TLP - CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUDIW Cybersecurity Certification

Draft candidate scheme

MARCH 2026

Document History

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

Date	Version	Modification
26/03/2025	0.1	Creation
07/05/2025	0.2	Addition of Annexes Corrections after proofreading
20/02/2026	0.3.608	For internal review
27/02/2026	0.3.609	For EUDIW AHWG review
31/03/2026	0.4.614	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

The present document is a draft candidate scheme towards establishing a European Cybersecurity Certification Scheme for European Digital Identity (EUDI) Wallets. It follows the guidance of the European Cybersecurity Certification Framework, as defined in Regulation (EU) 2019/881 (Cybersecurity Act).

Although this is presented as a single scheme, it is important to note that the certification of an EUDI Wallet is not going to be monolithic. The most critical hardware and software components will be certified using the EUCC scheme, other software components will be certified using other schemes, and conformance testing may be performed by yet another laboratory. Even on IT systems, the wallet provider's Information Security Management System (ISMS) may have been already evaluated because they already are a Trusted Service Provider, subject to the NIS2 regulation.

For this reason, the certification scheme must be considered as a certification system in the sense of ISO 17067, *i.e.*, a set of rules and procedures for the management of similar or related conformity assessment schemes. This may for instance occur at the national level, where certification will be tailored to a given architecture, defining precisely the schemes to be used for each component.

At the European level, the scheme is necessarily more abstract, so it is not as obvious to see the system behind, but it is obviously present in three different ways.

First, the scheme may be used to certify a complete solution, combining wallet solution and electronic identification means, but it also offers the possibility to certify separately a wallet solution or the services of a PID provider supporting the wallet.

Second, the scheme explicitly encourages composition with other certification schemes, including other European schemes, but also national and private schemes, at least those based on accreditation.

Finally, the scheme also encourages the reuse of evidence from other conformity assessment schemes, and even more generally the reuse of any assurance information, such as an attestation delivered by public auditors, through the reuse of the dependency analysis introduced for the certification of cloud services.

The scheme proposed below has been thought as an orchestrator, providing general guidelines for the evaluation and certification of the cybersecurity of services providing an EUDI Wallet, but leaving many degrees of freedom to the certification bodies and to the candidates for certification to organise their conformity assessment activities in the way that suits them best. It concludes with a positioning of the European scheme in a national certification system for EUDI Wallets, exploring possibilities that give it a more or less central role.

Foreword

CONSTRAINTS

The EUDI Wallet ecosystem remains immature. In early 2026, no EUDI Wallet has been deployed or certified, and the specification remains work in progress. Furthermore, regarding security, no standard or technical specification is available or foreseen to be available by the end of the year. This draft candidate scheme therefore includes technical specifications in annexes, established by ENISA, to be used in the first version of the scheme and that may be contributed to European Standardisation Organisations (ESOs) for their subsequent maintenance.

Most wallet implementations are designed to run on mobile personal devices, which until 2026 have rarely undergone any formal certification. Since these devices are provided by users and therefore not included in the object of certification, it is very difficult to rely on their security properties. One of the solutions is to include specific security measures in the mobile applications that run on these devices, but this approach is limited for some aspects, such as the authentication of users. Th draft candidate scheme therefore introduces a fraud management process to complement vulnerability management with fraud management, in an attempt to identify potential issues as early as possible.

MENTIONS OF REGULATIONS

The scheme makes few direct mentions to Regulation (EU) No 910/2014, commonly referred as eIDAS, because it is based on the assumption its certificates will be referenced in a National scheme for EUDI Wallets, so the obligations from the eIDAS, in particular from Article 5c, apply to that National scheme rather than to the present scheme. However, there may be an opportunity to use this EU scheme to satisfy the requirements of Article 5c, which is explored in Annex XIV.

Regulation (EU) 2024/2847, commonly referred to as the Cyber Resilience Act (CRA) does not apply directly to EUDI Wallets as they are certified in the context of the present scheme, since they are certified as ICT services, not ICT products. However, in particular when the wallet instance is a mobile application, the regulation would apply to the wallet instance when it is placed on the market by a commercial entity. Because the application of CRA will differ depending on the EUDI Wallet architecture and other parameters, the choice in the scheme has been to use CRA requirements where relevant, but no a systematic way, since the EUDIW certificates (applying on an ICT service, not on an ICT product) will not be suitable for presumption of conformity.

Directive 2022/2555 for Network and Information Systems (NIS2) does not apply directly to EUDI Wallets, although some Member States have extended the scope of application in their national transposition to include EUDI Wallet providers, and there is an ongoing proposal to include them in the scope of the next revision of the regulation. The cybersecurity constraints mostly apply, though, since the standard that we proposed to use as a basis for the evaluation of EUDI Wallets (ETSI EN 319 401) includes in its latest v2.3.1 requirements designed to meet the requirements of Commission Implementing Regulation (CIR) (EU) 2024/2690.

REFERENCES

The current scheme makes references to the following regulations:

- 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)
  - Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 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)
- 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
  - Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
  - Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets
  - Commission Implementing Regulation (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
  - Commission Implementing Regulation (EU) 2025/2162 of 27 October 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the accreditation of conformity assessment bodies performing the assessment of qualified trust service providers and the qualified trust services they provide, the conformity assessment report and the conformity assessment scheme
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
  - Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers
- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

It also makes references to the following standards and technical specifications:

- ISO/IEC 17065:2012, “Conformity assessment — Requirements for bodies certifying products, processes and services”
- ISO/IEC DIS 17067, “Conformity assessment — Fundamentals of and guidelines for conformity assessment schemes”
- ISO/IEC 17021-1:2015, “Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements”
- ISO/IEC 17025:2017, “Conformity assessment — General requirements for the competence of testing and calibration laboratories”
- ISO/IEC 17029:2019, “Conformity assessment — General principles and requirements for validation and verification bodies”
- ISO/IEC 17000:2020, “Conformity assessment — Vocabulary and general principles”
- ETSI EN 319 401 v3.2.1: “Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers”, January 2026
- EN ETSI 319 403-1 v2.3.1: “Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers”
- ISO/IEC 15408:2022, Parts 1 to 5, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security (Common Criteria)
- ISO/IEC 18045:2022, “Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation”
- CEN TS 18072:2022, “Requirements for Conformity Assessment Bodies certifying Cloud Services”, currently under revision to extend to all ICT services.
- EN 17640:2022, “Fixed-time cybersecurity evaluation methodology for ICT products” (FiTCEM)

0. Scheme Principles

0.1 Part of a larger conformity assessment system

Article 5c(1) of eIDAS requires the certification of “European Digital Identity Wallets and the electronic identification scheme under which they are provided” with respect to many different requirements defined in Article 5a. Some of these requirements are related to cybersecurity, but not all of them.

Because the EUDI Wallet ecosystem is harmonised and needs to provide a high-level of interoperability between the different implementations, the Commission has published a number of implementing acts that list technical specifications that define technical requirements applicable to the EUDI Wallet ecosystem, such as CIR (EU) 2024/2977, CIR (EU) 2024/2979 and CIR (EU) 2024/2982. These implementing acts are regularly updated to cover the evolution of the standards.

These standards are in many cases related to security, as they very often define the way in which sensitive assets are encoded and processed, including their protection. From a functional viewpoint, the requirements in these standards provide a good coverage of the risks and threats identified in the risk register from Annex I of CIR (EU) 2024/2981. Therefore, conformance testing to these standards, if it provides sufficient coverage, in particular of the negative use cases, will be an essential part of demonstrating that security functions are properly implemented.

The implementing acts that define functional specifications are currently under revision, but the Commission is already currently developing conformance test specifications for these standards, which should form a sound basis for the development of a functional certification scheme.

However, conformity to functional security requirements is a necessary but not sufficient condition to demonstrate that the expected level of assurance is achieved. In particular, Article 5c(2) of eIDAS mentions the possibility of using a European cybersecurity certification scheme, as defined in the CSA, which corresponds to the present scheme. However, this scheme is not expected to cover all the certification requirements of 5c(1), but only those related to cybersecurity.

The present scheme therefore comes together with a set of complementary security requirements, mostly non-functional. These requirements cover the technical elements of the scheme, like the wallet unit and the provisioning and management of wallets and PID, with a focus on implementation constraints and assurance requirements for the most sensitive security functions. The requirements also cover the security controls to be put in place by the various stakeholders of the EUDI Wallet ecosystem in their organisation and management systems. These requirements are work in progress, as they are expected to align with the revised implementing acts that are currently under negotiation.

Therefore, the present scheme is not intended to be a standalone scheme, but to be part of a larger conformity assessment system, or actually one larger conformity assessment system for each Member State. Each such conformity assessment system should contain at least one high-level, “overall” scheme, that will bear the responsibility of issuing the certificate that provides the demonstration that all requirements from Article 5c(1) are fulfilled, by leveraging the results from other schemes, such as the present one for cybersecurity aspects or a functional certification scheme as discussed above.

In addition, since each national conformity assessment system is intended to define the supported wallet architectures, each system should also refer to additional certification schemes that will be used to certify the components of the scheme, for instance the EUCC scheme, which is foreseen as being used for the certification of the most security-critical product components.

The definition of this certification system is beyond the scope of the present candidate certification scheme, but the architecture of the candidate scheme can only be understood with this certification system in mind.

0.2 Flexible certification paths

Because of the wide variety of potential architectures, and because candidates to certification are strongly encouraged to reuse the results of previous conformity assessments, the present scheme only provides limited guidance related to the implementation of security functions and controls, and only offers guiding principles. One such principles states that a wallet unit's critical assets are expected to be stored and processed in a WSCD and managed in a WSCA, and both these components are expected to resist to attackers with a high attack potential (typically through an EUCC certificate with an AVA_VAN.5 vulnerability assessment, but other paths are possible).

The overarching objective of certification is to demonstrate that the risks identified in the risk registry are mitigated, and that the eID scheme achieves the objectives of eIDAS assurance level high, as defined in CIR (EU) 2015/1502. Certification is therefore risk-based, and it is the architecture of a wallet that decide how the security functions and security controls defined in the various components of the EUDI wallet mitigate the risks from the risk registry.

Another layer of flexibility is linked to the integration of the cybersecurity scheme in the national certification system. Some Member States have limited capacities for certification, so it may be interesting for them to include more requirements in the scope of cybersecurity certification. Functional requirements are the main example. Since the CSA scheme needs to demonstrate that the security functions and controls are correctly and effectively implemented, it is possible to include the functional certification (conformance to functional standards) in it. This would allow some Member States to simplify their national conformity assessment system, while others would prefer to keep a separate functional certification scheme, whose certificates could actually be used as an input to the cybersecurity scheme.

Finally, the scheme introduces as first step of the assessment an evaluation of the service design, which together with the risk assessment, is intended to allow leave some freedom in the implementation while ensuring that the risks are all covered with an appropriate level of assurance.

0.3 Strict application of the principles

The consequence of this flexibility is that the conformity assessment body for the cybersecurity scheme bears a lot of responsibility, and in particular the responsibility to determine whether or not a set of externally provided certificates and other assurance information, together with specific conformity assessment activities, provide a sufficient demonstration that an EUDI Wallet meets its evaluation criteria.

For this reason, the present candidate scheme proposes to require the NCCA to validate this critical competence as part of an authorisation process, as a complement to the accreditation process.

The certification lifecycle includes four main stages:

- the preparation stage, during which the service provider prepares for the certification;
- the first stage of the evaluation, during which acceptability is checked and the second stage is prepared;
- the second stage of the evaluation, during which the main evaluation activities are performed, and which leads to the review, certification decision and certificate issuance; and
- the maintenance stage of the certificate, during which the certified service is monitored and regularly assessed.

Each phase is very important to guarantee the strict application of the principles of the scheme.

Preparation stage
The EUDIW service provider needs to prepare carefully, by preparing the required documentation, including a description of its service's architecture, a risk assessment, a description of its control framework, and a justification that its controls cover all the risks identified in the risk register, in particular if the service or some of its components deviate from the EUDIW criteria.

In addition, the EUDIW service provider needs to gather the assurance documentation for its components, which may imply to have some of then certified, such as its WSCA, wallet instance or ISMS.

First stage of the evaluation
This phase is mostly based on the documentation provided by the EUDIW service provider. The CAB assesses the accuracy of the documentation, the reasoning behind the justifications, by applying specific procedures such as the risk assessment evaluation and the design evaluation. They also define the list of evaluation activities required to verify all of this information.

Most importantly, the CAB determines in this phase that if the EUDIW service is provided accorded to its documentation, then it should indeed cover the risks identified in the risk assessment (including the risks from the risk register), and therefore meet the requirements of the scheme.

Second stage of the evaluation
This second stage is the main evaluation phase, during which the design and effectiveness of the controls are verified. It goes beyond a traditional audit in many ways. First, the evaluation is based on the principles of CEN TS 18072, which was previously developed for the evaluation of cloud services, and extended to all ICT services, and that is more rigorous than traditional ISMS audits.

In addition, the evaluation includes activities required by the Cybersecurity Act for assurance level 'high', related to functional testing of security functions and to vulnerability assessments ad penetration testing.

Certificate maintenance stage
Once the certification has been issued, the continuous monitoring starts, under the combined responsibility of the certificate holder, the CAB that issued the certificate, and the National Cybersecurity Certification Authority (NCCA).

The certificate maintenance schedule is also quite demanding, with an annual surveillance evaluation, which includes a verification of the effectiveness of key processes, together with a revision of the certified service's vulnerability assessment.

SECTION 1

Scheme Core

1. General requirements

1.1 Subject matter and scope

The scheme covers the cybersecurity certification of European Digital Identity (EUDI) Wallets, as required in Article 5c(2) of Regulation (EU) No 910/2014, and in accordance with the European cybersecurity certification framework set out in Regulation (EU) 2019/881 (CSA).

1. This document sets out the European cybersecurity certification scheme for European digital identity wallets (EUDIW), as intended in Article 5c(2) of Regulation (EU) No 910/2014..
2. This scheme applies to all information and communication technologies ('ICT') services, including their documentation, which are submitted for certification under the EUDIW, and it shall support the issuance of certificates for the cybersecurity of the following types of ICT services:
   (a) service for the provision and operation of a wallet solution and the electronic identification ('eID') scheme under which it is provided;
   (b) service for the provision and operation of a wallet solution;
   (c) service for the provision of person identification data (PID) for the purpose of providing an eID scheme under which a European digital identity wallet is provided;
   (d) service used to verify the validity of wallet units and relying parties.

RATIONALE

This first section defines the subject matter and lists the items that may be certified. All these items are ICT services, because they all include components that need to be provided as a service (*e.g.* the management of wallet units in a wallet solution).

Paragraph 1 establishes a link to Article 5c(2) of eIDAS, which introduces the need for a dedicated cybersecurity schemes for EUDI Wallets.

Paragraph 2 gives a clear indication that the certification is not supposed to be monolithic, as it is possible to certify subsets of the entire solution, and also by indicating that the scheme only covers the cybersecurity aspects.

Item 2(a) corresponds to the definition of the object of certification in Article 5c(1) of the eIDAS. The three other items correspond to parts of that service that may be provided by different entities:

- The service for the provision and operation of a wallet solution in item 2(b) is typically provided by a wallet provider, and includes the wallet implementation and the service that manages it.
- The service for the provision of PID in item 2(c) is typically provided by a PID provider, and it covers user on-boarding and PID activation, delivery and revocation according to the requirements of CIR (EU) 2015/1502 for assurance level high.
- The validation services in item 2(d) may be certified separately because Article 5a(8) of eIDAS assigns this responsibility to the Member State, so it may be provided by an entity that is neither the wallet provider nor the PID provider

The perimeter of the services in items 2(b) and 2(c) is flexible, with a minimum set of features, as the exact boundaries may depend on the EUDI Wallet's architecture and on the split of responsibilities between the different stakeholders.

1.2 Definitions

Some definitions are given to complement the definitions provided in Regulation (EU) 2019/881 (CSA), Regulation (EU) No 910/2014 (eIDAS)and CIR (EU) 2024/2981. A more complete terminology is provided in Annex XV.

1. For the purpose of this scheme, the following definitions shall apply.
(1)...

1.3 Assurance level

Due to the sensitivity of the assets managed by EUDI Wallets, all EUDIW certificates are issued at assurance level 'high' of the CSA.

1. Certification bodies shall issue EUDIW certificates at assurance level 'high', as defined in Article 52(7) of Regulation (EU) 2019/881.

RATIONALE
In the CSA, assurance level 'high' is "intended to minimise the risk of state-of- the-art cyberattacks carried out by actors with significant skills and resources". Since all the functions provided by the EUDI wallets are security functions, some of them of critical sensitivity, assurance level 'high' seems the most adequate.

This does not necessarily mean that every component of the certified service needs to be evaluated at the highest level of assurance available. For instance, the EUCC scheme, assurance level 'high' covers a wide range of evaluations, ranging from those based on an AVA_VAN.3 vulnerability assessment to those based on an AVA_VAN.5 vulnerability assessment.

Among the components that are products, these levels could apply. As mentioned in CIR (EU) 2024/2981, the WSCA, which manages the wallet unit's critical assets, should be evaluated at a level equivalent to AVA_VAN.5, relying on a WSCD evaluated outside of the scheme at a similar level. The wallet instance, another product component, could be evaluated as a lower level, and the EUDIW AHWG is working on a document that targets an evaluation at AVA_VAN.3 level,

Nevertheless, we already foresee some cases where lower assurance levels could be used and duly justified, either as part of the present scheme, of as part of the certification of a specific wallet solution. For instance, in cases where the WSCA runs outside of the WSCD (typically, in the remote HSM case, on a server connected to the HSM), then level AVA_VAN.3 could be considered sufficient, with strong assumptions on the protection provided by the operating environment that would need to be verified in the evaluation of another component.

About other components, like services and processes, it is less common to reason in terms of levels of assurance. Nevertheless, as described in Annex XI, the scheme requires the use of CEN TS 18072 at level 'high' for the evaluation, a methodology that was originally designed for the evaluation of cloud

services, and that provides a higher level of assurance that the audits performed in, for instance, assessments leading to ISO/IEC 27001 certification. The differences between assurance levels are not as precisely described than they are for products, so the expertise of the conformity assessment bodies will be essential to obtain good results.

1.4 Conformity self-assessment

Since conformity self-assessment is only allowed under assurance level ‘basic, which is not supported in this scheme, no conformity self-assessment is permitted.

1. A conformity self-assessment within the meaning of Article 53 of Regulation (EU) 2019/881 shall not be permitted.

2. Evaluation criteria and methods

2.1 Evaluation criteria for EUDIW ICT services

In the absence of applicable standard and technical specifications, the evaluation criteria applicable in the present scheme are defined in an Annex of the scheme.

1. An ICT service submitted for certification shall, as a minimum, be evaluated to be in conformity with
   (a) the applicable criteria defined in Annex X;
   (b) specific criteria related to the use of the components of the ICT service, based on the assumptions and user guidance provided about each component, and on the dependency analysis of the assurance information available for each component.

RATIONALE

The scheme defines criteria (called the EUDIW criteria in the present document), but additional criteria need to be considered about the proper use and integration of the components of the EUDIW ICT service. Because components are evaluated separately, then any assumption or user guidance (in the Common Criteria sense) about these components needs to be considered as requirement. In addition, any deviation from the EUDIW criteria or improper coverage of the EUDIW criteria identified in the dependency analysis may lead to additional requirements to be met by the EUDIW ICT service. The full criteria that apply for the certification of a given ICT service are called its evaluation criteria in the present document.

At the planned time for the delivery of the draft candidate scheme for ECCG opinion, no standard or technical specification is expected to be available from ESOs that defines detailed security requirements for the EUDI Wallet. Some of the functional specifications listed in the eIDAS CIRs include security considerations, but these fall short of evaluation requirements. In addition, the timeframe considered for the adoption of the scheme makes it difficult to expect technical specifications or standards to be available in time from ESOs.

The proposed solution consists in defining high-level security requirements and to include them as part of the candidate scheme. The first draft has been developed on the basis of the high-level requirements (HLRs) of the Commission's Architecture Reference Framework (ARF), and also on other standards and technical specifications, such as ETSI EN 319 401 and the OWASP guidelines for mobile and web applications. These high-level security requirements are in the process of being consolidated, and they could then be contributed to an ESO in order to be consolidated into a technical specification or standard for future versions of the scheme.

In parallel, work is continuing in ESOs and in the EUDIW AHWG, and some documents are expected to be available in time for the adoption of the scheme that will support the evaluation of essential components of the wallet solution:

- CEN TC224 WG17 is developing an EUCC Protection Profile for WSCAs.

- The EUDIW AHWG is developing a methodology and protection profile for the evaluation of mobile-based wallet instances.

ENISA will continue to coordinate with SDOs until the adoption of the scheme in order to maximise the use of standards and technical specifications issued by SDOs in the scheme.

2.2 Methods for evaluating EUDIW ICT services

The methodology for the evaluation of EUDIW ICT services is based on standard ETSI EN 319 403-1, complemented with process requirements and methods from Technical Specification CEN TS 18072, and by specific methods and requirements on methods defined in an Annex of the scheme.

1. An ICT service submitted for certification shall, as a minimum, be evaluated in accordance with the methods defined in Annex XI.
2. In the case of an ICT service undergoing a composite service evaluation, as defined in Annex IX, the CAB that carried out the evaluation of the underlying ICT service shall share the relevant information with the CAB performing the evaluation of the composite ICT service.
3. In the case of an ICT service including a component that has been certified with a European cybersecurity certification scheme, the CAB that issued the certificate for that component shall share the relevant information with the CAB performing the evaluation of the ICT service.

