

G-04

PL EUDI Wallet Certification System

Developing and maintaining the
risk register for EUDI Wallet
implementation and certification

project no. 224294

2026.04.02

Document reference	G-04
Version	Not relevant
Status	Not relevant
Date	02.04.2026
Document type	CEN TS XXXX project no. 224294
Parent framework	G-01
Scheme Owner	Republic of Poland / Minister of Digital Affairs
Certification target	Not relevant
Primary audience	EUDI Providers. PID Providers
Secondary audience	EUDI Wallet ecosystem stakeholders as indicated in the document
Assurance level <identity proofing CIR 2015/1502> or <evaluation, EU Regulation 2019/881>	Not relevant
Subsidiary Documents	Not relevant

CEN/TC 224

Date: 2026-03-30

Secretariat: AFNOR

WI Number: 00224294

Personal identification — Developing and maintaining the risk register for EUDI Wallet implementation and certification

ICS:

CCMC will prepare and attach the official title page.

Contents.....	Page
European foreword.....	3
Introduction	4
1 Scope	5
2 Normative references	5
3 Terms and definitions	5
4 Abbreviations	7
5 Sectoral cybersecurity assessment in the context of EUDI Wallet ecosystem ..	7
6 Risk management in the context of EUDI Wallet ecosystem	10
Annex A (informative) Examples of business objectives and requirements	31
Annex B (informative) Examples of normalized scales in risk assessment	34
Annex C (informative) Examples of risk register template	38
Annex ZA (informative) Relationship between this European Standard and therequirements of aimed to be covered	39
Bibliography	40

European foreword

This document (prEN:) has been prepared by Technical Committee CEN/TC"", the secretariat of which is held by.

This document is currently submitted to the CEN Enquiry.

This document will supersede EN:.

In comparison with the previous edition, the following technical modifications have been made:

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For relationship with EU Directive(s), see informative Annex ZA, which is an integral part of this document.

Introduction

The framework for cybersecurity assessment to be applied in the EUDI Wallet ecosystem is based on application of two standards:

- a) EN ISO/IEC 27005:2022 Guidance on managing information security risks; this standard provides approaches to risk management in the context of information security/cyber security risks which are identified in a multi-stakeholder ecosystem (specifically, see Annex A2 of this standard).
- b) EN 18037:2025 Guidance on a sectoral cybersecurity assessment; this standard specifies an approach for the risk-based identification of cybersecurity, certification, and assurance requirements for ICT products, processes, and services within complex, multi-stakeholder sectoral systems. The methodology offers the following key features:
 - **Business Process Contextualization:** The assessment begins with an analysis of the business processes supported by the sectoral ICT system, alongside the corresponding business objectives of each stakeholder. It identifies primary and supporting assets critical to secure implementation.
 - **Asset and System Mapping:** ICT systems, products, and processes under stakeholder control that are relevant to securing primary assets are mapped. A deep dive into the sectoral system architecture provides detailed insight into their intended use.
 - **Cyber Threat Intelligence (CTI):** CTI is used to gather insights into relevant attacker types, their motivations, and capabilities. This allows for prioritization of risk scenarios most deserving of further analysis, optimizing the use of analytical resources and supporting assignment of tailored cybersecurity and assurance requirements.
 - **Risk Assessment:** Risks are assessed based on the impact of cybersecurity incidents on business objectives and the likelihood of such incidents occurring. Likelihood is derived from attacker motivation and capability as determined through CTI. Risk data derived from an ISO/IEC 27005-compliant approach is supported by the concept of attack potential in relation to assurance introduced in EN ISO/IEC 15408 (multipart).
 - **Reference Levels:** The methodology introduces a system of reference levels for internal risk, security, assurance, and attack potential. When used collectively, these support consistency in defining cybersecurity risks.

<The clause on applicability in and beyond the national certification schemes>

1 Scope

The CEN/TS XXXXX specifies a risk register related to the implementation and certification of European Digital Identity Wallet (EUDIW) solutions. In this respect, this document defines:

- General aspects of managing the risks to be included to the register;
- Structured specification of the risk management including identification, analysis, assessment, treatment, communication and monitoring activities in regard to the risks related to the EUDI Wallet implementations;
- Developing and maintaining the risk registry.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 18037, *Guidelines on a sectoral cybersecurity assessment*

3 Terms and definitions

<Editor's note: The set of definitions will be complemented and then re-organized according to the systematic order in 2WD. Experts are kindly asked to review the terms and propose new entries, if necessary>

For the purposes of this document, the following terms and definitions apply/ the terms and definitions given in EN 18037:2025 and the following apply.

- ISO Online browsing platform: available at <http://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1

risk register

record of information relevant to the certification process about identified risks

[SOURCE: Commission Implementing Regulation 2024/2981, art. 2(7)]

3.2

asset

anything that has value to the organization

Note 1 to entry: Two kinds of information security related assets can be distinguished:

the primary assets;

- business processes & activities;

- information;

the supporting assets (on which the primary assets rely) of all types:

35 — software;

36 — network;

37 — personnel;

38 — site;

39 — organizational structure

40 Note 2 to entry: In the context of EUDIW, the primary assets can encompass functional assets considered
41 as the results of decomposition of high-level requirements set up in Regulation (EU) 2024/1183 and
42 subsequent Commission Implementing Regulations

43 [SOURCE: ISO/IEC 27002:2022, 3.1.2 modified - Note 2 to entry has been added]

44 **3.3**

45 **assurance**

46 <identity proofing> degree of confidence in the claimed or asserted identity of a person

47 Note 1 to entry: Note 1 to entry: The definition is derived from EU Regulation 2014/910, art. 8.

48 **3.4**

49 **assurance**

50 <evaluation> grounds for confidence that a target of evaluation (TOE) meets the security
51 functional requirements

52 [SOURCE: EN ISO/IEC 15408-1, 3. 6]

53 **3.5**

54 **attack potential**

55 measure of the effort needed to exploit a vulnerability in a target of evaluation (TOE)

56 Note 1 to entry: The effort is expressed as a function of properties related to the attacker (e.g. expertise,
57 resources, and motivation) and properties related to the vulnerability itself (e.g. window of opportunity,
58 time to exposure).

59 [SOURCE: EN ISO/IEC 15408-1, 3.8]

60 **3.6**

61 **Wallet Unit**

62 A unique configuration of a Wallet Solution provided by a **Wallet Provider** to an individual Wallet
63 **User**

64 [SOURCE: [0](#), Annex A modified - a phrase "that includes Wallet instances, Wallet Secure
65 Cryptographic Applications and Wallet Secure Cryptographic Devices" has been removed]

66 **3.7**

67 **Wallet Solution**

68 A combination of software, hardware, services, settings, and configurations, including Wallet
69 Instances, one or more Wallet Secure Cryptographic Applications and one or more Wallet Secure
70 Cryptographic Devices

71 Note 1 to entry: For a high-level description of the Wallet provider ICT system it is sufficient to say that
72 Wallet Instances, Wallet Secure Cryptographic Applications and Wallet Secure Cryptographic Devices are
73 components of the system.

74 [SOURCE: [0](#), Annex A modified - Note 1 to entry has been added]

75 **3.8**

76 **Trusted List**

77 repository of information about authoritative entities in a particular legal or contractual context
78 which provides information about their current and historical status

79 [SOURCE: [0](#), Annex A]

80 **4 Abbreviations**

EUDIW European Digital Identity Wallet

eIDAS electronic IDentification, Authentication and trust Services

GDPR General Data Protection Regulation

PID Personal Identification Data

EAA electronic attestation of attributes

QEAA qualified electronic attestation of attributes

QES qualified electronic signature

QC qualified certificate

TL trusted list

APL attack potential level

CTI cyber threat intelligence

MRC meta risk class

IC impact class

CSL common security level

AVA_VAN assurance vulnerability_vulnerability analysis

CAR common assurance reference

CAB conformity assessment body

81 **5 Sectoral cybersecurity assessment in the context of EUDI Wallet** 82 **ecosystem**

83 **5.1 Application of the sectoral cybersecurity assessment methodology**

84 Three main phases of the overall process (i.e., risk assessment – normalization of risk assessment
85 results – establishing security and assurance requirements) are presented with specific focus on

security and assurance requirements which need to be defined by national certification schemes for EUDI Wallet solutions.

Essential features of the approach are introduced i.e.:

- “attack potential levels” (APL) which rate the motivation, means and opportunities of attackers;

- “meta-risk classes” (MRC), to allow a common approach to risk assessment;

- “common security levels” (CSL), to allow a consistent approach to cybersecurity controls;

- “common assurance references” (CAR), with clear reference to the AVA_VAN concept from EN ISO/IEC 15408 (multipart) to allow comparability between implementations of assurance in several national certification schemes.

However, as the assurance requirements have been already fixed in the Commission Implementing Regulation 2024/2981, this aspect of methodology is reduced and the sectoral assessment is focused on security requirements.

The methodology supports creating a risk register as the result of risk assessment phase. The risk register is relevant to a particular national scheme although the unified methodology will allow the schemes to further harmonize risk registers at the European level.

5.2 EN 18037’s capabilities in supporting the EUDI Wallet ecosystem stakeholders in sectoral assessments

The process flow is presented in Figure 1.

