managed by the wallet unit service, verify that specific measures are taken to ensure that the user data cannot be accessed by employees, for instance using encryption and access control. If access can be allowed for exceptional reasons (*e.g.* forensics), ensure that the process is well-defined and that all accesses are logged.
For all data stored on the user's device, ensure that the wallet provider does not have any way to get access to the data.

WUG-8.1-Fun-09: [ARF WIAM_21] The wallet unit should define a process to ensure that cryptographic key material stored in the WSCA/WSCD gets eventually destroyed when the associated PID or attestation cannot be presented any longer to relying parties, for example because they have expired or because a once-only attestation was presented to a relying party already..

NOTE: This requirement focuses on the WSCA/WSCD because the destruction of keys can only be performed after successfully authenticating the user with WSCA/WSCD authentication.

NOTE ON ASSESSMENT:
Audit: Assess the process to verify that the destruction of keys is effective and secure.
Inspection: Verify that the check and removal of keys is happening when the process is applied, and that the accumulation of expired keys in the WSCA/WSCD is avoided.

8.2 Handling of PID and attestations

8.2.1 PID and EAA issuance

WUI-8.2.1-Sec-01: [ARF ISSU_05] A wallet unit shall not allow the presentation of a PID that has not been activated.

NOTE ON ASSESSMENT:
Inspection: Verify that the presentation of a PID is not allowed before the completion of the activation. The inspection may include some specific testing, but the tests will need to be specific for each implementation.

WUI-8.2.1-Sec-02: After the user approves the issuance of an abstract PID or abstract device-bound attestation, the wallet unit shall request the issuance of one or several PIDs or attestations.

NOTE: This requirement has simply been added to introduce the notion of “abstract PID” and “abstract attestation”, which are tied to the approval of the user during their initial issuance, in addition to the more concrete “PID”/”attestation” terms that refer to the technical representation of a PID or attestation (which may be renewed through re-issuance many times without renewing the user approval).

NOTE ON ASSESSMENT: There is no need for specific assessment here, as this is addressed through other requirements.

WUI-8.2.1-Sec-03: [ARF WUA_05a] Before the issuance of a device-bound attestation, a wallet unit shall retrieve the requirements of the attestation provider regarding key storage from the Credential Issuer metadata. The wallet unit shall then determine which of its WSCA/WSCD or keystore(s), if any, comply with these requirements. If a compliant WSCA/WSCD or keystore is available to the wallet unit, the wallet unit shall provide the attestation provider with a valid WUA describing the selected WSCA/WSCD or keystore.

NOTE 1: There are at least four settings defined in the OpenID4VCI protocols, corresponding to attacker potentials basic, enhanced basic, intermediate and high, as defined in ISO/IEC 18045, corresponding to levels AVA_VAN.2 to AVA_VAN.5. The highest level (high attack potential) could be reserved for the WSCA/WSCD, and the other levels assigned to keystores. Note that the setting is optional, which means that it is also possible to not provide any requirement, in which case the WSCA/WSCD and all keystores would be acceptable.

NOTE 2: There is no requirement to implement keystores, so a wallet unit may always answer with a WUA describing the WSCA/WSCD, which is supposed to satisfy the all levels of security.

NOTE 3: There is no direct link between the values that an attestation provider may require and the minimum level required in the certification of a wallet unit. Nevertheless, the response needs to rely on actual assurance, either because the keystore was in scope of the assessment of the wallet instance, or because assurance is available from other sources.

NOTE ON ASSESSMENT:
Testing: Test with different kinds of security requests and check the answers.
Inspection: Verify that the description of the WSCA/WSCD or keystore is accurate and for

keystores, that the mechanism that verifies the availability of appropriate assurance information is sound.

WUI-8.2.1-Sec-04: [ARF ISSU_12b] Before the issuance of a PID or device-bound attestation, the wallet unit shall request the WSCA/WSCD or a keystore to generate a new key pair for the new PID or attestation.

NOTE: This requirement is mostly a security requirement as its main focus is to ensure that critical assets like PID and EAA private keys are processed where intended (WSCD or keystore). Nevertheless, testing can be used to ensure that the generated keys can be properly used to implement specifications.

NOTE ON ASSESSMENT:
Inspection: Verify that all private keys are stored in the WSCD or in a keystore as needed and only processed inside it.

WUI-8.2.1-Sec-05: [ARF WUA_05] Before the initial issuance of a PID, the wallet unit shall provide the PID Provider with a valid WUA describing the WSCA/WSCD that generated the new PID private key.

NOTE ON ASSESSMENT:
Inspection: Verify that the description of the WSCA/WSCD is accurate.

WUI-8.2.1-Sec-06: Before requesting the initial issuance of a PID, the wallet unit shall request the user to set up the authentication factors for WSCA/WSCD authentication.

NOTE: There is no precise timing required for the setup of WSCA/WSCD authentication except for this requirement, although it should normally occur before the generation of the first WUA on the WSCD that will host the PID, even if the management of WUAs is supposed to be transparent for users (this requirement may be moved to wallet activation).

NOTE ON ASSESSMENT:
Inspection: Verify that it is impossible to request the initial issuance of a PID before setting up the authentication factors for WSCA/WSCD authentication.

WUI-8.2.1-Sec-07: [ARF ISSU_11] A wallet unit shall request the user's approval before concluding the initial issuance of a PID or attestation obtained from a PID provider or attestation provider, after displaying the contents of the PID or attestation to the user and informing 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.

NOTE ON ASSESSMENT:
Testing: Perform interactive tests to ensure that all the required information is presented in a truthful manner.

8.2.2 PID and attestation management

WUM-8.2.2-Fun-01: [ARF ISSU_37] A wallet unit shall support the once-only and limited-time methods for limiting the number of times a user can present the same PID or attestation to relying parties: In addition, a wallet unit may support the rotating-batch and per-Relying Party methods.

NOTE: These methods are under-defined in the ARF [i.8], so a Technical Specification would be eventually required if they are to be used.

NOTE ON ASSESSMENT:
Inspection: Ensure that the methods that are documented as supported actually are and ensure that at least the once-only and limited-time methods are supported.

WUM-8.2.2-Fun-02: [ARF_ISSU_43] All PIDs and attestations in a batch shall have the same attribute values and the same technical validity period.

NOTE ON ASSESSMENT:
Inspection: Ensure that if the expected property is used to optimise the implementation, then it is verified by the wallet unit when a batch is issued.

WUM-8.2.2-Fun-03: [ARF ISSU_50] When the selected presentation method cannot be used by lack of available instances, then the wallet provider shall define under which conditions the wallet unit may fall back to another method, including at least the choice of the method and the way in which transitions are performed to that method and then back to the default method when the conditions are met again.

NOTE: The conditions under which the wallet unit may fall back to another method are not clearly specified in the ARF, which we here consider as flexibility left to the wallet provider. This requirement simply mandates that the conditions in which this happens need to be clearly defined.

NOTE ON ASSESSMENT:
Audit: Assess the completeness and consistency of the proposed conditions
Inspection: ensure that the implementation matches that description, possibly using dedicated testing.

WUM-8.2.2- Fun-04: [ARF ISSU_58] A wallet unit shall give its user the option to manually initiate a re-issuance process for any of the abstract PIDs or attestations in their wallet unit.

NOTE: If the re-issuance is to be attempted immediately, the wallet unit may require the user to authenticate to the WSCA/WSCD.

NOTE ON ASSESSMENT:
Inspection: Ensure that the feature has been implemented.
Testing: Verify that the identified feature is effective, under appropriate security conditions.

WUM-8.2.2- Fun-05: [ARF ISSU_60] A wallet unit shall gracefully handle situations in which re-issuance of a PID, attestation, or WUA fails or is refused by the PID provider, attestation provider, or wallet provider, for example by attempting a retry after an appropriate delay.

NOTE ON ASSESSMENT:
Inspection: Ensure that there are more attempts to get attestations after a failure or refusal, under appropriate security conditions.

WUM-8.2.2- Fun-06: [ARF 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 attestations, and shall notify the user in case of any differences.

NOTE: This is a minimal requirement. The user may be given the possibility to remove the existing PID or attestation, or to reject the incoming one(s).

NOTE ON ASSESSMENT:
Testing: Ensure that differences are always identified, and that the user information is appropriate when differences are identified.

WUM-8.2.2-Sec-07: [ARF ISSU_65] The wallet unit shall implement a mechanism to prove that a re-issued PID or device-bound attestation is issued to the same wallet unit as the existing PID or attestation, and in the same WSCA/WSCD or keystore.

NOTE: This may be implemented through refresh tokens issued during the initial issuance of the PID or attestation, which need to be protected appropriately. Note that for re-issuance with the WSCA, the refresh token is likely to require the same level of security as the WSCA (i.e. probably stored and processed in the WSCA).

NOTE ON ASSESSMENT:
Audit: Assess the mechanism and ensure that it provides an adequate level of security.
Inspection: Ensure that the presence of a valid PID or attestation is tested.

WUM-8.2.2- Fun-08: [ARF ISSU_62] If a PID, attestation, or WUA was successfully re-issued with at least one change in the value of its attributes (including attributes being added or deleted), a wallet unit shall not present any further the obsolete PID, attestation, or WUA instances, and should delete them.

NOTE ON ASSESSMENT:
Testing: Ensure that the obsolete items are not presented in different situations, including at least one where all the up-to-date items have been “consumed”.
Inspection: Ensure that the obsolete items are identified and deleted or otherwise made unsuitable for presentation.

WUM-8.2.2- Fun-09: [ARF PAD_02] If the user indicates that a PID or attestation must be deleted, and the wallet unit contains multiple PIDs or attestations having the corresponding attestation type and provider, a wallet unit shall delete all of these PIDs and attestations simultaneously.

NOTE ON ASSESSMENT:
Testing: Verify that the deleted PID or attestation cannot be presented, and that they cannot be re-issued, even if there is a pending re-issuance request.
Inspection: Ensure that all concerned PID instances or attestation instances are identified and deleted.

WUM-8.2.2- Fun-10 [PRIVACY]: [ARF PAD_03] If the wallet unit deletes a PID or device-bound attestation on the user's request, the wallet unit shall not notify the respective PID provider or attestation provider.

NOTE ON ASSESSMENT:
Inspection: Ensure that the deletion operation does not trigger any communication with the PID or attestation provider.

WUM-8.2.2-Sec-11: [ARF 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 or keystore related to this PID or attestation is securely destroyed.

NOTE ON ASSESSMENT:
Inspection: Ensure that the deletion operation triggers the deletion of key material from the WSCA/WSCD or keystore.

8.2.3 PID and EAA presentation

WUP-8.2.3-Fun-01: [ARF RPA_03 RPA_04] A wallet unit shall perform relying party authentication in all PID or attestation presentation transactions to relying parties, whether proximity or remote, using an access certificate, to be verified only against trust anchors in the List of Trusted Entities of all Access Certificate Authorities notified by Member States.

NOTE 1: The requirement is mostly functional, but inspection may be useful to verify that the appropriate LoTEs are used.

NOTE ON ASSESSMENT:
Inspection: Ensure that the appropriate List of Trusted Entities is used.

WUP-8.2.3-Fun-02: [ARF 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.

NOTE ON ASSESSMENT:
Testing: Verify that the message is clear enough, especially if the user is given the possibility to present the attributes anyway (see requirement WUP-8.2.3-Fun-03 below).

WUP-8.2.3-Fun-03: [ARF RPA_06a] If relying party authentication fails for any reason, the wallet unit shall either not present the requested attributes to the relying party.

NOTE: This requirement is stronger than the ARF requirement, but accepting the level of risk is too high.

WUP-8.2.3-Fun-04: [ARF OIA_05] After verifying and processing a PID or attestation presentation request, the wallet unit shall display to the user the identity of the requesting relying party and the requested attributes and ask for the user's approval to present these attributes to that relying party.

NOTE ON ASSESSMENT:
Testing: Extensive testing needs to be performed to ensure that the display occurs only after the full verification of the request, and that the interaction with the user follows the requirements in 1.1.1.

WUP-8.2.3-Fun-05: [ARF 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.

NOTE ON ASSESSMENT:
Testing: Include test cases to ensure that the only way to successfully pass the interaction is to approve the presentation.

WUP-8.2.3-Fun-06: [ARF 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.

NOTE ON ASSESSMENT:
Testing: The testing should be integrated into the testing of WUP-8.2.3-Fun-01.

WUP-8.2.3-Fun-07 [CONDITIONAL]: [ARF EDP_05] If the embedded disclosure policy contains a link to the website of the attestation provider explaining the disclosure policy in layman's terms, the wallet unit shall display the link to the user and allow them to navigate to that website.

NOTE: The embedded disclosure policy should include this link.

NOTE ON ASSESSMENT:
Testing: The testing should be integrated into the testing of WUP-8.2.3-Fun-01, and it should ensure that navigating to the website does not disturb the process.

WUP-8.2.3-Fun-08 [CONDITIONAL]: [ARF RPI_07] In case a wallet unit receives a presentation request from an intermediary on behalf of an intermediated relying party, it shall display the names and identifiers of both the intermediary and the intermediated relying party to the user, as described in OIA_05.

NOTE ON ASSESSMENT:
Testing: The testing should be integrated into the testing of WUP-8.2.3-Fun-01.

WUP-8.2.3-Fun-09: For the presentation of PID, the approval by the user shall be linked to the appropriate authentication of the user.

NOTE ON ASSESSMENT:
Testing: Include test cases to ensure that the only way to successfully pass the interaction is to approve the presentation and to confirm it with WSCA/WSCD authentication.

WUP-8.2.3-Fun-10: [ARF RPA_11] When the presentation of a PID or attestation is denied by the user, the wallet unit shall behave towards the relying party as if the PID or attestation did not exist.

NOTE ON ASSESSMENT:
Testing: Include test cases to ensure that the response is appropriate.

WUP-8.2.3-Fun-11: [ARF OIA_06] After receiving the user's approval, the wallet unit shall present only the requested attributes to the relying party.

NOTE ON ASSESSMENT:
Testing: Test cases need to cover different types of requests and ensure that only the requested attributes are presented, after user approval.
Inspection: Ensure that the integrity of the list of attributes to be presented is protected from its creation to the creation of the response to the request.

WUP-8.2.3-Fun-12: [ARF OIA_10] If a wallet unit contains more than one PIDs having the same encoding 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.

NOTE 1: This is not about technical instances of the same PID, but about two different PID issued to the same person, possibly from different providers.

NOTE 2: This interaction is not described in detail, but it should occur before the authorisation to present the attributes.

NOTE 3: The way in which the wallet unit decides by context is not defined here, as it may depend greatly on specific use cases, but these decisions need to be described precisely by the wallet provider.

NOTE ON ASSESSMENT:
Audit: Confirm the existence of documentation about decisions made from context and confirm that the technical measures considered match the stated objectives.
Inspection: Ensure that the feature is implemented following its specification and that it is integrated in the flow in a way that is not confusing for the user.

WUP-8.2.3-Fun-13: [ARF OIA_11] If a wallet unit contains more than one attestations having the same encoding and attestation type, and a relying party requests an attestation, the wallet unit shall ask the user which of these attestations they want to release, unless the wallet unit can decide from context.

NOTE: See the notes on WUP-8.2.3-Fun-12 above.

WUP-8.2.3-Sec-14: The wallet unit shall ensure that the values communicated for PID and attestation attributes are the same values that were issued to them.

NOTE 1: This requirement is about the integrity of the attribute values at rest and in use, as their integrity are not by default protected by a mechanism from the platform itself, so attacks could be feasible on the wallet instance.

NOTE 2: The authenticity of the attributes in the attestation as it is distributed is protected within the attestation itself, but there is no guarantee that it has not been injected or replaced.