RATIONALE

The general idea for the evaluation is to consider the various EUDIW ICT services as specific categories of Trust Services, and therefore to base their evaluation on the principles defined in ETSI EN 319 403-1. This standard builds on EN ISO/IEC 17065, as required for the CSA.

In addition, this evaluation is based on high-level requirements, and it is expected to rely heavily on composition with other schemes. It will reuse assurance information from diverse origins, and because the evaluation is performed at assurance level ‘high’, the ETSI standard is here complemented by CEN TS 18072. This technical specification was initially developed for the evaluation of cloud services in the context of the development of the EUCS scheme, and it is currently being extended to apply to all EUDIW ICT services.

In addition, the scheme is defining requirements for a few specific methods to be used in the evaluation activities (both in the initial evaluation and in the maintenance evaluations).

The consequence is that the CAB will need at least to include inspection activities in addition to audit activities, and that they may need to add testing activities if they do not reuse the results of another certification scheme dedicated to functional testing.

Paragraph 2 is related to composition within the scheme, for instance when an overall certification (for services for the provision of wallets solutions and the eID schemes under which they are provided) is based on an existing EUDIW certificate (e.g., for services for the provision of wallet solutions). In that case, the relevant information is likely to be the reports issued with the certificate.

Paragraph 3 is mostly dedicated to EUCC[1], and in that case, the information required should be the one required to perform the dependency analysis (see Annex IX).

[1] The references to the EUCC scheme as defined in (EU) 2024/482, are motivated by the direct reference made to it in (EU) 2024/2981 in Article 4(1) and others.

3. Issuance, renewal and withdrawal of EUDIW certificates

3.1 Information necessary for certification

The applicant for certification needs to provide all information required by the certification body, and is encouraged to provide results from prior certification of relevant components of their service, for instance under EUCC, under eIDAS-related schemes, or under other conformity assessment schemes based on the accreditation of conformity assessment schemes.

1. An applicant for certification under EUDIW shall provide or otherwise make available to the certification body all information necessary for the conformity assessment activities.
2. The information referred to in paragraph 1 shall include the information listed in Annex IV.
3. Applicants for certification may provide to the certification body appropriate evaluation results from prior conformity assessments pursuant to:
   (a) the present scheme;
   (b) a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881;
   (c) qualification and certification by conformity assessment bodies accredited according to the requirements of CIR (EU) 2025/2162;
   (d) certification by conformity assessment bodies designated by Member States as described in Article 12a(1) and Article 30(1) of Regulation (EU) No 910/2014.
   (e) conformity assessment under any scheme by a CAB accredited to issue such conformity assessments by the national accreditation body of an EU Member State, according to Regulation (EU) 765/2008.
   (f) [to be completed].
4. After confirming the authenticity of the evaluation results, and after analysing the suitability, relevance and conformity to applicable requirements of the evaluation results, the certification body may reuse the evaluation results according to the results of the analysis.
5. Applicants for certification shall also provide the certification body with the link to their website containing the information to be made publicly available, as defined in Annex III.
6. All relevant documentation referred to in this Section shall be retained by the certification body and the applicant for a period of 5 years after the expiry of the certificate.

RATIONALE

The list of information to be provided is defined in an Annex, because it is quite long, but it is not intended to be exhaustive. Paragraph 1 clearly states that the applicant has to provide “all information necessary”, which of course takes precedence over the indicative list.

Regarding composition, the objective is here to allow the use of assurance information coming from a wide variety of conformity assessment schemes, but there is a requirement to analyse the suitability and relevance of the assurance information using the dependency analysis that is defined in CEN TS 18072 and has been integrated in CIR (EU) 2024/2981. The result of the analysis should be to limit the use of the assurance information, or to identify residual activities required to complement it.

Paragraph 4 (adapted from EUCC) encourages the reuse of evidence based on previous conformity assessments, which is another path for the reuse of evaluation results, without necessarily linking to a certificate.

The rationale for the 5 years in paragraph 6 is the consistency with the figure used in EUCC.

3.2 Conditions for issuance of an EUDIW certificate

In addition to a successful evaluation and subsequent review, the issuance of an EUDIW certificate is conditioned by the applicant undertaking commitments related to the provision of truthful and complete information to the certification body, and to the proper use of the certificate.

1. The certification body shall issue an EUDIW certificate where all of the following conditions are met:
   (a) the type of the ICT service, as defined in paragraph 2 of section 1.1 and all conformity assessment activities fall within the scope of the accreditation, and where applicable of the authorisation, of the certification body issuing the certificate;
   (b) the applicant for certification has signed a statement undertaking all commitments listed in paragraph 2;
   (c) the certification body has concluded the evaluation without objection in accordance with the evaluation criteria and methods referred to in Sections 2.1 and 2.2;
   (d) for an initial evaluation, if the effectiveness of the security controls has not been evaluated, there is no unresolved nonconformity to report at the end of the evaluation;
   (e) the certification body has concluded the review of the evaluation results without objection;
2. The applicant for certification shall undertake the following commitments:
   (a) to provide the certification body with all the necessary complete and correct information, and to provide additional necessary information if requested;
   (b) not to promote the ICT service as being certified under the EUDIW before the EUDIW certificate has been issued;
   (c) to promote the ICT service as being certified only with respect to the scope set out in the EUDIW certificate;
   (d) to cease immediately the promotion of the ICT service as being certified in the event of the suspension, withdrawal or expiry of the EUDIW certificate;
   (e) to ensure that the ICT service provided with reference to the EUDIW certificate is the ICT service subject to the certification;
   (f) to respect the rules of use of the mark and label established for the EUDIW certificate in accordance with Section 3.4.

RATIONALE

The conditions for issuance of an EUDIW certificate are rather usual, mostly requiring the certification body to perform all steps of the evaluation and subsequent review and certification decision before issuing a certificate, and requiring the applicant to commit to follow the rules of the scheme, and in particular to provide complete and correct information.

Point 1(d) refers to the specific situation of the initial evaluation. Because certification is mandatory to operate an EUDI Wallet, it is not possible on an initial certification to evaluate the effectiveness of the security controls, since the provider is not yet operating the an EUDIW ICT service. In that case, no nonconformity is allowed, even minor, on the existence and suitability of the controls.

Note that in the case of an EUDIW ICT service that has already been certified through a national scheme, and that has been operating for at least one year, this provision does not apply because it is possible to evaluate the effectiveness of the service's security controls.

This specific item 2(a) is really important, because it implies that the provision of wrong or incomplete information for the evaluation is not a nonconformity of the EUDIW ICT service but a non-compliance of the EUDIW ICT service provider, which leads to faster and stronger consequences.

The objective of item 1(a) is to ensure that the certification body has all the competences required to perform the conformity assessment. Although the scope of the scheme is very well defined, the competences required for the certification body may differ greatly depending on the documentation provided by the applicant, in particular on the assurance information provided. For instance, some certification bodies have the choice to include testing through ISO 17025 in their accreditation scope, or to systematically rely on an independent certification for functional conformance.

3.3 Issuance of an EUDIW certificate

Any certificate issued under EUDIW needs to be accompanied by a certification report. The required content of both the certificate and the report is defined in Annexes, and both are to be made publicly available. In addition, the certification body needs to produce a certification assessment report, containing more detailed information, to be shared only in the context with relevant national supervisory authorities (from both CSA and eIDAS Regulations).

1. An EUDIW certificate shall include at least the information set out in Annex V.
2. The scope and boundaries of the certified ICT service shall be unambiguously specified in the EUDIW certificate or the certification report.
3. The certification body shall provide the applicant with the EUDIW certificate at least in electronic form.
4. The certification body shall produce a certification report in accordance with Annex VI for each EUDIW certificate it issues. The certification report shall be based on the evaluation technical report. The certification report shall indicate the specific evaluation criteria and methods referred to in Sections 2.1 and 2.2 used for the evaluation.
5. The certification body shall produce an evaluation technical report for composite evaluation in accordance with Annex VII for each EUDIW certificate it issues, to be provided to the conformity assessment body that will perform the evaluation activities based on this EUDIW certificate.

6. The certification body shall provide the national cybersecurity certification authority and ENISA with every EUDIW certificate and certification report it issues in electronic form.

RATIONALE

The requirements related to the issuance of a certificate are also quite standard.

The certificate is likely to focus on the commercial name of the certified EUDI Wallet, but a more precise description of the object of certification needs to be provided in the certification report.

The certification report contains very basic information about the certification, without getting into the details of the evaluation. It includes a detailed description of the wallet and of its security model, but only a summary of the evaluation activities.

The evaluation technical report (ETR) for composite evaluation is intended for two distinct uses:

- If the certificate only covers a subset of the EUDI Wallet, then this report should be used by the CAB that will perform the evaluation of the overall EUDI Wallet and eID scheme.
- The report should also be used by the national certification scheme as input about the cybersecurity aspects of the certification, and also as a basis for writing their certification assessment report.

3.4 Mark and label

A mark and label are defined for pointing to the ENISA certification web site. Although it can be used for all certificates issued under EUDIW, the mark and label are intended to be used mostly for providers of wallet solutions, who may need the reference to market their EUDIW ICT service.

1. The holder of a certificate may affix a mark and label to a certified ICT service. Mark and label demonstrate that the ICT service has been certified in accordance with this scheme. Mark and label shall be affixed in accordance with this Section and with Annex XII.
2. the mark and label shall be displayed in a visible, legibly and unambiguous manner in connection with the certified ICT service, where applicable:
   (a) on the official website of the certificate holder describing the certified ICT service;
   (b) in service catalogues, datasheets or other service description material, whether in electronic or printed form;
   (c) in contractual or pre-contractual documentation relating to the certified ICT service.
3. The mark and label shall not be displayed in the wallet instance, where the EUDI Wallet Trust Mark should be the only trust indication that an EUDI wallet has been certified according to Article 5c(1) of Regulation (EU) No 910/2014.
4. The mark and label shall be set out as in Annex XII and contain:
   (a) the assurance level of the certified ICT service;
   (b) the unique identification of the certificate, consisting of:
      (1) the name of the scheme;
      (2) the reference number of the accreditation of the certification body that has issued the certificate;

(3) the year of issuance;
(4) the identification number assigned by the certification body that has issued the certificate.

4. The mark and label shall link to the ENISA Web site, directly or through a QR code, and the corresponding entry on the website shall contain at least:
(a) the information on the validity of the certificate;
(b) the necessary certification information as set out in Annexes V and VII;
(c) the information to be made publicly available by the holder of the certificate in accordance with Article 55 of Regulation (EU) 2019/881; and
(d) where applicable, the historic information related to the specific certification or certifications of the ICT service to enable traceability.

RATIONALE

EUDIW ICT services are going to be used in very specific circumstances, for the deployment on EUDI Wallets, under the direct supervision of Member States. For end users, the EUDI Wallet Trust Mark will be the main driver of trust, but it needs to be associated to the overall certification of the EUDI wallet, not just to the cybersecurity certification.

The direct customers of the services certified in the EUDIW scheme will therefore be Member States, so the mark and label, who are intended to avoid confusion among customers, will mostly be needed for wallet solutions developed by private companies, who will seek certification before offering their solutions to Member States, and will use the mark and label as a way to use the certification that they have obtained to promote their offer.

3.5 Period of validity of an EUDIW certificate

The period of validity of a certificate is set to five years in order to align with Article 5c(4) of the eIDAS. The vulnerability assessment activities that are also required in that Article have been integrated in the overall maintenance process of EUDIW certificates.

1. The certification body shall set a period of validity for each EUDIW certificate issued taking into account the characteristics of the certified ICT service.
2. The period of validity of the EUDIW certificate shall not exceed 5 years.

RATIONALE

The limitation is here the one set by Article 5c(4) of the eIDAS. Because this is a legal requirement, there is no derogation to allow for a longer validity period, even with the prior approval of the NCCA.

This deadline therefore needs to be carefully monitored, because an EUDI Wallet would need to be deactivated if it is not certified anymore, so the recommendation to initiate the re-certification conformity assessment early enough needs to be clearly stated.

3.6 Maintenance of an EUDIW certificate

In addition to maintenance activities related to changes in the provided EUDIW ICT service, regular conformity assessments are required in order to ensure that essential processes used in the provision

of the EUDIW ICT service are effectively operated, and to ensure that the evolution of the threat landscape is adequately considered. A maintenance schedule is defined, and each maintenance conformity assessment may lead to the confirmation, withdrawal or update of the certificate.

1. Following the schedule defined in Annex II, upon request of the holder of the certificate or for other justified reasons, the certification body shall regularly perform a maintenance conformity assessment and review the EUDIW certificate for an ICT service. The maintenance conformity assessment shall be carried out in accordance with Annex II.
2. Following the results of the maintenance conformity assessment and review, the certification body shall:
   (a) confirm the EUDIW certificate;
   (b) withdraw the EUDIW certificate in accordance with Section 3.7;
   (c) append an amendment to the EUDIW certificate that defines an updated scope; or
   (d) withdraw the EUDIW certificate in accordance with Section 3.7 and issue a new EUDIW certificate with an identical or updated scope and an extended validity period.
3. The certification body may decide to suspend, without undue delay, the EUDIW certificate in accordance with Section 6.3, pending remedial action by the holder of the EUDIW certificate.

RATIONALE

The maintenance schedule is rather simple, as it includes a yearly maintenance evaluation and review of the certificate, as well as a re-certification evaluation and review. In additional, a special maintenance evaluation can be triggered at any time, for instance in case of material change in the certified service.

Following a maintenance evaluation and review, the certificate may be confirmed without change, updated by adding an amendment that defines an updated scope, withdrawn, or in the case of a re-certification, withdrawn and replaced with a certificate with an extended validity period.

3.7 Withdrawal of an EUDIW certificate

The withdrawal of EUDIW certificates is a task assigned to the certification body that issued the certificate, following an issue that cannot be corrected (vulnerability or nonconformity) or non-compliance from the holder of the certificate, or following instructions from the holder of the certificate or from the NCCA.

1. Without prejudice to Article 58(8), point (e), of Regulation (EU) 2019/881, an EUDIW certificate shall be withdrawn by the certification body that issued that certificate.
2. The certification body referred to in paragraph 1 shall notify the national cybersecurity certification authority of the withdrawal of the certificate. It shall also notify ENISA of such withdrawal in view of facilitating the performance of its task under Article 50 of Regulation (EU) 2019/881.
3. The certification body shall notify other relevant market surveillance authorities.
4. The holder of an EUDIW certificate may request the withdrawal of the certificate.

RATIONALE

The rules for withdrawal of certificates are very simple. Certificates are to be withdrawn by the certification body that issued them, with an exception define in Article 58(8)(c)(e) of the CSA, which grants to the NCCA to withdraw certificates that “do not comply with [CSA] or with a European cybersecurity certification scheme”.

Paragraph 3 covers the case where the certificate could be the certificate notified by the eIDAS supervisory bodies, and potentially requirements from other regulations, as applicable.

Paragraph 4 covers the case where the holder of the certificate requests the withdrawal of the certificate, which in EN ISO/IEC 17065 is mentioned as termination of the certificate.

There is no mention of a procedure when the certificate expires. This is not an issue here, because there is no direct notification of services maintained under this scheme, but this may need to be reconsidered to avoid the “silent” expiration of a certificate.

4. Conformity assessment bodies

4.1 Requirements for accreditation of a conformity assessment body

The draft candidate scheme includes requirements for the accreditation of conformity assessment bodies issuing EUDIW certificates, based on ETSI EN 319 403-1. These requirements may be moved into a state-of-the-art document.

1. The accreditation of a conformity assessment body shall take into account the specification of requirements for accreditation of certification bodies as laid down in Annex VIII.

RATIONALE
The proposed requirements are explained in the Annex, and they draw from existing standards.

The use of EN ISO/IEC 17065 as the basis for accreditation of EUDIW certification bodies is required by point 19 of the CSA Annex.

In addition, CIR (EU) 2015/1502 includes many organisational requirements on the provider of eID means, and therefore to the providers of EUDIW ICT services, and this can be handled by referring to ETSI EN 319 403-1, which is well-known in the digital identity community, and which is based on EN ISO/IEC 17065.

The methods to be used, which are described in Annex XI, will refer to other standards, and in particular to CEN TS 18072.

The requirements from Annex VIII may need to be complemented with requirements on the accreditation process, which would typically be defined in a state-of-the-art document. One of the questions to be addressed is the requirement for a pilot evaluation, which also could impact the authorisation process. National accreditation bodies don't all have the same policy in this regard, so harmonisation would be welcome

The proposal that is made in the following section is to require a pilot evaluation, or an equivalent way to ensure that the conformity assessment body has the ability to put their competences in practice.

Since the scheme only defines requirements that complement existing standards, including EN ISO/IEC 17065, some aspects are not directly covered, but the certification bodies still need to satisfy the requirements of EN OSI/IEC 17065. For instance, the scheme does not specify any specific requirements for the handling of complaints and appeals, but the requirements for section 7.13 of EN ISO/IEC 17065 still apply.

4.2 Additional or specific requirements for a conformity assessment body

The scheme defines an authorisation process, to be performed by the NCCA to complement the accreditation process. The additional or specific requirements to which certification bodies need to conform still need to be defined.

1. A conformity assessment body shall be authorised by the national cybersecurity certification authority to perform EUDIW conformity assessment activities where that body demonstrates that, in addition to meeting the requirements laid down in Article 60(1) and the Annex to Regulation (EU) 2019/881 regarding accreditation of conformity assessment bodies, it meets the following:
   (a) it has the competences required for the certification decision at assurance level 'high';
   (b) it has the necessary competences for performing the evaluation activities to determine the resistance to state-of-the-art cyberattacks carried out by actors with significant skills and resources, including in particular:
      (i) the competence to perform the design evaluation as described in Annex IX;
      (ii) the competence to perform the dependency analysis as described in Annex IX;
      (iii) the competence to combine the assurance information available on the components of the ICT service and to determine the evaluation activities to be performed on the ICT service;
      (iv) the competence to perform a vulnerability assessment, including penetration testing as required, on the ICT service to be certified;
   (c) it has the requisite competences and put in place appropriate technical and operational measures to effectively protect confidential and sensitive information for assurance level 'high', in addition to the requirements set out in Section 9.4.
2. The national cybersecurity certification authority shall assess whether a conformity assessment body fulfils all the requirements set out in paragraph 1. That assessment shall include at least structured interviews and a review of at least one pilot conformity assessment performed by the conformity assessment body in accordance with this scheme, unless their ability to put the competences listed in paragraph 1 in practice has been demonstrated in another way.
   In its assessment, the national cybersecurity certification authority may reuse any appropriate evidence from prior authorisation or similar activities granted pursuant to:
   (a) this scheme;
   (b) another European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881;
   (c) a national scheme referred to in Section 12.2 of this document.
3. The national cybersecurity certification authority shall produce an authorisation report which is subject to peer review in accordance with Article 59(3), point (d), of Regulation (EU) 2019/881.
4. The national cybersecurity certification authority shall specify the ICT service and conformity assessment activities to which the authorisation extends. The authorisation shall be valid for a period no longer than the validity of the accreditation. It may be renewed upon request provided that the certification body

still meets the requirements set out in this Section. For the renewal of the authorisation, no pilot evaluations are required.

5. The national cybersecurity certification authority shall withdraw the authorisation of the certification body where it no longer meets the conditions set out in this Section. Upon withdrawal of the authorisation, the certification body shall cease immediately promoting itself as an authorised certification body.

RATIONALE

The EUCC scheme defines such requirements, to be checked using a specific authorisation process, that applies to conformity assessment bodies that perform conformity assessment activities at assurance level 'high'. The authorisation process is performed under the authority of the NCCA, and it is recommended to coordinate it with the accreditation process through a collaboration between the NAB and the NCCA. As discussed in the previous section, it includes a requirement for a pilot assessment, but it leaves the door open to alternative methods to demonstrate the practical abilities of the CAB. In addition, note that there is no formal obligation for a conformity assessment body to cover all activities in their accreditation or authorisation, which could allow the accreditation of specialised entities, similar to EUCC's ITSEFs.

These additional or specific requirements are limited to competence requirements, typically linked to advanced evaluation techniques, where the NCCA is considered to be better suited to assess the competences of the CABs.

The specific competences are limited, and all related to the difficulty of evaluating such a complex composite ICT service, so four specific competences have been identified:

- the competence to perform the design evaluation, and in particular to analyse the impact of deviations from the scheme's requirements and to justify the proposed alternatives;
- the competence to perform dependency analyses, including for all the assurance information types identified with specific criteria (as defined in Annex IX);
- the key competence to put all the information together (including different types of conformity assessments) and identifying clearly what additional activities need to be conducted, with a proper justification; and
- the competence to perform a vulnerability assessment in that context, and to perform the relevant penetration tests (possibly through a subcontractor).

The competences required for managing composition are covered by the accreditation requirements.

The specific competences listed here are the harmonised requirements that apply to all conformity assessment bodies across all Member States. If some Member States wish to add specific competences in their national implementation, they have the opportunity to do so, in particular because certification occurs at assurance level 'high', which means that the certificates are always issued under the control of the NCCA (directly, or through delegation to a private body). Therefore, these additional constraints could be enforced through that delegation.

Note however that these additional national requirements would not limit the mutual recognition of certificates issued in other Member States by bodies that don't satisfy these national requirements.

4.3 Notification of certification bodies

The notification process is required by the CSA, and will consist in adding relevant information related to the accredited and authorised bodies to the Commission's NANDO database.