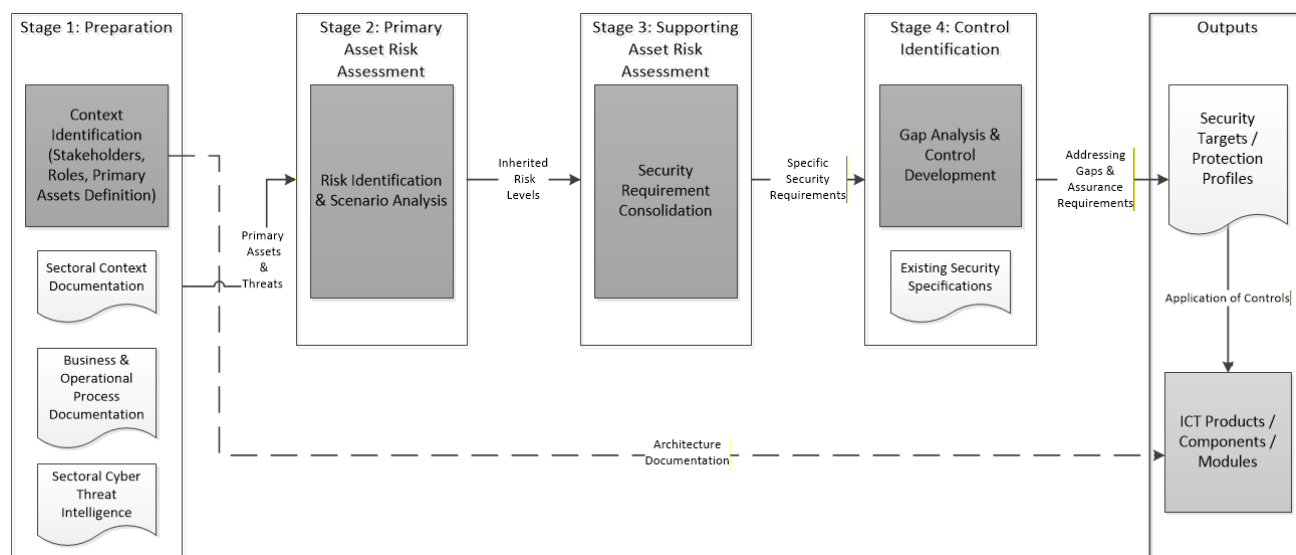


Figure 1— Sectoral cybersecurity assessment process

The first step of the EN 18037 cybersecurity sectoral assessment prepares the ISO/IEC 27005-conformant risk assessment. It starts with the documentation of the sectoral context, followed by the identification of assets, threats, risk scenarios, and potential attackers with their motivation.

The context documentation describes the environment in which the sectoral or application-specific risk and cybersecurity assessment should be conducted. Such documentation includes:

- 112 — Identification of stakeholders of the sectoral system and a description of their roles and
113 responsibilities within the sectoral system;
 - 114 — Documentation of business or operational processes to be supported, the involvement and
115 responsibilities of stakeholders and their objectives per process;
 - 116 — Identification of the sectoral stakeholder's business objectives, obligations and, based on this,
117 the definition of the sectoral primary assets;
 - 118 — Documentation of the sectoral ICT system architecture down to the ICT product level,
119 including a description of functions and data supported by the ICT product, or its components,
120 or system modules;
 - 121 — Documentation of sectoral cyber threat intelligence (CTI), which includes in assumptions on
122 potentially relevant attacker types, their attack potential and their motivation and
123 approaches to conduct attacks targeting the sectoral system.
- 124 The second stage of the EN 18037 cybersecurity assessment, encompasses the primary asset-
125 related risk assessment. It starts with the identification of primary assets which are typically
126 related to the stakeholder's objectives or obligations rather than the technical implementation of
127 the system. Thereafter, the risks to these assets are identified and the risk is analysed by using
128 risk scenarios. Relevant sectoral stakeholders conduct the risk level estimations.
- 129 The primary asset assessment focuses on risks concerning the primary assets and does not regard
130 the individual ICT product, its components or system modules. However, based on the
131 documentation of the sectoral context, a first identification of potentially security-critical system
132 functions and data can be conducted as well.
- 133 The third stage of the EN 18037 cybersecurity assessment, the supporting asset-related risk
134 assessment, focusses on consolidating the security requirements to those ICT products, or their
135 components, or system modules that are relevant for the treatment of a particular risk.
- 136 As a starting point, the risk-relevant supporting assets inherit the risk levels assessed for a
137 dedicated risk scenario in the previous assessment stage. This assessment is being repeated for
138 each relevant supporting asset, now considering product-specific attacker and threat information
139 as well as the ICT product's intended use, technology, and operational environment. As result, the
140 risk scenario-specific security requirements for the supporting asset are determined.
- 141 The fourth stage of the EN 18037 sectoral assessment supports the identification of appropriate
142 controls that match the requirements to the ICT product, or its components, or system modules
143 determined in the previous stages.
- 144 First, existing security specifications are applied to the product as far as possible. Then, an
145 analysis detects the gaps that remain between the security measures already defined for the
146 product, or its components, or modules and the security requirements identified by the previous
147 assessment steps. If the requirements are not completely covered, the remaining gaps should be
148 addressed by developing security controls and, for addressing assurance requirements, feasible
149 security targets, or protection profiles.

6 Risk management in the context of EUDI Wallet ecosystem

6.1 Context establishment

6.1.1 Identifying legal requirements

<tba>

6.1.2 Identification of stakeholders and their roles in EUDI Wallet ecosystem

The EUDI Wallet / Wallet ecosystem consists of several stakeholders performing various tasks and having different responsibilities. If one considers providing or using ICT services directly related to the EUDI Wallet, the stakeholders' relationships are presented in Figure 2.

NOTE 1 All stakeholders' names are written using **bold** font type.

NOTE 2 All descriptions of roles are adopted from [0](#).

Based on the relationships, the list of stakeholders and their roles in the EUDI Wallet ecosystem are the following:

Users of EUDI Wallets – entities that are defined as natural or legal persons using the EUDI Wallet to receive, store and share attestations (PID, QEAA or EAA) and particular attributes about the **user**, including to prove their identity. [0](#) defines 'wallet user' as 'a user who is in control of the wallet unit'. Being in control of the Wallet Unit implies being able to present a PID or attestation to a **Relying Party**. The **User**'s capabilities are dependent on the device where relevant Wallet Unit components are installed, provided by the **Device Manufacturer**.

EUDI Wallet providers – entities that are Member States or organisations either mandated or recognised by Member States making a Wallet Solution available to **Users**.

NOTE 3 All Wallet Solutions are subject to certification, according to [0](#).

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

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

NOTE 4 Wallet providers are subject to the process/service-oriented certification, according to [0](#), as a part of the Wallet Solution certification.

Person Identification Data (PID) providers – entities that verify the identity of the **User** with LoA high requirements, according to [0](#), issue the PID to the Wallet Unit maintain an interface to provide PID and making available, in a privacy-preserving way, information for **Relying Parties** to verify the validity of the PID. without having an ability to receive any information about the use of the PID.

NOTE 5 PID providers are subject to the process/service-oriented certification, according to CIR 2024/2981, as a part of the Wallet Solution certification.

Qualified electronic signature and related services (QES) providers – the trust service providers that provides the **User** means to create qualified electronic signatures or seals over any

189 data. The creation of a qualified electronic signature or seal by means of the Wallet Unit can be
190 achieved in several the following ways:

191 — the Wallet Unit itself could be certified as a qualified signature or seal creation device (QSCD),
192 or

193 — the Wallet Unit could implement secure authentication into an electronic signature or
194 electronic seal invocation capability, as part of a local QSCD or a remote QSCD managed by a
195 QTSP.

196 **Qualified electronic attestation of attributes (QEAA) providers** – the entity that issue a QEAA.
197 after the **User** identity is verified under the authentication process.

198 NOTE 6 It is likely that the **User** requesting a QEAA already possesses a PID. This would enable the **QEAA**
199 **provider** to conduct **User** identification and authentication at LoA high, by requesting and verifying **User**
200 attributes from the PID in the Wallet Unit.

201 NOTE 7 The trust service provider can be the **QEAA provider**.

202 **Non-qualified electronic attestation of attributes (EAA) providers** – entities that provides
203 **Users** with EAA.

204 NOTE 8 EAA can be issued by a trust or non-trust service providers.

205 **Authentic sources providers** – entities that operate public or private repositories or systems,
206 recognised or required by law, containing attributes about natural or legal persons. Authentic
207 Sources are required to provide an interface to **QEAA Providers** to verify the authenticity of the
208 above attributes, either directly or via designated intermediaries recognised at national level.

209 **Access Certificate Authority** – entities that issue access certificate to all PID Providers, QEAA
210 Providers, PuB-EAA Providers, non-qualified EAA Providers and Relying Parties in the EUDI
211 Wallet ecosystem. **Access Certificate Authorities** are notified by a Member State to the
212 Commission. As part of the notification process, the trust anchors of the Access CA are included
213 in a Trusted List by a **Trusted List Provider**.

214 **Providers of registration certificates** – entities that issue one or more registration certificates
215 to each registered Relying Party, PID Provider, QEAA Provider, PuB-EAA Provider, and non-
216 qualified EAA Provider. **Providers of registration certificates** are notified by a Member State to
217 the Commission. Their trust anchors are put on a Trusted List, such that they can be found by
218 Wallet Units and the **User** is able to verify a registration certificate received from a **Relying Party**.