NOTE ON ASSESSMENT:
Inspection: Ensure that measures are being taken that provides an adequate protection of the values of the attributes, compatible with the eIDAS level of assurance ‘high’.

8.3 Horizontal requirements

8.3.1 User authentication

WUH-8.3.1-Sec-01: Application-level authentication shall not enable the use of critical cryptographic assets whose access is protected by WSCA/WSCD authentication.

NOTE: This is guaranteed by the fact that part of the WSCA/WSCD authentication is performed on the WSCD itself, so errors in the other parts of the wallet unit would not enable such use.

NOTE FOR ASSESSMENT:
Inspection: Ensure that the protected keys are stored in the WSCD and that application-level authentication does not allow any access to these keys.

WUH-8.3.1-Sec-02: After the initial setup of application-level authentication, no operation shall be possible on the wallet unit before application-level authentication. In particular, WSCA/WSCD authentication shall not be possible before being authenticated with application-level authentication.

NOTE FOR ASSESSMENT:
Testing: Ensure through interactive tests that no operation is available.

WUH-8.3.1-Sec-03: Verification for application-level authentication shall be performed by the wallet instance using the underlying platform's authentication, unless this is technically impossible (for instance on some legacy devices), or the wallet unit-specific authentication, implemented by the wallet unit itself, is used.

NOTE: Like other aspects related to features provided by the user device, the robustness of the feature is questionable on some devices, which makes their use "technically impossible".

NOTE FOR ASSESSMENT:
Audit: Confirm the existence of a specification for application-level authentication, including conditions for eligibility of native authentication and a mechanism to enforce these conditions.
Inspection: Ensure that the specification is adequately implemented. Perform *ad hoc* tests to verify the implementation of the mechanisms.

WUH-8.3.1-Sec-04: In order to ensure that operating system-level authentication can be used and is sufficiently secure, during installation of the wallet user interface application, the wallet user interface application shall enforce the activation of an OS-level user authentication mechanism with adequate security policies.

NOTE FOR ASSESSMENT:
This should be part of the audit and inspection mentioned in WUH-8.3.1-Sec-03.

WUH-8.3.1-Sec-05: During installation of the wallet instance application, the wallet unit shall enable the user to indicate if they want to use a wallet unit-specific authentication for application-level authentication. The wallet unit shall enable the user to change this preference during the lifetime of the wallet unit.

NOTE: This requirement allows the use of a local authentication mechanism, which then needs to be fully described, including the mechanisms to be used, if any, for instance when the user forgot the value of the PIN.

NOTE FOR ASSESSMENT:
Audit: Confirm the existence of a specification for the mechanism, confirm that it contains all needed processes, including for managing authentication methods, and confirm that the specified mechanisms provide an adequate level of protection.
Inspection: Ensure that the specification is adequately implemented, with the expected level of countermeasures. If the implementation appears weak, consider penetration testing.

WUH-8.3.1-Sec-06: For application-level authentication, a wallet unit shall define and implement conditions after which user authentication shall again be required, including at least an idle timeout. The wallet unit should provide the user with the option to set the idle timeout to a duration shorter than the default timeout.

NOTE: Time is only one of the parameters to be considered, together with the device getting locked or the application losing focus.

NOTE FOR ASSESSMENT:
Audit: Confirm that there is a timeout, whose parameters are determined following a policy that may depend on the device being used.
Inspection: Ensure that the policy is adequately implemented, and that the user has the ability to set more restrictive conditions and to restore to the original conditions, but not less restrictive ones.

WUH-8.3.1-Sec-07: WSCA/WSCD authentication needs to be based on at least two factors of different categories.

NOTE: Typically, one of the factors is a knowledge factor, complemented by a possession factor, both of them to be verified on the WSCD and linked to the authorisation to use critical cryptographic assets on the WSCD.

NOTE FOR ASSESSMENT:
Inspection: Ensure that at least two factors of different categories are being used.

WUH-8.3.1-Sec-08: The final verification for WSCA/WSCD authentication should be performed on a WSCD, and its implementation shall resist to attacks by attackers possessing high attack potential. Operation on PIDs shall only be possible after WSCA/WSCD authentication on such a device.

NOTE: This requirement is directly inspired from CIR (EU)2015/1502, which requires the verification of authentication to resist to attackers with high attack potential. It is also linked to the next one, which sets lower expectations for the wallet instance.

NOTE: User authentication requirements may be satisfied by a wide variety of solutions, but the final step of the verification needs to be tied to the WSCD, in order to authorise operations on critical assets.

NOTE ON ASSESSMENT:
Verification for asset-level authentication will normally be included in the evaluation of the WSCD or of the WSCA, typically being performed using Common Criteria [i.11] (EUCC [i.6]).

WUH-8.3.1-Sec-09: Other mechanisms for WSCA/WSCD authentication, including device-side mechanisms, shall resist to attacks by attackers possessing basic attack potential, and should rely on mechanisms provided by the platforms underlying the wallet instance.

NOTE: This requirement focuses on the interaction with the user (knowledge, intrinsic) or with the device (possession), since other processes are covered in WUH-8.3.1-11.

NOTE ON ASSESSMENT:
Here, resistance to attacks is essential, so this could typically be handled through an

evaluation based on a scheme based on the EN 17640 [i.7] standard including at least AVA_VAN.3.

WUH-8.3.1-Sec-10: WSCA/WSCD authentication shall only be valid for a single user-authorised operation.

NOTE: This requirement is written from the viewpoint of the user, but other operations may happen in the background, in particular linked to the management of batches. When such operations may be “piggybacked” on a user-authorised operation, a policy needs to describe how only operations linked to a previously authorised operation can be performed.

NOTE FOR ASSESSMENT:
Audit: If a policy is defined to support background operations, confirm that this policy includes measures to prevent unauthorised operations from being performed.
Inspection: Ensure that the policy is appropriately implemented and would resist to an attacker with high attack potential (this policy is not standardised but may nevertheless be complex, so it may represent an opportunity for an attacker, both from potential vulnerable designs and potential vulnerable implementations).

WUH-8.3.1-Sec-11: Processes shall be defined for all required management operations on WSCA/WSCD authentication (initialisation, update, issuance, re-issuance of authentication factors). These processes shall ensure that the authentication factors represent the right person.

NOTE: There may be many such processes, and they all represent a potential opportunity for an attacker. The processes are typically grouped in a policy, and they need to be compatible with the requirements of eIDAS assurance level high.

NOTE ON ASSESSMENT:
Audit: Confirm that required processes are defined in a policy, and confirm that these processes are expected to provide a suitable assurance level is properly implemented.
Inspection/Audit: Ensure that the processes are effectively implemented.

8.3.2 Orchestration

WUH-8.3.2-Sec-01: The validity (formatting) of any external input or request shall be checked before using the input.

NOTE: A typical message includes several formats embedded one into another, and every layer needs to be thoroughly checked before being exploited, from basic tagged data to complex messages. For complex data, it is preferable to use libraries, provided that they are regularly maintained.

NOTE ON ASSESSMENT:
Inspection: Ensure that the format of every data received from the outside is checked before the data is exploited. When libraries are used, ensure that they are used appropriately and that they are mentioned in the dependencies (for vulnerability management).

WUH-8.3.2-Sec-02: Any invalid external input or request shall be rejected with a minimal error message, and the user shall be warned of the issue.

NOTE: Errors like that are not supposed to happen in production, so each one is to be considered like a potential attack, so the sender needs not be told what issue was encountered, just that the message or request was rejected.

NOTE ON ASSESSMENT:
Inspection: Ensure that for every error during the verification of a message, no explanation is provided to the sender, and that the user is warned, also with a simple message.

WUH-8.3.2-Sec-03: The validity and authenticity of any external input or request shall be checked before displaying its characteristics to the user.

NOTE ON ASSESSMENT:
Inspection: Ensure that any external data that is checked before being processed or displayed, and that the checks are sufficient for the processing being performed.

WUH-8.3.2-Sec-04: If the authenticity check of an input or request fails, then the input or request shall be rejected with a minimal error message.

NOTE: This is stronger than the ARF requirement, because the original one is most likely not certifiable, especially for PID. The requirement has been kept to ensure that this is enforced.

NOTE FOR ASSESSMENT:
Testing. This can be easily tested using conformance tests.

WUH-8.3.2-Sec-05: The relevant characteristics of any external input or request shall be displayed to the user before asking the user to take a decision on the action to perform.

NOTE: This is one of the critical aspects, since the content could be designed to fool the user, so the application should take great care to present the content of the request in a way that considers possible issues. There are several issues here, including the identification of the relevant aspects, and their proper presentation.

NOTE FOR ASSESSMENT:
Audit: Confirm the existence of a specification of the information to be displayed for each input or request, and that this information is suitable for the user to take an informed decision.
Inspection: Ensure that the specification is adequately implemented.

WUH-8.3.2-Sec-06: The user should confirm any action on critical assets by a WSCA/WSCD authentication.

NOTE: This is the main requirement for ensuring that all actions on critical assets are properly authorised by the user. It does not require them to be individually authorised, but the EUDI Wallet should be aware of the operations that are to be authorised by a WSCA/WSCD authentication before to request the authentication.

NOTE ON ASSESSMENT:
Audit: Confirm that a policy determining the possible operations has been defined, complemented by a specification defining how these operations are determined, and confirm that the policy and specification comply requirements in the present document.
Inspection: Ensure that the specification is adequately implemented and satisfies the policy.

WUH-8.3.2-Sec-07: An action on critical assets shall only be performed after verifying that all required steps have been followed.

NOTE: This goes beyond simply requiring to perform all steps, as it requires to record the steps performed and to check that record before allowing the operation to proceed.

NOTE ON ASSESSMENT:
Inspection: Ensure that verifications are recorded and that the record is checked before allowing the operation to proceed.

8.3.3 Authenticity and trust anchor checks

WUH-8.3.3-Sec-01: The consuming entity shall ensure that the relevant list of trusted entities is up-to-date before initiating an authenticity check.

NOTE: The frequency of the update depends on the list, but the wallet unit should perform this check at most 24 hours before the list is used. If the lists are stored in the online environment, the wallet provider may update the lists once for all wallet units.

NOTE ON ASSESSMENT:
Inspection: Ensure that the updates are performed. If the lists are shared and updated globally, then ensure that the latest version of the list is used.

WUH-8.3.3-Sec-02: The consuming entity shall ensure that the provider that issued the item currently being checked is in the relevant list of trusted entities.

NOTE: This check needs to happen first, since it enables the verification of the item's authenticity.

NOTE ON ASSESSMENT:
Inspection: Ensure that the presence in the list is the first test performed, before to use the public key to verify the signature.

WUH-8.3.3-Sec-03: The consuming entity shall use the trust anchor registered for the provider in the list of trusted entities to verify the authenticity of the item being checked.

NOTE: The trust anchor from the trusted list is used to verify the validity of the public key provided by the provider, and then to use this public key to verify the authenticity of the item being checked.

NOTE FOR ASSESSMENT:
Inspection: Ensure that the public key provided in the item being checked is valid (using the trust anchor), and then that the public key is used to validate the authenticity of the item being checked.

WUH-8.3.3-Sec-04: After verifying its authenticity, the consuming entity shall parse and validate the item, including at least a verification of its expiration date when present.

NOTE FOR ASSESSMENT:
Inspection: Ensure that once the origin of the item to be checked is validated, its content can be validated and its processing initiated.

WUH-8.3.3-Sec-05 [CONDITIONAL]: If the item is revocable, the consuming entity shall ensure that the relevant revocation list or status list is up-to-date before initiating a revocation check.

NOTE: The frequency of the update depends on the list, but the wallet unit should perform this check at most 24 hours before the list is used. If the lists are stored in the online environment, the wallet provider may update the lists once for all wallet units.

NOTE ON ASSESSMENT:
Inspection: Ensure that the updates are performed. If the lists are shared and updated globally, then ensure that the latest version of the list is used.

WUH-8.3.3-Sec-06 [CONDITIONAL]: If the item is revocable, the consuming entity shall verify that the item has not been revoked.

NOTE ON ASSESSMENT:
Inspection: that the revocation list or status list is used to check the status of the item to be checked.

WUH-8.3.3-Sec-07: Whenever possible, the consuming entity shall not use the item before successfully performing the checks in WUH-8.3.4-Sec-01 to WUH-8.3.4-Sec-06.

8.4 Wallet instance requirements

8.4.1 Protection of assets in the wallet instance

WIN-8.4.1-Sec-01: The wallet instance shall securely store and process data according to its sensitivity.

NOTE: The wallet provider shall rely on its asset management policies to determine the assets' sensitivity and then select the adequate conditions for storing and processing them according to the level of risk. This requirement comes from the OWASP framework for mobile applications [i.9], which provides additional details, including on evaluation activities.

WIN-8.4.1-Sec-02: The wallet instance should use the mechanisms provided by the underlying platform when they are suitable or provide alternative mechanisms when the platform mechanisms are not suitable.

NOTE: This recommends to carefully choose between using platform mechanisms (which may be corrupted) and in-application mechanisms (which may be vulnerable), based on a risk analysis.

NOTE ON ASSESSMENT:
Audit: When applicable, audit the specifications of the process used to determine the suitability of the underlying platform's mechanisms.
Inspection: Ensure that the implementation follows these specifications, if possible including tests with devices that should not be acceptable.

WIN-8.4.1-Sec-03: The wallet instance shall prevent leakage of sensitive data.

NOTE: This requirement comes from the OWASP framework for mobile applications [i.9], which provides additional details, including on evaluation activities.

WIN-8.4.1-Sec-04: [ARF ISSU_35 ISSU_35a] The wallet instance shall use a cryptographically secure random number generator for the generation of all random numbers used by the application (hash salts, identifiers, nonces, etc.).

NOTE: This does not require hardware-based random number generation, as pseudo-random number generation algorithms are available that provide a suitable level of security. Stronger requirements on random number generation are expected for the WSCD, in particular for the generation of cryptographic keys.

NOTE ON ASSESSMENT:
Audit: Audit the specifications of the process used to determine the suitability of the underlying platform's mechanisms, or the specifications of the mechanisms being implemented in the wallet instance to determine their conformity to the requirement.
Inspection: Ensure that the implementation follows these specifications.

WIN-8.4.1-Sec-05: [ARF 6.5.3.5] The wallet instance shall protect the private keys used to authenticate WIAs as suitable.

NOTE: There is no requirement to use a specific WSCA/WSCD or keystore, but the decision is left to the wallet provider.

WIN-8.4.1-Sec-06: All communication between the different components of the wallet unit shall be mutually authenticated and they shall be encrypted when the components are hosted on different systems or devices.

8.4.2 User interaction

WIN-8.4.2-Sec-01: The user interface application shall use the platform's user interface mechanisms securely.

NOTE: This requirement originates from OWASP's MAS framework [i.9]. More detailed information is available from OWASP, also covering assessment activities.

WIN-8.4.2-Sec-02: The user interface shall display information to the user in a consistent and unambiguous way, being aware of phishing attempts

NOTE: There are several user interactions that display content originating from other parties (providers, relying parties), so the user interface needs to be careful to present the information truthfully, to avoid potential abuse.

NOTE ON ASSESSMENT:
Audit: Confirm that the developer has defined measures to ensure that the user interface could not easily be used to misrepresent the content to be displayed and lead a user to wrongfully authorise an operation.
Inspection: Ensure that the measures are effectively implemented.

WIN-8.4.2-Sec-03: The user interface shall unambiguously inform the user about any decision that they are about to take, being aware of phishing attempts.

NOTE: For instance, when confirming an operation and then authorising it, a part of the screen may unambiguously mention the ongoing process.