1. The national cybersecurity certification authority shall notify the Commission of the certification bodies in their territory that are competent to certify at assurance level 'high' based on their accreditation and the authorisation decision.
2. The national cybersecurity certification authority shall provide at least the following information when notifying the Commission of the certification bodies:
   (a) the following information related to accreditation:
      (1) date of the accreditation;
      (2) name and address of the certification body;
      (3) country of registration of the certification body;
      (4) reference number of the accreditation;
      (5) scope and duration of validity of the accreditation;
      (6) the address, location and link to the relevant website of the national accreditation body; and
   (b) the following information related to authorisation:
      (1) date of the authorisation;
      (2) reference number of the authorisation;
      (3) duration of validity of the authorisation;
      (4) scope of the authorisation.
3. The national cybersecurity certification authority shall examine without undue delay any information regarding a change in the status of the accreditation provided by the national accreditation body. Where the accreditation or authorisation have been withdrawn, the national cybersecurity certification authority shall inform the Commission thereof, and may submit to the Commission a request in accordance with Article 61(4) of Regulation (EU) 2019/881.

RATIONALE

This section is very basic and it simply covers the conditions for notification, which here include both accreditation and authorisation, since all EUDIW certifications are issued at assurance level 'high'.

4.4 Termination of a certification body

This process is intended to cover the case where a certification body terminates its activities.

1. When a notified certification body decides to terminate its EUDIW-related activities, they shall:
   (a) inform without delay the national cybersecurity certification authority of the termination, together with a schedule of the termination;
   (b) prepare a termination plan, including the transfer of its activities towards another accredited certification body;
   (c) share the plan with the national cybersecurity certification authority and with their certificate holders;
   (d) assist the national cybersecurity certification authority and their certificate holders in the implementation of the transition plan.

2. When notified by a certification body of the termination of its EUDIW-related activities, the national cybersecurity certification authority shall:
   (a) notify the Commission of the certification bodies in their territory of the termination;
   (b) review the termination plan provided by the terminating certification body;
   (c) coordinate the implementation of the termination plan, and in particular:
      (i) identify the necessary documentation and evidence relative to currently valid EUDIW certificates, with the support of the terminating certification body and if needed of any other accredited certification body that may be in a better technical position to perform these activities;
      (ii) submit all identified documentation and evidence relative to currently valid EUDIW certificates to any other accredited certification body that may be in a better technical position to perform these activities. This includes in particular certification reports, and the evidence submitted by the applicant. Personal data or personal information such as emails shall not be included.
3. If an accredited body cannot be found immediately to take over the terminating certification body's activities, the national cybersecurity certification authority shall carry out the monitoring and surveillance activities for the impacted certificates for a transitional period.

RATIONALE

This section does not provide much details, but it recalls the responsibility of the NCCA for certificated issued at assurance level 'high'. This is not supposed to happen very often, and mostly in cases where the NCCA delegates the issuance of certificates to private certification bodies.

5. Compliance monitoring

5.1 Monitoring activities by the NCCA

As required in Article 58(7) of the CSA, NCCAs have an important role in the compliance monitoring of all certified services and also of certificate holders and certification bodies. Their activities include specific reviews of a sample of certificates, which may here be limited to partial reviews focusing on specific topics, because of the limited number of certificates. The operating rules are expected to be further defined by the dedicated maintenance subgroup of the ECCG.

1. Without prejudice to Article 58(7) of Regulation (EU) 2019/881, the national cybersecurity certification authority shall monitor the compliance of:
   (a) the certification bodies with their obligations pursuant to this scheme and Regulation (EU) 2019/881;
   (b) the holders of an EUDIW certificate with their obligations pursuant to this scheme and Regulation (EU) 2019/881;
   (c) the certified ICT services with the requirements set out in the EUDIW;
   (d) the assurance expressed in the EUDIW certificate addressing the evolving threat landscape.
2. The national cybersecurity certification authority shall perform its monitoring activities in particular on the basis of:
   (a) information coming from certification bodies, national accreditation bodies and relevant market surveillance authorities;
   (b) information resulting from its own or another authority's audits and investigations;
   (c) complaints received.
3. The national cybersecurity certification authority shall select certified ICT services to be checked using objective criteria, including:
   (a) holder of a certificate;
   (b) certification body;
   (c) specific points of attention defined by the national cybersecurity certification authority;
   (d) any other information brought to the authority's attention.
4. The national cybersecurity certification authority shall inform the holders of the EUDIW certificate about the selected ICT services and the selection criteria.
5. The certification body that certified the sampled ICT service shall, upon request of the national cybersecurity certification authority, conduct additional review as directed by the national cybersecurity certification authority and inform the national cybersecurity certification authority of the results.
6. Where the national cybersecurity certification authority has sufficient reason to believe that a certified ICT service is no longer in compliance with this scheme or Regulation (EU) 2019/881, it may carry out investigations or make use of any other monitoring powers set out in Article 58(8) of Regulation (EU) 2019/881.

7. The national cybersecurity certification authority shall inform the certification body concerned about ongoing investigations regarding selected ICT services.
8. Where the national cybersecurity certification authority identifies that an ongoing investigation concerns ICT services that are certified by certification bodies established in other Member States, it shall inform thereof the national cybersecurity certification authorities of the relevant Member States in order to collaborate in the investigations, where relevant. Such national cybersecurity certification authority shall also notify the European Cybersecurity Certification Group of the cross-border investigations and the subsequent results.

RATIONALE

The CSA requires in Article 54(1)(j) that EU cybersecurity certification schemes include rules for monitoring the compliances of certified items, and attributes an important role in this monitoring to the NCCA in Article 58(7). Beyond the compliance of ICT products, services and processes, NCCAs need to monitor all other stakeholders, including the certificate holders and the certification bodies.

One of the ways to fulfil this obligation is to sample some certificates and to perform reviews on them, to ensure that all conformity assessment activities have been performed adequately, and that the certified EUDIW ICT service still complies to the scheme's requirements. In EUCC, this sampling is performed by selecting a number of products to be reviewed, based on objective criteria. This approach is also described here, but it has been slightly modified because it is likely that at least in some Member States, the NCCA will only monitor a very small number of certificates. Therefore, this section includes requirements that allow the NCCA to only monitor products on specific aspects, which it has identified as critical, for instance those for which the threat landscape is evolving rapidly.

Note that this mechanism is not intended to cover emergency situations, where a new threat is being exploited and needs to be mitigated. In this case, the approach would rather be to notify the certification body so they can launch if required a special evaluation to determine how the threat is mitigated by the EUDIW ICT service that they have certified.

5.2 Monitoring activities by the certification body

The certification body is also in charge of performing compliance monitoring activities on certified EUDIW ICT services and certificate holders, as foreseen in standard EN ISO/IEC 17065.

1. The certification body shall monitor the compliance of:
   (a) the compliance of the holders of a certificate with their obligations under this scheme and Regulation (EU) 2019/881 towards the EUDIW certificate that was issued by the certification body;
   (b) the compliance of the ICT services it has certified with their respective evaluation criteria.
2. The certification body shall undertake its monitoring activities on the basis of:
(a) the information provided on the basis of the commitments of the applicant for certification referred to in Section 3.2;
(b) information resulting from activities of other relevant market surveillance authorities;
(c) complaints and appeals received;
(d) vulnerability information that could impact the ICT services it has certified.

RATIONALE

The certification body also has monitoring obligations, also as part of the surveillance activities defined in section 7.9 of EN ISO/IEC 17065. The monitoring obligations cover both the certified EUDIW ICT services and its provider, since the scheme defines obligations for providers.

The section only defines the basis on which the monitoring activities are performed, but it does not describe the activities themselves. When the certification body becomes aware of a potential issue (vulnerability, threat, nonconformity), it should contact the certificate holder to initiate an impact assessment, possibly followed by a special evaluation.

5.3 Monitoring activities by the holder of the certificate

The holder of the certificate also has obligations related to the compliance monitoring of the certified EUDIW ICT services that they provide, in particular to identify relevant vulnerabilities and possible nonconformities.

1. The holder of an EUDIW certificate shall perform the following tasks to monitor the conformity of the certified ICT service with its security requirements:
   (a) monitor vulnerability information regarding the certified ICT service, including known dependencies by its own means but also in consideration of:
      (1) a publication or a submission regarding vulnerability information by a user or security researcher through the contact provider to that avail;
      (2) a submission by any other source;
   (b) monitor the assurance expressed in the EUDIW certificate, and in particular the evolution on the status of any certificate or assurance report used as objective evidence in the evaluation of the ICT service.
2. The holder of an EUDIW certificate shall work in cooperation with the certification body and, where applicable, the national cybersecurity certification authority to support their monitoring activities.
3. The holder of an EUDIW certificate shall notify the certification body without undue delay when the following events occur:
   (a) any breach or compromise of the ICT service they provide;
   (b) any material change to the ICT service.

RATIONALE

The certificate holder also has monitoring obligations, in particular regarding the vulnerabilities that may affect the provision of its service. Beyond the traditional sources for identifying new vulnerabilities, following the requirements of Article 55(1)(c) of the CSA, the certificate holder needs to implement a way for researchers to submit vulnerabilities in their service, and they need to analyse these submissions and to notify without delay their certification body if they identify a vulnerability with material impact on the security of their service.

In addition, because the EUDIW scheme intends to rely heavily on composition and on independent certification of EUDI Wallet components, a specific obligation is added to monitor the evolution of the certificates on which the certification of the service relies, and to take appropriate measures when one of the components is updates, when the scope of its certification is modified, or when a certificate is withdrawn.

Finally, the certificate holder has an obligation to notify the certification body of any breach or compromise of their certified service, and of any material change that they perform on the service. For breaches, there is no threshold, because any breach, even minor, will likely be associated to a nonconformity to the scheme's requirements, so a special evaluation needs to be considered. The reasoning is the same for material changes, but the certificate holder remains in charge of the impact assessment of the changes, to establish its materiality. However, since the effectiveness of the change management process is evaluated at each annual surveillance evaluation, the certification body will review these impact assessments and determine whether or not the certificate holder has notified them when required.

6. Nonconformities and non-compliance

6.1 Consequences of nonconformity of a certified EUDIW ICT service

The management of nonconformities is centred around the certification body, which decides on the actions to be performed, starting by a notification of the certificate holder and a request for a remediation plan. Depending on the severity of the nonconformity, the certification body may also notify the NCCA and the eIDAS supervisory body. The certification body may also decide to suspend the certificate.

1. When the certification body becomes aware of a nonconformity of a certified ICT service with the requirements laid down in this scheme and in Regulation (EU) 2019/881, the certification body shall inform the holder of the EUDIW certificate about the identified nonconformity and request remedial actions.
2. Where an instance of nonconformity with the requirements of this scheme might affect compliance with Regulation (EU) No 910/2014, the certification body shall inform the national cybersecurity certification authority without delay, as well as the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014 about the instance of nonconformity identified.
2. Upon receipt of the information referred to in paragraph 1, the holder of the EUDIW certificate shall within the time period set by the certification body, which shall not exceed 30 days, propose to the certification body an assessment of the materiality of the nonconformity and the remedial action necessary to address the non-conformity.
3. The certification body may suspend, without undue delay, the EUDIW certificate in accordance with Section 6.3 in case of emergency, or where the holder of the EUDIW certificate does not duly cooperate with the certification body.
4. The certification body shall carry out an analysis of the proposed assessment and a validation to assess whether the proposed remedial action addresses the nonconformity, and if the nonconformity is material, a verification to assess the effectiveness of the remedial action.
5. Where the holder of the EUDIW certificate does not propose appropriate remedial action during the period referred to in paragraph 2, the certificate shall be suspended in accordance with Section 6.3 or withdrawn in accordance with Section 3.7.
6. Where the certified ICT service is a composite ICT service and a component of the ICT service is identified as participating to the nonconformity, the conformity assessment body shall notify the conformity assessment body who issued the certificate for that component of the issue.

RATIONALE

Article 54(1)(l) of the CSA requires schemes to describe the consequences of nonconformity of certified services. This section describes a process in which the certification body, when becoming

aware of a nonconformity, needs to notify the certificate holder and request an impact assessment as well as a proposal for remediation.

Then, the certification body will assess the impact assessment and the suitability of the proposed remediation. Following the principles of CEN TS 18072, the effectiveness of the remediation only needs to be verified if the nonconformity is material. Otherwise, the verification may be deferred until the next annual conformity assessment.

In practice, this process is likely to be much simplified, because it is likely that the certificate holder will be the entity making the certification body aware of the nonconformity. In such a case, they are quite likely to immediately provide a first impact assessment proposal and possibly a remediation proposal, which may also have been implemented already.

If the certificate holder does not follow the rules, the certification body has a number of ways to make them act, including the suspension of the certificate, and if necessary, its withdrawal.

6.2 Consequences of non-compliance by the holder of the certificate

When the holder of a certificate does not comply to its obligations, a specific process is triggered, with a strict delay to get in compliance, and a possibility of subsequent suspension or withdrawal of the certificate, under the appreciation of the certification body.

1. Where the certification body finds that:
   (a) the holder of the EUDIW certificate or the applicant for certification is not compliant with its commitments and obligations as set out in Sections 3.2, 5.3 and 9.2; or
   (b) the holder of the EUDIW certificate does not comply with Article 56(8) of Regulation (EU) 2019/881 or Chapters 7 and 8 of this scheme;
   it shall set a time period of not more than 30 days within which the holder of the EUDIW certificate shall take remedial action.
2. Where the holder of the EUDIW certificate does not propose appropriate remedial action during the time period referred to in paragraph 1, the certificate shall be suspended in accordance with Section 6.3 or withdrawn in accordance with Section 3.7.
3. Continued or recurring infringement by the holder of the EUDIW certificate of the obligations referred to in paragraph 1 shall trigger the withdrawal of the EUDIW certificate in accordance with Section 3.7.
4. The certification body shall inform the national cybersecurity certification authority of the findings referred to in paragraph 1. The national cybersecurity certification authority shall immediately notify the supervisory body referred to in Article 46a of Regulation (EU) No 910/2014.

RATIONALE

Some of the scheme's requirements apply to the service provider itself, such as the obligation to provide complete and truthful information or to properly handle vulnerabilities. When an EUDIW ICT service provider does not comply to these requirements, they expose themselves to direct consequences.

The terms of the Article are stronger than those on the previous Article, because non-compliance (a direct failure to apply well-defined rules) is considered more significant than a nonconformity (which is more likely to be accidental). Suspensions and withdrawal are more likely to be used, and the various authorities are notified of the issue.

6.3 Suspension of the EUDIW certificate

A certificate may be suspended because of a nonconformity or vulnerability in the certified EUDIW ICT service, or because of non-compliance from the certificate holder, when the certification body believes that the issue can be addressed by the certificate holder in a timely manner. A suspended certificate remains valid, but it is an indication to users to be careful with this service, and the suspension is always accompanied with guidance for the users of the service whose certificate is suspended.

1. Where this scheme refers to suspension of an EUDIW certificate, the certification body shall suspend an EUDIW certificate concerned for a period appropriate to the circumstances triggering suspension, that does not exceed 42 days. The suspension period shall begin on the day following the day of the decision of the certification body. The suspension shall not affect the validity of the certificate.
2. The certification body shall notify the holder of the certificate and the national cybersecurity certification authority of the suspension without undue delay and shall provide the reasons for the suspension, the requested actions to be taken and the suspension period.
3. The holder of the certificate shall notify the users of the ICT services concerned about the suspension and the reasons provided by the certification body for the suspension, except those parts of the reasons the sharing of which would constitute a security risk or which contain sensitive information, as well as guidance for users of the ICT service. This information shall also be made publicly available by the holder of the certificate.
4. The national cybersecurity certification authority may inform the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014 about the suspension.
5. The suspension of a certificate shall be notified to ENISA in accordance with Section 9.3.
6. In duly justified cases, the national cybersecurity certification authority may authorise an extension of the period of suspension of an EUDIW certificate. The total period of suspension may not exceed 1 year.

RATIONALE

The suspension of a certificate is an intermediary step before the more radical withdrawal of a certificate. It is particularly useful in the context of a Regulation that makes certification a legal requirement (hence triggering the impossibility to use an EUDI Wallet that has lost its certification).

However, suspension is often misunderstood. A suspended certificate remains valid, but it becomes publicly known that it is facing some issues, which may lead to trust issues. For this reason, this section requires specific information of users, containing at least some recommendations for the continued use of the service in acceptable security conditions.

A suspension is normally short (42 days maximum, inherited from EUCC), but the NCCA has the power to extend it as needed. This is expected to happen in particular when there exist effective compensating measures, but that the actual remediation of the issue takes more time.

6.4 Consequences of non-compliance by the certification body

Non-compliance by the certification body of course may impact its accreditation, authorisation and notification, and it may as well impact certificates issued by that certification body, if it is found that the operation of the certification body when issuing a certificate was inadequate and casts doubts on the validity of the certificate. The NCCA may organise a review of impacted certificates by another certification body, and if issues are identified, require some conformity assessment activities to be performed again.

1. In case of non-compliance by a certification body with its obligations, the national cybersecurity certification authority shall, without undue delay:
   (a) identify the potentially affected EUDIW certificates;
   (b) where necessary to support that identification, request conformity assessment activities to be performed on one or more ICT services by either the certification body which issued the certificate, or any other accredited and authorised certification body that may be in a better technical position to perform these activities;
   (c) analyse the impacts of non-compliance by the certification body;
   (d) notify the holders of the EUDIW certificates affected by non-compliance by the certification body.
2. For every certificate affected by non-compliance of the certification body, the national cybersecurity certification authority shall, without undue delay:
   (a) identify the conformity assessment activities that have to be reperformed, if required with the support of the non-compliant certification body or of another accredited and authorised certification body that may be in a better technical position to perform these activities;
   (b) for every such conformity activity, request the activity to be performed by either the certification body which issued the certificate, or any other accredited and authorised certification body that may be in a better technical position to perform this activity.
3. Any nonconformity of a certified ICT service identified while reperforming conformity assessment activities shall be processed according to Section 6.1.
4. The non-compliant certification body shall be responsible for the costs related to the activities in paragraph 2.
5. On the basis of the measures referred to in paragraph 1, the national cybersecurity certification authority shall:
   (a) where necessary, report the non-compliance of the certification body to the national accreditation body;
   (b) where applicable, assess the potential impact on the authorisation.

RATIONALE

This last Article on consequences is the most complex, because if a certification body does not comply with the requirements of the scheme, there may be consequences at several levels.

First, the certification body may see its accreditation and/or authorisation suspended or withdrawn, limiting its ability to perform its activities. Because the present scheme includes annual surveillance

activities, this may lead to issue for certificate holders, exposing them to possible withdrawal of their certificates.

In addition, depending on the non-compliance by the certification body, the validity of the certificates issued by the certification body may be questioned, possibly leading to their suspension or withdrawal, or to the necessity of a special evaluation to re-perform the conformity assessment activities that the non-compliant certification body had possibly not performed adequately.

The Article attempts to protect the certificate holders, since they may also be victims of the non-compliance of the certification body. In particular, a non-compliant certification body bears the costs of any special conformity assessment caused by its non-compliance, even if the additional activities are performed by another conformity assessment body.

7. Vulnerability management

7.1 Vulnerability management procedures

All providers of EUDIW ICT services need to manage vulnerabilities following defined procedures, and the requirements need to be aligned with best practices, including standards like EN ISO/IEC 30111 and for relevant products, regulations such as the CRA.

1. The holder of an EUDIW certificate shall establish, maintain and operate all necessary vulnerability management procedures in accordance with the rules laid down in this Chapter and, where necessary, supplemented by the procedures set out in EN ISO/IEC 30111.
2. For all relevant components of the ICT service, the vulnerability management procedures mentioned in paragraph 1 shall include:
   (a) the use of a software bill of materials in a commonly used and machine-readable format, covering at the very least the top-level dependencies of the component;
   (b) the use of security updates to remediate vulnerabilities, and when technically feasible, separate from functional updates;
   (c) mechanism to securely distribute updates, including a mechanism to ensure that the vulnerabilities are remediated without delay, where applicable, an automated distribution of security updates, and where applicable, a mechanism to disable the operation of a wallet unit until required security updates have been applied;
   (d) the distribution in relation to updates of advisory messages providing users with the relevant information, including on potential action to be taken.
3. The holder of an EUDIW certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, conformity assessment bodies and security researchers.
4. Where a holder of an EUDIW certificate detects or receives information about a potential vulnerability affecting a certified ICT service, it shall record it and carry out a vulnerability impact analysis.
5. When a potential vulnerability impacts an ICT product underlying a composite ICT service, the holder of the EUCC certificate shall inform the holder of dependent EUDIW certificates about potential vulnerability.
6. When a potential vulnerability on a composite certified ICT service is identified in one of the components of the ICT service, the conformity assessment body shall notify the certification body who issued the certificate for that component of the potential vulnerability.
7. In response to a reasonable request by the certification body that issued the certificate, the holder of an EUDIW certificate shall transmit all relevant information about potential vulnerabilities to that certification body.

RATIONALE
This section established the basis of vulnerability management in the context of the scheme. It mostly draws from other regulations, such as CSA's Article 55 for the requirement to have a mechanism to declare vulnerabilities, and also from the CRA for the more detailed requirements in paragraph 2.

These requirements inspired from the CRA are defined for "relevant components" of the EUDIW service. The first requirement, requiring a SBOM, could apply to many components, including to the online implementation of the service. On the other hand, the subsequent requirements on security updates only apply to software components that are deployed on user devices.