219 **Relying parties** – entities that are natural or legal persons that rely upon an electronic
220 identification or a trust service. In the context of EUDI Wallets, they would request the necessary
221 attributes contained within the PID dataset, QEAA and EAA from the **Users**. To rely on Wallet
222 Units for the purpose of providing a service, **Relying Parties** inform the Member State where
223 they are established about their intention for doing so, and register themselves at the repository
224 provided by the **Provider of registration certificates** along with the attributes that they intend
225 to request.

226 **Trusted List providers** – bodies responsible for maintaining, managing, and publishing a
227 Trusted List. Within the EUDI Wallet ecosystem, Trusted Lists exist for the following entities:

228 — Wallet providers,

229 — PID providers,

- 230 — QEAA providers,
- 231 — PuB-EAA providers,
- 232 — Qualified Electronic Signature (QES) Providers,
- 233 — Access Certificate Authorities,
- 234 — Providers of registration certificates

235 NOTE 9 There is no Trusted List for Relying Parties. The expected number of Relying Party throughout
 236 the Union would make this infeasible. Instead, a Relying Party receives an access certificate from an **Access**
 237 **Certificate Authority**, and this certificate allows a **User** by using the Wallet Unit to authenticate the Relying
 238 Party.

239 **Device manufacturers and related subsystems providers** - entities that provide a platform on
 240 which a Wallet Unit can be built. The components of the Wallet Unit provided by **Device**
 241 **manufacturers and providers of related subsystems** can include, among others, hardware,
 242 operating systems, secure cryptographic hardware, libraries, and app stores.

243 There are several other stakeholders that are not directly involved in the operation of EUDI
 244 Wallet ecosystem although play important roles. They include:

245 **Supervisory bodies/scheme owners** - bodies that supervise the proper functioning of **Wallet**
 246 **providers** and other stakeholders in the EUDI Wallet ecosystem. **Supervisory Bodies** are
 247 created and appointed by the Member States. The **Supervisory Bodies** are notified to the
 248 Commission by the Member States.

249 **National Accreditation Bodies (NAB)** - bodies that perform accreditation with authority
 250 derived from the Member State. NABs accredit **CABs** and then monitor the **CABs** to which they
 251 have issued an accreditation certificate.

252 **Conformity assessment bodies (CAB)** – public or private bodies that are accredited by a **NAB**.
 253 CABs are accredited to conduct assessments on which Member States will rely before issuing a
 254 Wallet Solution or providing the 'qualified' status to a **Trust Service Provider**.

255 NOTE 10 Wallet Solutions will be certified by CABs. QTSPs will be audited regularly by CABs.

256 **Attribute Schema providers** – entities that publish attribute schemas describing the structure
 257 of QEAAAs, PuB-EAAs and EAAs, including the identifier, semantics, and encoding of all attributes.
 258 For PIDs and mDLs, the applicable Rulebooks are published by the Commission.

259 NOTE 11 A catalogue of published Attestation Rulebooks will enable other entities such as **Relying**
 260 **Parties** to discover which attestations exist within the EUDI Wallet ecosystem, and how attributes from
 261 these attestations can be requested and validated.

262 The stakeholders that play roles in respective national EUDI Wallet ecosystems can be different.
 263 For example, a PID provider and EUDI Wallet provider can be the same entity. A relying Party can
 264 be the EAA provider.

265 As the scheme owner is responsible for the risk register development and maintenance, it is
 266 beneficial for all stakeholders, which are obliged to contribute to the scheme risk register, to
 267 implement the same sectoral context establishment.

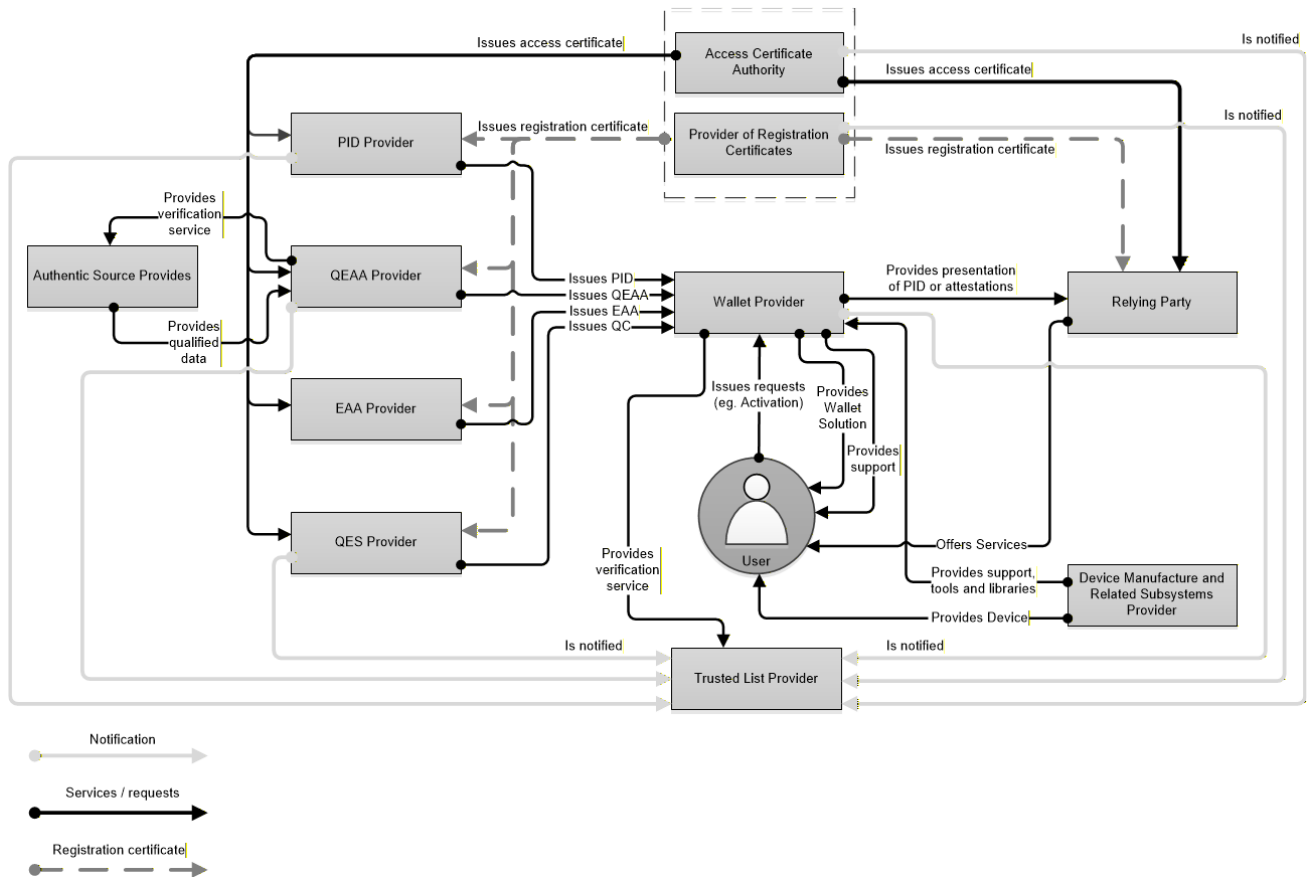


Figure 2— Stakeholders in EUDI Wallet ecosystem

6.1.3 Business and operational processes, identification of stakeholders' objectives

The business and operational processes that are essential for the provision of EUDI Wallet services should be identified. Processes that involve more than one stakeholder type should be selected for the documentation in the sectoral context.

The documentation of the identified business or operational processes is conducted per process in a step-by-step approach and should include the following information:

- Business objectives and related business requirements,
- Preconditions that need to be in place at the start of the process;
- A brief description of every step of the process;
- The stakeholder responsible for implementing and operating the process or individual process steps;
- The stakeholder(s) contributing to individual process steps;
- The stakeholder(s) depending on the results of the process;
- Data generated, stored, processed, or distributed by the process including a first estimation of the criticality of data for the process and the services supported by the process.

After the process is documented, critical objectives or obligations that could be impacted in case of an incident affecting the process should be identified and documented. An example of the documentation for business process is contained in Annex <tba>.

6.1.4 ICT system architecture

After describing the organizational and business aspects of the stakeholder, the technical layer that supports the EUDI Wallet ecosystem stakeholders' processes and services should be documented.

EN 18037, 6.1 introduces the definitions that should be used and the principle, how ICT services, ICT system, ICT processes, and ICT products are interrelated. The relevance of the sectoral ICT system architecture for the risk assessment is described in EN 18037 6.1.4.

The EUDI Wallet ecosystem consists of interrelated ICT systems that provide – jointly or separately - services to the **Users**. Relevant ICT systems are implemented and operated by different stakeholders as indicated in 6.1.2.

The documentation of the ICT system architecture can be described at functional level and with respect to the services provided within the EUDI Wallet ecosystem. The following aspects should be covered:

- a) The ICT system operated by the stakeholder;
- b) The interfaces connecting the stakeholder ICT system in the EUDI Wallet ecosystem;
- c) ICT processes supporting the ICT system, for instance system update processes;
- d) ICT products implemented in the stakeholder ICT system;
- e) ICT processes supporting ICT products, for instance for information on vulnerabilities, software updates or replacements;
- f) ICT infrastructures and ICT infrastructure services employed by the ICT system;
- g) Existing standards and specifications that apply for the ICT system and its components.