NOTE ON ASSESSMENT: Include in the scope of the audit for WUI-8.4.2-Sec-02.

WUI-8.4.2-Sec-04: The user interface shall remind the user of the decision that they are about to confirm when asking for WSCA/WSCD authentication.

NOTE: The interaction through which the user authorises an operation by authenticating needs to include information about the operation that is being authorised. It may also include a way for the user to get more information or to get back to the previous step.

NOTE ON ASSESSMENT: Include in the scope of the audit for WIN-8.4.2-Sec-02.

8.4.3 Wallet instance (mobile application)

NOTE ON ASSESSMENT:
Requirements WIN-8.4.2-Sec-01 to WIM-8.4.2-Sec-08 come from the OWASP framework for mobile applications [i.9], which provides additional details, including on evaluation activities

WIN-8.4.3-Sec-01: All wallet instance variants shall require an up-to-date platform version.

NOTE: The platform should be in a version that is recognised as up-to-date by the device manufacturer or platform vendor, and is up-to-date with critical security patches.

WIN-8.4.3-Sec-02: All wallet instance variants shall include a mechanism to enforce its updates.

WIN-8.4.3-Sec-03: All wallet instance variants shall only use software components without known vulnerabilities.

NOTE: This requirement is more complex than the previous ones, since it requires to implement a vulnerability management process that allows them to identify vulnerabilities, assess their impact, and take required actions.

WIN-8.4.3-Sec-04: All wallet instance variants shall validate and sanitize all untrusted inputs.

NOTE: This requirement may be redundant of some horizontal requirements, but the intention is here to ensure that the OWASP MAS [i.9] recommendations are considered.

WIN-8.4.3-Sec-05: All wallet instance variants shall validate the integrity of the platform.

NOTE: This requirement may be refined further. For instance, CEN TS 18098 [i.4] adds in section .2.3.2.2.3.2 that at least the bootloader should be checked, as well as checking whether or not the device has been rooted or jailbroken. Some of these checks may also need to rely on other mechanisms and may be performed by the wallet provider when assessing the suitability of the user device.

WIN-8.4.3-Sec-06: All wallet instance variants shall implement anti-tampering mechanisms.

WIN-8.4.3-Sec-07: All wallet instance variants shall implement anti-static analysis mechanisms.

WIN-8.4.3-Sec-08: All wallet instance variants shall implement anti-dynamic analysis techniques.

WIN-8.4.3-Sec-09: [ARF WIAM_03] All wallet instance variants shall start the wallet instance activation process immediately after installation or when the user first opens the wallet instance application.

NOTE: The wallet instance cannot be used if it has not been activated, this ensures that no other possibility is offered to the user.

WIN-8.4.3-Sec-10: [ARF WIAM_03] All wallet instance variants shall ensure that it starts its activation process only with the secure backend of the wallet provider, by authenticating this backend.

WIN-8.4.3-Sec-11: If a wallet instance determines that the conditions are not fulfilled for initiating the activation process, the wallet instance shall inform the user of the reason(s) that led to that decision.

NOTE: In some cases, the wallet user interface application can determine by itself that it is not running on acceptable conditions, and this should be clearly explained to the user without even authenticating to the wallet provider backend.

WIN-8.4.3-Sec-12: [ARF WIAM_13] If the user uninstalls their wallet instance, 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: This requirement is difficult to meet, because the uninstallation may not allow any communication with the WSCA. The requirement should be reconsidered, but measures should be taken to remove unneeded data from the WSCA. This may also be managed at the platform level, if the uninstallation of an application may trigger the deletion of secure element applications that were only used by this application.

8.4.4 Wallet instance (web application)

WIN-8.4.4-01 [CONDITIONAL]: If a wallet instance is a web application, it shall implement all applicable controls of the OWASP Application Security Verification Standard [i.10] at level 3.

NOTE: Application security verification level 3 is the highest level in this framework, and represents the lowest possible level to be considered for a wallet user interface application.

NOTE ON ASSESSMENT:
The OWASP standard [i.10] includes a chapter on assessment and certification, and the assessment should follow their principles, in particular regarding reporting and scope of assessment.

WIN-8.4.4-02 [CONDITIONAL]: If a wallet instance is a web application, it shall only use the cryptographic algorithms recommended in the ECCG's Agreed Cryptographic Mechanisms document [2].

NOTE: This requirement is mentioned explicitly here because the OWAP Application Security Verification Standard [i.6] includes an appendix on cryptographic mechanisms, which should not be considered sufficient.

8.5 WSCA requirements

NOTE ON ASSESSMENT:
The requirements below are expected to be assessed using the Common Criteria [i.11] methodology, and the requirements below should be included in a Common Criteria [i.11] protection profile or covered by a security target. If equivalent methodologies are used, these requirements nevertheless need to be covered.

WSA-8.5-01: The WSCA shall authenticate the wallet provider before accepting any request from the wallet provider.

WSA-8.5-02: The WSCA shall authenticate the wallet instance before accepting any request from the wallet instance.

WSA-8.5-03: The WSCA shall authenticate the WSCD before performing any request to the WSCD.

NOTE: When the WSCA runs within the WSCD, this authentication may be implicit, as described in the WSCD's security guidance.

WSA-8.5-04: The WSCA shall allow the wallet provider to create one user, and may allow the wallet provider to create several users.

NOTE: This is intended to support both the secure element-based local use case (one user) and the HSM-based remote use case (several users).

WSA-8.5-05 [CONDITIONAL]: If the WSCA allows the wallet provider to create several users, the WSCA shall ensure that the data from a given user, and in particular its own keys, is only accessed after the successful authentication of that user in the same session with the WSCA.

NOTE: The intention is to ensure that on a HSM, only a user can use its keys, but since several sessions may be active in parallel with different users, this needs to be qualified more precisely.

WSA-8.5-06: [ARF WIAM_17] The WSCA shall include mechanisms for user authentication with at least two authentication factors of different categories that meet the requirements of assurance level high in sections 2.2.1 and 2.3 of CIR (EU)2015/1502.

NOTE: This is the WSCA/WSCD authentication, so it needs to satisfy the highest requirements.

WSA-8.5-07: The WSCA shall include mechanisms to manage and use keys on behalf of a user, including the creation of a secret key or of an asymmetric key pair, the use of these keys for their foreseen use (encryption, decryption signature verification, signature validation), and for the export of public keys.

NOTE: These are the core cryptographic feature of the EUDI Wallet, which may need to be further updated to cover all functions.

WSA-8.5-08: [ARF WIAM_14 WIAM_14a WIAM_14b] The WSCA shall only allow the use of cryptographic assets managed by the WSCD after the successful authentication by the WSCD of the user to whom the assets belong.

NOTE: This is the essential requirement to ensure that the user is in control of its data.

WSA-8.5-09: The WSCA shall ensure that only the expected operations can be performed after a successful user authentication.

NOTE: Because a single operation may require several cryptographic operations, and because of the management of assets that happen in the background, we need a requirement to ensure that only the planned operations can be performed.

WSA-8.5-Sec-10: The WSCA/WSCD shall enforce strict rules about the performance of multiple operations following a single authentication.

NOTE: This intention behind this requirement is to ensure that the rules related to the generation of new key pairs by the WSCA/WSCD are well defined, including the support for the re-issuance of PID, attestations, and WUA.

NOTE ON ASSESSMENT:
Audit: Ensure that a set of rules have been defined, and that these rules guarantee that only the planned key pairs can be generated.
Inspection: Ensure that the rules are adequately implemented. Some penetration testing may be required if there are doubts about the enforcement of the rules.

WSA-8.5-Sec-11: [ARF WUA_16] The WSCA shall not export private keys.

NOTE: Even if the WSCD has the possibility to export keys, the WSCA is not expected to use this feature, as there is no need to export private keys. If the WSCD support key export, then the use of this feature is limited to management uses like backups or device replacements.

WSA-8.5-Sec-12 [CONDITIONAL]: [ARF WIAM_20] If the WSCD is able to export private keys, the resulting level of protection of the exported keys shall be equivalent to the protection level of the private key when stored in the WSCD.

WSA-8.5-Sec-13: The WSCA shall not extract critical assets from the WSCD.

NOTE: The critical assets that are managed by the WSCD are intended to be processed in the WSCD, so the WSCA is not expected at any time to extract these assets from the WSCD, regardless of their nature (keys, authentication data, *etc*.).

8.6 Keystore requirements

WKS-8.6-Fun-01: [ARF WIAM_08] The wallet unit may include one or more keystores.

WKS-8.6-Sec-02: The wallet unit shall assign a level assurance to every keystore offered, with the following possible values: iso_18045_moderate, iso_18045_enhanced-basic, iso_18045_basic or none, corresponding to the level of resistance for which the keystore was certified (respectively AVA_VAN.5, AVA_VAN.4, AVA_VAN.3, AVA_VAN.2 and no certification).

NOTE 1: These values can be used by attestation providers when they require a security level in their OpenID4VCI request.

NOTE 2: Level iso_18045_basic may not be suitable for the EUDI Wallet, as it only corresponds to assurance level ‘substantial’ in EUCC.

NOTE 3: Level iso_18045_high is considered to be covered by the WSCA/WSCD, so it is not applicable to keystores.

NOTE ON ASSESSMENT:
Audit: For every keystore, ensure that assurance information is available that it matches the declared level, or that a mechanism is available to ensure that the keystore reaches that level (if it is provided by the user device).
Inspection: Ensure that the mechanisms are adequately implemented. Some penetration testing may be required if there are doubts on the implementation.

9. Wallet provider services requirements

IMPORTANT NOTE:
By default for these requirements, the assessment method is based on an audit to confirm the existence and effectiveness of a policy covering the requirement, complemented by an inspection if required.

Notes on assessment are therefore only added when specific assessment activities, typically related to security, are needed.

9.1 Wallet unit activation and monitoring

WSU-9.1-01: [ARF WUA_04] The wallet provider shall ensure that a non-revoked wallet unit in the "Operational" and "Valid" states is able to present a temporally valid and non-revoked WUA to a PID provider or attestation provider during the issuance process of a PID or device-bound attestation.

> NOTE: If a wallet unit lacks an active WUA, it transitions to temporary states "Operational Expired" and "Valid Expired" until the wallet provider issues a new WUA.

WSU-9.1-02: [ARF WURevocation_09] During the lifetime of a wallet unit, the wallet provider shall regularly verify that the security of the wallet unit is neither breached nor 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 the wallet unit and shall immediately revoke the corresponding WUA(s), and shall extend the analysis to other wallet units that may potentially be impacted. 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 the WSCA/WSCD it uses for managing critical cryptographic assets, 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.

> NOTE 1: The wallet provider should define security measures to perform these checks, both within the wallet unit (integrity and data authenticity checks) and outside of the wallet unit, for instance leveraging mechanisms offered by the execution platforms (for monitoring the authenticity of a wallet instance and of the underlying platform).

NOTE 2: The wallet provider should also engage in fraud management activities, and in particular, when a breach is detected, they should extend the analysis of the cause(s) and impact(s) to other wallet units that may be impacted.

WSU-9.1-03: If within three months from an administrative suspension of a wallet solution the security breach or compromise is remedied, the wallet provider shall inform the users of the wallet units that were revoked that they may activate again their wallet unit.

NOTE: Renewing the activation is the only way to re-activate a wallet unit, but in that case, the operation may be simplified. For instance, the user may have the possibility to authenticate using their existing credentials rather than creating new ones.

WSU-9.1-04 [CONDITIONAL]: [ARF WIAM_01] If such a mechanism exists, the wallet provider should make a wallet instance application available only through the official application store of the relevant platform (*e.g.*, Android, iOS).

NOTE: This is the preferred solution because it may give access to specific mechanisms allowing in particular to verify the authenticity of the wallet user interface application.

WSU-9.1-05 [CONDITIONAL]: If the wallet provider makes a wallet instance application available through an alternative application store, the wallet provider shall ensure that this application store provides sufficient guarantees about the integrity and authenticity of the application.

NOTE: Evidence needs to be provided that such mechanisms are available, preferably backed by assurance information. If the evidence is considered insufficient, the auditor may need to run specific tests.

WSU-9.1-06 [CONDITIONAL]: [ARF WIAM_02] If the wallet provider makes a wallet instance application available through other means, the wallet provider shall provide the user with instructions on how to verify the integrity and authenticity of the application before installing it.

NOTE: That information needs to be accessible and implementable by all users, without requiring specific competences.

WSU-9.1-07 [CONDITIONAL]: [ARF WIAM_02] If the wallet provider makes a wallet instance application available outside of application stores, then the wallet provider shall provide the user with 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 user interface application has been installed.

NOTE: That information needs to be accessible and implementable by all users, without requiring specific competences.

WSU-9.1-08: [ARF 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 a wallet instance application.

NOTE: This typically requires support from the underlying platform. If the application verifies its own authenticity, the mechanism needs to be clearly specified and its effectiveness demonstrated.

WSU-9.1-09: During the activation process of a new wallet unit, the wallet provider shall carry out eligibility checks of the user's device.

NOTE: Checks may be based on information known on the model and version of the device and of its most important components, complemented by checks performed on the device itself.

WSU-9.1-10: The wallet provider shall inform users if their devices are not eligible to be used with the wallet unit.

NOTE: This is most likely going to be done through the wallet instance, but the wallet provider may decide to use an out-of-band communication means if the issue is severe enough.

WSU-9.1-11: [WIAM_05] During the activation process of a new wallet unit, the wallet provider shall process information about the user device and the available WSCA/WSCD and keystores, as far as necessary to issue WUAs and WIAs to the wallet unit.

NOTE: In case the wallet provider provides the WSCA and WSCD, no specific checks need to be performed. In the case of a secure element on the user device, if the WSCA is provided by the wallet provider, then the checks are likely to happen when authenticating the WSCD to load and initialise the WSCA. If the WSCA is included in the user device, then its authenticity needs to be confirmed during the initialisation of the wallet instance.

WSU-9.1-12 [PRIVACY]: [WIAM_05] 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.

WSU-9.1-13 [PRIVACY]: [WIAM_05] 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.

WSU-9.1-14: [WIAM_06] During the activation process of a new wallet unit, the wallet provider shall ensure through the wallet instance that user has a user account at the wallet provider, either by authenticating the user to this account or by setting up a new user account.

NOTE: In some cases, typically if this is not the first wallet unit that a user installs, a user may already have an account with the wallet provider, so the wallet provider should offer to the user the possibility to use existing credentials.

WSU-9.1-15: [WIAM_06] When setting up a user account, the wallet provider shall inform the user of the way to use this user account 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.

NOTE: This authentication methods used for this user account are not related to the methods used to authenticate the user to the wallet unit or to the WSCA/WSCD, as they are intended to

allow the user to get authenticated without using the user device on which the wallet instance is installed.

WSU-9.1-16: [ARF WIAM_08] A wallet provider shall only activate a new wallet unit if it has verified that the wallet unit includes a WSCA/WSCD that is certified to be compliant with applicable requirements, for Level of Assurance High in CIR (EU) 2015/1502] section 2.2.1.

NOTE: This verification should in most cases by part of the verifications performed to fulfil requirement WSU-9.1.1-11. This requirement is particularly important when the WSCA/WSCD is included in the user device.

WSU-9.1-17: [ARF WIAM_10] During the activation process of a new wallet unit, a wallet provider shall verify that the private key corresponding to the public key in the WUA for a given WSCA/WSCD or keystore is protected by the respective WSCA/WSCD or keystore under control of the user.

NOTE: The notion of control by the user is not always easy to define, since the user often does not have the ability to control the content of the WSCA/WSCD (even when the WSCD is on the user device, the user normally does not have the ability to manage the content of the WSCD). The control by the user is therefore exercised by the obligation for the user to authenticate themselves before any operation can be performed, and by linking this authentication to an explicit approval of the operation by the user, complemented with an implicit approval for background operations.