The first activity to be performed by the certificate holder when becoming aware of a vulnerability is to perform a vulnerability impact analysis, as described in the following article, and then to generate a vulnerability impact analysis report, which may need to be shared with the certification body, as described below.

7.2 Vulnerability impact analysis

Certificate holders need to perform a vulnerability impact analysis for every vulnerability identified to potentially impact the certified EUDIW ICT service, and they need to notify the certification body of every vulnerability that is determined to be material for the security of the certified EUDIW ICT service. Non-material vulnerabilities are analysed by the certification body during regular maintenance conformity assessments.

1. The vulnerability impact analysis shall refer to the description of the object of certification and the assurance statements contained in the certificate. The vulnerability impact analysis shall be carried out in a timeframe appropriate for the exploitability and criticality of the potential vulnerability of the certified ICT service.
2. The materiality of the impact shall be determined in accordance with the relevant methodology defined in Annex XI, in order to determine the exploitability and impact of the vulnerability.

RATIONALE
The objective of a vulnerability impact analysis is to determine how much a potential vulnerability may impact the certified service. There is no strict deadline on the establishment of this analysis, but the generic assessment of the vulnerability, for instance based on the score of the vulnerability in a system like CVSS, makes the handling of critical vulnerabilities more urgent than the handling of vulnerabilities of low and medium severity.

The objective of the vulnerability impact analysis is to translate this initial assessment into an assessment that is specific to the certified service. In this assessment, a critical vulnerability may have no impact at all if it relies on a feature that is not used in the implementation of the service. On the opposite, a vulnerability with a lower score may be considered material if the conditions for its exploitation are met in the certified service.

7.3 Vulnerability impact analysis report

Any notification of a vulnerability with material impact to the certification body needs to include a vulnerability impact analysis report that describes the vulnerability, its impact, and the possible remediation of the vulnerability. If the vulnerability impact analysis report contains sensitive information, in particular related to possible exploitation methods, specific precautions are required for the communication between the certificate holder and the certification body.

1. The certificate holder shall produce a vulnerability impact analysis report where the impact analysis shows that the vulnerability has a material impact on the security of the ICT service, as defined in Annex II, which in turn has a likely impact on the conformity of the ICT service with its certificate.
2. The vulnerability impact analysis report shall contain an assessment of the following elements:
   (a) the impact of the vulnerability on the certified ICT service;
   (b) possible risks associated with the proximity or availability of an attack;
   (c) whether the vulnerability may be remedied;
   (d) where the vulnerability may be remedied, possible resolutions of the vulnerability.
3. The vulnerability impact analysis report shall, where applicable, contain details about the possible means of exploitation of the vulnerability. Information pertaining to possible means of exploitation of the vulnerability shall be handled in accordance with appropriate security measures to protect its confidentiality and ensure, where necessary, its limited distribution.
4. The holder of an EUDIW certificate shall transmit a vulnerability impact analysis report to the certification body, without undue delay.
5. Where the vulnerability impact analysis report determines that the vulnerability has a material impact on the security of the ICT service, and that it can be remedied, Section 7.4 shall apply.
6. Where the vulnerability impact analysis report determines that the vulnerability has a material impact on the security of the ICT service and that it cannot be remedied, the EUDIW certificate shall be withdrawn in accordance with Section 3.7.
7. The holder of the EUDIW certificate shall monitor any residual vulnerabilities to ensure that they cannot be exploited in case of changes in the operational environment.

RATIONALE

The result of the vulnerability impact analysis is a report that needs to contain information about the exploitability of the vulnerability, and where relevant, of the remediation of the vulnerability. Because the report may contain information on the possible exploitation of a vulnerability that has not yet been remediated, it needs to be considered highly sensitive by all stakeholders.

One of the important information of the vulnerability impact analysis report is the materiality of the vulnerability impact. If this impact is material on the security of the certified service, then a remediation needs to be implemented without delay, possibly with temporary compensating measures. The certification body will also need to verify the effectiveness of the remediation.

On the other hand, when the impact is not material, the certification body is not directly involved. The certificate holder applies their vulnerability assessment procedures as defined, and the certification

body verifies the effectiveness of these procedures in the annual maintenance conformity assessment. If some vulnerabilities are not fully remediated, leading to residual vulnerabilities, these vulnerabilities need to be considered at every maintenance conformity assessment.

7.4 Vulnerability remediation

The certificate holder designs and implements a remediation plan in a delay that is commensurate with the potential impact of the vulnerability, and submit the remediation plan to the certification body, which may decide to trigger a special conformity assessment to ensure that the vulnerability has been appropriately addressed and that the certified EUDIW ICT service is being provided in a secure manner.

1. The holder of an EUDIW certificate shall design and implement a remediation plan in a timely manner for all vulnerabilities that may impact the certified ICT service.
2. Where the holder of an EUDIW certificate has submitted a vulnerability impact assessment report to their certification body, the holder of an EUDIW certificate shall also submit a proposal for an appropriate remedial action to the certification body. The certification body shall review the certificate in accordance with Section 3.6. The scope of the review shall be determined by the proposed remediation of the vulnerability.

RATIONALE

The rules for remediation of a vulnerability are quite simple. Of course, all vulnerabilities eventually need to be remediated, in a timely manner that is proportional to their impact on the security of the certified service.

For material vulnerabilities (here defined by the fact that the service provider has delivered a vulnerability impact analysis report), the service provider needs to also deliver a remediation plan to the certification body (typically together with the report), and to implement this plan. After implementation, the certification body needs to perform a review, which may lead to a surveillance conformity assessment (in practice, such an assessment may not be necessary in simple cases, like applying a security update to a commonly used library and performing appropriate subsequent testing).

8. Vulnerability disclosure

8.1 Coordinated vulnerability disclosure

Since the present scheme requires notifying some stakeholders very early, possibly before remediating the vulnerability, and since it may be important to notify scheme users if they have to participate to the remediation, it is necessary for the certificate holder to define and implement a coordinated vulnerability disclosure policy.

1. The holder of an EUDIW certificate shall establish, maintain and operate a coordinated vulnerability disclosure policy and related procedures, in accordance with the rules laid down in this Chapter and, where necessary, supplemented by the procedures set out in EN ISO/IEC 29147.
2. The holder of an EUDIW certificate shall make their coordinated vulnerability disclosure policy and procedures publicly available.

RATIONALE

The requirement for coordinated vulnerability disclosure stems from the fact that in case of a difficult vulnerability crisis, an EUDIW ICT service provider may need to coordinate the reaction of its customers before publicly disclosing a (possibly unpatched) vulnerability, and will at the same time need to keep their certification body and regulatory authorities informed of the situation.

This is much easier to achieve if a policy has been established for coordinated vulnerability disclosure, allowing the service provider to follow a known procedure in case of a crisis rather than having to improvise a solution, taking the risk to make the crisis worse.

The Article is extremely simple, and it also requires the policy to be made publicly available.

8.2 Information shared with the supervisory authorities

The coordinated vulnerability disclosure policy needs to mention the NCCA, who may then decide to further share the information with other NCCAs or with the eIDAS supervisory bodies.

1. The information provided by the certification body to the national cybersecurity certification authority shall include all elements necessary for the national cybersecurity certification authority to understand the impact of the vulnerability, the changes to be made to the ICT service and, where available, any information from the certification body on the broader implications of the vulnerability for other certified ICT services.
2. The information provided in accordance with paragraph 1 shall not contain details of the means of exploitation of the vulnerability. This provision is without prejudice to the investigative powers of the national cybersecurity certification authority.

3. The national cybersecurity certification authority shall share the relevant information received in accordance with Section 7.2 with other national cybersecurity certification authorities and ENISA.
4. The national cybersecurity certification authority shall share the relevant information received in accordance with Section 7.2 with national supervisory bodies established in their country pursuant to Article 46a(1) of Regulation (EU) No 910/2014.
5. The national supervisory bodies established in their country pursuant to Article 46a(1) of Regulation (EU) No 910/2014 shall share the relevant information received in accordance with Section 7.2 with the national supervisory bodies established in other Member States.

RATIONALE

This section indicates the information to be shared in particular by the certification body, but this means that the situation needs to be foreseen in the service provider's CVD policy, allowing their certification body to share the information with the NCCA and with the eIDAS supervisory body, and indirectly to other NCCAs and eIDAS supervisory bodies.

This section is one of the very few where the eIDAS supervisory bodies are explicitly mentioned, because there is here a strong requirement to notify them of significant vulnerabilities. The last paragraph may be out of place for a CSA CIR, since it creates an obligation on a body defined in another regulation.

8.3 Publication of the vulnerability

Once a vulnerability has been remediated, the certificate holder publishes it at least in the European vulnerability database and in the databases that it has declared to use for this purpose.

1. Upon withdrawal of a certificate or upon remediation of a vulnerability, possibly including the addition of an amendment to a certificate, the holder of the EUDIW certificate shall disclose and register any publicly known and remediated vulnerability in the ICT service or its components on the European vulnerability database, established in accordance with Article 12 of Directive (EU) 2022/2555 of the European Parliament and of the Council or other online repositories referred to in the description of the certified ICT service.

RATIONALE

The service provider finally needs to make the vulnerability public, at least through the public database that they have declared (following Article 55(1)(d) of the CSA). The Article also makes reference to EU vulnerability database, as defined in NIS2, as it is of wider application than just NIS2.

9. Retention, disclosure and protection of information

9.1 Retention of records by conformity assessment bodies

Certification bodies keep the information about certificates for five years after their withdrawal, and if applicable, after the withdrawal of certificates that extend this certificate.

1. The conformity assessment bodies shall maintain a record system, which shall contain all documents produced in connection with each evaluation and certification they perform.
2. Conformity assessment bodies shall store the records in a secure manner and shall keep those records for the period necessary for the purposes of this scheme and for at least 5 years after the expiration or withdrawal of the relevant EUDIW certificate. When the certification body has issued a new EUDIW certificate in accordance with Section 3.3, paragraph 2, point (c), it shall retain the documentation of the withdrawn EUDIW certificate together with and as long as for the new EUDIW certificate.

RATIONALE

The principle of the rule is rather simple: All information should be kept for five years after the expiration or withdrawal of a certificate. The actual implementation is not as simple, because the validity of a certificate may be extended after a re-certification conformity assessment. In that case, the documents from all conformity assessments need to be kept as long as the chain of certificates is valid, and then for five more years.

9.2 Information made available by the holder of a certificate

In addition of maintaining publicly available information, the certificate holder needs to keep all the information provided to the certification body in the context of the evaluation for at least 5 years after the withdrawal of the certificate, and if applicable, after the withdrawal of the certificates that extend this certificate.

1. The information identified in Annex III as being made available publicly shall be available in a language that can be easily accessible to users.
2. The holder of an EUDIW certificate shall store the following securely for the period necessary for the purposes of this scheme and for at least 5 years after the withdrawal of the relevant EUDIW certificate:
   (a) records of the information provided to the certification body during the certification process;
   (b) specimen of the product components of the certified ICT service.

3. When the certification body has issued a new EUDIW certificate in accordance with Section 3.3, paragraph 2, point (c), the holder shall retain the documentation of the withdrawn EUDIW certificate together with and as long as for the new EUDIW certificate.
4. Upon request by the certification body or the national cybersecurity certification authority, the holder of an EUDIW certificate shall make available the records and copies referred to in paragraph 2.

RATIONALE

The same rules apply to the certificate holders, both for the information that they shared for certification and for the specimens of products in use. This is particularly important for the documents that the certificate holder allowed the certification body to consult but without delivering them a copy. This documentation should be archived carefully, because the CABs should keep some means to verify the integrity of the documents (typically, a cryptographic checksum).

9.3 Information made available by ENISA

According to Article 50(1) of the CSA, ENISA maintains a certification web site that lists all relevant and publicly available information about the EUDIW scheme, which needs to be available at least in English. In support of this activity, all stakeholders need to inform ENISA without delay of all decisions that affect the content and status of EUDIW certificates.

1. ENISA shall publish the following information on the website referred to in Article 50 of Regulation (EU) 2019/881:
   (a) all EUDIW certificates;
   (b) the information on the status of an EUDIW certificate, notably whether it is in force, suspended, withdrawn, or expired;
   (c) certification reports corresponding to each EUDIW certificate;
   (d) for every certificate, links to the cybersecurity information provided in accordance to Article 55 of Regulation (EU) 2019/881;
   (e) a list of accredited and authorised conformity assessment bodies;
   (f) the state-of-the-art documents listed in Annex TBD;
   (g) the opinions of the European Cybersecurity Certification Group referred to in Article 62(4), point (c), of Regulation (EU) 2019/881;
   (h) peer assessment reports issued in accordance with Section 11.3;
   (i) if applicable, references to the national cybersecurity schemes that have been replaced by the EUDIW scheme.
2. The information referred to in paragraph 1 shall be made available at least in English.
3. Certification bodies and, where applicable, national cybersecurity certification authorities shall inform ENISA without delay about their decisions which affect the content or the status of an EUDIW certificate referred to in paragraph 1, point (b).
4. ENISA shall ensure that the information published in accordance with paragraph 1 points (a), (b) and (c), clearly identifies the versions of a certified ICT service which are covered by an EUDIW certificate.

RATIONALE
This section provides additional details of the information to be published by ENISA on their dedicated certification website regarding the EUDIW scheme. It also requires stakeholders to keep ENISA informed of events impacting certificates.

Paragraph 2 makes the use of English mandatory, but not necessary as primary language. For instance, a formal certificate may be labelled in any language of the European Union, provided that the certificate also comes with an English translation of the information.

There is a reference to state-of-the-art documents in item 1(f), mostly because some of the annexes may be published as such. If there is no need for such documents, the reference should be removed.

9.4 Protection of information

Because the information exchanged between and stored by the stakeholders can be very sensitive, all stakeholders need to protect this information with a level of security proportionate to the sensitivity of the information.

> 1. Conformity assessment bodies, national cybersecurity certification authority, supervisory bodies, ENISA, the Commission and all other parties shall ensure the security and protection of business secrets and other confidential information, including trade secrets, as well as the preserving intellectual property rights, and take the necessary and appropriate technical and organisational measures.

RATIONALE
This section is directly taken from EUCC, and it acknowledges the fact that some of the information shared in the context of the EUDIW scheme can be highly sensitive and needs to be appropriately protected.

Note that the verification of how CABs implement this aspect is expected to be covered by accreditation and authorisation, to be verified by the NCCA.

10. Mutual recognition

The mutual recognition provisions as defined for EUCC do not apply to the EUDI Wallet, as the context is very different.

In the context of the EUDIW, mutual recognition may only be used to recognise a wallet from a third country in a more general context of mutual recognition of EUDI wallets. This would most likely involve the establishment of a scheme that would set up conditions that would be equivalent to those established by the present scheme, together with relevant provisions of the CSA.

These conditions may be added in a later phase.

11. Peer assessment

11.1 Peer assessment procedure

Because EUDIW certificates are issued at assurance level 'high', a peer assessment procedure needs to be established between the certification bodies that issue EUDIW certificates, including the national cybersecurity certification authorities who issue EUDIW certificates.

1. A certification body issuing EUDIW certificates shall undergo a peer assessment on a regular basis and at least every 5 years. The different types of peer assessment are listed in Annex XIII.
2. The European Cybersecurity Certification Group shall draw up and maintain a schedule of peer assessments ensuring that such periodicity is respected. Except in duly justified cases, peer assessments shall be performed on-site.
3. The peer assessment may rely on evidence gathered in the course of previous peer assessments or equivalent procedures of the peer-assessed certification body or national cybersecurity certification authority, provided that:
   (a) the results are not older than 5 years;
   (b) the results are accompanied by a description of the peer assessment procedures established for that scheme where they relate to a peer assessment conducted under a different certification scheme;
   (c) the peer assessment report referred to in Article 35 specifies which results were reused with or without further assessment.
5. The peer-assessed certification body and, where necessary, the national cybersecurity certification authority shall ensure that all relevant information is made available to the peer assessment team.
6. The peer assessment shall be carried out by a peer assessment team set up in accordance with Annex XIII.

RATIONALE

Peer assessment is not absolutely required in EU cybersecurity certification schemes, but since the certification of EUDI Wallets is a condition for their deployment and that a basis for the mutual recognition of EUDI Wallets throughout the EU, it seems reasonable to define a peer assessment procedure.

This procedure is exactly the same as the procedure defined for EUCC. This procedure has not yet been applied, since the first EUCC certificates have been issued less than one year ago.

11.2 Peer assessment phases

The peer assessment needs to follow a well-established process, with several phases, from preparation to reporting, which should be harmonised with other peer assessment processes in other relevant schemes, such as EUCC.

1. During the preparatory phase, the members of the peer assessment team shall review the certification body's documentation, covering its policies and procedures, including the use of state-of-the-art documents.
2. During the site visit phase, the peer assessment team assesses the body's technical competence.
3. The duration of the site visit phase may be extended or reduced depending on such factors as the possibility of reusing existing peer assessment evidence and results.
4. In the reporting phase, the assessment team shall document their findings in a peer assessment report including a verdict and, where applicable, a list of observed nonconformities, each graded by a criticality level.
5. The peer assessment report must be first discussed with the peer-assessed certification body. Following those discussions, the peer-assessed certification body establishes a schedule of the measures to be taken to address the findings.

RATIONALE

The phases are very classic, with preparation, audit and reporting.

11.3 Peer assessment report

The peer assessment procedure results in a report, and the peer assessed certification body is given the opportunity to address the identified nonconformities, if any, within an appropriate time limit set by the ECCG. The peer assessment report, after removing sensitive information from it, is published by ENISA, possibly with a negative opinion of the ECCG if the certification body has not addressed the nonconformities in the allotted time.

1. The peer assessment team shall provide the peer-assessed certification body with a draft of the peer assessment report.
2. The peer-assessed certification body shall submit to the peer assessment team comments regarding the findings and a list of commitments to address the shortcomings identified in the draft peer assessment report.
3. The peer assessment team shall submit to the European Cybersecurity Certification Group a final peer assessment report, which shall also include the comments and the commitments made by the peer-assessed certification body. The peer assessment team shall also include their position on the comments and on whether those commitments are sufficient to address the shortcomings identified.
4. Where nonconformities are identified in the peer-assessment report, the European Cybersecurity Certification Group may set an appropriate time limit for the peer-assessed certification body to address the nonconformities.
5. The European Cybersecurity Certification Group shall adopt an opinion on the peer assessment report:
   (a) where the peer-assessment report does not identify nonconformities or where nonconformities have been appropriately addressed by the peer-assessed certification body, the European Cybersecurity Certification Group may issue a positive opinion and all relevant documents shall be published on ENISA's certification website;
   (b) where the peer-assessed certification body does not address the nonconformities appropriately within the set time limit, the European

Cybersecurity Certification Group may issue a negative opinion that shall be published on ENISA's certification website, including the peer assessment report and all relevant documents.

6. Prior to the publication of the opinion, all sensitive, personal or proprietary information shall be removed from the published documents.

RATIONALE

Once again, the rules are the same as the rules proposed for EUCC. The peer assessment report is important, because it is an incentive for certification bodies to fix the issues identified. There is no enforcement mechanism other than the threat of a report with a negative conclusion.

However, in practice, a negative peer assessment report is likely to trigger an investigation for the NAB and the NCCA, and to lead to a challenge of the certification body's accreditation and/or authorisation.

12. Maintenance and final requirements

12.1 Maintenance of the EUDIW

Provisions for the maintenance of European cybersecurity certification schemes are defined in the CSA, and the requirements below complement them with a few simple rules, in particular related to state-of-the-art documents.

1. The Commission may request the European Cybersecurity Certification Group to adopt an opinion in view of maintaining the EUDIW and to undertake the necessary preparatory works.
2. The European Cybersecurity Certification Group may adopt an opinion to endorse state-of-the-art documents.
3. State-of-the-art documents which have been endorsed by the European Cybersecurity Certification Group shall be published by ENISA.

RATIONALE

The CSA includes in Article 49(8) an obligation to regularly evaluate the effectiveness of European cybersecurity certification schemes and to update them as needed, so the legal basis for maintenance of the scheme is present. In addition, one may note that the EUCC scheme has already been updated twice in the two years since its initial adoption.

The same may be expected for the EUDIW scheme, in particular since additional standards and technical specifications may become available and will need to be covered. If the requirements of the scheme are updated, there will be a need to establish a timeline for the new requirements, but this timeline should be defined on the basis of the extent of the changes in the requirements, and they should be accepted by a qualified majority of Member States through a committee procedure, so there is no provision here in this direction.

12.2 National schemes covered by the EUDIW

The CSA requires national schemes to cease operations once an equivalent European scheme has been adopted. Here, a national scheme may initiate certifications for an additional 12 months, with a possibility to issue a certificate at the latest 24 months after the adoption of the EUDIW.

1. In accordance with Article 57(1) of Regulation (EU) 2019/881 and without prejudice to Article 57(3) of that Regulation, all national cybersecurity certification schemes and the related procedures for ICT services that are covered by the EUDIW shall cease to produce effects from 12 months after the entry into force of this scheme.
2. A certification process may be initiated under a national cybersecurity certification scheme within 12 months from the entry into force of this scheme provided that the certification process is finalised no later than 24 months after entry into force of this scheme.

3. Certificates issued under national cybersecurity certification schemes may be subject to review. New certificates replacing the reviewed certificates shall be issued in accordance with this scheme.

RATIONALE

This paragraph really is a placeholder. The situation of national schemes needs to be re-evaluated when the scheme will be ready to be adopted as a CIR, in order to reflect the situation at this time. Nevertheless, the proposed timelines (one year to start new certification procedures, and two years to finalise them) is a sound basis, which was also used for EUCC.