EXAMPLE

ICT system high-level architecture for the **Wallet provider** is presented in Figure 3.

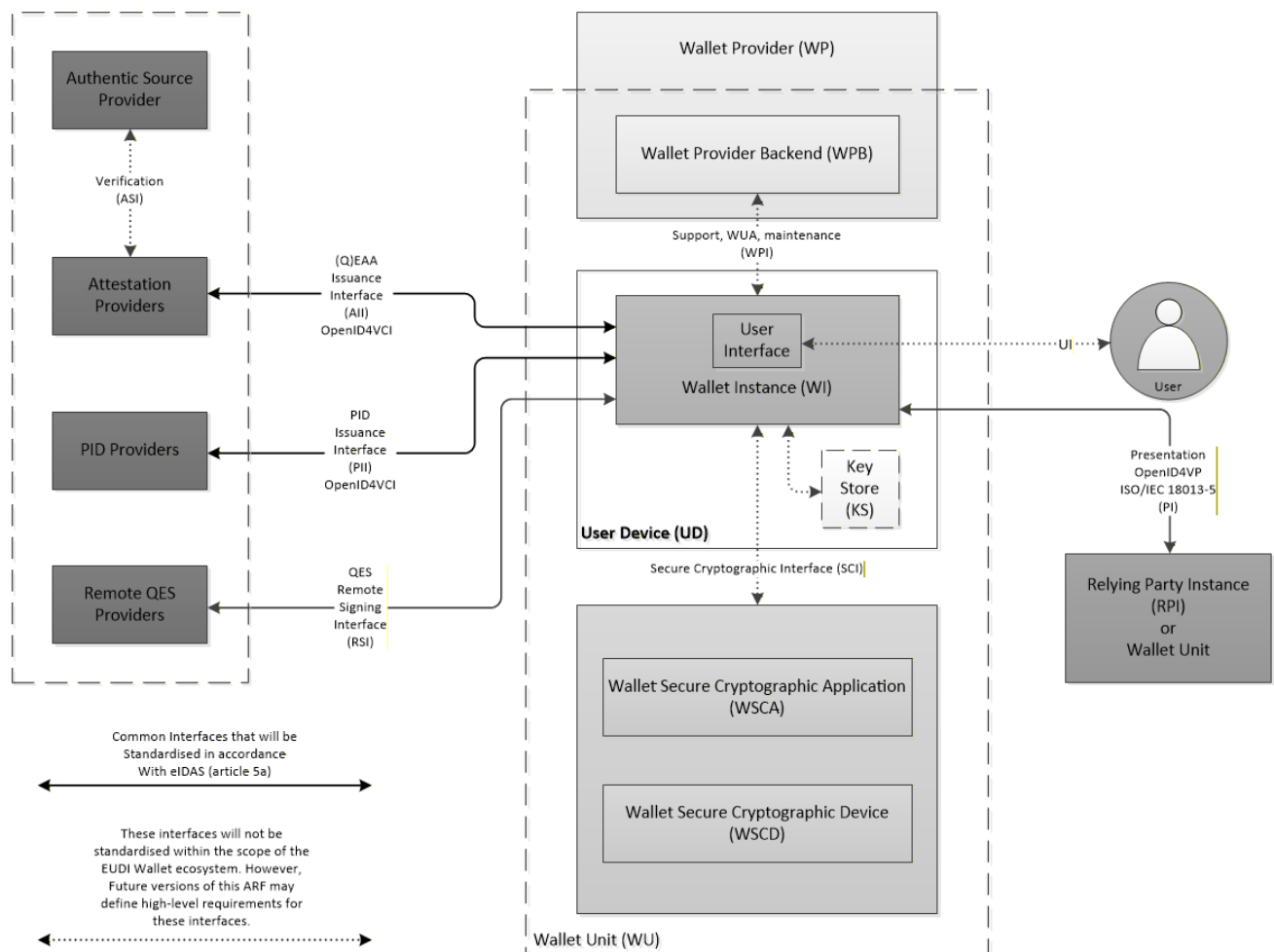


Figure 3— High-level architecture for the Wallet provider ICT system (example)

<Editor note: Experts are kindly asked to provide additional examples for an ICT system of the stakeholder other than the Wallet provider (e.g., PID provider, EAA provider, Access Certificate Authority)>

6.1.5 Subsystems and identification of primary and supporting assets

As risks are identified and assessed in relation to the stakeholder business objectives, the impact of ICT security incidents concerning the ICT system architecture, its ICT products, or its ICT processes on such objectives should be determined.

Based on the documentation of the business processes and the stakeholder's ICT system architecture, it is possible to identify which business process is supported by which components and functions of the system architecture. This establishes the required link between the technical and the business views on the ICT system.

The documentation should be conducted per documented business and operational processes in the following steps:

- a) Those components of the ICT system architecture that support a dedicated business or operational process are identified and documented as subsystems or modules supporting this process;

- 329 b) Data flows between the components of the subsystem are documented to identify the
330 functions and data that are relevant for the processes' functioning and security;
- 331 c) Functions and data that, if compromised, would have significant impact on the business or
332 operational process are identified and documented;
- 333 d) Critical functions and critical data are documented as primary assets associated with the
334 specific process;
- 335 e) An initial criticality rating of primary assets is conducted which is used in the following steps
336 of cybersecurity assessment for the identification of risks and prioritization of risk scenarios
337 to be assessed;
- 338 f) The subsystem's ICT products or other stakeholders' ICT systems that implement, store or
339 process information assets are determined and documented as supporting assets.
- 340 Based on the identification of the ICT products a detailed description should include the following
341 information:
- 342 g) The security-relevant functions of the ICT product (security architecture);
- 343 h) The information (primary) assets supported by the ICT product;
- 344 i) The stakeholder in charge of the secure deployment, operation, and maintenance of the ICT
345 product;
- 346 j) The operational environment of the ICT product.

347 **6.1.6 Documentation of CTI information related to the EUDI Wallet ecosystem**

348 The documentation of cyber threat intelligence information includes considerations on relevant
349 threats and attacker types, the relevant attack potential level and the likelihood of security
350 incidents caused by the attacks. The quality and comprehensiveness of sectoral CTI information
351 have a considerable influence on the risk and cybersecurity assessment results. EN 18037 , Annex
352 B introduces the fundamentals of CTI and its use for the EN 18037-based assessment.

353 CTI information should be documented in the following steps:

- 354 a) Collection and review of the sectoral history of security incidents based on information from
355 the stakeholders, governmental or public sources;
- 356 b) Identification of attacker types and their objectives concerning the EUDI Wallet ecosystem;
- 357 c) Classification of the identified attacker types in accordance with the attacker type
358 classification given in EN 18037 , Annex B.2;
- 359 d) Identification of the attacker type's motives to conduct attacks that could potentially impact
360 primary assets;
- 361 e) Identification of the relevant attacker type's attack potential, particularly opportunity and
362 means, in accordance with the attack potential classification given in EN 18037 , 7.3;

363 There are trustworthy sources of CTI in the field of digital identity. See [0](#) or relevant governmental
364 sources. In case no such sources are available, or the existing ones do not contain appropriate
365 information, cybersecurity experts, and their personal judgment can be implemented.

366 **6.1.7 Choosing the risk approach**

367 [0](#), Annex I recognizes two types of risks:

- 368 — High-level risks (Rx), which are related to the use of wallets by users and relying parties, and
369 they are associated to direct threats targeting the assets of wallets
- 370 — System-related risk (SRx), which would typically result from a combination of threats
- 371 — applying to the entire wallet system.

372 EXAMPLE R4. Identify theft, defined as the unauthorised acquisition of the wallet unit or loss of
373 authentication factors enabling to impersonate a person.

374 SR2. Reputation damage, defined as the harm caused to an organisation's or governmental body's
375 reputation. Reputational damage can lead to further risks, such as loss of trust, stemming from the user's
376 reasonable doubts, and loss of ecosystem, when the full ecosystem collapses.

377 To perform ISO/IEC 27005-conformant risk assessment, two types of risks can be recognized:

- 378 — Strategic risks, which relates to business objectives and business requirements,
- 379 — Operational risks, which focus on technical behavior of the ICT system.

380 System-related risks can be considered as strategic risks, while high-level risks relate rather to
381 operational risks.

382 Considering systematic risk identification, for both ISO/IEC 27005 – based types of risks the
383 current catalogue of risks contained in [0](#) can be extended according to actual needs of EUDI Wallet
384 ecosystem stakeholders.

385 For both types of risks the approach based on the risk scenario concept is proposed. See EN
386 18037, 6.3.5 for details.

387 **6.1.8 Defining risk assessment criteria**

388 **6.1.8.1 Introducing risk scenarios**

389 According to EN 18037 , 6.3.5, risk scenario is a method used to simplify the risk assessment by
390 limiting the number of possible risk variants and matching business objectives with risks.