WSU-9.1-18: [ARF WIAM_10] During the activation process of a new wallet unit, after performing all required verifications, a wallet provider shall create and sign at least one WUA for the wallet unit's WSCA/WSCD, and issue them to the wallet unit.

NOTE: The issuance of a WUA is the indication of the success of the activation process, and the minimum requirement is to issue one for the WSCA/WSCD to support the PID issuance process.

WSU-9.1-19: [ARF 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.

NOTE: This is the role of the EUDI Wallet trust mark, so one way to satisfy this requirement is to draw the user's attention to the EUDI Wallet trust mark.

WSU-9.1-20: [ARF WIAM_12] All communication between the wallet provider and the wallet unit shall be mutually authenticated and should be encrypted.

NOTE: This extends as well to the communication between different components of the wallet provider's IT system if they are distributed. The encryption recommendation becomes a requirement when the components are hosted on different systems.

WSU-9.1-21: [ARF WPSM_04] During the lifetime of the wallet unit, the wallet provider shall update the wallet unit as necessary to ensure its continued security and functionality.

NOTE: When updating wallet unit components, the wallet provider should be cautious not to introduce discrepancies in the versions of the various components, which could lead to functional issues or to exploitation by attackers.

WSU-9.1-22: [ARF WPSM_01] A wallet provider shall monitor their installed base of operational wallet instances for maintenance purposes, and determine in a transparent manner the data it needs and is allowed to monitor to deliver the requires support.

NOTE: The data or attributes that should be monitored include:
1) Runtime errors, for uncaught errors in production code;
2) UX and telemetry information, for UX field analysis;
3) OS version and health information, for detection of OS level vulnerabilities;
4) Wallet instance SDK and software library version information, for wallet instance code vulnerabilities;
5) User locale/localisation data, for catching localisation related errors;
6) Wallet instance version, for catching errors or vulnerabilities due to outdated versions;
7) Supported WSCA/WSCDs and their supported capabilities, for detection of cryptography incompatibilities;
8) Unique device identifier such as IDFV or persisted UUID (iOS) or AndroidID (Android), for maintaining an up-to-date list of wallet instance-related device installations and for detecting potential malicious use (unrecognised identifier);
9) Device sensor identifiers and patch levels, for checking if sensor hardware in the device is up-to-date;
10) hardware-level details about the device, to identify known hardware-based problems or vulnerabilities;
11) BLE and NFC support by device, for analysing the security and feasibility of proximity use cases with a given wallet instance.

WSU-9.1-23: [ARF WPSM_03] A wallet provider shall monitor the security posture of its operational wallet instances for the purpose of detecting critical security risks in the environment the wallet instance is run at, and determine and document in a transparent manner the data it needs and is allowed to monitor.

NOTE: Information that should be monitored for software and hardware level problems/vulnerabilities on device includes
1) detection of device rooting/jailbreaking;
2) emulator detection;
3) device OS version and health data;
4) Wallet instance SDK and SW library versions;
5) Wallet instance version;
6) Supported WSCA/WSCD; and
7) Sensor identifiers and patch levels.

9.2 Issuance and management of wallet unit attestations

WSU-9.2-01: [ARF WURevocation_03] A wallet provider shall have a policy governing all aspects of WUA issuance and management. The policy shall distinguish between WUAs for WSCA/WSCDs and WUAs for keystores. For WUAs describing a WSCA/WSCD, the policy shall comply with at least the extended normalised certificate policy ('NCP+') requirements as specified in ETSI EN 319 411-1, insofar applicable for the issuance of WUAs rather than public key certificates. For WUAs describing a keystore, the policy shall comply with at least the normalised certificate policy ('NCP') requirements as specified in ETSI EN 319 411-1, insofar applicable for the issuance of WUAs rather than public key certificates.

WSU-9.2-02: A wallet provider shall not include any information about the user of the wallet unit in the WUA.

NOTE: The WUA is a technical attestation about the wallet unit components (and in particular about its WSCA/WSCD), so it may contain information about the user device, but it should not contain any unique identifier of that device (*e.g.*, serial number).

WSU-9.2-03: [ARF VCR_01a] A wallet provider shall not issue short-term WUAs with a lifetime under 24 hours.

NOTE: The consequence is here that all WUAs should be explicitly revocable, and that a wallet provider always needs to implement a revocation mechanism for its WUAs.

WSU-9.2-04 [PRIVACY]: [ARF WUA_17] The 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.

WSU-9.2-05: [ARF WUA_04] The wallet provider shall only rely on cryptographic algorithms included in the ECCG Agreed Cryptographic Mechanisms v2.0 for the design and implementation of the WUA and shall follow all recommendations associated to those algorithms.

NOTE: This should also allow the other stakeholders that rely on the WUA to only use acceptable algorithms.

WSU-9.2-06: [ARF WUA_08] The wallet provider shall include an identifier for the wallet unit in the WUA.

NOTE 1: The objective of this identifier is to allow the PID provider to request the wallet provider to revoke the wallet unit. This identifier can be the same as the one used for revoking the WUA.

NOTE 2: This is a legal requirement from CIR (EU) 2024/2977.

WSU-9.2-07 [PRIVACY]: [ARF WUA_08] The wallet provider shall ensure that the wallet unit identifier included in the WUA does not enable tracking of the user.

NOTE: Since WUAs are only presented during issuance of PID and attestations, this implies that the identifiers should not be identical for all WUAs, and that they should not be linkable either.

WSU-9.2-08: [ARF ISSU_35a] The wallet provider shall use a cryptographically secure random number generator for the generation of all random numbers used by the WUA (hash salts, identifiers, nonces, etc.).

NOTE: This does not require hardware-based random number generation, as pseudo-random number generation algorithms are available that provide a suitable level of security.

WSU-9.2-09 [PRIVACY]: [ARF ISSU_36] When issuing WUAs in a batch to a wallet unit, a wallet provider shall ensure that the timestamps in these WUAs do not enable relying parties to conclude that they are part of the same batch (and therefore belong to the same user).

WSU-9.2-10 [PRIVACY]: [ARF ISSU_35b] After issuing a WUA, a wallet provider shall discard the values of all unique elements, 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.

NOTE: These unique elements could be used to track the user, or they could be used in an attempt to impersonate the user.

WSU-9.2-11: [ARF ISSU_41] To the maximum extent possible, wallet providers shall ensure that users do not notice which method is used to manage the re-issuance of their WUAs.

NOTE: This requirement applies to users who are not aware of the management of their WUAs. The requirement does not extend to more advanced users, who would for instance trace the exchanges between the wallet provider and the wallet unit.

WSU-9.2-12: [ARF ISSU_42] To the maximum extent possible, wallet providers shall ensure that no user action is needed for the re-issuance of WUAs.

NOTE: This needs to be defined by the wallet provider, basically by “piggybacking” the re-issuance of WUAs to other operations requiring the approval of the user to access the WSCA/WSCD.

WSU-9.2-13: [ARF ISSU_43] The wallet provider shall ensure that all WUAs in a batch have the same attribute values and the same technical validity period.

WSU-9.2-14: [ARF ISSU_50 ISSU_54] As relevant to the applied method, the wallet provider shall inform the wallet unit about the size of the batch and about the moment at which the wallet unit should request the re-issuance of a batch, relative to the expiration date of the existing one.

NOTE: This information should be provided as part of the metadata, together with the WUA management methods to be used.

9.3 Revocation of wallet unit attestations

WSU-9.3-01: [ARF VCR_05] The wallet provider shall have a policy specifying under which conditions a WUA it issued will be revoked.

WSU-9.3-02: [ARF WURevocation_07] A wallet provider shall be able to revoke a wallet unit by revoking its WUA(s).

NOTE: This is how a wallet unit is revoked, but it is the responsibility of the wallet unit to notice that it does not have any valid WUA and consider itself revoked.

WSU-9.3-03: [ARF 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 delegate the operation of the revocation process to a third party, provided that they remain responsible for the revocation decision.

WSU-9.3-04: [ARF VCR_04] The wallet provider that revoked a WUA shall not reverse the revocation.

WSU-9.3-05: [ARF WURevocation_10] A wallet provider shall revoke a wallet unit upon the explicit request of the user registered during the wallet unit activation process and offer to its users an

interface to make such a request. To do so, the wallet provider shall revoke all valid WUA(s) for that wallet unit.

NOTE: This is intended in particular to be used by the user if their user device has been lost or stolen, or if they otherwise have lost trust in their wallet unit.

WSU-9.3-06: [ARF 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 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: This requirement implies that there should be a reliable direct communication channel between the wallet provider and PID providers.

WSU-9.3-07: [ARF WURevocation_12] Before revoking a wallet unit upon request of a PID provider, the wallet provider shall verify that the party requesting revocation is indeed a valid PID provider listed in the List of Trusted Entities of PID Providers.

NOTE: This verification should include at least a verification that the request for revocation has been signed with the private key associated to the public key included in the record in the Trusted List.

WSU-9.3-08: [ARF 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.

NOTE: This should apply to all requests, including those triggered externally by the user or by a PID provider.

WSU-9.3-09: [ARF 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.

NOTE: This is important in particular if the wallet provider suspects that the wallet unit may be compromised.

WSU-9.3-10: Wallet providers shall include specific protections against denial-of-service attacks for the mechanisms used to download their Attestation Status Lists.

NOTE: A specific mechanism may be required because no authentication is required to download these lists,

9.4 Issuance and management of wallet instance attestations

WSU-9.4-01: [ARF WUA_20a] The wallet provider shall ensure that all the WIAs they issue has a lifetime of under 24 hours.

NOTE: As a consequence, there is no need to manage the revocation of WIAs.

WSU-9.4-02: [ARF WUA_20a] The wallet provider shall verify the integrity of the wallet instance before signing a WIA.

WSU-9.4-03: [ARF WUA_23] The wallet provider shall only rely on cryptographic algorithms included in the ECCG Agreed Cryptographic Mechanisms v2.0 for the design and implementation of the WIA and shall follow all recommendations associated to those algorithms.

NOTE: This should also allow the other stakeholders that rely on the WIA to only use acceptable algorithms.

WSU-9.4-04: [ARF WUA_22] The wallet provider shall ensure that a non-revoked wallet unit is able at all times to present a temporally valid and non-revoked WIA to a PID provider or attestation provider during the issuance process of a PID or attestation.

NOTE: This requirement applies to both device-bound and non-device-bound attestations.

10. Requirements on PID provider services supporting EUDI Wallets

10.1 Issuance of PID (as eID means)

PSI-10.1-01: [ARF ISSU_67] The PID provider shall have a policy governing all aspects of PID issuance and management.

NOTE: The extended normalised certificate policy ('NCP+') requirements as specified in ETSI EN 319 411-1 could be used as basis to develop this policy.

PSI-10.1-02: [ARF ISSU_35] The PID provider shall use a cryptographically secure random number generator for the generation of all random numbers used by the PID (hash salts, identifiers, nonces, etc.).

NOTE: This does not require hardware-based random number generation, as pseudo-random number generation algorithms are available that provide a suitable level of security.

PSI-10.1-03 [PRIVACY]: [ARF ISSU_36] When issuing PIDs in a batch to a wallet unit, the PID provider shall ensure that the timestamps in these PIDs do not enable relying parties to conclude that they are part of the same batch (and therefore belong to the same user).

PSI-10.1-04 [CONDITIONAL]: [ARF PID_07] If the PID provider defines a domestic namespace, they shall publish the namespace, including all attribute identifiers, their definition, presence and encoding format, in an Attestation Rulebook.

NOTE: The objective is here to identify if some of the attributes should require specific attention in the evaluation, for instance because of possible confusion of users.

PSI-10.1-05 [CONDITIONAL]: [ARF PID_16] If the PID provider defines a domestic type, they shall publish information about the type, including all claim identifiers, their definition, presence and encoding format, in an Attestation Rulebook.

NOTE: This requirement complements the previous one in case new types are defined.

PSI-10.1-06: [ARF ISSU_19 ISSU_21] During issuance of a PID, the PID provider shall verify that the wallet provider mentioned in the WIA is present in a Wallet Provider List of Trusted Entities, then authenticate the WIA using the trust anchor(s) registered for the wallet provider in that List of Trusted Entities.

PSI-10.1-07: [ARF WUA_25] During issuance of a PID, the PID provider shall verify the content of the WIA.

NOTE: The verification of the WIA is important because the wallet instance authenticity check is linked to the issuance of the WIA.

PSI-10.1-08: [ARF ISSU_18] Before the activation of a PID, the PID provider shall verify the identity of the subject of the PID in compliance with level of assurance high requirements from section 2.1.2 of the Annex of CIR (EU)2015/1502 [i.2].

PSI-10.1-09: [ARF ISSU_40] The PID provider shall include in their OpenID4VCI Issuer metadata a list of the methods that they wish to be used, ordered by preference. The list shall include at least one of the once-only and limited-time methods, and may include the rotating-batch and per-Relying Party methods.

PSI-10.1-10: [ARF ISSU_41] To the maximum extent possible, the PID provider shall ensure that users do not notice which method is used to manage the re-issuance of their PIDs.

NOTE: This requirement applies to users who are not aware of the management of their PIDs. The requirement does not extend to more advanced users, who would for instance trace the exchanges between the wallet provider and the wallet unit.

PSI-10.1-11: [ARF ISSU_42] To the maximum extent possible, the PID provider shall ensure that no user action is needed for the re-issuance of PIDs.

NOTE: This needs to be defined by the PID provider, basically by “piggybacking” the re-issuance of PIDs to other operations requiring the approval of the user to access the WSCA/WSCD.

PSI-10.1-12: [ARF ISSU_43] The PID provider shall ensure that all PIDs in a batch have the same attribute values and the same technical validity period.

PSI-10.1-13: [ARF ISSU_50 ISSU_54] As relevant to the applied method, the PID provider shall inform the wallet unit about the size of the batch and about the moment at which the wallet unit should request the re-issuance of a batch, relative to the expiration date of the existing one.

NOTE: This information should be provided as part of the metadata, together with the PID management methods to be used.

PSI-10.1-14: [ARF ISSU_35b] After issuing a PID, a PID provider shall discard the values of all unique elements, 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.

NOTE: These unique elements could be used to track the user, or they could be used in an attempt to impersonate the user.

10.2 Management of PID

PSI-10.2-01: [ARF 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, as required for assurance level high in section 2.2.2 of the Annex of CIR (EU)2015/1502 [i.2].

PSI-10.2-02: [ARF ISSU_65] A PID Provider shall verify that a re-issued PID is issued to the same wallet unit and the same WSCA/WSCD or keystore as the existing PID or attestation.

NOTE: This is based on refresh tokens.

10.3 Revocation of PID

PSI-10.3-01 [CONDITIONAL]: [ARF VCR_05] If a PID is revocable, the PID provider shall have a policy specifying under which conditions a PID it issued will be revoked.

PSI-10.3-02 [CONDITIONAL]: [ARF VCR_06] If a PID is revocable, the PID provider shall revoke the PID when its security has been compromised.

PSI-10.3-03 [CONDITIONAL]: [ARF VCR_07a] If a PID is revocable, the PID provider shall revoke that PID upon the explicit request of the user to whom the PID was issued.

PSI-10.3-04 [CONDITIONAL]: [ARF VCR_07c] If a PID is revocable, the PID provider shall revoke that PID if the Wallet Unit on which it resides is revoked.

PSI-10.3-05 [CONDITIONAL]: [ARF VCR_08] If a PID is revocable, the PID provider shall revoke that PID upon the death of the natural person who is the subject of the PID.