More information about the integration of the present scheme into national schemes is provided in Annex XIV.

SECTION 2

Scheme annexes

I Scope of certification

WHAT?	**This annex defines the scope of certification, based on the discussion held in TG2 of the EUDIW AHWG.**
HOW?	**The annex defines the scope of certification, composed of the object of certification and of a high-level view of the requirements on each component of the service.** **This version of the Annex is an initial version, which is expected to evolve when new documents are published that define relevant requirements for the security of EUDI Wallets.**

I.1 Overall scope

1. Certificates are issued under the present scheme to ICT services related to European Digital Identity wallets and to the electronic identity schemes under which they are provided, including as defined in Article 1 of the present scheme:

a. service for the provision and operation of a wallet solution and the electronic identification ('eID') scheme under which it is provided;
b. service for the provision and operation of a wallet solution;
c. service for the provision of person identification data (PID) for the purpose of providing an eID scheme under which European digital identity wallets are provided
d. service used to verify the validity of European digital identity Wallets and relying parties.

NOTE I.1.1: The definition of a component is imported from Common Criteria, and it is essential for the rest of this Annex:

> **component** smallest selectable set of elements on which requirements may be based
> [From ISO/IEC 15408-1:2022, 3.17]

2. A certificate issued for a service for the provision and operation of a wallet solution and the electronic identification ('eID') scheme under which it is provided shall not include any assumption on the operating environment to be provided by the ICT service provider.

NOTE I.1.2: Such a certificate is an "overall" certificate, so it is not allowed to include any unresolved assumption about an operating environment of the ICT service provider, since all dependencies should be addressed at this point. It may include assumptions on user devices, provided that a mechanism is included to verify these assumptions (see below).

I.2 Common scope for all services

1. Each certified ICT service is built by combining components, which may themselves be ICT products, ICT services, information security management systems (ISMS), or processes.

NOTE I.2.1: An ISMS is included as mandatory component, because it is mentioned in CIR (EU) 2015/1502, but it would be possible to consider the mention of ICT systems instead, in order to leave more freedom on the means available to demonstrate the conformity of ICT systems to requirements.

NOTE I.2.2: The mention of processes (without an ICT qualifier) is voluntary, since some of the processes used may not strictly be ICT processes, but human-based processes supporting the provision of an ICT service.

2. Each ICT service certified under the present scheme shall include at least the following components, which shall be demonstrated in conformity with the listed requirements:

NOTE I.2.3: In the table below, the “reference” requirements are the main requirements to be met, and they are complemented by the “other” documents listed.

Component	Description	Applicable requirements
ICT system	The ICT system on which the ICT service relies for its provision. Note that the IT system is covered as a “full stack”, so evidence of conformity is expected to be available for the entire system.	**Reference**: • ETSI EN 319 401 • NIS2 CIR (EU) 2024/2690 • CIR (EU) 2015/1502, at eIDAS assurance level high **Other** • CEN TS 18026, level ‘substantial’ • EN ISO/IEC 27001
Development process	The process operated by the ICT service provider for the development of its ICT service.	**Reference**: • ETSI EN 319 401 **Other** • NIS2 CIR (EU) 2024/2690 • CEN TS 18026, level ‘substantial’ • ISO/IEC 27001
Change management process	The process operated by the ICT service provider for the management of the changes in the ICT service.	**Reference**: • ETSI EN 319 401 **Other** • NIS2 CIR (EU) 2024/2690 • CEN TS 18026, level ‘substantial’ • ISO/IEC 27001
Vulnerability management process	The process operated by the ICT service provider for the management and handling of vulnerabilities in the ICT service.	**Reference**: • ETSI EN 319 401 • CRA Annex I, Section 2 **Other** • NIS2 CIR (EU) 2024/2690 • CEN TS 18026, level ‘substantial’ • ISO/IEC 27001
Incident management process	The process operated by the ICT service provider for the management and handling of cybersecurity incidents in the ICT service.	**Reference**: • ETSI EN 319 401 **Other** • NIS2 CIR (EU) 2024/2690 • CEN TS 18026, level ‘substantial’ • ISO/IEC 27001

Fraud management process	The process operated by the ICT service provider for the management of fraud in the ICT service.	**Reference**: • Annex X

NOTE I.2.4: These processes are most likely to be defined and connected to each other as part of an Information Security Management System (ISMS), which could be evaluated separately. If the services are provided by different entities, the ISMS used by every entity needs to be evaluated, in particular to comply with the requirements of CIR (EU) 2015/1502 Annex, section 2.4.

NOTE I.2.5: The choice of level "substantial" for CEN TS 18026 (requirements for cloud services) is justified by the fact that this is the closest level to the requirements of CIR (EU) 2024/2690 that are applicable to TSPs.

4. The ICT service provider shall define assumptions on the environment used by components of the ICT service that allow the components to meet the requirements applying to them.

5. The ICT service provider shall demonstrate the validity of the assumptions defined on the environment used by components of the ICT service:

a. if the environment is supplied by the ICT service provider, then the provider shall provide evidence that the environment satisfies all the assumptions defined for it;
b. if the environment is supplied by the wallet user, then the ICT service provider shall define appropriate controls to verify the assumptions on the environment, and they shall validate the sufficiency of these measures and verify their effectiveness.

NOTE I.2.6: The notion of "supplied by the ICT service provider" includes environments that are provided by a third-party contracted by the ICT service provider (e.g., cloud service provider).

I.3 Service for the provision and operation of a wallet solution and the electronic identification scheme under which it is provided

1. In order to be certified under the present scheme, an ICT service used to provide EUDI wallets and the electronic identification scheme under which they are provided shall be in conformity with Article 5c(4) and 5c(5) of eIDAS, and shall in particular satisfy the requirements of an eID means for an eID scheme at assurance level 'high'.

2. In addition to the components listed in section I.2, such an ICT service shall include at least the following components, which shall be demonstrated in conformity with the listed requirements in order for the ICT service to be certified under the present scheme:

Component	Description	Applicable requirements
Wallet instance (all variants)	The application that defines the wallet solution's user interface. There may be several variants of the wallet instance, of different types (web, mobile, PC, *etc.*), and targeting different architectures.	**Reference**: • CIR (EU) 2015/1502 at eIDAS assurance level high (as applicable) • FiTCEM Wallet instance Protection Profile • Annex X

WSCA	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.	**Reference**: • CIR (EU) 2015/1502 at eIDAS assurance level high • WSCA Protection Profile under development in CEN TC224 WG17 • Annex X
Wallet unit service	The service hosted on the wallet provider's ICT system that supports individual wallet units.	**Reference**: • CIR (EU) 2015/1502 at eIDAS assurance level high (as applicable) • Annex X
Loading and update process	The process(es) operated by the ICT service provider for the loading and update of the wallet instance and WSCA.	**Reference**: • ETSI EN 319 401 • Annex X
Wallet provisioning and management service	The ICT service operated by the ICT service provider for the provisioning of the EUDI wallet and for its management throughout its lifecycle.	**Reference**: • CIR (EU) 2015/1502 at eIDAS assurance level high • ETSI EN 319 401 • Annex X
User onboarding and management	The process(es) operated by the ICT service provider for the onboarding of the users and for the management of user information.	**Reference**: • CIR (EU) 2015/1502 (for the eID means) • Annex X
PID provisioning and management service	The ICT service operated by the ICT service provider for the provisioning of person identification data and for its management throughout its lifecycle.	**Reference**: • CIR (EU) 2015/1502 at eIDAS assurance level high • ETSI EN 319 401 • Annex X

NOTE I.3.1: CIR (EU) 2015/1502 and CIR (EU) 2024/2981 define minimum evaluation activities for operations related to the management and presentation of PID, but not for other operations (management of presentation of EAAs, pseudonyms, logs, etc), so additional requirements are defined in Annex X.

3. Depending on the architecture of the wallet solution, the ICT service may include the following components, which shall be demonstrated to be in conformity with the listed requirements:

Component	Description	Applicable requirements
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.	**Reference**: • CIR (EU) 2015/1502 at eIDAS assurance level high • Relevant EUCC technical domains
Wallet unit service	ICT service provisioned by the wallet provider to implements on its ICT systems some features of the wallet unit.	**Reference**: • CIR (EU) 2015/1502 at eIDAS assurance level high • Annex X

4. When a WSCA from the ICT service relies on a WSCD that is not included as a component of the ICT service, the ICT service provider shall define assumptions about that WSCD that are sufficient for the WSCA to meet all applicable requirements, and the validity of the assumption shall be demonstrated.

NOTE I.3.2: The scheme does not define any direct requirements on the WSCD, but only constrains the WSCD through the needs of the WSCA.

I.4 Service for the provision and operation of a wallet solution

1. In order to be certified under the present scheme, an ICT service used for the provision and operation of a wallet solution shall be in conformity with Article 5c(4) and 5c(5) of the eIDAS, and shall in particular satisfy the relevant requirements of an eID means for an eID scheme at assurance level 'high'.

NOTE I.4.1: The "relevant requirements" are a reference to the relevant requirements of CIR (EU) 2015/1502, since the wallet solution is not a complete implementation of an eID means (as it lacks the services provided by the PID Provider).

2. From the lists defined in sections I.2 and I.3, at least the following components such an ICT service shall include at least the following components, which shall be demonstrated in conformity with the listed requirements in order for the ICT service to be certified under the present scheme:

a. ICT system;
b. development process
c. change management process
d. vulnerability management process
e. incident management process
f. fraud management process;
g. wallet instance (all variants);
h. WSCA;
i. loading and update process;
j. wallet provisioning and management service;
k. if applicable, WSCD; and
l. if applicable, wallet unit service.

I.5 Service for the provision of person identification data (PID) for the purpose of providing an eID scheme under which European digital identity wallets are provided

1. In order to be certified under the present scheme, an ICT service used for the provision of person identification data (PID) for the purpose of providing an eID scheme under which European digital identity wallets are provided shall be in conformity with Article 5c(4) and 5c(5) of the eIDAS, and shall in particular satisfy the relevant requirements of an eID means for an eID scheme at assurance level 'high'.

NOTE I.5.1: The "relevant requirements" are a reference to the relevant requirements of CIR (EU) 2015/1502, since the PID provider is only responsible for a few components of an eID means.

2. From the lists defined in sections I.2 and I.3, such an ICT service shall include at least the following components, which shall be demonstrated in conformity with the listed requirements in order to be certified under the present scheme:

a. ICT system;
b. development process;
c. change management process;
d. vulnerability management process;
e. incident management process;
f. fraud management process;
g. user onboarding and management; and
h. PID provisioning and management service.

I.6 Service used to verify the validity of European digital identity Wallets and relying parties

1. In order to be certified under the present scheme, an ICT service used to verify the validity of European digital identity Wallets and relying parties shall be in conformity with Article 5c(8) of the eIDAS.

2. From the lists defined in sections I.2 and I.3, such an ICT service shall include at least the following components, which shall be demonstrated in conformity with the listed requirements in order to be certified under the present scheme:

a. ICT system;
b. development process;
c. change management process;
d. vulnerability management process;
e. incident management process; and
f. fraud management process.

II Assurance continuity and certification lifecycle

WHAT?	**This annex defines the measures to put in place in order to guarantee that certified services remain in conformity with the scheme requirements after the issuance of the certificate.**
HOW?	**The annex defines a lifecycle for certificates, including the definition of activities to be performed by the certificate holder and by the certification body throughout the lifecycle of the certificate.**

II.1 Surveillance evaluations

1. The objective of surveillance evaluations is to ensure the ongoing validity of the demonstration of fulfilment of the scheme requirements, which shall cover three aspects:

(a) provision of the certified ICT service over a period of time;
(b) changes in the certified ICT service over a period of time;
(c) changes in the threat environment over a period of time.

2. The present scheme uses three different types of evaluations for the maintenance of the certificate: annual surveillance evaluation, recertification evaluation and special evaluation.

II.1.1 Annual surveillance evaluation

1. The purpose of the annual surveillance evaluation is to confirm the continued conformity and effectiveness of the certified ICT service over a period of time (typically, one year).

2. The evaluation team shall:

(a) perform an analysis of the changes since the last evaluation in the certified ICT service including
  (i) assessment of the suitability of the design of the modified controls;
  (ii) verification of the existence and implementation of modified controls;
  (iii) assessment of any change in the assurance information available for components of the certified ICT service;
(b) perform functional tests on functions and components impacted by the changes;
(c) select a subset of requirements, considering:
  (i) requirements where observations or nonconformities were identified in previous evaluations or since the previous evaluation by the certificate holder;

(ii) changes in the threat environment or guidance identified by the certification body or provided by the ECCG;

(d) evaluate the suitability of the design of the controls associated to the previously selected requirements;

(e) evaluate the operating effectiveness of a subset of the controls to be determined at each evaluation since the last evaluation, including at least:
   (i) the new or modified controls, from the date of modification;
   (ii) the controls associated to the previously selected requirements;
   (iii) all controls related to incident, vulnerability and fraud management;
   (iv) all controls related to development and change management.

NOTE II.1.1: In the case of composition, changes may have occurred in components that are certified in other schemes and have undergone surveillance activities on their own, or other events. In such a case, the evaluation team should ensure that the component continues to meet the requirements of the scheme (including certificate validity and scope), and that any updates in the user guidance have been considered in the implementation of the service.

3. In the first surveillance evaluation following the initial issuance of a certificate, the evaluation team shall evaluate the operating effectiveness of all controls.

NOTE II.1.2: This requirement is due to the obligation to certify the wallet before to operate it, which implies that operating effectiveness cannot be checked in the initial certification, or only on test conditions. It simplifies the initial certification, but it increases significantly the chances of identifying material nonconformities during the first annual surveillance evaluation, so specific care should be considered when scheduling that evaluation.

4. The activities performed in the context of the annual surveillance evaluation shall be sufficient to cover the legal requirement from Article 5c(4) or Regulation (EU) No 910/2014 for a vulnerability assessment every two years.

II.1.2 Recertification evaluation

1. The purpose of the recertification evaluation is to confirm the continued conformity and effectiveness of the ICT service as a whole, and its continued relevance and applicability for the scope of certification. A recertification evaluation shall be planned and conducted to evaluate the continued fulfilment of all of the evaluation criteria. This shall be planned and conducted in due time to enable for timely renewal before the certificate expiry date.

2. In addition to the recertification evaluation, the recertification activity shall include the review of previous surveillance evaluation reports and consider the performance of the certified ICT service over the most recent certification cycle.

NOTE II.1.3: Recertification needs to cover the effectiveness of all controls. If in surveillance evaluations the effectiveness assessment has only been performed on a minimal set of requirements, then the work to be done for recertification may be very significant. It is therefore recommended to carefully select the activities to be performed during these surveillance evaluations, in order to avoid deferring potential difficulties to the recertification evaluation.

II.1.3 Special evaluation

1. If a special evaluation is necessary then the certification body shall determine any evaluation activities necessary to decide about the potential termination, reduction, suspension or withdrawal of the certification.

2. A special evaluation shall be performed when a certificate has been suspended, before the suspension is lifted and the certificate is fully restored.

NOTE II.1.4 The objective of a special evaluation is to perform an evaluation focused on the measures taken by the certificate holder to fulfil the requirements for which nonconformities have been detected, on the measures taken by the certificate holder to mitigate a vulnerability or on the changes made by the certificate holder to their service or to their control framework.

3. The evaluation team shall

(a) perform an analysis of the changes and nonconformities identified since the last evaluation of the certified ICT service including:
  (i) assessment of the suitability of the design of the affected controls;
  (ii) verification of the existence and implementation of affected controls.
(b) evaluate the operating effectiveness of affected controls over the period since the previous evaluation.

II.2 Surveillance schedule

1. Surveillance activities shall be performed at least once a year, with the following rules:

(a) At least an annual surveillance evaluation shall be performed every year;
(b) A recertification evaluation shall be performed the months before the certificate is set to expire, in due time for renewal before the certificate expiry date;
(c) A special evaluation shall be performed when decided by the certification body, possibly on request of the certificate holder, following material changes or a material nonconformity.

2. In addition, after each evaluation, a review and certification decision shall take place, with the following possible outcomes:

(a) continuation of the certificate, without any change;
(b) suspension of the certificate, including guidance for users defined by the certificate holder and validated by the certification body, accompanied by requirements for the certificate holder to fix the identified nonconformities in the defined timeline;
(c) withdrawal of the certificate in case of nonconformities that cannot be addressed;
(d) addition of an amendment to the certificate with a new description and guidance but the same end date.

3. In the case of a recertification evaluation, the following outcome is also possible:

(e) withdrawal of the certificate and issuance of a new certificate with an updated description and guidance, and with an updated end date, which shall not be more than five years after the certification decision.

II.3 Parameters for surveillance and monitoring processes

The providers of EUDIW ICT services certified in the present scheme are required to implement processes related to the day-to-day maintenance of their services (see Annex I). One of the key objectives of these processes is to reduce the number of interactions between the EUDIW ICT service provider and the certification body, by establishing a distinction between material events and other events, and by assigning different ways to process these events:

- A material event (nonconformity, change or vulnerability, see the following subsections for details) shall be notified to the certification body without waiting for the end of the year, and the certification body shall follow up and provide feedback on the handling of the event by the EUDIW ICT service provider.
- Other events shall be handled directly through the process defined by the EUDIW ICT service provider, with an assessment of the effectiveness of this process performed every year by the certification body.

The assessment of the effectiveness of these processes shall include an assessment of the process used to determine the materiality of events. In the case where the certification body identifies a nonconformity in this assignment, the certification body shall take appropriate measures to ensure that the nonconformity is addressed, including where necessary an obligation to notify all events to the certification body over a given period, so the certification body can determine whether the event was assigned to the appropriate category.

The rest of this section provides definitions for the materiality of nonconformities, and of events in the following processes: change management and vulnerability management.

Overall, the definition of material is “capable of influencing the decisions of intended users”. The rationale therefore is that materiality is determined by considering the consequences of an event towards the intended users.

II.3.1 Materiality of nonconformities

A nonconformity is considered material if it makes a measure or control used to meet a requirement ineffective. A nonconformity may be considered as not material if it simply leads to a decreased effectiveness of the measure or control.

In addition, a nonconformity that is not considered material by itself may lead to a material nonconformity if it is repeated too often, actually making a measure or control ineffective.

> EXAMPLE
> In a control that implements a backup system to guarantee the availability of data:
> - the loss of backup data or the inability to restore it is very likely to be considered material;
> - a failure to perform the backup of a system once may not be considered material;
> - the same failure repeated over several days is very likely to be considered material.

When assessing materiality, more than a parameter is taken into account, such as the amount of data concerned, its sensitivity, and the effectiveness of the provider to identify the issue and mitigate it.

II.3.2 Materiality of changes

Since the materiality of changes needs to be estimated by the certificate holder, a detailed procedure needs to be defined in the change management policy and evaluated by the CAB.

The following principles should be followed:

- A change should be considered material if it may lead to a material nonconformity.
- Functional changes that do impact the security of the ICT service or impact the implementation of its interfaces should be considered material.
- Changes to the organisation and architecture underlying the ICT services should be considered material.
- Changes to critical components such as the WSCD or WSCA should be considered material.

II.3.3 Materiality of the impact of vulnerabilities

Like changes, the materiality of the impact of vulnerabilities needs to be estimated by the certificate holder, a detailed procedure needs to be defined in the vulnerability management policy and evaluated by the CAB.

NOTE II.3.2: This is about the impact of vulnerabilities, not about the vulnerabilities themselves. A vulnerability may be critical, but its impact minor if a patch is available to mitigate it and the patch is easy to apply and has been applied timely while ensuring that the vulnerability has not been exploited (which actually happens regularly on complex IT systems).

III List of publicly available information

WHAT?	**This Annex lists the information that the certificate holders need to make available publicly.**
HOW?	**The list has been built from the CSA requirements and some of the CRA requirements.**

1. The provider of an ICT service certified under EUDIW shall make the following information publicly available, pursuant to Article 55(1) of Regulation (EU) 2019/881:

(a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the certified ICT service and its components;
(b) any limitations on the use of the certified ICT service;
(c) the period during which security support will be offered to end users, in particular as regards to the availability of cybersecurity related updates;
(d) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;
(e) a reference to online repositories listing publicly disclosed vulnerabilities related to wallets and to any relevant cybersecurity advisories.

2. The provider of an ICT service certified under EUDIW and that includes a wallet solution in its scope shall make available a policy specifying the conditions and the timeframe for the revocation of wallet unit attestations, pursuant to Article 7(2) of CIR (EU) 2024/2979.

3. If an ICT service certified under EUDIW includes software components that are provided to wallet users to run on their own devices, the provider of the ICT services shall make the following information publicly available for every such component:

(a) detailed instructions or an internet address referring to such detailed instructions and information on:
  (i) the necessary measures during initial commissioning and throughout the lifetime of the component to ensure its secure use;
  (ii) how changes to the component can affect the security of data;
  (iii) how security-relevant updates can be installed;
  (iv) the secure decommissioning of the component, including information on how user data can be securely removed;
  (v) recommendations in case of loss or theft of the user device on which the component is installed;

(b) where applicable, the internet address at which the EU declaration of conformity and the information required by Regulation (EU) 2024/2847 can be accessed;

NOTE III.1: The objective is here to require only the part of the CRA documentation that provides direct instructions to end users, and access to the rest of the documentation only for those applications that are subject to CRA.