391 Further, risk scenarios should encompass the following:

- 392 — Business perspective, i.e., targeted business process, involved stakeholders and their
393 objectives and requirements concerning the targeted business process;
- 394 — Architecture perspective, i.e. the primary asset (information or functional) in relation to the
395 targeted business process and supporting assets identified in the ICT system;
- 396 — Attacker perspective, i.e., attacker types which can be motivated (to get access to primary
397 assets) and capable (in terms of skills and resources) to conduct attacks with required attack
398 potential on the supporting assets that protect the primary asset.

399 The same risk scenarios defined for primary assets should be applied to relevant supporting
400 assets to obtain more accurate risk assessment results.

6.1.8.2 Assessment of consequences in risk scenarios

NOTE Since stakeholders, depending on their objectives, could have different perceptions of the consequences and likelihood in their risk assessments and select different types and values of consequences and likelihood, defining a common perception among the EUDI Wallet ecosystem stakeholders is necessary. The scales and values for risk estimation should be introduced.

To establish an appropriate scale for measuring consequences, the stakeholders of the EUDI Wallet ecosystem should consider several areas of consequences including:

- business operations and functionality;
- users;
- the type of data processed;
- reputation and trust;
- compliance with legal, regulatory, and contractual requirements;
- health and life.

An example of qualitative scale and its level values for consequences are presented in Annex <tba>

6.1.8.3 Assessment of likelihood in risk scenarios

Information on likelihood criteria can be obtained from different sources:

- The experience of the stakeholders of the EUDI Wallet ecosystem;
- The analysis of the potential attackers, their motivations, skills and resources. Such an information should be provided by CTI as described in <tba> and is referenced by the risk scenario, possibly by developing relevant attack scenarios and assigning relevant attack potential levels to these scenarios;
- If the risk scenario is not specific to the ecosystem, then the likelihood can be estimated based on information of similar events or attacks in other ICT systems, those with a similar characteristics.

In case CTI information is not sufficient or not available, the expert group should be established and propose an appropriate scale and its level values for likelihood estimation.

More details on likelihood estimation can be found in EN 18037 6.3.7.

An example of qualitative scale and its level values for likelihood is presented in Annex <tba>

6.1.8.4 Risk level estimation

A risk level value is usually a combination of values of consequences and likelihood for each risk scenario.

To get the risk model as simple as possible EN 18037 , 7.1. proposes the concept of meta-risk class, resulted for applying qualitative scales for both risk factors, i.e., consequences and likelihood. An appropriate value of meta-risk class is assigned to each risk scenario.

436 An example of qualitative scale and its level values for risk is presented in Annex <tba>.

437 **6.1.9 Defining risk acceptance criteria**

438 NOTE in some methodologies, risk acceptance is a synonym to risk tolerance.

439 In contrary to the risk assessment criteria which can be unified across the EUDI Wallet ecosystem,
440 risk acceptance criteria can vary among the stakeholders. It is due to the fact that various
441 organizations have different risk appetite. It means, one organization accepts the risk (i.e., leaves
442 it intact) while another organization decides to mitigate (i.e. applies controls to) the same risk.

443 Nevertheless, while defining risk acceptance criteria in the EUDI Wallet ecosystem, the
444 stakeholder should consider the following:

- 445 — risks that can result in non-compliance with regulations cannot be retained;
- 446 — risk acceptance criteria should be defined based upon the risk appetite that indicates amount
447 and type of risk that the stakeholder is willing to pursue or retain;
- 448 — risk acceptance criteria can be based on likelihood and consequence alone (i.e., values
449 resulted from implementation of controls), or can be extended to also consider the
450 cost/benefit balance between prospective losses and the cost of controls;
- 451 — risk acceptance criteria can include requirements for future additional treatment (e.g. a risk
452 can be retained on a short-term basis even when the level of risk exceeds the risk acceptance
453 criteria if there are approval and commitment to take action to implement a chosen set of
454 controls to reach an acceptable level within a defined period).

455 **6.2 Risk identification**

456 **6.2.1 Identification of primary and supporting assets**

457 For the EUDI Wallet ecosystem, the list critical assets contains main cryptographic material (i.e.
458 cryptographic keys that require protection of confidentiality and integrity), and these critical
459 assets should be considered as primary assets. These assets are presented in Table 1. The list is
460 not exhaustive, and stakeholders can even prepare their own lists.

Table 1

Asset	Type	Storage	Handler	Purpose	Linked to	Owner	Description
Eco-system access master key	key; asymmetric	secure back-end of the Authority	secure front-end of the Authority	authentication	all authorized ecosystem stakeholders	Access Certificate Authority	Serves as the trust anchor for initiating any communication within the ecosystem. The public key along with additional metadata is notified by the Commission and published at the Trusted List.
Eco-system Registration master key	key; asymmetric	secure back-end of the operator	secure front-end of the operator	authentication		Provider of Registration Certificates	Serves as the trust anchor for authentication of any request from a Relying Party to the User regarding its (Q)EAA. The public key along with additional metadata is notified by the Commission and published at the Trusted List.
PID Master Key	key; asymmetric	WSCD	WSCA	encryption	PID Master Token	WSCD operator	Intercepted during first personalisation/ onboarding and before the creation of all other keys. Exactly one PID Master Key per wallet unit. Ownership is a prerequisite for issuing new PID credentials
PID Master Signing Key	key; asymmetric	PID HSM		signing and verifying PID Master Tokens		Provider	Represents any provider (wallet, PID) Use of the private and public key exclusively by the PID provider Use only after identification of the user (with online ID function)
PID Master Encryption Key	key	PID HSM		de-/encrypting PID Master Tokens		Provider	Represents any provider (wallet, PID) Use for decryption exclusively in the process of PID credential issuance Use for encryption exclusively in PID Master Token (re)-issuance

PID Credential Signing Key	key; asymmetric	PID HSM		signing PID credentials		Provider	Represents any provider (wallet, PID) Use of the key only after prior authentication with PID Master Key can only be used to sign PID credentials for the holder of the PID Master Token Public key of the root certificate must be published securely (Trusted List)
PID Master Token	mixed data	Wallet user			PID Master Encryption Key	PID Provider	X.509 certificate representing the identity of the PID provider
Device Attestation	mixed data	WSCA	WSCA	attestation		Wallet Provider	Device Attestation (DA) certifies the user's device and its compliance with the requirements for EUDI wallets. The DA may only be issued for devices that the wallet provider has explicitly approved for use with the EUDI wallet. The DA shall have a limited period of validity.
Wallet Unit Attestation/ PID-Provider	mixed data		WSCA	attestation	Wallet Unit Attestation Key	Wallet Provider	The Wallet Unit Attestation/ PID-Provider (WUA-PP) may only be issued for WSCA and WSCD that the wallet provider has explicitly approved for use with the EUDI wallet. The WUA-PP shall be signed with the wallet provider's Wallet Unit Attestation Key. The WUA-PP shall be encrypted with the PID provider's public key.

Wallet Unit Attestation/ Issuer	mixed data		WSCA	attestation			The Wallet Unit Attestation/ Issuer (WUA-I) may only be issued for WSCA and WSCD that the wallet provider has explicitly approved for use with the EUDI wallet. The WUA-PP shall contain information about where its validity status can be retrieved. The WUA-I shall be signed with the wallet provider's Wallet Unit Attestation Key. The WUA-I MAY be encrypted with the public Wallet Instance Key of the wallet instance.
Wallet Unit Attestation Key/ PID-Provider	key; asymmetric	WSCD	WSCA	attestation		Wallet Provider	encrypts attestations WUA-PP and WUA-I
PID	mixed data	Wallet user		not relevant		person	Data representing the data of a natural or legal person in accordance with CIR 2024/2977, Art 3, i.e. a provider or wallet user
PID Credential Key	key; asymmetric	WSCD	WSCA	encryption	PID Credentials	WSCD operator	During PID issuance at the user's request Key Association Attestation with PID Master Key required. For identification vis-à-vis relying parties.
Strong Attestation Key	key; asymmetric	WSCD	WSCA	encryption	(Q)EAA-Credentials	WSCD operator	During (Q)EAA issuance at the user's request requires Key Association Attestation with PID Credential Key, which was used for identification vis-à-vis the Trust Service Provider. For presenting (Q)EAA with strong user binding.

462 Additionally, if the stakeholders decide to extend their list of primary asset to functional modules
463 or components they should use a systematic approach to the decomposition of high-level
464 requirements to respective components or functional mod Activation process steps > During the
465 activation process, at least the following steps happen: 1. The Wallet Provider requests data about
466 the User's device from the Wallet Instance. 2. The Wallet Provider requests the User to set up at
467 least one User authentication mechanism. 3. The Wallet Provider issues one or more Wallet Unit
468 Attestations to the Wallet Unit. 4. The Wallet Provider sets up a User account for the User. ules.
469 See <CEN TS xxxx on decomposition> for details.

470 **EXAMPLE** A functional module of user onboarding as a primary asset for the EUDI Wallet provider.

471 **Description:**

472 This module is to assist the user in activating a first wallet instance plus corresponding WSCA/ WSCD for
473 its wallet solution at a wallet provider. This module should also allow to create additional wallet instances
474 at the same wallet provider linking to the same WSCA/WSCD. This module should also allow the user to
475 deactivate wallet instances or even deactivate the user's complete wallet unit at a wallet provider.

476 **Wallet Initiation and Holder Registration:**

477 **Objective:** Enable secure wallet unit activation by establishing WSCA/WSCD cryptographic infrastructure,
478 verifying device security posture, and registering wallet users with Wallet Providers meeting LoA High
479 certification requirements.