PSI-10.3-06: [ARF VCR_03] The PID provider of a given PID shall be the only party in the EUDI Wallet ecosystem responsible for executing the revocation of that PID.

NOTE: A wallet provider may delegate the operation of the revocation process to a third party, provided that they remain responsible for the revocation decision.

PSI-10.3-07: [ARF VCR_04] The PID provider that revoked a PID shall not reverse the revocation.

PSI-10.3-08 [CONDITIONAL][PRIVACY]: [ARF VCR_17] When using an Attestation Status List for revocation, the PID provider shall randomly assign the index for each PID.

NOTE: The objective is to prevent this index from becoming a correlator.

PSI-10.3-09 [CONDITIONAL][PRIVACY]: [ARF VCR_18] When using an Attestation Status List for revocation, the PID provider shall randomly assign the index for each PID.

NOTE: The objective is to prevent this index from becoming a correlator.

PSI-10.3-10: [ARF 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.

NOTE: This can be achieved by using the revocation information in the WUA it received during issuance of that PID.

PSI-10.3-11: [ARF WURevocation_18] When the PID provider finds out that the wallet unit on which one of its PID resides is revoked, the PID Provider shall immediately revoke the respective PID.

SECTION 4

Annexes

A Mapping to standards and reference documents

Requirement	ARF HLR	Standard, Regulation	Note
GEN-4.2-01		EN 319 401, 4.2	
GEN-4.2-02			Added to flag privacy requirements
GEN-5-01		EN 319 401, 5	
GEN-5-02		(EU)2024/2981, Annex 1	
GEN-6.1-01		EN 319 401, 6.1	
GEN-6.2-01		EN 319 401, 6.2	
GEN-6.2-02		CIR (EU) 2015/1502, section 2.4.2, point 1	
GEN-6.2-03		CIR (EU) 2015/1502, section 2.4.2, point 2	
GEN-6.2-04		CIR (EU) 2015/1502, section 2.4.2, point 3	
GEN-6.2-05		(EU)910/2014, 5a(5)(g), 5a(13)	
GEN-6.3-01		EN 319 401, 6.3	
GEN-7.1.1-01		EN 319 401, 7.1.1	
GEN-7.1.1-02		CIR (EU) 2015/1502, section 2.4.3	
GEN-7.1.2-01		EN 319 401, 7.1.2	
GEN-7.1.3-01		EN 319 401, 7.1.3	
GEN-7.2-01		EN 319 401, 7.2	
GEN-7.3.1-01		EN 319 401, 7.3.1	
GEN-7.3.2-01		EN 319 401, 7.3.2	

Requirement	ARF HLR	Standard, Regulation	Note
GEN-7.3.2-02		(EU)2024/2981, 2(11)	
GEN-7.3.2-03			Added recommendation
GEN-7.3.2-04			Added requirement to ensure that attestations are covered
GEN-7.3.3-01		EN 319 401, 7.3.3	
GEN-7.4.1-01		EN 319 401, 7.4.1	
GEN-7.4.2-01		EN 319 401, 7.4.2	
GEN-7.4.3-01		EN 319 401, 7.4.3	
GEN-7.4.4-01		EN 319 401, 7.4.4	
GEN-7.4.5-01		EN 319 401, 7.4.5	
GEN-7.4.6-01		EN 319 401, 7.4.6	
GEN-7.5-01		EN 319 401, 7.5	
GEN-7.5-02		ECCG ACM	
GEN-7.5-03			Added a requirement for protection of critical assets in other systems → May need to be moved
GEN-7.6-01		EN 319 401, 7.6	
GEN-7.6-02			Recalling the scheme's requirements for composition and evidence reuse
GEN-7.7-01		EN 319 401, 7.7	
GEN-7.8-01		EN 319 401, 7.8	
GEN-7.9.1-01		EN 319 401, 7.9.1	
GEN-7.9.2-01		EN 319 401, 7.9.2 (EU)910/2014, 5a(20)	
GEN-7.9.3-01		EN 319 401, 7.9.3 (EU)910/2014, 5a(10)	
GEN-7.9.4-01		EN 319 401, 7.9.4	
GEN-7.9.5-01		EN 319 401, 7.9.5	
GEN-7.10-01		EN 319 401, 7.10	
GEN-7.11.1-01		EN 319 401, 7.11.1	
GEN-7.11.2-01		EN 319 401, 7.11.2	
GEN-7.11.3-01		EN 319 401, 7.11.3	
GEN-7.12-01		EN 319 401, 7.12	
GEN-7.13-01		EN 319 401, 7.13	
GEN-7.14.1-01		EN 319 401, 7.14.1	
GEN-7.14.2-01		EN 319 401, 7.14.2	

Requirement	ARF HLR	Standard, Regulation	Note
GEN-7.14.3-01		EN 319 401, 7.14.3	
GEN-7.14.3-02			Reminding that EUDIW is a full-stack certification scheme, due to (EU) 2015/1502 requirements.
WUG-8.1-Fun-01	AS-WP-40-007		The requirement has been modified to apply to the wallet unit rather than to the wallet provider
WUG-8.1-Fun-02			Added a recommendation to have a PID issued before an attestation.
WUG-8.1-Sec-03	AS-WP-09-010		
WUG-8.1-Fun-04	AS-WP-09-010a		The requirement should be split as it applies to several stakeholders
WUG-8.1-Sec-05	AS-WP-09-021		The requirement has been split. This one only applies to the WSCD (see WSA-8.5-Sec-10 for the WSCA aspect)
WUG-8.1-Sec-06	AS-WP-40-009		
WUG-8.1-Sec-07	AS-WP-40-014		Split requirement, fully applying to data on user devices.
WUG-8.1-Sec-08	AS-WP-40-014		Split requirement, slightly weakened when the wallet unit data is stored on the wallet provider's servers.
WUG-8.1-Fun-09	AS-WP-40-030		
WUI-8.2.1-Sec-01	AS-AP-10-005		The ARF requirement has been split
WUI-8.2.1-Sec-02			Added to introduce PID/EAA instances
WUI-8.2.1-Sec-03	AS-WP-09-006		Modified for clarification
WUI-8.2.1-Sec-04	AS-AP-10-015		
WUI-8.2.1-Sec-05	AS-WP-09-005		
WUI-8.2.1-Sec-06		CEN TS 18098, 8.3.7.3	
WUI-8.2.1-Sec-07	AS-AP-10-054		
WUM-8.2.2-Fun-01	AS-AP-10-060		
WUM-8.2.2-Fun-02	AS-AP-10-064		Split requirement.
WUM-8.2.2-Fun-03	AS-AP-10-065 AS-AP-10-068		Now a requirement on the definition of conditions for falling back to other methods.
WUM-8.2.2-Fun-04	AS-AP-10-084		
WUM-8.2.2-Fun-05	AS-AP-10-086		Extended the requirement to failures
WUM-8.2.2-Fun-06	AS-AP-10-082		
WUM-8.2.2-Sec-07	AS-AP-10-091		Added a WU-side requirement with a note on security that could be a standalone requirement.
WUM-8.2.2-Fun-08	AS-AP-10-088		Some clarification in the requirement.

Requirement	ARF HLR	Standard, Regulation	Note
WUM-8.2.2-Fun-09	AS-WP-51-002		
WUM-8.2.2-Fun-10	AS-WP-51-003		
WUM-8.2.2-Sec-11	AS-WP-51-004		
WUP-8.2.3-Fun-01	AS-WP-06-004 AS-WP-06-005		Joined two requirements
WUP-8.2.3-Fun-02	AS-WP-06-006		
WUP-8.2.3-Fun-03	AS-WP-06-008		
WUP-8.2.3-Fun-04	EW-PIO-01-008		
WUP-8.2.3-Fun-05	AS-WP-06-016		
WUP-8.2.3-Fun-06	AS-WP-43-006		
WUP-8.2.3-Fun-07	AS-WP-43-004		
WUP-8.2.3-Fun-08	AS-RP-51-008		
WUP-8.2.3-Fun-09			This requirement has been added to clarify the link between the operations.
WUP-8.2.3-Fun-10	AS-WP-06-015		
WUP-8.2.3-Fun-11	EW-PIO-01-009		Clarified the wording of the requirement
WUP-8.2.3-Fun-12	EW-PIO-01-018		Changed “two” to “several”
WUP-8.2.3-Sec-13	EW-PIO-01-019		Changed “two” to “several”
WUP-8.2.3-Fun-14			Added a generic requirement to protect the integrity of PID and EAA.
WUH-8.3.1-Sec-01		MASVS-AUTH	
WUH-8.3.1-Sec-02		MASVS-AUTH MASVS-PLATFORM	
WUH-8.3.1-Sec-03		ISO/IEC 18013 (Biometric Profile) MASVS-AUTH MASVS-PLATFORM	
WUH-8.3.1-Sec-04		MASVS-PLATFORM (Partially)	
WUH-8.3.1-Sec-05			
WUH-8.3.1-Sec-06			
WUH-8.3.1-Sec-07		MASVS-AUTH	
WUH-8.3.1-Sec-08		(EU)2015/1502 Annex, 2.3.1 MASVS-CRYPTO MASVS-RESILIENCE	
WUH-8.3.1-Sec-09		MASVS-AUTH MASVS-CRYPTO MASVS-PLATFORM	
WUH-8.3.1-Sec-10			

Requirement	ARF HLR	Standard, Regulation	Note
WUH-8.3.1-Sec-11			
WUH-8.3.2-Sec-01		ISO 18013-5 RFC 7515 (JWS) & RFC 8725 (JWT Best Current Practices) W3C VC Data Model OID4VP/OID4VCI	
WUH-8.3.2-Sec-02		RFC 6749 (OAuth 2.0) RFC 8725 (JWT Best Current Practices) OID4VP/OID4VCI	
WUH-8.3.2-Sec-03		RFC 7515 (JWS) & RFC 8725 (JWT Best Current Practices) W3C VC Data Model OID4VP (SD-JWT)	
WUH-8.3.2-Sec-04			
WUH-8.3.2-Sec-05			
WUH-8.3.2-Sec-06		W3C VC Data Model OID4VP/OID4VCI	
WUH-8.3.2-Sec-07			
WUH-8.3.3-Sec-01			
WUH-8.3.3-Sec-02	AS-AP-10-028		
WUH-8.3.3-Sec-03	AS-AP-10-028	RFC 7515 (JWS) & RFC 8725 (JWT Best Current Practices)	
WUH-8.3.3-Sec-04		RFC 7519 (JWT) RFC 8725 (JWT Best Current Practices) OpenID4VP / OpenID4VCI	
WUH-8.3.3-Sec-05			
WUH-8.3.3-Sec-06	AS-AP-10-028	W3C VC DM OID4VP	
WUH-8.3.3-Sec-07	AS-AP-10-028		
WIN-8.4.1-Sec-01		MASVS-STORAGE-1	
WIN-8.4.1-Sec-02			
WIN-8.4.1-Sec-03		MASVS-STORAGE-2	
WIN-8.4.1-Sec-04	AS-AP-10-054 AS-AP-10-055	RFC 7515 (JWS) & RFC 8725 (JWT Best Current Practices) OpenID4VP / OpenID4VCI	Reformulated the requirement to focus on random numbers.
WIN-8.4.1-Sec-05	ARF 6.5.3.5		Included as a reminder

Requirement	ARF HLR	Standard, Regulation	Note
WIN-8.4.1-Sec-06			Added a requirement about secure communication between the various components of the wallet unit
WIN-8.4.2-Sec-01		MASVS-PLATFORM	
WIN-8.4.2-Sec-02		W3C VC Data Model OID4VP MASVS-RESILIENCE	
WIN-8.4.2-Sec-03		W3C VC Data Model OID4VP MASVS-PRIVACY	
WIN-8.4.2-Sec-04			
WIN-8.4.3-Sec-01		MASVS-CODE-1	
WIN-8.4.3-Sec-02		MASVS-CODE-2	
WIN-8.4.3-Sec-03		MASVS-CODE-3	
WIN-8.4.3-Sec-04		MASVS-CODE-4	
WIN-8.4.3-Sec-05		MASVS-RESILIENCE-1 CEN TS 18098, 8.2.3.2.2.3.1	
WIN-8.4.3-Sec-06		MASVS-RESILIENCE-2	
WIN-8.4.3-Sec-07		MASVS-RESILIENCE-3	
WIN-8.4.3-Sec-08		MASVS-RESILIENCE-4	
WIN-8.4.3-Sec-09	AS-WP-40-003		Spit requirement
WIN-8.4.3-Sec-10	AS-WP-40-003	OID4VCI / OID4VP	Split requirement
WIN-8.4.3-Sec-11		CEN TS 18098, 8.2.3.2.2.3.3	
WIN-8.4.3-Sec-12	AS-WP-40-015		
WIN-8.4.4-Sec-01		ASVS	
WIN-8.4.4-Sec-02		ECCG ACM	
WSA-8.5-Sec-01			Inspired from the WSCA PP under development in CEN TC224 WG17
WSA-8.5-Sec-02			Inspired from the WSCA PP under development in CEN TC224 WG17
WSA-8.5-Sec-03			Inspired from the WSCA PP under development in CEN TC224 WG17
WSA-8.5-Sec-04			Inspired from the WSCA PP under development in CEN TC224 WG17
WSA-8.5-Sec-05			Inspired from the WSCA PP under development in CEN TC224 WG17
WSA-8.5-Sec-06			Inspired from the WSCA PP under development in CEN TC224 WG17

Requirement	ARF HLR	Standard, Regulation	Note
WSA-8.5-Sec-07			Inspired from the WSCA PP under development in CEN TC224 WG17
WSA-8.5-Sec-08	AS-WP-40-017 AS-WP-40-018 AS-WP-40-019		Inspired from the WSCA PP under development in CEN TC224 WG17
WSA-8.5-Sec-09			Inspired from the WSCA PP under development in CEN TC224 WG17
WSA-8.5-Sec-10			Added in particular to support re-issuance
WSA-8.5-Sec-11	AS-WP-09-021		Added a recommendation to forbid the export of individual keys from the WSCA.
WSA-8.5-Sec-12	AS-WP-40-029		
WSA-8.5-Sec-13			Added a requirement to strengthen the storage in the WSCD.
WKS-8.6-Fun-01	AS-WP-40-008		
WKS-8.6-Sec-02		OpenID4VCI	Defining possible assurance levels for keystores
WSU-9.1-01	AS-WP-09-004		
WSU-9.1-02	EW-DM-38-007		
WSU-9.1-03			
WSU-9.1-04	AS-WP-40-001	CEN TS 18098, 8.2.2.1	
WSU-9.1-05		CEN TS 18098, 8.2.2.1	Added to define requirements on alternative stores
WSU-9.1-06	AS-WP-40-002	CEN TS 18098, 8.2.2.1	Requirement has been split
WSU-9.1-07	AS-WP-40-002		Requirement has been split
WSU-9.1-08	AS-WP-40-004	CEN TS 18098, 8.2.3.3.1	
WSU-9.1-09		CEN TS 18098, 8.2.3.2.2.1	
WSU-9.1-10		CEN TS 18098, 8.2.3.2.2.2.3	
WSU-9.1-11	AS-WP-40-005		
WSU-9.1-12	AS-WP-40-005		Privacy requirement
WSU-9.1-13	AS-WP-40-005		Privacy requirement
WSU-9.1-14	AS-WP-40-006		
WSU-9.1-15	AS-WP-40-006		
WSU-9.1-16	AS-WP-40-008	(EU) 2015/1502 Annex, 2.2.1	Requirement has been split
WSU-9.1-17	AS-WP-40-010		Requirement has been split
WSU-9.1-18	AS-WP-40-010		Requirement has been split
WSU-9.1-19	AS-WP-40-010a		