4. The information referred to in paragraphs 1 to 3 shall be available in electronic form and shall remain available and be updated as necessary at least until the expiry or withdrawal of the EUDIW certificate.

IV List of information required

WHAT?	**This Annex lists the information that the certificate holders need to make available at the beginning of the certification process.**
HOW?	**This list is mostly derived from the activities to be performed by the CAB, and the input required by the CAB to perform them.**

1. An applicant for certification of an ICT service under EUDIW shall make at least the following information available to the certification body when initiating the evaluation of their ICT service[2]:

(a) all information described in Annex III as information to be provided publicly at the end of the certification process;
(b) a description of the organisation and architecture of the ICT service, including:
  (i) a description of the ICT service, indicating the role of every component;
  (ii) a description of the interfaces, including the external interfaces and the internal interfaces between components;
  (iii) a description of the locations and premises from which the ICT service is operated;
  (iv) a description of the assumptions (for example on components provided by the end user);
(c) a certification plan, including:
  (i) a list of the components certified or planned to be certified with certificates or potential dates when the components will be certified
  (ii) security targets or equivalent documents describing the scope of certification for each component;
  (iii) associated guidance or any kind of integration document. Any certification should be performed taking into account some integration requirements. These requirements must be provided to the evaluator to check that the integration has been correctly performed.
(d) a risk assessment[3] describing the cybersecurity risks against the wallet solution is designed, developed, produced, delivered and maintained, as defined in Annex XI. It shall include a mapping between this risk assessment and the risk register as provided in Annex I of CIR (EU) 2024/2981.

2. If some of the components are still under certification, draft documents may be provided at the beginning of the evaluation, but final documents shall be provided when the component is certified, and analysed by the certification body.

[2] This list is strongly inspired from the list of documentation required in Article 8(5) of CIR (EU) 2024/2981.
[3] This risk assessment is required in Article 4(4)(d) of CIR (EU) 2024/2981, and their transmission to the CAB by Article 4(5) of the same regulation.

V Content of a certificate

WHAT?	**This Annex lists the required content of certificates.**
HOW?	**The content of the certificate draws from CIR (EU) 2024/482 (EUCC IA) and from CIR (EU) 2024/2981 (eIDAS 5c IA).**

1. An EUDIW certificate shall at least contain:

(a) a unique identifier allocated by the certification body issuing the certificate, in accordance with paragraph 3 of Section 3.4;
(b) information related to the certified ICT service, and about the holder of the certificate, including the following:
  (i) name of the ICT service;
  (ii) type of the ICT service, as one of the options listed in paragraph 2 of Section 1.1;
  (iii) version of the ICT service that was evaluated;
  (iv) name, address and contact information of the holder of the certificate;
  (v) link to the website of the holder of the certificate of conformity containing the information that is required to be made publicly available, as defined in Annex III.
(c) information related to the evaluation and certification of the ICT service, including the following:
  (i) name, address and contact information of the certification body that issued the certificate;
  (ii) where applicable, name of the subcontractors that contributed to the evaluation;
  (iii) name of the responsible national cybersecurity certification authority;
  (iv) references to this scheme;
  (v) a reference to the certification report associated with the certificate referred to in Annex VI;
  (vi) a reference to the certification assessment report associated with the certificate referred to in Annex VII;
  (vii) a reference to the standards used for the evaluation, including their versions;
  (viii) the date of issuance of the certificate;
  (ix) the period of validity of the certificate.
(d) the mark and label associated with the certificate in accordance with Section 3.4.

2. The information shall be provided in an official language of the EU, and an English translation shall be available within the certificate.

NOTE V.1: There may be a need to formally define how versioning should occur, in particular by mandating the identification of material changes (e.g., in a “major.minor.release” three-level numbering, material changes should at least trigger an increase of the “minor” version.

VI Content of a certification report

WHAT?	**This Annex lists the required content of a certification report (to be made publicly available together with the certificate).**
HOW?	**This Annex was built from CIR (EU) 2024/482 (EUCC IA) and from CIR (EU) 2024/2981 (eIDAS 5c IA).**

1. On the basis of the evaluation technical reports resulting from the evaluation, the certification body establishes a certification report to be published together with the corresponding EUDIW certificate.

2. The certification report is the source of detailed and practical information about the ICT service and about the ICT service's secure provision and shall therefore include all publicly available and sharable information of relevance to users and interested parties. Publicly available and sharable information can be referenced by the certification report.

3. The certification report shall at least contain the following sections:

(a) executive summary;
(b) identification of the ICT service;
(c) description of the ICT service;
(d) the security information to be made publicly available, as listed in Annex III;
(e) a summary of the preliminary audit and evaluation plan, including a summary of the results of the evaluation;
(f) summary of the review and certification decision;
(g) when available, the mark or label associated to the scheme;
(h) bibliography.

4. The executive summary shall be a brief summary of the entire certification report. The executive summary shall provide a clear and concise overview of the evaluation results and shall include the following information:

(a) name of the certified ICT service, enumeration of the ICT service's components that are part of the evaluation and the ICT service version;
(b) the name and NANDO identification of the certification body issuing the certificate and, where applicable, the list of subcontractors who contributed to the evaluation;

(c) the name of the national cybersecurity certification authority responsible for the certification body;
(d) completion date of evaluation;
(e) reference to the evaluation technical report established by the evaluation team;
(f) brief description of the certification results, including:
  (i) the name and version of all components evaluated in the context of the certification, together with a list of the references of the requirement documents considered (as listed in sections I.2 to I.6 of Annex I;
  (ii) the name and version of all components that have been evaluated prior to the certification, together with a reference to their certificate or other relevant assurance information;
  (iii) assumptions about the operating environments, including user devices;
  (iv) special configuration requirements;
  (v) disclaimer(s).

NOTE VI.1: All the information in the executive summary is duplicated, as it appears later in the document in a more detailed version. This is voluntary, as the idea is to allow a reader to get a first impression of the content by simply reading the executive summary.

5. The evaluated ICT service shall be clearly identified, including the following information:

(a) the name and version number of the evaluated ICT service;
(b) the type of ICT service, as one of the options listed in paragraph 2 of Section 1.1;
(c) an enumeration of the ICT service's components that are part of the evaluation, including their version number at the time of the evaluation;
(d) an enumeration of the ICT service's components that have been evaluated prior to the evaluation, including their version number at the time of the evaluation, a reference to the certificate or assurance information provided, and the date of issuance of that information;
(e) name and contact information of the holder of the EUDIW certificate;
(f) link to the website of the holder of the EUDIW certificate where publicly available information is provided, including the publicly available information in accordance with Annex III.

6. The information included in the section defined in paragraph 5 shall be as accurate as possible in order to ensure a complete and accurate representation of the ICT service that can be re-used in future evaluations.

7. The description of the ICT service shall include:

(a) a description of the ICT service's architecture and components, including required hardware, software, processes and ICT subservices;
(b) a description of the ICT service's security policies that are relevant for the ICT service's users, which may refer to the description of the information security management system component and of other components that define such security policies and processes;
(c) a description of the ICT service's control framework, including a mapping between the controls, the components in which they are implemented and the risks identified on the ICT service;
(d) the list of additional assumptions and requirements to the operating environments of the certified ICT service for the compliant provision of the ICT service;

8. A complete listing of the information to be made publicly available, as listed in Annex III shall be provided. All relevant documentation shall be denoted by the version numbers.

9. The summary of the evaluation shall include:

(a) a description of the evaluation and its results;
(b) a description of the resulting evaluation plan, including a list of the evaluation activities;
(c) the results of the evaluation activities;
(d) in the case of a maintenance evaluation, a summary of the nonconformities encountered since the previous evaluation.

10. The summary of the review and certification decision shall include the following information:

(a) confirmation of the attained assurance level, including when available a reference to the levels defined in Article 52 in Regulation (EU) 2019/881 or in Article 8 of Regulation (EU) No 910/2014;
(b) detailed description of the assurance requirements, as well as the details of how the ICT service meets each of them;
(c) date of issuance and period of validity of the certificate;
(d) unique identifier of the certificate.

NOTE VI.2: Point (b) most likely needs to be revised, but it indicates that the review ensures that the scheme requirements regarding evaluation have been met.

11. The bibliography section shall include references to all documents used in the compilation of the certification report. That information shall include the following:

(a) the security evaluation criteria, state-of-the-art documents and further relevant specifications used;
(b) the evaluation technical report;
(c) the evaluation technical reports for composite evaluation, where applicable;
(d) technical reference documentation, including technical specifications and standards;
(e) developer documentation used in the evaluation activities.

12. In order to guarantee the reproducibility of the evaluation, all documentation referred to has to be uniquely identified with the proper release date, and proper version number.

VII Content of an evaluation technical report for composition

WHAT?	**This Annex lists the required content of an ETR for composition (to be made available in case of composition, and in particular as a basis for the certification assessment report that the issuer of the "overall" certificate need to share with the members of the EDICG together with the certificate and certificate report).**
HOW?	**This Annex was built from CIR (EU) 2025/2162, which defines the content of the conformity assessment report required for the qualification of trust service providers, and from the EUCC template for an ETR for composition evaluation. The content has been adapted, but further changes are required.**

1. The certification assessment report as referred to in Section 3.3 shall:

(a) contain a reference to the certificate to which it is associated and to the certified ICT service, including at least its name and version as indicated in the certificate;
(b) specify the name of the certificate holder and, where applicable, its registration number, as stated in the official records, its official postal address, and its electronic address as well as, where applicable, the same information for all subsidiaries, affiliated legal entities, contractors and subcontractors that are producing, providing or operating components in the scope of the certificate on behalf of the certificate holder;
(c) include a detailed description of the scope of the ICT service covered by the assessment, including all ICT product, process and ICT service components, together with the risk assessment and the specific evaluation plan;
(d) contain sufficient evidence to demonstrate that the certificate holder and the ICT service it provides fulfil the requirements of this scheme;
(e) specify the name of the certification body that issued the certificate, and, where applicable its registration number, as stated in the official records, its registered postal address, and its electronic address;
(f) specify the following:
    (i) the name and country of the national accreditation body having accredited the certification body;

(ii) the link to the official website of the national accreditation body and containing the accreditation certificate issued by the national accreditation body to the certification body;
(iii) where applicable, the digital accreditation symbol;
(iv) the name and country of the national cybersecurity certification authority having authorised the certification body;
(v) the link towards the entry in the NANDO database that mentions the accreditation and authorisation of the certification body;
(vi) the list of subcontractors involved in the conformity assessment;
(vii) the names of the natural persons involved by the certification body and its subcontractors in performing the conformity assessment and their respective role in that assessment;
(viii) the evaluation activities conducted, the rationale behind their selection, and the methodology employed, including sampling methodology and test procedures;

(g) contain at least one qualified electronic signature, where the report is provided in an electronic form, or handwritten signature, where provided paper-based, identifying the name and title of the responsible person or persons that authorised to adopt the certification decision on behalf of the certification body;
(h) include, in accordance with point (a)
(i) an exhaustive list of third parties, including subcontractors, which provide components by indicating their name, as identified in point (a);
(ii) an indication whether those third parties and components have been subject to the conformity assessment and to which extent;
(i) describe, where appropriate, the content of the entry to be included, or to be updated, in the list of European Digital Identity Wallets by the Commission, in accordance with the result of the assessment;
(j) include an exhaustive list of public and certificate holder's internal documents, which are properly identified including versioning, which have been part of the scope of the conformity assessment, including at least the following documentation, for which a copy shall be either provided together with the evaluation technical report for composition or made otherwise available to the national cybersecurity certification authority on its request:
(i) the terms and conditions related to wallet user agreements;
(ii) the result of the risk assessment, including a rationale to explain how the risks and threats identified in Annex I of CIR (EU) 2024/2981 are covered;
(iii) the list of all internal documents supporting the effective provision of the certified ICT services by the certificate holder;
(iv) the list of standards with which the operation of the ICT service is claimed to be compliant;
(v) the list of WSCDs and their certification related information when the certificate holder delivers or makes available such devices to its users;
(vi) the list of devices used by the certificate holder as trustworthy system or product, including hardware security modules or secure cryptographic devices, to protect its own keys, and information related to their certification, when the certificate holder uses such devices to secure the processes supporting the ICT service it provides;
(k) contain a description of the certificate holder's control framework, and for each requirement from Annex X:
(i) if the requirement is not applicable to the ICT service, an indication of this non-applicability, together with a rationale;
(ii) otherwise, a list of the controls that contribute to the fulfilment of the requirement;
(iii) where applicable, references to assurance information available for components of the ICT service that have been evaluated elsewhere;

(l) contain an assessment of the fulfilment of the requirements that apply to the relevant ICT services pursuant to this scheme, as defined in Annex X, containing at least for each evaluation activity:
  (i) the nature of the activity;
  (ii) the timing of the activity, either as a point of time or as a period to be covered;
  (iii) the extent of the activity, including a rationale is sampling is used;
  (iv) the relevance of the activity, with references to requirements and controls;
  (v) a summary description of the activity;
  (vi) the result of the activity, including a rationale where required;

(m) contain a statement declaring, where applicable, the absence of any material nonconformities at the time of the certification decision;

(n) contain for every nonconformity identified in the report, a plan of corrective actions and their timescale, provided by the certificate holder and agreed by the certification body, together with the description of the planned evaluation activities the certification body shall undertake to evaluate that those nonconformities have been corrected;

(o) contain for every material nonconformity identified in the report, the date where the corrective actions have been completed, and the reference to the evaluation activities undertaken by the certification body to verify that the nonconformity has been effectively corrected;

(p) contain a summary of the review and certification decision, including a rationale of how the ICT service as a whole meets the requirements of assurance level 'high' as defined in Article 52(7) of Regulation (EU) 2019/881, and how the eID means or components thereof and the eID scheme under which it is provided meet the requirements of assurance level high as defined in Article 8(2) of Regulation (EU)No 910/2014.

(q) identify, for each stage of the conformity assessment, including documentation audit, implementation assessment and onsite inspections, the period in relation to which the assessment has been conducted and the time taken by the certification body in person-days to conduct the assessment;

(r) indicate the deadline within which the next surveillance evaluation must be conducted in accordance to the present scheme;

(s) contain an explicit declaration stating that the certification documents, including the evaluation technical report for composition, are also intended for the use by the national cybersecurity certification authority.

NOTE VII.1: The list above is adapted from Annex III of CIR (EU) 2025/2162, complemented with elements from the EUCC template for ETRs and from the draft candidate EUCS scheme. This list requires additional discussions on tis content, and also on the intended use of the certification assessment report.

VIII Requirements for conformity assessment bodies

WHAT?	**This Annex provides a list of the requirements to be fulfilled by the CABs contributing to the EUDIW conformity assessment.**
HOW?	**This Annex defines requirements to complement the existing ETSI EN 319 403-1 standard.**
AND?	**This list of potential requirements is based on hypotheses that make the certification of the most sensitive components of the wallet solution mandatory under other schemes.**

VIII.1 Introduction

VIII.1.1 Principles

The requirements defined in standard ETSI EN 319 403-1 (Requirements for conformity assessment bodies assessing Trust Service Providers) are a good starting point, although there are significant differences, which are introduced here, with a specific focus on two aspects:

- The competence requirements for personnel defined in section 6.2.1
- The process requirements defined in chapter 7

Overall, the main difference is of course that the EUDI wallet is certified as an ICT service, which differs from the certification of a service provider. In particular, the scope of certification for the EUDI wallet includes several product components, and also includes functional requirements.

For the purpose of the present document, we therefore assume that the following evaluation activities are performed in the context of another certification scheme:

- Cybersecurity evaluation of the WSCA.
- Cybersecurity evaluation of wallet instance applications running on user devices.

The reason for this hypothesis is to remove the need for the certification body to have the expertise required to review the results of these assessments and to take certification decisions concerning them.

Instead, the certification body simply needs to have knowledge of the technologies used, and an ability to determine that the specific component is indeed suitable for their purpose, and to determine how well they integrate in the overall wallet solution (i.e., how wallet provider and the

components relying on these externally certified components follow their security guidance, and if needed, that the components on which they operate satisfy the stated objectives on environment).

Conformance testing of the wallet solution should also be an optional requirement for certification bodies, in the sense that they may add compliance to EN ISO/IEC 17025 for that purpose, but they are also offered the possibility to rely on a certificate of conformity issued by another body.

Eventually, the description of these activities should be grouped with other requirements into a document defining the requirements for conformity assessment bodies that participate to the conformity assessment of EUDI wallets.

VIII.1.2 Inspection activities

The object of evaluation includes the implementation of the wallet unit and of the wallet services on the wallet provider's own IT infrastructure, and some of the requirements defined on these components are very technical, requiring an examination of the components, of their design, of their implementation. In addition, because the fulfilment of the requirements depends greatly on the architectural and design choices made by the wallet provider, determination of the conformity to these requirements is likely to be done on the basis of the evaluator's professional judgement.

For all these reasons, these evaluation activities seem to fall under the qualification of inspection rather than audit, mostly because of the design and implementation expertise required to determine the conformity of the wallet provider's implementation to the requirements.

This addition of inspection is the main change in the requirements of the CABs, and a consequence of the presence of product components and associated requirements in the scope of certification.

In addition, there remain a number of requirements about the implementation of the wallet unit or of the wallet services on the wallet provider's own IT infrastructure whose conformity needs to be evaluated through inspection of the software developed by the wallet provider. This presence of inspection is the main change in the requirements for CABs.

NOTE VIII.1.1: The qualification of these activities as inspection still needs to be discussed with the EUDIW AHWG and finalised. This decision only impacts the qualification of the conformity assessment activities as audit or inspection, and the assignment of the related competences to inspectors or technical experts. On the other hand, it impacts neither the nature of the activities to be performed nor the competences required to perform them.

VIII.2 Additional competences

1. The personnel in charge of determining the conformity of the implementation of the technical components of the provider's wallet solution shall:

(a) satisfy the following requirements
  (i) formal academic qualifications or professional training or extensive experience indicating general capability to determine the properties of software through examination of its design and implementation; and

(ii) at least four years full time practical workplace experience in an activity related to software development, of which at least two years in a role or function relating to identity services or other sensitive services,

(b) have knowledge of:
  (i) examination principles, practices and techniques in the field of cybersecurity of IT services and identity services;
  (ii) the issues related to various security architectures of wallet services, different types of WSCDs and WSCAs, including the risk and threats listed in the Annex I of (EU) 2024/2981;
  (iii) the applicable standards, publicly available specifications and regulatory requirements for wallet providers and other relevant publicly available specifications including standards for the evaluation of ICT product and ICT services; and
  (iv) the conformity assessment body's processes.

(c) have the following competences:
  (i) language skills appropriate for members of the development team;
  (ii) code and design analysis, report-writing and interviewing skills;
  (iii) vulnerability assessment, identification of vulnerabilities, penetration testing, evaluation of attack potential; and
  (iv) personal attributes: objective, mature, discerning, analytical, persistent and realistic.

The public standards mentioned in item (b)(iii) shall include at least the standards used for the evaluation of components (*e.g.*, ISO/IEC 15408, ISO/IEC 18045, CEN EN 17640), together with relevant protection profiles, and publicly available specifications shall include at least the OWASP Application Security Verification Standard

VIII.3 Additional process requirements

The requirements on the audit process, as defined in section 7.4.4 of ETSI EN 319 403-1, need to be complemented by additional requirements dedicated to the technical aspects, which are described in greater details in Annex XI. In particular:

- The audit process will be based on the principles of CEN TS 18072, which includes stricter requirements.
- Specific activities will be required during stage 1, in particular related to the evaluation of the ICT service design, and the evaluation of the risk assessment performed by the ICT service provider.
- Specific activities will be required during stage 2, in particular related to functional testing and to vulnerability assessment and penetration testing, as required by Article 52(7) of the CSA for assurance level 'high'.

IX Criteria to assess the acceptability of assurance information

WHAT?	**This Annex should define the specific criteria to assess the acceptability of different kinds of assurance information.**
HOW?	**There will be two parts in the content, the first part is inspired from the corresponding Annex VI in the 5c IA to define a generic method, and the second part by the content developed in TG3 for specific schemes.**

IX.1 Composite service evaluation

1. In a composite ICT service evaluation, the composite ICT service is evaluated together with an ICT product, ICT service, ICT process or managed security service that has already received a certificate from a scheme recognised by the present scheme, and on whose security functionalities or security controls the composite service depends.

2. In the case of an ICT service undergoing a composite ICT service evaluation, the certification body that issued the certificate for the underlying ICT product, ICT service, ICT process or managed security service shall share the relevant information with the CAB performing the evaluation of the composite ICT service.

3. Where the CAB allows the product to undergo a composite ICT service evaluation, the applicant for certification shall make available to the CAB all necessary elements.

4. The security user guidance from the underlying ICT product, ICT service, ICT process or managed security service shall be considered as a part of the evaluation criteria to be met by the composite ICT service.

NOTE IX.1.1: ISO/IEC 15408 Part 1 defines in section 14.2 several composition models for products. Similarly, different models will apply here, which should be further defined in guidance.

5. The CAB shall verify that the certificate has not been withdrawn or suspended, and that it is up-to-date for the evaluated component. A withdrawn or expired certificate shall not be used for assurance purposes. A suspended certificate may be used, provided that it is fully reinstated before the end of the evaluation.

6. The monitoring of the certificate shall start immediately, and if the certificate is updated, or if it is withdrawn and replaced by a new one, the CAB shall perform a differential dependency analysis on the changes to the certificate.