480 **Uses:**

- 481 — Capture modules
- 482 — Verification modules
- 483 — Wallet attestation & authentication modules
- 484 — Wallet Activation Portal
- 485 — Wallet lifecycle management services
- 486 — WSCA/WSCD

487 **Is used by:**

- 488 — Wallet UI
- 489 — Wallet core module

490 **Wallet Unit activation requirements:**

491 A Wallet Provider shall activate a new Wallet Unit before a User can use it to have issued an PID or
492 attestation. A Wallet Provider shall only activate a new Wallet Unit if it has verified that: The Wallet Unit
493 includes a WSCA/WSCD that is certified to be compliant with applicable requirements. The private key
494 corresponding to the public key in the WUA is protected by the respective WSCA/WSCD under control of
495 the User.

496 **A Wallet unit authenticity and validity:**

497 Wallet providers shall ensure that each wallet unit contains wallet unit attestations. Wallet providers shall
498 ensure that the wallet unit attestations referred to in paragraph 1 contain public keys and that the
499 corresponding private keys are protected by a wallet secure cryptographic device. Wallet providers shall:

- 500 (a) inform wallet users of their rights and obligations in relation to their wallet unit;
- 501 (b) provide mechanisms, independent of wallet units, for the secure identification and authentication of
- 502 wallet.

503 **Activation process steps:**

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

- 505 1. The Wallet Provider requests data about the User's device from the Wallet Instance.
- 506 2. The Wallet Provider requests the User to set up at least one User authentication mechanism.
- 507 3. The Wallet Provider issues one or more Wallet Unit Attestations to the Wallet Unit.
- 508 4. The Wallet Provider sets up a User account for the User.
- 509 <Editor's note: Experts are kindly asked to complement the example or provide additional
- 510 examples of primary assets>

511 **6.2.2 Defining risk scenarios for primary assets**

512 The EUDI Wallet stakeholders should define respective risk scenarios for any relevant primary

513 asset. The risk scenario definition include:

- 514 a) Short description of the risk scenario, including its ID (for documentation purpose)
- 515 b) Type of risk (strategic or operational)
- 516 c) The stakeholder (process owner)
- 517 d) Other stakeholders involved
- 518 e) Business process / business objectives impacted (see 6.1.3 and Annex A for reference);
- 519 f) Primary asset(s) involved
- 520 g) Supporting assets attacked
- 521 h) CTI-related information (at least, information on related threats and motivation of the
- 522 attacker, including related threats)
- 523 i) Estimation of attack potential

524 NOTE 1 Refer to EN 18037 , Annex B.5.5 for estimation of attack potential.

525 <Editor's note: The experts are kindly asked to review the examples and improve them, if

526 necessary or provide more illustrative cases. >

527 NOTE 2 Threat identifiers (TT - threat type) and TR (Threat to the wallet)) used in examples are from [0](#),

528 Annex I.

529 **EXAMPLE 1**

- 530 — Scenario SR-01: Massive attack on the whole EUDI Wallet ecosystem by breaking the registration root
- 531 certificate infrastructure and manipulate the master key.

- 532 — Type of risk: strategic
- 533 — Process owner: Provider of registration certificates
- 534 — Other stakeholders involved: all stakeholders of the EUDI Wallet ecosystem
- 535 — Business process: Providing registration service to the stakeholders of the EUDI Wallet (see 6.1.2)/
536 Business objectives: Protection of reputation
- 537 — Primary asset impacted: Ecosystem Registration master key
- 538 — Supporting assets attacked: Physical infrastructure of data centre, HSMs
- 539 — CTI-related information: such attack requires coordination of several attacks of different nature, e.g.,
540 breaking into the data centre, taking administrative control on the HSM configuration, getting access
541 to the master key and poison the software that is responsible for the key management service;
- 542 — Related threat(s): malware (TT.5 Malicious actions, 5.7)
- 543 — Attack potential: beyond high (state-sponsored attack).
- 544 **EXAMPLE 2**
- 545 — Scenario SP-01: Successful remote onboarding using false identity
- 546 — Type of risk: operational
- 547 — Process owner: Wallet provider
- 548 — Other stakeholders involved: User
- 549 — Business process: Providing registration service to the stakeholders of the Users (see 6.1.2)/ Business
550 objectives: Protection of personal data
- 551 — Primary asset impacted: Onboarding module
- 552 — Supporting assets attacked: a cryptographic protocol implemented on the User interface
- 553 — CTI-related information: several attacks on remote onboarding service are described in [ENISA];
554 attacks on registration services based on audio/video recognition are recently quite popular in relation
555 to presenting false confirmation on the applicant age
- 556 — Related threat(s): An attacker can propose an application that mimics a specific legitimate wallet to
557 users (TR 56); An attacker can circumvent the verification by the PID provider that the wallet is
558 controlled by the user and have a PID issued into a compromised wallet under the attacker's control
559 (TR 12)
- 560 — Attack potential: moderate (presentation attacks are well known method to deceive biometric
561 recognition see [4](#)).

562 **6.3 Risk assessment**

563 **6.3.1 Assessment of consequences in risk scenario**

564 From the identification of the risk scenarios, it should be possible for the stakeholders to estimate
565 possible consequences on business objectives if the scenario will occur.

It is worth to remark that a risk scenario can concern several stakeholder's objectives, and at the same time, different stakeholders of the sector can have a different view on the related consequence.

Based on the scale introduced in Annex B, and considering the example given in the following continuation in respective examples occurs:

EXAMPLE 1 For the risk scenario included in EXAMPLE 1 in the 6.2.2 value of consequences is estimated to IC=5 (Disruption of an entire ecosystem).

EXAMPLE 2 For the risk scenario included in EXAMPLE 2 in 6.2.2 the value of consequences is estimated to IC=2 (breach of personal data protection).

6.3.2 Assessment of likelihood in risk scenario

In the next step, likelihood of the risk scenario is assessed.

According to EN 18037 , 6.3.7 information on likelihood can be obtained from different sources:

- The experience of the stakeholders;
 - The analysis of the potential attackers, their motivations, means and opportunities. Such an information should be provided by CTI as described in and is referenced by the risk scenario, possibly by developing relevant attack scenarios and assigning relevant attack potential levels to these scenarios.
 - If the risk scenario is not specific to the EUDI Wallet ecosystem then likelihood can be estimated based on information of similar attacks in other ICT systems, those with a similar supply chain.
- EN 18037 provides additional guidelines to be applied if CTI information is not available. In such circumstances, the expert group can assess likelihood considering several factors, including:
- alignment with objectives – an attacker possible motivations are subject to analyse;
 - historical context - patterns in past behaviour offer clues about an attacker's consistent motivation;
 - financial incentives - financial motivation is a common driver, and the potential for monetary reward significantly influences an attacker's intent;
 - risk vs reward analysis - this includes the likelihood of success and potential repercussions, which shape the motivation behind the attack.

Based on the scale introduced in Annex B, and considering the examples given in 6.2.2 the following continuation in respective examples occurs:

EXAMPLE 1 For the risk scenario included in EXAMPLE 1 in 6.2.2 the value of likelihood is estimated to L3 (Risk scenario is somewhat likely to occur)

EXAMPLE 2 For the risk scenario included in EXAMPLE 2 in 6.2.2 the value of likelihood is estimated to L4 (Risk scenario is highly likely to occur).

6.3.3 Estimation of meta-risk class for risk scenario

First estimation of the risk level is related to the risk scenarios defined for primary assets. The results of these two assessments of consequences and likelihood as described in 6.3.2 and 6.3.2 , respectively, are used to determine the meta-risk class (MRC) of the risk scenario (see EN 18037 7.1).

EXAMPLE 1 For the risk scenario included in EXAMPLE 1 in 6.2.2 the risk level is estimated to MRC5 (Extreme)

EXAMPLE 2 For the risk scenario included in EXAMPLE 2 in 6.2.2 the risk level is estimated to MRC3 (High).

6.3.4 Risk scenario re-assessment for supporting assets

At the start of the supporting asset assessment, it is assumed that all ICT products identified as supporting assets inherit the risk level identified in the primary asset assessment for a specific risk scenario.

As the primary asset assessment's results are associated with risk scenarios, the product-specific re-assessment should be conducted using the same risk scenario.

In the first step of the re-assessment, a product-specific review of the applied attack scenario, for instance by an estimation if the product will be in the preferred attack path of the relevant attacker type, should be conducted. If this should not be the case, the likelihood of an attack against the ICT product could be lower than initially expected.

In the second step of the re-assessment, the intended use, the commonly used security features of the ICT products and the history of product-specific attacks should be considered.

As result of the re-assessment, the product-specific risk level might need to be adapted.

All information, assumptions and decisions that alter the security requirements inherited from the primary asset assessment should be documented.

EXAMPLE Considering an exemplary risk scenario presented in 6.2.2, and the use of HSM for protecting all relevant private keys of the Provider of registration certificates, the result of risk level estimation is lowered from MRC5 to MRC4.

6.3.5 Creation of risk register

Based on provisions of [0](#), a risk register shall be created and maintained to collect all relevant risk assessment results. The risk-based cybersecurity requirements shall be included in the certification scheme. Therefore, due consideration of risks and threats included in this risk register should be part of the requirements of national certification schemes.