Requirement	ARF HLR	Standard, Regulation	Note
WSU-9.1-20	AS-WP-40-012		
WSU-9.1-21	AS-WP-56-004		
WSU-9.1-22	AS-WP-56-001		
WSU-9.1-23	AS-WP-56-003		
WSU-9.2-01	EW-DM-38-001		
WSU-9.2-02		CEN TS 18098, 8.2.5.2.5	Privacy
WSU-9.2-03	AS-AP-07-002		
WSU-9.2-04			
WSU-9.2-05	AS-WP-09-004		
WSU-9.2-06	AS-WP-09-009		Split requirement
WSU-9.2-07	AS-WP-09-009		Split requirement
WSU-9.2-08	AS-AP-10-057		The requirement is based on the note.
WSU-9.2-09	AS-AP-10-059		
WSU-9.2-10	AS-AP-10-058		
WSU-9.2-11	AS-AP-10-065		
WSU-9.2-12	AS-AP-10-066		
WSU-9.2-13	AS-AP-10-067		The identity requirement may need to be extended to at least some metadata
WSU-9.2-14	AS-AP-10-078		
WSU-9.3-01	AS-AP-07-007		
WSU-9.3-02	EW-DM-38-007		
WSU-9.3-03	AS-AP-07-002		
WSU-9.3-04	AS-AP-07-005		
WSU-9.3-05	EW-DM-38-011		
WSU-9.3-06	EW-DM-38-012		
WSU-9.3-07	EW-DM-38-013		
WSU-9.3-08	EW-DM-38-015		
WSU-9.3-09	EW-DM-38-017		
WSU-9.3-10			Additional requirement to protect this unauthenticated request
WSU-9.4-01	AS-WP-29-026		Requirement from TS3 2.2.1
WSU-9.4-02	AS-WP-29-026		Requirement from TS3 2.2.1.1
WSU-9.4-03	AS-WP-29-029		
WSU-9.4-04	AS-WP-29-028		
PIS-10.1-01	AS-AP-10-093		
PSI-10.1-02	AS-AP-10-056		
PSI-10.1-03	AS-AP-10-059		

Requirement	ARF HLR	Standard, Regulation	Note
PSI-10.1-04	EW-DM-03-007		
PSI-10.1-05	EW-DM-03-016		
PSI-10.1-06	AS-AP-10-025 AS-AP-10-028		
PSI-10.1-07	AS-WP-09-031		
PSI-10.1-08	AS-AP-10-023		
PSI-10.1-09	AS-AP-10-064		
PSI-10.1-10	AS-AP-10-065		
PSI-10.1-11	AS-AP-10-066		
PSI-10.1-12	AS-AP-10-067		
PSI-10.1-13	AS-AP-10-074 AS-AP-10-078		
PSI-10.1-14	AS-AP-10-058		
PSI-10.2-01	AS-AP-10-024		
PSI-10.2-02	AS-AP-10-091		
PSI-10.3-01	AS-AP-07-007		
PSI-10.3-02	AS-AP-07-008		
PSI-10.3-03	AS-AP-07-010		
PSI-10.3-04	AS-AP-07-012		
PSI-10.3-05	AS-AP-07-014		
PSI-10.3-06	AS-AP-07-004		
PSI-10.3-07	AS-AP-07-006		
PSI-10.3-08	AS-AP-07-024		
PSI-10.3-09	AS-AP-07-025		
PSI-10.3-10	AS-WP-38-018		
PSI-10.3-11	AS-WP-38-018		

B Mapping to the Risk Register

B.1 Introduction

B.2 Threats to the Wallet

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR1	An attacker can revoke pseudonyms without justified reasons.	Creation or use of a fake electronic identity (R2)	-EN 319 401 (chapter 7) -ETSI EN 319 411-1 (chapter 6)	N/A in the current analysis
TR2	An attacker can issue fabricated electronic identities that do not exist.	Creation or use of a fake electronic identity (R2)		8.2.1 PID and EAA issuance
TR3	An attacker can start to issue unauthorized PID.	Creation or use of a fake electronic identity (R2)		8.2.1 PID and EAA issuance 8.3.4 Authenticity and trust anchor checks
TR4	An attacker can get an administrator to enter a wrong PID provider into the PID provider trusted list.	Creation or use of a fake electronic identity (R2)		
TR5	An attacker can bypass the remote identity proofing service.	Creation or use of an existing electronic identity (R1) /		8.3.1 User authentication

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
		Creation or use of a fake electronic identity (R2)		
TR6	An attacker can bypass the physical identity proofing service.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)	CEN TS 18098	
TR7	An attacker can bypass the identity proofing services related to the use of a remote (qualified) certificate.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	8.3.1 User authentication
TR8	An attacker can get access to a wallet that is not bound to a person.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6)	8.3.1 User authentication 9.1.3 Revocation of wallet unit attestation
TR9	An attacker can defeat technical and procedural controls to create wrong PIDs.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6)	

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR10	An attacker can activate a new wallet on an invalid WSCD.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	8.5 WSCA requirements
TR11	An attacker can bypass the identity proofing service related to the use of existing eID means.	Creation or use of an existing electronic identity (R1) / Identify theft (R4) / Unauthorised transaction (R9)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	8.3.1 User authentication
TR12	An attacker can circumvent the verification by the PID provider that the wallet is controlled by the user and have a PID issued into a compromised wallet under the attacker's control.	Creation or use of an existing electronic identity (R1) / Identify theft (R4) / Unauthorised transaction (R9)	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6)	9.1.1 Wallet unit activation and monitoring
TR13	An attacker can get a valid PID into an invalid wallet unit.	Creation or use of an existing electronic identity (R1) / Identify theft (R4) /	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6)	9.1.1 Wallet unit activation and monitoring

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
		Unauthorised transaction (R9)	-ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6)	
TR14	An attacker can issue a PID of another state to access data / digital assets of targeted citizens	Creation or use of an existing electronic identity (R1) / Identity theft (R4) / Unauthorised transaction (R9)	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6)	
TR15	An attacker can link a PID with the wrong wallet because the PID provider is not able to link the PID to the correct wallet.	Creation or use of an existing electronic identity (R1) / Identify theft (R4) / Unauthorised transaction (R9)		8.2.1 PID and EAA issuance 9.1.1 Wallet unit activation and monitoring
TR16	An attacker can make the user approving the activation of a new wallet unit/instance under the attacker's control – with subsequent control of attestations as well.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2) / Identify theft (R4) / Unauthorised transaction (R9)	-EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6.2)	9.1.1 Wallet unit activation and monitoring
TR17	An attacker can issue a PID of another state to access data / digital assets of targeted citizens.	Creation or use of an existing electronic identity (R1) / Identity theft (R4) / Unauthorised transaction (R9)	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6)	

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR18	An attacker can defeat technical and procedural controls to create fake (Q)EAAs.	Creation or use of fake attributes (R3)	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6.2)	
TR19	An attacker can present (Q)EAAs that are not validly issued to them.	Creation or use of fake attributes (R3)	-EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6)	8.2 Handling of PID and EAA
TR20	An attacker can attack the cryptographic linking mechanism of the wallet between the PID and a (Q)EAA that should not be issued to them.	Creation or use of fake attributes (R3)	-EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6.2) -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	8.5 WSCA requirements
TR21	An attacker can use a (Q)EAA in a wallet, although the physical counterpart of the (Q)EAA is expired or invalid.	Creation or use of fake attributes (R3)	-EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6.2) -Using timestamps and validity period	8.2.2 PID and EAA management

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR22	An attacker can circumvent the verification by the (Q)EAA provider that the wallet is in control of the user and have a (Q)EAA issued into a compromised wallet under the attacker's control.	Creation or use of fake attributes (R3)	-EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6.2)	9.1.1 Wallet unit activation and monitoring
TR23	An attacker can forge electronic attestations of attributes.	Creation or use of fake attributes (R3)	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6.2)	
TR24	An attacker can inject forged electronic attestations of attributes into a wallet.	Creation or use of fake attributes (R3)	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -ETSI TS 119 431-1 (chapter 6.2)	8.3.3 Orchestration 8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)
TR25	The wallet can present attributes to a relying party without the approval of a user.	Data disclosure (R6)	-OWASP MAS Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002)	8.2.3 PID and EAA presentation

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			control 8.20, 8.22, 8.25 to 8.32) -Testing EAA presentation	
TR26	PID, (Q)EAAs or pseudonyms can be presented to a wrong relying party.	Data disclosure (R6)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -Testing EAA presentation	8.2.3 PID and EAA presentation
TR27	An attacker can initiate a malicious renewal of EAA.	Data disclosure (R6)	-ETSI 319 411-1 (chapter 6) -ETSI 319 411-2 (chapter 6) -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	8.2.2 PID and EAA management 8.3.1 User authentication
TR28	An attacker can get a user into wrongfully approving a request for electronic attestations of attributes (phishing or other).	Data disclosure (R6)	-User guidance	8.3.2 User interaction

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR29	An attacker can leak attributes from the wallet and identify the wallet user where identification is not required/allowed.	Data disclosure (R6)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI TS 119 431-1 (chapter 6)	8.4.1 Protection of assets in the wallet unit 9.1.1 Wallet unit activation and monitoring
TR30	An attacker can defeat technical and procedural controls to extract data.	Data disclosure (R6)	-ISO/IEC 27001 or SiHa or SFB or comparable -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI TS 119 431-1 (chapter 6)	

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR31	A request can be leaked to an attacker.	Data disclosure (R6)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -EN 319 401 (chapter 7) -ETSI 319 411-1 (chapter 6) -ETSI TS 119 431-1 (chapter 6) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.4.1 Protection of assets in the wallet unit 9.1.1 Wallet unit activation and monitoring
TR32	An attacker can obtain knowledge on the embedded disclosure policy for attributes and present attributes contained in the current request by wallet units.	Data disclosure (R6)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -Testing EAA presentation	8.4.1 Protection of assets in the wallet unit 9.1.1 Wallet unit activation and monitoring
TR33	An attacker can extract logs, or parts of them.	Data disclosure (R6)	-ISO/IEC 27001 or SiHa or SFB or comparable -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or	8.4 Wallet instance requirements

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	
TR34	An attacker can know whether a wallet is installed on the same device he is using, or on another one, and get information on it.	Data disclosure (R6)	-ISO/IEC 27001 or SiHa or SFB or comparable -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -EN 319 401 (chapter 7)	8.3.1 User authentication 8.4 Wallet instance requirements 9.1.1 Wallet unit activation and monitoring
TR35	An attacker can obtain a knowledge factor used for user authenticating to the WSCA.	Data disclosure (R6)	-User guidance -ISO/IEC 27001 or SiHa or SFB or comparable -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or	8.5 WSCA requirements

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -EN 319 401 (chapter 7)	
TR36	The electronic attestation of attributes about a person that is presented in multiple transactions with a relying party, or across different relying parties, unintentionally allows to link multiple transactions to the relevant person.	Data disclosure (R6)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -Testing EAA presentation	8.2.2 PID and EAA management
TR37	A public attestation/relying party revocation list can contain information about the user's usage of their attestation (e.g., location, IP address …).	Data disclosure (R6)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	
TR38	Not being able to prove user's consent for shared attributes, relying parties can affect the integrity of logs.	Data disclosure (R6)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	8.2.3 PID and EAA presentation (Fun-02) 9.1.1 Wallet unit activation and monitoring (14)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR39	An attacker can unlawfully trace wallet users using unique/traceable identifiers.	Data disclosure (R6) / Surveillance (R14)	-EAA construction following ARF rulebooks	
TR40	A relying party that consists of multiple units/entities that each have a different scope of what they are allowed to request/process, can request and process data for which they do not have lawful grounds for.	Data disclosure (R6) / Unauthorised transaction (R9)	-Testing EAA presentation	
TR41	An attacker can subvert the integrity and authenticity checks by the wallet of PIDs to always return success.	Data manipulation (R7)	-EN 319 401 (chapter 7) -ETSI EN 319 411-1 (chapter 6) certified HSM e.g., EUCC or NIST FIPS 140-2/3 -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic	8.4 Wallet instance requirements 9.1.1 Wallet unit activation and monitoring

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			techniques/primitives pursuant to ECCG ACM	
TR42	An attacker can bypass or subvert the performance of checks by the wallet that verify the integrity and authenticity of requested attributes to always return success.	Data manipulation (R7)	-EN 319 401 (chapter 7) -ETSI EN 319 411-1 (chapter 6) certified HSM e.g., EUCC or NIST FIPS 140-2/3 -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.4 Wallet instance requirements 9.1.1 Wallet unit activation and monitoring 9.1.3 Revocation of wallet Unit attestations
TR43	An attacker can bypass or subvert the performance of checks by the wallet that verify all requested attributes belonging to the same user to always return success.	Data manipulation (R7)	-EN 319 401 (chapter 7) -ETSI EN 319 411-1 (chapter 6) certified HSM e.g., EUCC or NIST FIPS 140-2/3 -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.4 Wallet instance requirements 9.1.1 Wallet unit activation and monitoring 9.1.3 Revocation of wallet Unit attestations
TR44	An attacker can bypass or subvert the performance of checks by the wallet that verify the PID is valid and issued by a trusted PID provider to always return success.	Data manipulation (R7)	-EN 319 401 (chapter 7) -ETSI EN 319 411-1 (chapter 6) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.4 Wallet instance requirements 9.1.1 Wallet unit activation and monitoring 9.1.3 Revocation of wallet Unit attestations

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR45	An attacker can bypass or subvert the performance of checks by the wallet that verify that a QEAA is valid and issued by a qualified TSP, who is registered to issue the QEAA, to always return success.	Data manipulation (R7)	-EN 319 401 (chapter 7) -ETSI EN 319 411-1 (chapter 6) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.4 Wallet instance requirements 9.1.1 Wallet unit activation and monitoring 9.1.3 Revocation of wallet Unit attestations
TR46	An attacker can bypass or subvert the performance of checks by the wallet that verify whether the PID has been revoked by the PID provider to always return success.	Data manipulation (R7)	-EN 319 401 (chapter 7) -ETSI EN 319 411-1 (chapter 6) certified HSM e.g., EUCC or NIST FIPS 140-2/3 -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.4 Wallet instance requirements 9.1.1 Wallet unit activation and monitoring 9.1.3 Revocation of wallet Unit attestations
TR47	An attacker can bypass or subvert the performance of checks by the wallet that verify whether the (Q)EAA has been revoked by the (Q)EAA provider to always return success.	Data manipulation (R7)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -Testing EAA issuance	8.4 Wallet instance requirements 9.1.1 Wallet unit activation and monitoring 9.1.3 Revocation of wallet Unit attestations

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR48	An attacker can modify the content of backup and recovery data that should be exclusively under the user's control.	Data manipulation (R7) / Data loss (R8)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	8.3.1 User Authentication 8.4 Wallet instance requirements
TR49	An attacker can modify the transaction history for a given wallet instance from the activity logs.	Data manipulation (R7) / Data loss (R8)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	8.3.1 User Authentication 8.4 Wallet instance requirements
TR50	An attacker can eavesdrop during the connection from the wallet to relying parties.	Data theft (R5) / Data disclosure (R6)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.4.1 Protection of assets in the wallet unit