IX.2 Specific criteria for recognised certification schemes

The following schemes are recognised as a basis for composition:

(a) the European Common Criteria-based cybersecurity certification scheme (EUCC) as defined in CIR (EU) 2024/482;
(b) the present scheme.

IX.2.1 EUCC

1. An EUCC certificate brings strong enough guarantees about the issuer competence and impartiality, the rigour and depth of evaluation, and about the findings and exceptions.

2. Regarding the scope, the following rules apply:

(a) if the certificate claims conformance to a Protection Profile listed in Annex X, the scope shall be considered appropriate for the certified component, with full reliance for the applicable criteria;
(b) in other cases, reliance needs to be determined for all criteria applicable to the component that has been certified.

3. The CAB shall consider the assumptions on the ICT product's usage and deployment and the assumptions on the operating environment listed in the certificate report[4] as requirements to be met as part of the evaluation of the composite ICT service,

IX.2.2 EUDIW

1. An EUDIW certificate brings strong enough guarantees about the issuer competence and impartiality, the scope of evaluation and the rigour and depth of evaluation.

2. If deviations have been identified in the base EUDIW certificate, these deviations shall also be considered in the composite evaluation, and the pending additional evaluation activities need to be included in the composite evaluation plan.

3. If the correction of a nonconformity is pending in the certification report, its impact on the composite ICT service shall be assessed, and if it is material, the results of the special evaluation following the correction shall be considered in the composite evaluation.

NOTE IX.2.1: This may imply that the composite evaluation cannot be concluded until the nonconformity has been corrected in the base ICT service.

[4] As listed in the certification report, as required in item 9 of Annex V.1 of CIR (EU) 2024/482.

IX.3 Dependency analysis

1. Before to rely on assurance information provided by the provider of the ICT service under evaluation, the evaluator shall assess the relevance and acceptability of this assurance information.

2. The evaluator shall assess the acceptability of assurance information in accordance with the methodology set out in Annex B of CEN TS 18072. The evaluation shall address, as a minimum, the following dimensions:

(a) **Issuer competence and impartiality**. The evaluator shall verify the professional competence and impartiality of the body or person that issued the assurance report or certificate. For state-accredited auditors issuing ISAE reports, this includes verification that the auditor is subject to the oversight of a national professional body or competent authority and holds a relevant professional qualification. For certification bodies, accreditation under the relevant standard (ISO/IEC 17021-1, ISO/IEC 17065, or equivalent) by a national accreditation body appointed pursuant to Regulation (EC) No 765/2008 shall be verified. In the absence of relevant accreditation, qualification by a national cybersecurity authority or agency may be considered, provided that the competence and impartiality criteria for qualification are sufficient.
(b) **Scope adequacy**. The evaluator shall verify that the scope of the assurance documentation covers the services, processes, controls and systems that are relevant to the requirements being evaluated under this certification scheme.
(c) **Currency**. The assurance documentation shall be current at the time of the evaluation. Certificates shall be within their validity period. Assurance reports shall cover a reporting period that is sufficiently recent to provide confidence that the controls described remain in operation. Where a gap exists between the end of the reporting period and the date of the evaluation, the evaluator shall require a bridge letter or equivalent statement confirming that no material changes have occurred, or shall perform its own supplementary evaluation of the period not covered.
(d) **Rigour and depth of evaluation.** The degree of confidence provided by the assurance documentation shall be commensurate with the criticality of the requirements it covers. The evaluator shall consider the rigour of the evaluation methodology applied, the depth of testing performed, and the nature of the assurance opinion or conclusion expressed.
(e) **Assumptions**. If the assurance documentation makes assumptions on the environment in which they are integrated, the evaluator shall add evaluation criteria that correspond to these assumptions for the certification of the ICT service.
(f) **Findings and exceptions**. The evaluator shall review any nonconformities, findings, qualifications, exceptions or caveats noted in the assurance documentation. Where material findings or nonconformities exist, the evaluator shall determine whether they are relevant to the requirements of this scheme and, if so, whether they have been adequately addressed.

3. Based on the evaluation, the evaluator shall determine, for each relevant evaluation criteria, one of the following outcomes:

(a) **Full reliance**. The assurance documentation provides sufficient evidence that the requirement is met. No supplementary evaluation activity is required for this requirement. The evaluator shall document the basis for this determination.
(b) **Partial reliance**. The assurance documentation covers part of the requirement, or provides assurance at a level that requires supplementation. The evaluator shall specify the supplementary evaluation activities needed and perform them as part of the evaluation.

(c) **No reliance**. The assurance documentation is not available, is not adequate, or does not cover the requirement. The evaluator shall perform its own evaluation of the requirement in full.

The evaluator shall document its evaluation and determination of reliance for each piece of assurance information as part of the evaluation records. The evaluator remains fully responsible for the certification decision regardless of the extent to which reliance is placed on external assurance information.

4. Where applicable, the evaluator shall use the specific criteria defined in section IX.4.

IX.4 Specific criteria to assess the acceptability of assurance information

NOTE IX.4.1: The content of the present section is preliminary and incomplete, and it is only provided as example of criteria to be considered.

IX.4.1 EN 17640 (FiTCEM)

1. EN 17640 (Fixed-time cybersecurity evaluation methodology for ICT products) is a standard for the evaluation of ICT products that is often used for the certification of ICT products that don't require a more extensive Common Criteria evaluation, around which national certification schemes have been built in several Member States, and that can be used for assessing the security of some of the product components of an ICT EUDIW service.

2. For the purposes of this certification scheme, the following requirements apply to the dependency analysis of FiTCEM certificates intended to support the certification:

(a) **CAB qualification**. The evaluator shall verify the credentials of the CABs involved in the FiTCEM conformity assessment. The laboratory that performed the evaluation shall be accredited under EN ISO/IEC 17025 with FiTCEM in scope, and the certification body that issued the certificate shall be accredited to EN ISO/IEC 17065 with FiTCEM in scope. In the context of national schemes, accreditation may be replaced by qualification by a national cybersecurity authority, provided that qualification criteria include relevant impartiality and competence requirements.

(b) **Scope**. If the certificate claims conformance to a Protection Profile and evaluation requirements listed in Annex X, the evaluator shall consider the scope appropriate for the certified component, with full reliance for the applicable criteria. In other cases, the evaluator shall determine reliance for all criteria applicable to the component that has been certified. A FiTCEM certificate does not provide any assurance regarding any organisational controls, which need to be evaluated separately.

(c) **Currency**. The evaluator shall verify that the certificate has not been withdrawn or suspended, and that it is up-to-date for the evaluated component. A withdrawn or expired certificate shall not be used for assurance purposes. A suspended certificate may be used, provided that it is fully reinstated before the end of the evaluation.

(d) **Assumptions**. The evaluator shall consider the assumptions on the ICT product's usage and deployment and the assumptions on the operating environment listed in the certificate report as requirements to be met as part of the evaluation of the ICT service.

(e) **Findings**. Some findings may be reported in a FiTCEM certificate, such as a nonconformity to the security target, or a potential vulnerability or technical issue that could not be exploited. The evaluator shall consider all these findings and assess their impact on the security of the component and of the ICT service.

IX.4.2 Assurance engagements under ISAE 3000

1. ISAE 3000 (Revised) is the international standard for assurance engagements on subject matter other than historical financial information. It provides a framework under which a qualified auditor may issue an assurance opinion on whether an ICT service provider conforms to a defined set of criteria. The EUDIW criteria that do not relate to product components constitute suitable criteria for an ISAE 3000 engagement within the meaning of that standard.

2. Where an ICT service provider commissions an ISAE 3000 engagement covering EUDIW criteria, the following engagement model applies:

(a) The ICT service provider, as the responsible party, prepares a description of its system of controls and asserts conformity with the applicable criteria (the evaluation criteria that apply to the ICT service).
(b) The auditor performs the assurance engagement and issues a report expressing an assurance opinion on the ICT service provider's conformity with the stated criteria.
(c) The evaluator assesses the assurance report and determines the extent of reliance in accordance with the criteria defined in Section IX.3.

3. For the purposes of this certification scheme, the following requirements apply to the dependency analysis of ISAE 3000 engagements intended to support the certification:

(a) **Level of assurance**. The evaluator shall only accept reasonable assurance engagements for full reliance. Limited assurance engagements, which employ less rigorous procedures and express a negative-form conclusion, may support partial reliance only.
(b) **Criteria**. The evaluator shall verify that the criteria used in the engagement are the evaluation criteria determined for the ICT service through its design evaluation, or a mapping thereof that the CAB has verified to be complete and accurate. Where the engagement uses other criteria (such as an internal control framework), the evaluator shall evaluate the extent to which those criteria correspond to the ICT service's evaluation criteria.
(c) **Reporting period**. For engagements covering the operating effectiveness of controls, the reporting period shall be at least six months. For surveillance purposes, a twelve-month reporting period aligned with the surveillance cycle is preferred. Where the reporting period does not extend to the date of the evaluation, a bridge letter or equivalent statement shall be provided.
(d) **Auditor qualification**. The evaluator shall verify that the auditor holds a state-recognised professional qualification and is subject to the oversight of a national professional body or competent authority, and that the auditor is independent of the ICT service provider.
(e) **Scope**. The engagement may cover all or part of the evaluation criteria applicable to the ICT service provider. Where the engagement covers only a subset of the requirements, the evaluator shall perform its own evaluation of the requirements not covered.
(f) **Assumptions**. If the description of the system of controls includes complementary user entity controls (CUECs) or complementary subservice organisation controls (CSOCs), the evaluator shall add to the ICT service's evaluation criteria that correspond to these CUECs and CSOCs.
(g) **Findings**. If a finding listed in the report has not been corrected, the evaluator shall consider it as a nonconformity and assess the materiality of its impact on the ICT service.

IX.4.3 EN ISO/IEC 27001 Certificates

1. ISO/IEC 27001 certification attests to the conformity of the information security management system itself (the processes of establishing, implementing, maintaining and continually improving the ISMS); it does not, on its own, provide sufficient assurance that the individual controls selected in the statement of applicability are designed and operating at the level of rigour required by this scheme. The evaluator shall therefore perform its own evaluation of the design and operating effectiveness of the specific controls required by the evaluation criteria, even where an ISO/IEC 27001 certificate is in place.

NOTE IX.4.2: This is not satisfactory, so further investigations will be conducted, but this is linked to the use of CEN TS 18072 methodology, which includes specific requirements for the evaluation of the design and operating effectiveness of controls.

X Evaluation criteria

WHAT?	**This Annex is a placeholder for the Annex defining the evaluation criteria. Its goal is to explain the principles that will be followed for the definition of the evaluation criteria. For now, the evaluation criteria are in a separate document.**
HOW?	**Mostly external pointers.**

X.1 References to standards and technical specifications

X.1.1 ETSI EN 319 401 and related standards

The current proposal is to use ETSI EN 319 401 as a basis for the definition of requirements. This standard defines “General Policy Requirements for Trust Service Providers”, which are then complemented by service-specific requirements for different kinds of trust services.

The main advantages of reusing this standard are that the different candidates for certification under EUDIW are likely to be familiar with the EUDIW, and that the CABs are very familiar with the eIDAS concepts. In addition, the other standards from this series can also be used as a source of relevant requirements.

X.1.2 WSCA protection profile

A WSCA Protection Profile is currently being defined in CEN TC224 WG17, which should be referenced in the EUDIW scheme as the reference for WSCAs.

NOTE X.1.1: There is a draft that is currently open for comments in CEN TC224 WG17, which is distributed with the current draft.

There is currently an ongoing discussion about this Protection Profile, in particular for its application outside of EUCC’s technical domains, more specifically in the case where the WSCD is a remote HSM and the WSCA does not run on the HSM but beside it, typically on the server to which the HSM is connected:

The Protection Profile so far requires AVA_VAN.5 for all WSCAs. This is not an issue for any WSCA running on a secure element or on an HSM (both within technical domains), but it is an issue when the WSCA runs outside of the HSM, because in the absence of a technical domain, then the Protection Profile needs to define a methodology for the implementation of AVA_VAN.5.

In a similar situation (certification of Signature Activation Modules), certificates issued with AVA_VAN.5 relied heavily on assumptions on the secure crypto hardware (for the actual

protection of the assets) and on the operating environment (for the protection of the WSCA operation, mostly) to reach that level, with very limited measures actually implemented in the certified application.

Since the WSCA is solely intended to be used as a component of a wallet solution, one solution could be to reduce the assurance level required to AVA_VAN.3, acknowledging that most of the security measures will need to be included in the WSCD or in the operating environment. That would simplify the certification of these WSCAs, and also better reflect the reality of the security architecture than an AVA_VAN.5 assessment relying mostly on an assumption.

X.1.3 Mobile wallet instance profile

There is ongoing work on the definition of an evaluation methodology and profile for mobile wallet instances in the EUDIW AHWG itself. The intention is to use the resulting technical specification as is in the initial release of the EUDIW scheme, and to then identify a path, possibly through an ESO, to maintain the document over time.

The document currently covers both evaluation criteria and evaluation methodologies, and some work needs to be done to clarify this.

X.1.4 Additional standards

There needs to be a discussion on the additional standards on which the scheme may rely on its initial release and on its subsequent releases. There are many possibilities, but our current proposal for criteria would be that the scheme would refer to only a few standards, and that other standards related to EUDI Wallets should map to these standards. Regarding criteria, the reference standard could be a standard extending ETSI EN 319 401 to define specific requirements for the EUDI Wallet ecosystem. The criteria to be included on these standards could be based on the additional criteria discussed in section X.2.

Other standards may be defined by to provide more detailed requirements, such as the decomposition of the EUDI Wallet currently under development in CEN TC224 WG20, or the revision of the CEN TS 18098 technical specification on on-boarding. Such additional standards would then need to include a mapping to the EUDIW criteria defines in the scheme.

X.1.5 Evolution of standards

The evaluation of the EUDI Wallet and of its different components relies on a large number of standards, which will continue to evolve. Each standard is referenced in implementing acts in a specific version.

When a new version of a standard is released, it is not considered as applicable to the certification of EUDI Wallets until the relevant implementing act is updated. However, in specific cases where the updated version brings significant benefits, the ECCG may decide to allow the use of a new standard as a temporary exception.

X.2 Additional criteria

The additional criteria have been defined in a document that extends ETSI EN 319 401 for all entities involved in the operations of EUDI Wallets and the eID schemes under which they are provided. The document may later be split into several documents targeting the different stakeholders (wallet provider, PID provider, validation service operator).

The additional criteria are based as a starting point on the ARF's High-Level Requirements (HLRs). Each HLR is then associated to one or more or more evaluation activities:

- Conformance testing.
  The requirement is covered by the specifications to which conformity is required.
- Specific testing.
  The requirement defines a function that needs to be functionally tested but whose specification is defined by the developer (this is typically linked to inspection).
- Interactive testing.
  The requirement includes a user interaction, so specific points of attention apply to reduce the risk of fraud. This typically complements conformance or functional testing.
- Inspection.
  The requirement cannot be functionally tested (typically because it constrains the implementation of a function, *e.g.*, the key pair shall be generated on the WSCD), so an inspection of the design and implementation is required.
- Audit.
  The requirement mentions a policy or other documentation that needs to be audited.

The list of activities for a given requirement may not be exhaustive, in particular when audit and inspection are required, as they may lead to additional activities. For instance, the audit of a policy may uncover derived requirements that may themselves lead to additional inspection or testing requirements.

NOTE X.2.1: Not all HLRs from the ARF are applicable, as the EUDIW scheme does not cover all stakeholders. For instance, all requirements applying to relying parties are considered out of scope, as well as the requirements that apply only to attestation providers.

NOTE X.2.2: In the requirements documents, the HLRs that are addressed solely through conformance testing are not mentioned. Only those that require other activities are mentioned.

XI Methods and procedures for evaluation activities

WHAT?	**This Annex is a placeholder for the Annex defining the methods and procedures for evaluation activities. Its goal is to explain the principles that will be followed in the final Annex, including justifications.**
HOW?	**Combining several standards and providing requirements for a few critical activities.**

XI.1 References to standards and technical specifications

Since the EUDIW criteria are based on the ETSI EN 319 401 criteria, the natural choice for the assessment is to use as a basis ETSI EN 319 403-1, the general standard for CABs assessing TSPs[5]. In addition, we are referring other standards and regulations to provide additional details for specific conformity assessment activities.

XI.1.1 ETSI EN 319 403-1

Most of the requirements of ETSI EN 319 403-1 are directly applicable. A few of them are actually more precise in the draft candidate scheme, for instance on the surveillance schedule.

It is important to note that although the title of ETSI EN 319 403-1 mentions the assessment of TSPs (and not of services), the standard is nonetheless based on the EN ISO/IEC 17065 harmonised standard for certification of services, so it is suitable for our purpose.

XI.1.2 CEN TS 18072

CEN TS 18072 has originally been designed as a basis for the audit of cloud services for the EUCS scheme, and it is currently being revised to cover all ICT services. Its dependency analysis procedure is referred to in Annex IX, and the intention is also to reuse some of the concepts used for the audit with “reasonable assurance”, which has been designed to be suitable for assurance level ‘high’.

For instance, the assessment of the operating effectiveness of security controls is defined in details in section 7.4.4.2.2.3 of CEN TS 18072. The basic definition provided in CEN TS 18072 is as follows:

[5] The ETSI EN 319 403-1 standard is also used as a basis for Annex VIII, defining requirements for CABs, and these two annexes are likely be merged into a single (external) document.

A control is operating effectively, if
— it was consistently applied as designed throughout the specified period, and
— in case of manual controls, they were applied by individuals who have the appropriate competences and authority (e.g. changes being only approved by personnel who are responsible for the service being provided.

The activities from the evaluation team depend on the nature of the control, but they always need to determine how the control was applied, the consistency with which the control was applied, by who or by what means the control was applied.

This assessment is intended to achieve an elevated level of assurance, and it needs to rely on objective evidence.

CEN TS 18072 also provides a framework to consider how requirements are covers by a "subservice provider", which here corresponds to the components of the ICT service, which may be service, product, or process components. The mechanism allows to handle a wide range of components, in particular by providing a mechanism to demonstrate how the components contribute to the fulfilment of the evaluation criteria.

Such a mechanism is very important, because the present scheme is a "full-stack" certification, which means that all the components of an ICT service, whether they are products, services or processes, are part of the scope of certification, and evidence needs to be provided at the that all these components satisfy the scheme's requirements that apply to them.

NOTE XI.1.1: The applicable requirements include the generic requirements that apply to the service provider, for instance related to the implementation of vulnerability management, change management and fraud management processes. When a component does not fulfil some of these requirements or there is no sufficient evidence that it does, CEN TS 18072 defines processes to identify compensating controls or additional controls.

XI.1.3 Common Criteria and EUCC

The proposal is to make the use of EUCC mandatory for the evaluation of the WSCA, and optional for the evaluation of the other software components. Please refer to the discussion on the WSCA Protection Profile in Section X.1.2.

Note that since the reference is explicitly to the EUCC scheme, there is no need for the EUDIW certification body to have specific competences for the evaluation of the WSCA. They nevertheless need to have technical competences on Common Criteria, including the ability to understand a security target, certification report, the guidance associated to the certificate and the elements on the ETR for composition required to verify that the WSCA is deployed adequately.

NOTE XI.1.2: The EUDIW CAB should not need to be able to understand the full extent of the penetration tests that were performed on the EUCC-certified components. .

In addition to this explicit reference, the Common Criteria SARs are being used as reference for the definition of requirements for specific evaluation activities, in particular related to functional testing and vulnerability assessment.

XI.1.4 CEN EN 17640

CEN EN 17640 (FiTCEM) is a fixed-time methodology for the evaluation of products, for which the EUDIW AHWG is developing a specific profile for mobile wallet instances.

The proposal is to make schemes based on FiTCEM a possible alternative to EUCC for the evaluation of mobile wallet instances.

Like for EUCC, the references will be to the national schemes based on FiTCEM, to limit the competence requirements for the EUDIW certification body.

XI.2 Organisation of the evaluation

In CEN TS 18072, the evaluation is performed in two stages, with the first stage (as described in section 7.4.4.1 of CEN TS 18072) mostly dedicated to an initial documentation review and to the preparation of the main audit phase. For the EUDIW scheme, this phase will include two additional steps:

- design evaluation, to evaluate how the developer claims to cover the EUDIW criteria and the risks identified in the risk register from Annex I of CIR (EU) 2024/2981;
- risk assessment evaluation, to evaluate the risk assessment performed by the developer and understand how the controls cover the risks identified.

The sequence is going to be important, with the design evaluation focusing on the analysis of the claim from the developer (based on its risk assessment), and the risk assessment evaluation focusing on the evaluation of the risk assessment itself, including the mapping of controls to risks, which will then be essential for the definition of the conformity assessment activities to be performed,

In addition, during phase 2 of the evaluation (as described in section 7.4.4.2 of CEN TS 18072), two evaluation activities have been defined to cover the requirements from the CSA's definition of assurance level 'high' in Article 52(7):

- functional testing, to demonstrate that the ICT service "correctly implement[s] the necessary functionalities at the state of the art";
- vulnerability assessment, as an "assessment of their resistance to skilled attackers, using penetration testing", which is actually a refinement of the vulnerability identification activity defined in section 7.4.3.8.3 of CEN TS 18072.