The risk-based approach shall be a part of evaluation activities i.e., the audit of the implementation of the wallet solution and the electronic identification scheme under which they are provided, based on the risk register, set out in Annex I and complemented where necessary by implementation-specific risks shall be performed by a conformity assessment body (see [0](#) , art. 13).

The risk assessment results should be a basis for selecting cybersecurity controls for each specific architecture supported by the scheme (see 6.4). However, as the whole EUDI wallet ecosystem is functioning in strong relationships among stakeholders, the risk register concept should be the

ecosystem wide. Thus, all risks related to the EUDI Wallet ecosystem should be included in the risk register.

The risk register should consist of at least the following elements:

<Editor's note: Based on national implementations, experts are asked to review the list of the risk register elements and update it, if necessary>

- Risk scenario with short description;
- Primary assets the risk scenario is related to;
- CTI information, if available;
- Threats related to the risk scenario;
- Estimated attack potential;
- Values of likelihood, consequences and risk in an agreed scale;
- Description of supporting assets if they are used in re-assessment of the risk scenario.

Exemplary templates of risk register are presented in Annex C.

6.4 Cybersecurity and assurance requirements - selecting cybersecurity controls

According to [Q](#), art 8, the EUDI Wallet providers shall prepare the documentation of risk coverage in their implementations. It includes the coverage provided by the controls of the cybersecurity risks and threats identified in the risk register, complemented by controls of risks and threats specific to the implementation, at the appropriate assurance level.

Following EN 18037, a common security levels (CSL) concept is introduced where security levels are commensurate with the levels of risk and attack potential.

To meet the requirements, the EUDI Wallet providers should consider their approach to the assurance concept which is included in [Q](#) (see assurance). Usually, selecting controls relates to the attack potential expressed by CTI and evaluation standards such as ISO/IEC 18045 (see assurance). For that reason, a common assurance reference (CAR) that contains attack potential levels (APL) should be introduced along with CSL.

As a starting point, the attack potential equivalence between the attack potential concept defined in EN-ISO/IEC 18045 and the attack potential defined in CTI can be demonstrated. Broad discussion of equivalency is presented in EN 18037, Annex B. In particular, the equivalency analysis results are presented in Table B.16.

However, according to [Q](#), assurance levels characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. Consequently, assurance levels use the attack potential concept only in relation to authentication mechanisms. [Q](#) introduces the authentication mechanism on a specified assurance level if it implements security controls for the verification of the electronic identification means, so it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with defined attack potential can subvert the authentication mechanism. For assurance levels, the attack potential relationship is assigned as follows:

- 679 — low - enhanced-basic
- 680 — substantial – moderate
- 681 — high – high.

682 It is not clearly written in [0](#), but attack potential levels are like these defined in EN-ISO/IEC
 683 15403-3 with the following AVA_VAN.x components equivalency to the attack potential levels:

- 684 — AVA_VAN.1 – Basic
- 685 — AVA_VAN.2 - Basic
- 686 — AVA_VAN.3 - Enhanced-Basic
- 687 — AVA_VAN.4 - Moderate
- 688 — AVA_VAN.3 - High

689 To decide whether the attack potential is on a specified level, several factors should be considered
 690 with specific values assigned to get the overall score and then fix the score to pre-defined range
 691 of values. EN-ISO/IEC 18045 gives a general scoring system which is usually adjusted to the
 692 specific context (for example, to the technical domains established under the EUCC program (see
 693 [0](#)). No such context is defined for the EUDI Wallet ecosystem or the wallet solution itself.

694 Therefore, for risk mitigation in the context of EUDI Wallet provider, the tables defined for CTI in
 695 EN 18037, Annex B or simpler approach in EN-ISO/IEC 18045, Annex B4 are recommended. The
 696 equivalency between the two is presented in <Table 2>.

697 **Table 2**

CTI attack potential scoring factors (EN 18037, Annex B)	ISO/IEC 18045:2022 attack potential scoring factors	APL1 Unskilled	APL2 Skilled, limited resources and opportunity	APL3 Skilled, significant resources and opportunity	APL4 Highly skilled, significant resources and opportunity	APL5 Highly sophisticated, significant resources and opportunity
Expertise	Expertise	Layman	Proficient	Proficient	Expert	Multi Expert
Knowledge	Knowledge of the target	Public	Public	Restricted	Sensitive	Critical
Resources	Equipment	Standard	Standard	Specialized	Specialized	Bespoke
Opportunity	Windows of opportunity Elapsed Time	Unlimited/ Easy	Easy	Moderate	Difficult	Difficult

698 Therefore, the matrix of equivalency for assurance related to identity proofing can be developed
 699 only in the context of authentication mechanisms. All risks which are not related to this
 700 mechanism should rely on equivalency defined in EN 18037.

701 Importantly, the coherence among all stakeholders in the EUDI Wallet ecosystem can be achieved
702 though the implementation of CSL and APL.

703 During the risk assessment, any identified risk should be associated with a meta-risk class. In the
704 risk treatment phase, the dedicated group of experts should be established to specify a control
705 controls or group of controls that meet the required CSL. Exemplary CSL description can be found
706 in Clause B.6.

707 The second condition for choosing controls is that controls should withstand the assumed types
708 of attackers and their capabilities expressed by the attack potential value. The APL takes priority
709 i.e., if the risk assessment results in assigning lower MRC than the relevant attack potential level,
710 choosing controls should be based on the APL.

711 **EXAMPLE** The risk of unauthorised access is assessed to 'medium' level and the attack potential is
712 assessed to 'high' level. It means the control like "use of passwords" could not effectively counter the attack.
713 In such case, a multifactor authentication can be considered.

714 Examples of the Common Security Level applications that consider the attack potential levels can
715 be found in EN 18037 Annex C. Additionally, the catalogue of controls which reflect the CSL
716 concept can be found in CN/TS 18026.

717 During the risk treatment, the stakeholders may deviate from this default relationship in specific
718 cases. Such deviations should be justified and documented.

719 **6.5 Risk register monitoring and updating**

720 According to [0](#), the risk register should be maintained and regularly updated to keep in line with
721 the continuously evolving threat landscape.

722 As the risk register should encompass all critical risks with related threats in the whole EUDI
723 Wallet ecosystem, the scheme owner should take responsibility for the register maintenance.
724 Leading role of scheme owner among stakeholders should ensure harmonization and efficiency
725 of collecting information.

726 **6.6 Risk register communication and consultation**

727 Regular reporting on risk registers maintained by national certification schemes.

728 Coordinating role of EUDI Wallet Cooperation Group.

729 <To be added at later stage>

Annex A (informative)

Examples of business objectives and requirements

A.1 General

Business objectives and related requirements can be analysed using processes defined in the EUDI Wallet ecosystem. This Annex presents an analysis of the exemplary system process of EUDI Wallet Instance Lifecycle.

A.2 System process overview

The process encompasses the following steps:

- a) Installation of the EUDI Wallet Instance by the User
- b) Activation of the EUDI Wallet Instance by the User (via EUDI Wallet provider)
- c) PID issuing into the EUDI Wallet Instance by PID Provider
- d) Usage of EUDI Wallet Instance by the User
- e) Updating the EUDI Wallet instance by the EUDI Wallet provider
- f) Revocation of the wallet attestation by the EUDI Wallet provider
- g) De-Installation of the EUDI Wallet Instance by the User

A.3 Stakeholders involved in the process

Responsible stakeholders: EUDI Wallet Provider, PID provider

Depending stakeholders: User, stakeholders which provide their services based on proven information on identity of the User (e.g., Relaying Parties, (Q)EAA providers)

Risk owners: Users and stakeholders that could be impacted by ICT security incidents.

A.4 Business objectives and requirements

Table A.1 contains business objectives, denoted as BO-0x and business requirements, denoted as BR-0x-0y that relate to relevant business objectives. Some of business objectives require risk and cybersecurity assessment, while some - not.

Table A.1— Business objectives and related business requirements

Stakeholder objectives, related business requirements	
BO-01	Appropriate protection of identity information
Stakeholders directly involved: User, EUDI Wallet provider, PID Provider	

Stakeholder objectives, related business requirements	
Description of the objective: Resistance against the relevant attacker types is required due to system or legal rules	
Business requirements for BO-01 (risk and cybersecurity assessment is required)	
BO-01/BR-01	Protection of the PID
	Additional stakeholders involved: Relying Party
BO-01/BR-02	Protection of further attribute attestations
	Additional stakeholders involved: Relying Party, (Q)EAA provider
BO-01/BR-03	Protection of user-controlled data management functions
	Stakeholders involved: User
	Description: Prevention of unauthorized data management (consent, attribute release, de-activation, etc.)
BO-02	User / market acceptance
	Stakeholders directly involved: User, EUDI Wallet provider, Relying Party
	Description of the objective: Acceptance of the EUDI Wallet solution by users and relying parties
Business requirements for BO-02 (risk and cybersecurity assessment is beyond the scope)	
BO-02/BR-01	User-friendly interface
	Stakeholders involved: User, EUDI Wallet provider
	Description: Useability at same or better level than big tech wallet implementations
BO-02/BR-02	User-friendly wallet installation and life-cycle management
	Stakeholders involved: User, EUDI Wallet provider
	Description: Useability at same or better level than big tech wallet implementations
BO-03	Viable business case, user value
	Stakeholders directly involved: User, EUDI Wallet provider, Relying Party
	Description of the objective: Maximization of the addressable market / minimization of cost
Business requirements for BO-03 (risk and cybersecurity assessment is required)	
BO-03/BR-01	Support for RP from a broad range of market sectors (Broad offer of services from different market sectors)
	Stakeholders involved: EUDI Wallet provider, Relying Party

Stakeholder objectives, related business requirements	
	Description: it requires business and ICT system flexibility to adapt to security and assurance needs of supported providers and Relying Parties
BO-03/BR-02	Minimize necessity for platform-specific certifications of the Wallet Instance by using existing secure open platforms
	Stakeholder involved: EUDI Wallet provider
BO-03/BR-03	Minimize necessity and effort for re-certification (example: changes of the business logic should not lead to a need for re-certification of the EUDI Wallet Instance)
	Stakeholder involved: EUDI Wallet provider

Annex B (informative)

Examples of normalized scales in risk assessment

B.1 General

This annex is adopted from EN 18037 Annex A to reflect specific nature of the EUDI Wallet ecosystem.