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR51	An attacker can convince a user to share personal data (i.e., PID, EAA-s, pseudonyms, electronic signatures, logs and other data) with the attacker or with a third party that the user did not intend to do so.	Data theft (R5) / Data disclosure (R6)	-User guidance	
TR52	An attacker can read the transaction history for a given wallet instance from the activity logs.	Data theft (R5) / Data disclosure (R6)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.3.1 User Authentication 8.4 Wallet instance requirements
TR53	An attacker can export or extract cryptographic key material outside of the WSCD.	Data theft (R5) / Data disclosure (R6) / Unauthorised transaction (R9)	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI EN 319 411-1 (chapter 6) certified HSM e.g., EUCC or NIST FIPS 140-2/3 using HW-key of HSM and in general using sufficient cryptographic techniques/primitives pursuant to ECCG ACM (in Frontend) Using hardware elements of end user devices (e.g., Secure Enclave, TEE)	7.5 Cryptographic controls 8.1 General and lifecycle requirements 8.5 WSCA requirements

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -EN 319 401 (chapter 5, chapter 6, chapter 7, for browser based)	
TR54	An attacker can read the content of backup and recovery data that should be exclusively under the user's control.	Data theft (R5) / Data disclosure (R6)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM -User guidance	8.3.1 User Authentication 8.4 Wallet instance requirements
TR55	An attacker can bypass the user authentication method to use a	Identity theft (R4)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or	8.3.1 User Authentication

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
	pseudonym generated by a wallet unit.		ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	8.4 Wallet instance requirements
TR56	An attacker can propose an application that mimics a specific legitimate wallet to users.	Identity theft (R4)	-ISO/IEC 27001 or SiHa or SFB or comparable -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	9.1.1 Wallet unit activation and management
TR57	An attacker can export wallet data, including PID, (Q)EAAs or logs.	Identity theft (R4)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	8.2 handling of PID and EAA 8.3.2 User Authentication 8.4 Wallet instance requirements

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR58	An attacker can export cryptographic binding material.	Identity theft (R4)	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI EN 319 411-1 (chapter 6) certified HSM e.g., EUCC or NIST FIPS 140-2/3 using HW-key of HSM and in general using sufficient cryptographic techniques/primitives pursuant to ECCG ACM (in Frontend) Using hardware elements of end user devices (e.g., Secure Enclave, TEE) -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -EN 319 401 (chapter 5, chapter 6, chapter 7, for browser based)	7.5 Cryptographic controls 8.1 General and lifecycle requirements 8.5 WSCA requirements

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR59	An attacker can take over identities through the cryptographic keys of the wallet.	Identity theft (R4)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -Using hardware elements of end user devices	7.5 Cryptographic controls 8.1 General and lifecycle requirements 8.5 WSCA requirements
TR60	An attacker can duplicate another user's personal wallet unit on their personal device and use it.	Identify theft (R4) / Creation or use of an existing electronic identity (R1)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	The current analysis is under the assumption that only one instance is supported.
TR61	Authorities of another state can ask the user to show and/or share all the wallet data in a situation of proximity, such as when crossing the border of that state.	Identify theft (R4) / Surveillance (R14)	-User guidance -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM or e.g., in hardware element of the device	
TR62	Users cannot transfer their transaction logs after failure of a user device, resulting in a loss of	Repudiation (R11)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI	

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
	traceability of previous transactions on the new wallet.		319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	
TR63	Users cannot recover their transaction logs after failure of a user device, resulting in a loss of traceability on the new wallet.	Repudiation (R11)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32)	
TR64	Relying parties can have difficulties proving consent for remote electronic signatures.	Repudiation (R11)	N/A in the current analysis	
TR65	An attacker can flood the connection(s) with requests during the connection to relying parties.	Service disruption (R13)	-ISO/IEC 27001 or SiHa or SFB or comparable	7.7 operation Security 7.8 Network Security 7.9 Vulnerabilities and incident management 7.11 Business continuity management
TR66	An attacker can flood a status provisioning service with connections to relying parties.	Service disruption (R13)	-ISO/IEC 27001 or SiHa or SFB or comparable	7.7 operation Security 7.8 Network Security 7.9 Vulnerabilities and incident management

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
				7.11 Business continuity management
TR67	An attacker can make the attribute presentation appearing as contested/denied, despite the attribute presentation stating its validity.	Service disruption (R13)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -Testing EAA presentation	8.3.3 Orchestration
TR68	An attacker can revoke a PID without justified reason.	Service disruption (R13)	-ISO/IEC 27001 or SiHa or SFB or comparable -ETSI 319 411-1 (chapter 6.2.4, chapter 6.3.9) -ETSI 319 411-2 (chapter 6.2.4, chapter 6.3.9)	9.1.3 Revocation of wallet unit attestation
TR69	An attacker can revoke a PID without user consent.	Service disruption (R13)	-ISO/IEC 27001 or SiHa or SFB or comparable -ETSI 319 411-1 (chapter 6.2.4, chapter 6.3.9) -ETSI 319 411-2 (chapter 6.2.4, chapter 6.3.9)	9.1.3 Revocation of wallet unit attestation

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR70	An attacker can revoke a (Q)EAA without justified reason.	Service disruption (R13)	-ISO/IEC 27001 or SiHa or SFB or comparable -ETSI 319 411-1 (chapter 6.2.4, chapter 6.3.9) -ETSI 319 411-2 (chapter 6.2.4, chapter 6.3.9)	9.1.3 Revocation of wallet unit attestation
TR71	An attacker can revoke a (Q)EAA without user consent.	Service disruption (R13)	-ISO/IEC 27001 or SiHa or SFB or comparable -ETSI 319 411-1 (chapter 6.2.4, chapter 6.3.9) -ETSI 319 411-2 (chapter 6.2.4, chapter 6.3.9)	9.1.3 Revocation of wallet unit attestation
TR72	An attacker can trigger multiple identification requests without them being recognised as intentional orphan requests.	Service disruption (R13)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -ETSI 319 411-1 (chapter 6.2, chapter 6.3, chapter 6.5) -ETSI 319 411-2 (chapter 6.2, chapter 6.3) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as: cryptographic tokens,	

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			electronic signatures, hashing, timestamps	
TR73	An attacker can send multiple requests with no follow-up transaction.	Service disruption (R13)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -ETSI 319 411-1 (chapter 6.2, chapter 6.3, chapter 6.5) -ETSI 319 411-2 (chapter 6.2, chapter 6.3) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as: cryptographic tokens, electronic signatures, hashing, timestamps	
TR74	An attacker can allow a relying party to request identification without a matching identification (response) and full control.	Service disruption (R13)		8.2.3 PID and EAA presentation
TR75	An attacker can send a response to a request after its timeout, or similar situations leading to a service disruption.	Service disruption (R13)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and	8.3.3 Orchestration 8.4.2 Wallet user interface application (mobile application)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -ETSI 319 411-1 (chapter 6.2, chapter 6.3) -ETSI 319 411-2 (chapter 6.2, chapter 6.3, chapter 6.5) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as: cryptographic tokens, electronic signatures, hashing, timestamps, sessionID, session	8.4.3 Wallet user interface application (web application)
TR76	A relying party can send multiple invalid requests.	Service disruption (R13)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as: cryptographic tokens, electronic signatures, hashing, timestamps, sessionID, session	8.3.3 Orchestration 8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR77	An attacker can send multiple invalid requests to a wallet provider.	Service disruption (R13)	-ETSI 319 411-1 (chapter 6.2, chapter 6.3, chapter 6.5) -ETSI 319 411-2 (chapter 6.2, chapter 6.3, chapter 6.5) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as: cryptographic tokens, electronic signatures, hashing, timestamps, sessionID, session	7. Wallet provider management and operation
TR78	An attacker can make a Member State unable to revoke an untrusted PID provider from the trusted PID provider trusted list.	Service disruption (R13)		
TR79	An attacker can prevent suspension or revocation of a wallet.	Service disruption (R13)	-ISO/IEC 27001 or SiHa or SFB or comparable -ETSI 319 411-1 (chapter 6.2, chapter 6.3, chapter 6.5) -ETSI 319 411-2 (chapter 6.2, chapter 6.3, chapter 6.5) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as: cryptographic tokens, electronic signatures, hashing, timestamps, sessionID, session	7.7 operation Security 7.8 Network Security 7.9 Vulnerabilities and incident management 7.11 Business continuity management 9.1.3 Revocation of wallet unit attestations

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR80	An attacker can block transactions by relying parties, users and/or PID provider.	Service disruption (R13)	-ISO/IEC 27001 or SiHa or SFB or comparable	7.7 operation Security 7.8 Network Security 7.9 Vulnerabilities and incident management 7.11 Business continuity management
TR81	An attacker can disable or make a WSCD unavailable.	Surveillance (R14)	-ISO/IEC 27001 or SiHa or SFB or comparable	7.7 operation Security 7.8 Network Security 7.9 Vulnerabilities and incident management 7.11 Business continuity management
TR82	An attacker can make the PID provider unable to revoke or suspend PIDs.	Surveillance (R14)	-ISO/IEC 27001 or SiHa or SFB or comparable	7.7 operation Security 7.8 Network Security 7.9 Vulnerabilities and incident management 7.11 Business continuity management 9.1.3 Revocation of wallet unit attestations
TR83	A relying party can derive the user's identity data beyond data shared with them.	Surveillance (R14)	-using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.1 General and lifecycle requirements

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR84	A group of colluding relying parties or PID providers can derive the user's identity data beyond data known to them.	Surveillance (R14)	-EAA construction following ARF rulebooks -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.1 General and lifecycle requirements
TR85	An attacker can track and trace a user by using person identification data of the user where identification of the user is not required.	Surveillance (R14)	-EAA construction following ARF rulebooks -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.2.3 PID and EAA presentation
TR86	An attacker can combine a 'forged' presentation of (Q)EAA combinations.	Transaction manipulation (R10)	-ETSI 319 411-1 (chapter 6.2, chapter 6.3, chapter 6.5) -ETSI 319 411-2 (chapter 6.2, chapter 6.3, chapter 6.5) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.3.3 Orchestration 8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)
TR87	An attacker can activate/take over the wallet remotely (e.g., a bank app embedding an authentication or attestation request) without the explicit consent or sole control of the user, in situations where the user is unaware of (e.g., asleep), or cannot see the relying party.	Transaction manipulation (R10)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -User authentication (knowledge, biometrics) -using sufficient cryptographic	8.2.3 PID and EAA presentation 8.3.1 User Authentication 8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			techniques/primitives pursuant to ECCG ACM such as protection of private key material in hardware of user device	
TR88	Attackers can make changes to a request's metadata (service name, usages, etc.).	Transaction manipulation (R10)	-ISO/IEC 27001 or SiHa or SFB or comparable -ETSI 319 401 (chapter 7.4, chapter 7.5) -ETSI EN 319 411-1 (chapter 6.5) -ETSI 319 411-2 (chapter 6.5) -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as protection of private key material in hardware of user device	TBD

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR89	Attackers can make changes to response information (service state, nonce, etc.).	Transaction manipulation (R10)	-ISO/IEC 27001 or SiHa or SFB or comparable -ETSI 319 401 (chapter 7.4, chapter 7.5) -ETSI EN 319 411-1 (chapter 6.5) -ETSI 319 411-2 (chapter 6.5) -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as protection of private key material in hardware of user device	8.3.3 Orchestration 8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)
TR90	Attackers can make changes to a request's attribute information (over asking, etc.).	Transaction manipulation (R10)	- ISO/IEC 27001 or SiHa or SFB or comparable -ETSI 319 401 (chapter 7.4, chapter 7.5) -ETSI EN 319 411-1 (chapter 6.5) -ETSI 319 411-2 (chapter 6.5) -OWASP MAS -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as protection of private key material in hardware of user device	8.3.3 Orchestration 8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR91	A relying party can replay elements from a previous session in another session.	Transaction manipulation (R10)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as protection of private key material in hardware of user device	8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)
TR92	An attacker can replace or modify the PID during its transfer from the PID provider to the wallet unit.	Transaction manipulation (R10)	-protection of channels (e.g., mutual authentication, channel/token binding, short-lived access tokens with proof of possession) and relying on sufficient cryptographic mechanisms pursuant to ECCG ACM	8.4 Wallet instance requirements 9.1.1 Wallet activation and monitoring (18)
TR93	An attacker can replace or modify the PID during its transfer from the wallet unit to the online relying party.	Transaction manipulation (R10)	-protection of channels (e.g., mutual authentication, channel/token binding, short-lived access tokens with proof of possession) and relying on sufficient cryptographic mechanisms pursuant to ECCG ACM	8.4 Wallet instance requirements 9.1.1 Wallet activation and monitoring (18)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR94	An attacker can replace or modify the PID during its transfer from the wallet unit to the offline relying party.	Transaction manipulation (R10)	-protection of channels (e.g., mutual authentication, channel/token binding, short-lived access tokens with proof of possession) and relying on sufficient cryptographic mechanisms pursuant to ECCG ACM	8.4 Wallet instance requirements 9.1.1 Wallet activation and monitoring (18)
TR95	An attacker can issue a PID without the user's consent.	Unauthorised transaction (R9)	-User authentication (knowledge, biometrics, possession) using sufficient cryptographic techniques/primitives pursuant to ECCG ACM e.g., cryptographic key material stored in hardware element of user device	8.3.1 User authentication 8.3.2 User interaction
TR96	An attacker can use revoked or invalid embedded disclosure policies, possibly without the relying parties' knowledge.	Unauthorised transaction (R9)	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -Testing EAA presentation	9.1.3 Revocation of wallet unit attestations
TR97	An attacker can trick the wallet into verifying wrong electronic signatures.	Unauthorised transaction (R9)	N/A in the current analysis	

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR98	An attacker can use the wallet outside of the user's control.	Unauthorised transaction (R9)	-OWASP MAS - Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -User authentication (knowledge, biometrics, possession) using sufficient cryptographic techniques/primitives pursuant to ECCG ACM e.g., cryptographic key material stored in hardware element of user device	8.2.3 PID and EAA presentation 8.3.1 User authentication 8.3.2 User interaction 8.3.4 Authenticity and trust anchor checks 8.4 Wallet instance requirements
TR99	An attacker can convince a user to authenticate and approve transactions with an attacker or unauthorised third party.	Unauthorised transaction (R9)	-User guidance -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM e.g., cryptographic key material stored in hardware element of user device	8.3.2 User interaction

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR100	An attacker can make a user electronically sign without presenting the content to the user or after presenting wrong content.	Unauthorised transaction (R9)	N/A in the current analysis	
TR101	An attacker can bypass access control of the user's account with the wallet provider.	Unauthorised transaction (R9)	-Multi-factor authentication (Possession, knowledge, inherence) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.3.1 User authentication
TR102	An attacker can impersonate relying parties during the connection to relying parties.	Unauthorised transaction (R9) / Data disclosure (R6)	-using sufficient cryptographic techniques/primitives pursuant to ECCG ACM mutual authentication, certificate-based authentication	8.3.4 Authenticity and trust anchor checks
TR103	The user behind the relying party – browser connection can be different from the user behind the relying party – wallet connection.	Unauthorised transaction (R9) / Data disclosure (R6) / Identity theft (R4)	-using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as using cryptographic binding of transactions	8.3.4 Authenticity and trust anchor checks
TR104	An attacker can convince the user to revoke the user's wallet without reason.	Unauthorised transaction (R9) / Service disruption (R13)	-ETSI EN 119 431-1 (chapter 6.2.4, chapter 6.3.9) -ETSI EN 119 431-2 (chapter 6.2.4, chapter 6.3.9)	9.1.3 Revocation of wallet unit attestations

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR105	An attacker can perform man-in-the-middle attacks.	Unauthorised transaction (R9) / Data disclosure (R6) / Surveillance (R14)	-protection of channels (e.g., mutual authentication, channel/token binding, short-lived access tokens with proof of possession) and relying on sufficient cryptographic mechanisms pursuant to ECCG ACM	8.4 Wallet instance requirements 9.1.1 Wallet activation and monitoring (18)
TR106	An attacker can present invalid or revoked attributes from a wallet that does not regularly connect to the network.	Effect on various risks	-time-based refresh of attributes using e.g., a timestamp -time-based invalidation of attributes using e.g., a timestamp	8.1 General and lifecycle requirements (Sec-01)
TR107	An attacker can steal information from a user by spoofing a wallet.	Effect on various risks	-Cryptographic linking (or binding) of a wallet instance to a particular end-user device such as using private key material of a hardware element (e.g., Secure Enclave, TEE or comparable) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)
TR108	An attacker can impersonate the user by replaying/imitating a data request (e.g., authentication), which would appear as valid.	Effect on various risks	-using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as using cryptographic binding of transactions, sessionID, sessions, nonce and change of sessionID after successful or unsuccessful authentication attempt	8.3.1 User authentication 8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR109	An attacker can replay an embedded disclosure policy towards a user, to imitate an approved request.	Effect on various risks	-Testing EAA presentation using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as using cryptographic binding of transactions, sessionID, sessions, nonce or comparable	8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)
TR110	An attacker can exploit the lack of information of wallet users, or undue delays, after a security breach or compromise.	Effect on various risks	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7.9, chapter 7.11)	9.1.1 Wallet unit activation and monitoring
TR111	An attacker can modify a previously installed legitimate wallet instance to add malicious features.	Effect on various risks	-ISO/IEC 27001 or SiHa or SFB or comparable -prevent rooted end user devices	8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application) 9.1.1 Wallet unit activation and monitoring
TR112	An attacker can modify a legitimate wallet instance and propose it to users as a legitimate one.	Effect on various risks	-ISO/IEC 27001 or SiHa or SFB or comparable -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as using cryptographic binding of transactions, cryptographic hash functions, electronic signatures or comparable	9.1.1 Wallet unit activation and monitoring

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR113	An attacker can defeat the user authentication mechanism itself to bypass the authentication of the wallet user.	Effect on various risks	-Multi-factor authentication (possession, knowledge, inherence) for user authentication based on independent factors of authentication	8.3.1 User Authentication
TR114	An attacker can introduce malicious code or backdoors into the wallet code during its deployment to the user device.	Effect on various risks	-ISO/IEC 27001 or SiHa or SFB or comparable -EN 319 401 (chapter 7) -ETSI EN 319 411-2 (chapter 7, chapter 8) -ETSI T 119 431-1 (chapter 5) -EN 319 403-1 -using sufficient cryptographic mechanisms pursuant to ECCG ACM e.g., electronically signing the Source Code	7.9 Vulnerability Management
TR115	An attacker can introduce malicious code or backdoors into the wallet code during its development.	Effect on various risks	-ISO/IEC 27001 or SiHa or SFB or comparable -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as using cryptographic binding of transactions, cryptographic hash functions, electronic signatures or comparable	7.9 Vulnerability Management
TR116	An attacker can tamper with the generation of random numbers to	Effect on various risks	-ISO/IEC 27001 or SiHa or SFB or comparable -Certified HSM for random number	8.4.1 Protection of assets in the wallet instance (Sec-04)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
	reduce their entropy sufficiently to enable attacks.		generation (e.g., EUCC or NIST FIPS 140-2/3) -ETSI TS 119 431-1 (chapter 6) -EN 319 401 (chapter 7), relying on sufficient cryptographic mechanisms pursuant to ECCG ACM	8.4.2 Wallet user interface (mobile application) (Sec-06) 8.4.3 Wallet user interface application (web application)
TR117	An attacker can tamper with user devices in the supply chain to include code or configurations that do not meet the conditions of use of the wallet.	Effect on various risks	-ISO/IEC 27001 or SiHa or SFB or comparable -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -Art. 21 NIS2 Directive -EN 319 401 (chapter 5, chapter 7.14)	8.4.2 Wallet user interface (mobile application) (Sec-06) 8.4.3 Wallet user interface application (web application)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR118	An attacker can activate a wallet unit while using a spoofed WSCD controlled by the attackers.	Effect on various risks	-ISO/IEC 27001 or SiHa or SFB or comparable -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -Art. 30 certified remote QSCD ETSI EN 319 411-1 (chapter 6) ETSI EN 319 411-2 (chapter 6)	
TR119	An attacker can read information sent to the WSCA and/or the WSCD.	Effect on various risks	-using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as using cryptographic binding of transactions, cryptographic hash functions, electronic signatures, TLS mutual authentication	8.5 WSCA requirements
TR120	An attacker can send arbitrary information to the WSCA.	Effect on various risks	-using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as using cryptographic binding of transactions, cryptographic hash functions, electronic signatures, TLS mutual authentication	8.5 WSCA requirements

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR121	An attacker can steal information by intercepting the exchanges between the WSCA and the WSCD.	Effect on various risks	-using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as using cryptographic binding of transactions, cryptographic hash functions, electronic signatures, TLS mutual authentication	8.5 WSCA requirements
TR122	An attacker can send arbitrary information to the WSCD.	Effect on various risks	-using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as using cryptographic binding of transactions, cryptographic hash functions, electronic signatures, TLS mutual authentication	8.5 WSCA requirements
TR123	An attacker can send information to the WSCD, circumnavigating the WSCA.	Effect on various risks	-using sufficient cryptographic techniques/primitives pursuant to ECCG ACM such as using cryptographic binding of transactions, cryptographic hash functions, electronic signatures, TLS mutual authentication	8.5 WSCA requirements
TR124	An attacker can use phishing to get users to a fake wallet and PID management web application.	Effect on various risks	-Multi-factor authentication (possession, knowledge, inherence) using end user device -Mutual authentication of wallet and RP	8.3.1 User authentication (Sec-12) 8.3.2 User Interaction (Sec-02, Sec-03)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR125	An attacker can replace a wallet's keys with other keys to create messages to be used in another attack.	Effect on various risks	-EN 319 401 (chapter 7, hardware key in device, device attestation before critical action, multi-factors of authentication (possession, knowledge, inherence) -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM	8.5 WSCA requirements
TR126	An attacker can modify or destroy a wallet's keys, making some functions of the wallet unusable.	Effect on various risks	-EN 319 401 (chapter 7) -Private key in device hardware such as TEE, Secure Enclave (or comparable), device attestation before critical action -multi-factors of authentication (possession, knowledge, inherence) -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or	8.4.1 Protection of assets in the wallet instance 8.5 WSCA requirements

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) using sufficient cryptographic techniques/primitives pursuant to ECCG ACM or e.g.	
TR127	An attacker can control a malware to access data stored in the wallet.	Effect on various risks	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM or e.g., in hardware element of the device	8.4.1 Protection of assets in the wallet instance 8.4.2 Wallet user interface application (mobile application) 8.4.3 Wallet user interface application (web application)

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
TR128	An attacker can access evidence generated in the wallet.	Effect on various risks	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM or e.g., in hardware element of the device	7.3 Asset Management 7.4 Access Control
TR129	Wallet providers can access objects in the wallet.	Effect on various risks	- EN 319 401 (chapter 7, hardware key in device, device attestation before critical action, multi-factors of authentication (possession, knowledge, inherence) -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG	8.1 General and lifecycle requirements

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			ACM or e.g., in hardware element of the device	
TR130	Wallet providers can access evidence generated in the wallet	Effect on various risks	- User authentication (possession, knowledge, inherence) -OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM or e.g., in hardware element of the device	8.1 General and lifecycle requirements
TR131	An attacker can steal an unlocked wallet device.	Effect on various risks	-User guidance -Unlock timeouts -User authentication for presentations (possession, knowledge, inherence) (partly	8.3.1 User Authentication
TR132	An attacker can manipulate the system to prevent certain events from being logged.	Effect on various risks	-OWASP MAS -Secure Software Lifecycle (e.g., ETSI 319 401 chapter 7.8. and chapter 7.14, or ETSI TS 119 431-1 chapter 6.4 and chapter 6.5, or ETSI 319 411-1 chapter 6.4 and chapter 6.5, or ISO 27001 (Annex	7.9.1 Monitoring and logging

Id	Threat Description	Risk title	Standards coverage	Coverage in the document
			A, or ISO 27002) control 8.20, 8.22, 8.25 to 8.32) -using sufficient cryptographic techniques/primitives pursuant to ECCG ACM or e.g., in hardware element of the device	
TR133	An attacker can intercept communication between the wallet instance and the WSCA, or replay/imitate a user (e.g., by hijacking authentication mechanism).	Effect on various risks	-EN 319 401 (chapter 7) -ETSI TS 119 431-1 (chapter 5) protection of channels (e.g., using TLS, mutual authentication, channel/token binding, short-lived access tokens with proof of possession)	8.4.1 Protection of assets in the wallet instance (Sec-05) 8.5 WSCA requirements

C Mapping to CIR (EU) 2015/1502

C.1 Introduction

C.2 Mapping to requirements

ID	CIR Requirement	Covered by	Rationale
2.1	**Enrolment**		
2.1.1	*Application and registration*		
2.1.1-L1	Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.	Section 6.2	Requirements on terms and conditions from EN 319 401
2.1.1-L2	Ensure the applicant is aware of recommended security precautions related to the electronic identification means.	Scheme, Annex III	This is part of the documentation to be made publicly available
2.1.1-L3	Collect the relevant identity data required for identity proofing and verification.		
2.1.2	*Identity proofing and verification (natural person)*	PSI-10.1-08	To be enhanced through references to standards or schemes
2.1.3	*Identity proofing and verification (legal person)*	Out of scope	Legal persons not in scope
2.1.4	*Binding between the electronic identification means of natural and legal persons*	Out of scope	Legal persons not in scope
2.2	**Electronic identification means management**		
2.2.1	*Electronic identification means characteristics and design*		
2.2.1-S1	The electronic identification means utilises at least two authentication factors from different categories.	WUH-8.3.1-Sec-07	The requirement is an exact match

ID	CIR Requirement	Covered by	Rationale
2.2.1-S2	The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.	WUG-8.1-Fun-01 WUI-8.2.1-Sec-06 WUH-8.3.1-Sec-08 WUP-8.2.3-Fun-09 PSI-10.1-06	This is guaranteed by a chain of bindings between the user and the wallet (setting authentication means), the PID means and the user (identity proofing), the wallet and the PID means (cryptographic binding), and finally the authentication of the user during presentation.
2.2.1-H1	The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential.	Functional specs WUP-8.2.3-Sec-14	Protection against duplication is embedded in the encoding. There is a specific requirement on integrity verification between
2.2.1-H2	The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.	Section 8.3.1 Section 8.4	There are strong requirements on user authentication, as well as requirements on the wallet instance intended to make it difficult to use a stolen device.
2.2.2	*Issuance, delivery and activation*		
2.2.2-H1	The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.		This is a combination of the binding between the user and the wallet (with authentication to the WSCA/WSCD), combined with identity proofing to be performed when issuing a PID.
2.2.3	*Suspension, revocation and reactivation*		
2.2.3-L1	It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner.	WSU-9.1.1-14 WSU-9.1.1-15 Section 10.3	The eID means can be revoked by revoking the PID or the wallet unit. An offline mechanism is available for the revocation of the wallet unit.
2.2.3-L2	The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation.	WSU-9.1.1-14 WSU-9.1.1-15	A specific and out-of-band authentication mechanism is set up specifically for this purpose.
2.2.3-L3	Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.	See issuance	Reactivation is only possible as a new issuance.
2.2.4	*Renewal and replacement*		
2.2.4-L	Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level.	Full new issuance?	
2.2.4-H	Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.	Full new issuance?	
2.3	**Authentication**		

ID	CIR Requirement	Covered by	Rationale
2.3.1	*Authentication mechanism*		
2.3.1-S1	The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication.	WUP-8.2.3-Sec-14	PID is intended to be stored signed and encrypted and its integrity verified.
2.3.1-L2	Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.	GEN-7.3.2-02 WSA-8.5-Sec-13	The WSCA/WSCD authentication mechanism is considered as critical, so all assets related to it are managed by the WSCD.
2.3.1-H3	The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.	Section 8.3.1 Section 8.2.3	The WSCA/WSCD user authentication mechanism, which protects access to PID, is highly protected. In addition, mechanisms are in place for the authentication of the other stakeholders. They are all evaluated against the risk register, which includes the mentioned threats.
2.4	**Management and organisation**		
2.4.1	*General provisions*		
2.4.1-L1	Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognised as such by national law of a Member State, with an established organisation and fully operational in all parts relevant for the provision of the services.	Out of scope	Not related to cybersecurity
2.4.1-L2	Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service, including the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long.	Out of scope	Not related to cybersecurity
2.4.1-L3	Providers are able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services.	Out of scope	Not related to cybersecurity
2.4.1-L4	Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.	Section 7.14 GEN-7.14.3-02	A full section describes requirements on supply chain policy and procedures, and the same level of evidence needs to be presented about the tasks fulfilled by the supplier.
2.4.1-L5	Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of	Section 7.12	Termination is covered

ID	CIR Requirement	Covered by	Rationale
	service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.		
2.4.2	*Published notices and user information*		
2.4.2-L1	The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.	Section 6.2 GEN-6.2-02	
2.4.2-L2	Appropriate policy and procedures are to be put in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service.	Section 6.2 GEN-6.2-03	
2.4.2-L3	Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.	Section 6.2 GEN-6.2-04	
2.4.3	*Information security management*		
2.4.3-L1	There is an effective information security management system for the management and control of information security risks.	GEN-7.1.1-02 Chapters 6 and 7	The various sections constitute the essential parts of an ISMS, so altogether, they form an ISMS, and they apply to all entities that get one of the services they provide certified.
2.4.3-S2	The information security management system adheres to proven standards or principles for the management and control of information security risks.	GEN-7.1.1-02	The requirements are matching
2.4.4	*Record keeping*		
2.4.4-L1	Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.	GEN-7.10-01	The requirements on collection of evidence from ETSI EN 319 401 cover this requirement
2.4.4-L2	Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.	GEN-7.10-01	The requirements on collection of evidence from ETSI EN 319 401 cover this requirement
2.4.5	*Facilities and staff*		

ID	CIR Requirement	Covered by	Rationale
2.4.5-L1	The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.	GEN-7.3.2-01	This is addressed explicitly by ETSI EN 319 401, in particular REQ-7.2-02 and REQ-7.2-04.
2.4.5-L2	The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.		
2.4.5-L3	Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.	Section 7.6	Physical security requirements from ETSI EN 319 401 cover all the mentioned aspects and more. A requirement has been added specifically to cover the cases of the
2.4.5-L4	Facilities used for providing the service ensure that access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.	GEN 7.6-01	This is specifically covered by requirement REQ-7.6-02 of ETSI EN 319 401.
2.4.6	*Technical controls*		
2.4.6-L1	The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.	Many sections	There are many sections covering technical controls, and the certification scheme itself requires a demonstration that the risks identified on the provider's systems are mitigated.
2.4.6-L2	Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.	Section 7.5 Section 7.8	This is addressed by a combination of requirements on networking and on cryptography, combined with the requirement to address at least the risks in the risk register (including all risks listed here and more).
2.4.6-L3	Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text.	GEN-7.5-0.3	This requirement extends the protection requirements to critical assets when they are stored on the wallet provider's and PID provider's systems.
2.4.6-L4	Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.	Section 7.11	The business continuity requirements address these issues, including a specific subsection wit requirements related to the management of crises.
2.4.6-L5	All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.	Section 7.3.3	The requirements from ETSI EN 319 401 are rqther extensive on this matter.
2.4.7	*Compliance and audit*		

ID	CIR Requirement	Covered by	Rationale
2.4.7-H1	The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.	EUDIW	The EUDIW certification scheme requires a strict schedule for surveillance evaluations.
2.4.7-H2	Where a scheme is directly managed by a government body, it is audited in accordance with the national law.	Out of scope	

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union