All scales and tables presented in the Annex are examples used for illustrative purposes.

B.2 Qualitative scale for assessment of consequences

NOTE Terms “consequence” and “impact” are used interchangeably.

Table B.1— Impact Classes (IC) per risk area

Risk Area	IC1	IC2	IC3	IC4	IC5
1. Impact on Business operations and functionality	Limited impact on single stakeholder	Significant impact on single stakeholder	Limited impact on multiple stakeholders in a EUDI Wallet ecosystem or Significant impact on few stakeholders in a EUDI Wallet ecosystem	Significant impact on multiple stakeholders in a EUDI Wallet ecosystem	Disruption of an entire ecosystem and/or significant impact on the business, economy and society as a whole
2. Impact on direct and in-direct Users (e.g., failure to meet expected availability of services)	Minor impact on daily activities of direct and in-direct Users		Major impact on daily activities of direct and in-direct Users		Severe impact on daily activities of direct and in-direct Users
3. Impact according to the type of data processed	EUDI Wallet-related Intellectual Property	Personal data	Special categories of personal data	Data essential for critical infra-structures	Data affecting national security
4. Impact on reputation and trust	Minor damage to reputation of a few stakeholders	Minor damage to reputation of many stakeholders/	Major damage to reputation of many stakeholders/	Major damage to reputation of the EUDI Wallet ecosystem	Beyond the EUDI Wallet ecosystem

Risk Area	IC1	IC2	IC3	IC4	IC5
		or EUDI Wallet ecosystem	or EUDI Wallet ecosystem		

B.3 Qualitative scale for likelihood assessment

A scale for likelihood assessment with five levels is presented in Table B.2

Table B.2— Likelihood assessment

L1	L2	L3	L4	L5
Risk scenario is highly unlikely to occur	Risk scenario is unlikely to occur	Risk scenario is somewhat likely to occur	Risk scenario is highly likely to occur	Risk scenario is almost certain to occur

B.4 Attack potential assessment

The approach used in CTI is looking from the attacker's perspective to support the risk assessment by introducing the attacker's motivation to target certain information or other primary assets. This concept directly influences the likelihood assessment.

This annex applies the scale referenced in ISO/IEC18045 which express resistance of the supporting assets (called the target of evaluation) against a certain attack potential is achieved.

This concept is further qualified using 5-level scale and is presented in Table B.3.

Table B.3— Attack potential level (APL) description

Attack potential level (APL)	Associated baseline contents for the AVA_VAN assurance components according to ISO/IEC 15408-3	Related attack potential according to ISO/IEC 18045
1	AVA_VAN.1 Vulnerability survey	Basic
2	AVA_VAN.2 Vulnerability analysis	Basic
3	AVA_VAN.3 Focused vulnerability analysis	Enhanced-basic
4	AVA_VAN.4 Methodical vulnerability analysis	Moderate
5	AVA_VAN.5 Advanced methodical vulnerability analysis	High

B.5 Qualitative scale for risk estimation

Qualitative approaches to risk estimation include a formula that merge information on consequences and likelihood. Qualitative levels of risk can be expressed as a function of levels of

likelihood and consequences (see Table B.1 and Table B.2 , respectively) The function resulted in 5-level meta-risk classes (MRC) is included in Table B.4.

Table B.4— Meta-risk classes

Impact Class	Likelihood levels				
	L1	L2	L3	L4	L5
IC5	MRC4	MRC5	MRC5	MRC5	MRC5
IC4	MRC3	MRC3	MRC4	MRC4	MRC5
IC3	MRC2	MRC2	MRC3	MRC3	MRC4
IC2	MRC1	MRC1	MRC2	MRC3	MRC3
IC1	MRC1	MRC1	MRC1	MRC2	MRC3

Five levels of Meta-risk class scale can be expressed in a widely recognized, color-driven classification of risk with the use of following descriptions:

— Low - MRC1

— Moderate - MRC2

— High - MRC3

— Very high - MRC4

— Extreme- MRC5

B.6 Qualitative approach to risk mitigation

The exemplary scale of Common Security Level (CSL) approach encompasses five levels. Each CSL addresses a specific meta-risk class and shows the resistance to a specified level of attack potential (APL). This concept is illustrated in Table B.5

Table B.5— Common Security Levels — Relationships to meta-risk classes and attack potential levels

Common Security Level	Description	Default relationships between CSL and MRC, APL	
		CSL mitigates risk of	CSL protects against attack potential level
CSL1	CSL 1 provides a basic level of security against unskilled attackers.	MRC1	APL1
CSL2	CSL 2 adds requirements to CSL1, providing security against skilled attackers with a limited resources and opportunity to attack a system.	MRC2	APL2 or lower

Common Security Level	Description	Default relationships between CSL and MRC, APL	
		CSL mitigates risk of	CSL protects against attack potential level
CSL3	CSL 3 extends the coverage of the security against skilled attackers with significant resources and/or significant opportunity to attack a system.	MRC3	APL3 or lower
CSL4	CSL 4 provides security against a highly skilled attacker with significant resources and opportunity.	MRC4	APL4 or lower
CSL5	CSL 5 provides the highest level of security, capable to protect against highly sophisticated attackers with significant resources at their disposal and/or opportunity for an attack.	MRC5	APL5 or lower

799
800
801
802

Annex C
(informative)

Examples of risk register template

Annex ZA
(informative)

**Relationship between this European Standard and the requirements
of aimed to be covered**

This European Standard has been prepared under a Commission's standardization request to provide one voluntary means of conforming to requirements of.

Once this standard is cited in the Official Journal of the European Union under that, compliance with the normative clauses of this standard given in confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding requirements of that, and associated EFTA regulations.

Table ZA.1— Correspondence between this European Standard and

[Essential]/ [interoperability]/[...] Requirements of [Directive]/[Regulation]/[Decision] [...]	Clause(s)/sub-clause(s) of this EN	Remarks/Notes

WARNING — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING — Other Union legislation may be applicable to the falling within the scope of this standard.

822

Bibliography

- 823 [1] Architecture and Reference Framework (ARF), [https://eudi.dev/2.4.0/architecture-and-](https://eudi.dev/2.4.0/architecture-and-reference-framework-main/)
824 [reference-framework-main/](https://eudi.dev/2.4.0/architecture-and-reference-framework-main/)
- 825 [2] COMMISSION IMPLEMENTING REGULATION (EU) 2024/2981 of 28 November 2024
826 laying down rules for the application of Regulation (EU) No 910/2014 of the European
827 Parliament and the Council as regards the certification of European Digital Identity
828 Wallets
- 829 [3] REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
830 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the
831 European Digital Identity Framework
- 832 [4] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on
833 setting out minimum technical specifications and procedures for assurance levels for
834 electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014
835 of the European Parliament and of the Council on electronic identification and trust
836 services for electronic transactions in the internal market
- 837 [5] ENISA Report - REMOTE IDENTITY PROOFING: ATTACKS & COUNTERMEASURES,
838 January 2022 (updated June 2022)
- 839 [6] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on
840 setting out minimum technical specifications and procedures for assurance levels for
841 electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014
842 of the European Parliament and of the Council on electronic identification and trust
843 services for electronic transactions in the internal market (Text with EEA relevance)
- 844 [7] EN ISO/IEC 18045:2023, *Information security, cybersecurity and privacy protection -*
845 *Evaluation criteria for IT security - Methodology for IT security evaluation (ISO/IEC*
846 *18045:2022)*
- 847 [8] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE
848 COUNCIL of 23 July 2014 on electronic identification and trust services for electronic
849 transactions in the internal market and repealing Directive 1999/93/EC
- 850 [9] EN ISO/IEC 15408-3:2023, *Information security, cybersecurity and privacy protection -*
851 *Evaluation criteria for IT security - Part 3: Security assurance components (ISO/IEC 15408-*
852 *3:2022)*
- 853 [10] COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying
854 down rules for the application of Regulation (EU) 2019/881 of the European Parliament
855 and of the Council as regards the adoption of the European Common Criteria-based
856 cybersecurity certification scheme (EUCC) (Text with EEA relevance)
- 857 [11] CEN/TS 18026:2024, *Three-level approach for a set of cybersecurity requirements for*
858 *cloud services*