XI.3 Additional methods and procedures

XI.3.1 Design evaluation

DEVELOPER ACTIONS

1. The developer shall provide a claim related to the conformity of the design of its ICT service:

(a) Determine evaluation criteria

(i) Based on a risk assessment as described in section XI.3.2, determine the EUDIW criteria that are applicable to the ICT service
(ii) Based on a dependency analysis for all components for which assurance information is available, remove the evaluation criteria that are covered by the assurance information and add criteria that correspond to the assumptions made in the assurance information

(b) Handling of gaps and deviations
(i) Identify and document all deviations from the applicable EUDIW criteria and assessment, including gaps
(ii) Describe and justify how certification assurance is maintained and how the identified risks are mitigated

DEVELOPER DELIVERABLES

2. The design documentation shall include at least the following components:

(a) ICT service design documentation
(b) References to the components of the ICT service
(c) Cross reference matrix between the components and their conformity assessment
(d) List of evaluation criteria following the results of the dependency analysis
(e) Description of gaps and deviations from the applicable EUDIW criteria and from the assessment methods
(f) Description of the impacted risks from the risk register
(g) Mitigation plans including additional criteria and alternative evaluation activities to achieve the required assurance levels and the required CAB competencies

EVALUATOR ACTIONS

3. The evaluator shall perform the following actions:

(a) Evaluate the ICT service design
(i) Identify the architecture and the main components of the ICT service
(ii) Verify the list of evaluation criteria with the results of the dependency analysis
(ili) Identify the deviations from the applicable EUDIW criteria and assessment

(b) Evaluate the deviations
(i) Evaluate the identified deviations, the associated risks, the proposed mitigation measures and the additional evaluation activities
(ii) Demonstrate that the mitigation measures are appropriate to mitigate the risks
(iii) Demonstrate that the additional criteria and additional evaluation activities are adequate to achieve the required level of assurance under the EUDIW scheme.

ADDITIONAL ACTIONS

3. If deviations have been identified and the evaluator proposes that the evaluation proceeds, additional review steps are required:

(a) The evaluator shall notify the certification body about the deviations and provide them with the demonstration that led to the proposal to proceed with the evaluation.
(b) The certification body shall review the conclusion
(c) If the certification body supports the decision, they shall notify their NCCA for an additional review
(d) If the NCCA supports the decision to process with the evaluation and the certificate is for a service for the provision and operation of a wallet solution and the eID scheme under which it is provided, they shall notify relevant entities as required by regulation.

NOTE XI.3.1: In point (d), we would expect a requirement from the NCCA to notify an entity under the eIDAS regulation, that would perform a final review to ensure the integrity, consistency, and sustainability of the national certification systems and their underlying system elements. Note that this applies only for “global” certificates, since deviations are transmitted through EUDIW composition.

NOTE XI.3.2: The overall review of the certification body cannot be considered conclusive until all the review steps indicated in point 3 have concluded without objections, so no certificate can be issued.

NOTE XI.3.3: There is no obligation to perform the review before proceeding with the evaluation, but not doing so may incur evaluation costs for an evaluation that will not be allowed to conclude, so the ICT service provider should be made aware of this risk.

XI.3.2 Risk assessment evaluation

DEVELOPER ACTIONS

1. The developer shall perform a risk assessment of the proposed ICT service, including the following steps:

(a) Relevance check
  (i) Review each risk scenario from the risk register and evaluate its applicability for the ICT service architecture and components.
  (ii) If a risk scenario is not applicable, provide a rationale to explain why (e.g., this risk scenario is applicable only if the WSCD is remote).
  (iii) If a risk scenario is applicable but can be difficult to interpret depending on the architecture, propose a new formulation for this risk and explain how it could apply.
(b) Completeness check
  (i) Regarding this specific ICT service, check that all the risks are covered, especially the risks related to the specific interfaces, assumptions, and security mechanisms.
  (ii) Complete by adding risks specific to the ICT service architecture if necessary.
(c) Risk evaluation
  (i) For each risk, evaluate the impact and the likelihood.
  (ii) Determine the risk level according to Impact and Likelihood.
(d) Security controls
  (i) For each risk, identify the controls in place for the ICT service. These controls can be implemented by a component or a set of components of the ICT service.
  (ii) For each control, explain how the control effectiveness is checked (component certified, service/process audited, etc.).
  (iii) Determine the residual risks and how they are monitored.

DEVELOPER DELIVERABLES

2. The risk assessment deliverable shall include at least the following elements:

(a) List of relevant risks and risk scenarios, including relevance justification for all risks and risk scenarios from the risk register and for the risks specific to the ICT service
(b) Evaluation of the impact and likelihood for each relevant risk
(c) A list of the controls, including assurance information available to control the sufficiency and effectiveness of each control (or a reference to the same list in the ICT service description)

(d) A mapping of controls to risks, with a justification of the coverage, identification of residual risks

EVALUATOR ACTIONS

3. The evaluator shall perform the following actions:

(a) Check the coverage of the risk register
For each risk scenario of the risk register, check that:
  (i) It has a direct equivalent.
  (ii) Or it is not applicable, and the rationale is consistent with the ICT service architecture.
  (iii) Or it is replaced by a more specific risk and the rationale is consistent with the ICT service.

(b) Check the completeness of the risk assessment
  (i) Check if risks have been added from the risk register. If yes, these risks may be applicable to other solutions and should be communicated to the organisation in charge of the risk register maintenance.
  (ii) Check if the risks cover correctly the interfaces of the ICT service.
  (iii) Check if the risks are consistent with the assumptions.
  (iv) Check if the risks are complete regarding the ICT service.

(c) Assess the quality of the risk level evaluation
  (i) Check the evaluation of the risk level of each risk.

(d) Assess the coverage of the risks by the controls and the justification provided for residual risks

NOTE XI.3.4: The suitability and effectiveness of the controls are verified in the main audit of the controls; the focus in this activity is the coverage of the risks with a control with an acceptable assurance claim.

XI.3.3 Vulnerability assessment

NOTE XI.3.5: This is preliminary content, inspired from Common Criteria, but leaving a number of key questions to be further studied and discussed.

DEVELOPER ACTIONS AND DELIVERABLES

1. The developer shall:

(a) provide access to the ICT service under evaluation in a version that is suitable for testing;
(b) provide a list of third-party components used in the implementation of the ICT service.

NOTE XI.3.6: This list only includes items that are specific to this activity, but the vulnerability assessment activity will also leverage the documentation provided by the developer, in particular regarding the design and implementation of the ICT service.

NOTE XI.3.7: This list is based on the assumption that the penetration tests are solely under the responsibility of the CAB. Another possible model, similar to that proposed in the EUCS, consists in making the developer responsible for penetration testing, leaving to the CAB a duty to review the penetration tests and their results, and, if necessary, to complement them with their own penetration tests.

EVALUATOR ACTIONS

2. The evaluator shall perform the following actions:

(a) confirm that the elements provided by the developer meet all requirements.
  (i) the access provided to the ICT service is suitable for testing;
  (ii) the list of third-party components includes all the components used in the implementation of the ICT service.
(b) perform a search of public domain sources to identify potential vulnerabilities
  (i) in the ICT service, including
  (ii) the components in the list of third-party components, and
  (iii) specific ICT products and services in the environment that the ICT service depends on.
(c) perform an independent vulnerability analysis of the ICT service to identify potential vulnerabilities in the ICT service, using documentation by the developer
  (i) the user documentation;
  (ii) the ICT service's specification, architecture, design and source code;
  (iii) the ICT service's risk analysis and description of security controls.
(d) conduct penetration testing, based on the identified potential vulnerabilities, to determine that the ICT service is resistant to attacks performed by an attacker possessing the required attack potential

NOTE XI.3.8: This set of actions is inspired directly from CC's AVA_VAN evaluator actions, which are the same from AVA_VAN.3 to AVA_VAN.5, only differing by the qualifier of the vulnerability analysis (point 3), and the attack potential for the penetration testing (point 4). Both aspects have been removed on purpose, as the concepts from CC cannot be directly reused here.

NOTE XI.3.9: The organisation of the activity is quite suitable. It starts by an identification of "potential" vulnerabilities, based on a search of known vulnerabilities and on an analysis of the documentation provided by the developer. Then, the evaluator tries to find in the ICT service some of those "potential" vulnerabilities using penetration testing.

NOTE XI.3.10: Common Criteria uses qualifiers for the vulnerability analysis ("focused" for AVA_VAN.3, "methodical" for AVA_VAN.4 and AVA_VAN.5), which are not directly applicable. Further requirements or guidance about the appropriate level of vulnerability analysis are required.

NOTE XI.3.11: Common Criteria uses different attack potentials ("Enhanced-Basic" for AVA_VAN.3, "Moderate" for AVA_VAN.4 and "High" for AVA_VAN.5). The definition of these attack potentials uses concepts and figures that cannot easily be translated for use on services. Further requirements or guidance about the appropriate attack potentials will need to be considered.

NOTE XI.3.12: An additional difficulty comes from the fact that the level of assurance required may not be the same for all functions. All functions related to the management and presentation of PID will require a higher level of assurance than most other functions.

XI.3.4 Functional testing

NOTE XI.3.13: This is preliminary content, inspired from Common Criteria, but leaving a number of key questions to be further studied and discussed.

DEVELOPER ACTIONS AND DELIVERABLES

1. The developer shall:

(a) provide evidence of the test coverage of the security functions;
(b) test the ICT service and document the results;
(c) provide test documentation, including a test strategy, test plans, expected test results and actual test results;
(d) provide the ICT service, suitable for testing.

EVALUATOR ACTIONS

2. The evaluator shall perform the following actions:

(a) analyse the test coverage information to confirm that the ICT service's security functions are covered by the test;
(b) analyse the test documentation and confirm that the test strategy is appropriate and that the actual test results are consistent with the expected test results;
(c) confirm the suitability of the provided ICT service for testing;
(d) perform one of the two following options
    (i) test a subset of the ICT service to confirm that the ICT service operates as specified.
    (ii) observe the execution of a subset of the ICT service and confirm that the results are the identical to the expected results.

NOTE XI.3.14: The list is strongly inspired from the ATE requirements at level EAL4, with 2 exceptions: (1) ATE_DPT is not covered, because it is unclear how to translate the CC notions for an ICT service, and (2) an option is given to only observe the re-performance of tests by the developer instead of independent testing.

XI.4 Surveillance evaluation activities

A few simple methods are here proposed for assessing the materiality of changes to the certified EUDIW ICT service and of changes to the threat environment. These activities are specific to surveillance evaluations and to the maintenance of assurance throughout the certification lifecycle.

XI.4.1 Service change impact assessment

1. At every surveillance or recertification evaluation, the changes made to the certified ICT service since the last evaluation shall be described by the developer, and their impact on the security of the certified ICT service shall be assessed.

NOTE XI.4.1: A change may trigger a special evaluation if its impact to the security of the overall service is considered material.

2. The service change impact assessment provided by the developer shall consider:

(a) The impact on the risk assessment associated to the changes performed, in particular when changes are performed on the definition or implementation of a security control;
(b) The additional third-party components and the associated potential vulnerabilities.

3. The developer shall then estimate the materiality of the change and transmit the service change impact assessment to the CAB if the ICT service change is considered material. The CAB shall then review the service change impact assessment and determine whether or not a special evaluation is required, and if so, the evaluation activities to be performed.

NOTE XI.4.2: The impact assessment is performed as part of the change management process, whose effectiveness needs to be reviewed yearly. The impact assessment is by default only submitted to the CAB when the impact is considered material. However, on the first year, or when a CAB has found nonconformities in the effectiveness of the change management procedure, they may require the developer to submit to them all their impact assessments for review over a period of time.

XI.4.2 Threat environment change impact assessment

1. The threat environment is defined in the wallet-specific risk register (one of the key outputs of the risk management process). There are two main sources of information to identify changes in the threat environment:

(a) updates of the risk register from CIR (EU) 2024/2981; and
(b) identification of vulnerabilities or new threats impacting the specific implementation of the wallet.

2. When the risk register included in CIR (EU) 2024/2981 is updated, the wallet-specific risk register shall be updated accordingly.

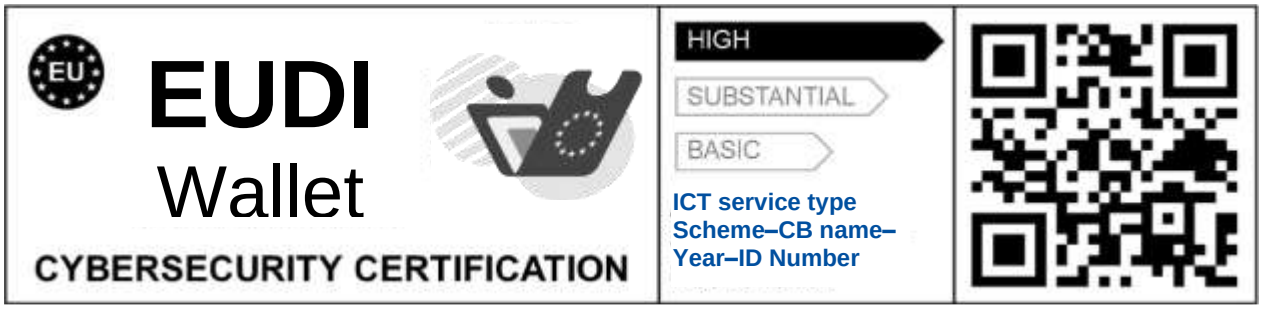
3. When the vulnerability management process identifies a vulnerability of a new nature or category that may lead to a more general change in the threat environment (*e.g.*, when a theoretical attack becomes actually exploitable), the wallet-specific risk register shall be updated to include this new risk and/or threat. In addition, the evaluator should monitor the potential impact of residual vulnerabilities.

4. When the wallet-specific risk register is updated, the change shall be considered material, unless the ICT service provider is able to demonstrate in the impact assessment that the new risks identified are not applicable to their ICT service, or that they are fully mitigated by the controls already in place.

XII Mark and labels

WHAT?	**This Annex defines the rules for marks and labels to be used for certificates.**
HOW?	**The content is inspired from the corresponding Annex in CIR (EU) 2024/482 (EUCC IA).**

1. The form of mark and label:



2. If the mark and label are reduced or enlarged, the proportions given in the drawing above shall be respected.

3. Where physically present, the mark and label shall be at least 5 mm high.

4. When displayed on a web site, the mark and label shall link to the entry of the certificate on ENISA's certification web site, and the QR-code may be removed.

XIII Scope and team composition for peer assessment

WHAT?	**This Annex complements the articles on peer assessment by more detailed requirements.**
HOW?	**This Annex is inspired from the corresponding Annex in CIR (EU) 2024/482 (EUCC IA), changing it only as required.**

XIII.1 Scope of the peer assessment

1. The peer-assessed certification body shall submit the list of certified ICT services that may be candidate for the review by the peer assessment team.

2. The candidate products shall cover the technical scope of the certification body authorisation, of which at least two different ICT service evaluations at assurance level ‘high’ will be analysed through the peer assessment.

3. If the certification body is not been able to meet the requirements in paragraph 2, then the peer assessment team shall decide whether to perform the peer assessment on the available ICT services, or to postpone the peer assessment.

NOTE XIII.1: This last paragraph has been introduced because some certification bodies may issue a very small number of certificates. The decision to proceed or not is left to the peer assessment team because the issue may persist for several years.

XIII.2 Peer assessment team

1. The assessment team shall consist of at least two experts each selected from a different certification body from different Member States that issues certificates at the assurance level ‘high’. The experts should demonstrate the relevant expertise in the evaluation activities related to the criteria included in Annex X, the evaluation methods and procedures defined in Annex XI and state-of-the-art documents that are in scope of the peer assessment.

2. In the case of a delegation of certificate issuance or prior approval of certificates as referred to in Article 56(6) of Regulation (EU) 2019/881, an expert from the national cybersecurity certification authority related to the concerned certification body shall in addition participate in the team of experts selected in accordance with paragraph 1 of this Section.

3. Each member of the assessment team shall have at least two years of experience of carrying out certification activities in a certification body in a relevant domain.

NOTE XIII.2: The technical competence requirements are slightly difficult to define as the different flavours of authorisation are not yet fully defined (they will mostly depend on an obligation (or not) to rely on external certification for some components).

4. The national cybersecurity certification authority monitoring and supervising the peer-assessed certification body and at least one national cybersecurity certification authority whose certification body is not subject to the peer assessment shall participate in the peer assessment as an observer. ENISA may also participate in the peer assessment as an observer.

5. The peer-assessed certification body is presented with the composition of the peer assessment team. In justified cases, it may challenge the composition of the peer assessment team and ask for its review.

XIV Integration into national certification

WHAT?	**This Annex is describing how this scheme fits in the overall certification requirements for EUDI Wallets. This is provided for information and discussion, not necessarily for inclusion as an Annex, with the possible exception of conditions for using the EU certificate as "main" certificate proposed in XIV.2, if they are deemed appropriate.**
HOW?	**The inspiration is an analysis of the requirements from eIDAS.**

XIV.1 Integration into a national certification scheme or system

Article 5c(1) of the eIDAS requires certification of the conformity of EUDI Wallets and the eID schemes under which they are provided to a number of articles:

- 5a(4), which defines the features to be made available to the user;
- 5a(5), which provides additional details, including the support of common protocols and interfaces, various privacy and security requirements, and the requirement to achieve eIDAS's assurance level high for eID means;
- 5a(8), which defines the validation mechanisms to be provided by Member States;
- 5a(14), which requires the isolation of personal data related to EUDI Wallets from other data.
- 5a(24), which mentions the possibility of adopting an Implementing Act to define conditions under which to onboard users from an eID means conforming to eIDAS assurance level substantial.

Although Article 5a(23) it is not directly mentioned, the Implementing Acts adopted under that Article to list standards that apply to the requirements from 5a(4), 5a(5) and 5a(8) are also important and need to be taken into consideration.

Except for parts of 5a(5) and 5a(14), most of these requirements are functional. Yet, the functions they define are often security functions related to strong identification and authentication, so it is not always simple to strictly differentiate between functional and security requirements.

Once the EUDIW scheme is adopted, a certificate covering a service providing EUDI Wallets and the eID schemes under which they are provided will cover all cybersecurity requirements. The national scheme would then need to cover mostly the functional conformance requirements, privacy requirements, as well as requirements related to the service itself, for instance on the free availability under some conditions.

The expected way of handling this would be to define a national certification scheme or certification system with three schemes, and an optional fourth one:

1. a valid EUDIW certificate for the cybersecurity aspects;
2. functional conformance testing by a lab, including at least a set of reference conformance tests;
3. an audit to assess conformity to the remaining requirements;
4. if applicable, a valid certification of conformity to Regulation (EU) 2016/679 and the data protection requirements defined in Article 5a.

These activities can be performed in specific conformity assessment schemes as part of a conformity assessment system, or as evaluation activities in the main certification scheme, according to the choices of the owner of the national scheme.

The relationship between the EUDIW cybersecurity scheme and the related functional schemes is not defined precisely, but since there is a mandatory functional testing activity to which the functional conformance could contribute significantly. If the EUDIW scheme is used, it could therefore be preferable to perform the functional conformance certification in advance of the cybersecurity certification, in order to reuse its results for its functional testing activity (an obligation of the CSA for assurance level 'high').

The national scheme would then need to include a review and certification decision, but the independent certification of conformity to cybersecurity requirements would greatly simplify the competence requirements for certification bodies in the national scheme.

In addition, for both functional and privacy requirements, the EUDIW scheme could cover them under some conditions:

- For all certificates issued at assurance level 'high' as defined in Article 52(7) of CSA, evaluation activities need to include "testing to demonstrate that [ICT services] correctly implement the necessary security functionalities at the state of the art". This implies that functional testing of security functions is already a requirement, here to demonstrate that they are implemented as specified. However, especially for all security functions that rely on standards for their implementation, conformance testing is often an important part of that testing, so the EUDIW testing requirements could satisfy the conformance testing requirements.
- Regarding privacy requirements, most of them are supported through protocols and controls that are in scope of the cybersecurity audit. The addition of the privacy requirements would not add much effort, as they are tightly related to cybersecurity requirements.

The main gain from this optimisation would be to gain in efficiency, and to avoid performing two very similar audits. Regarding functional conformance, an alternative approach would be to use the functional conformance certification as an input to the cybersecurity scheme.

Section XIV.3 highlights the differences between the requirements of the scheme and the requirements from 5c(1) on the two identified topics of functional conformance testing and privacy conformance evaluation.

XIV.2 Notification of eIDAS entities

There are many requirements in the draft candidate scheme to notify relevant supervisory authorities about important events. Among these, there are only a few that make an explicit reference to the eIDAS bodies.

Therefore, it would be very important to better define these interactions, and this can be done in two ways that complement each other:

- through a revision of CIR (EU) 2024/2981 to include requirements for the interface between the EUDIW scheme and the national certification schemes or systems, as well as the eIDAS supervisory bodies;
- in each national certification scheme or system.

In most cases, it would be preferable to use the national certificate schemes or systems as an interface between the European cybersecurity certification ecosystem and the EUDI Wallet ecosystem, because they are in the best position to understand both viewpoints and facilitate the required exchanges.

XIV.3 Conditions for using the EU certificate to optimise other processes

1. An EUDIW certificate may be considered to fulfil the requirements for certification of functional compliance of Article 5c(1), provided that it meets the following requirements.

(a) the tests that are used to demonstrate that the certified ICT service correctly implements the necessary security functionalities shall include the conformance tests that are listed in [TBD];
(b) the evaluation team shall have executed all the conformance tests that are listed in [TBD]

NOTE XIV.3.1: The conformance tests are currently under definition by the Commission, so the list of required conformance tests remains to be identified at this stage. An alternative would be to replace this list by a list of standards and technical specifications to which conformance would need to be demonstrated.

NOTE XIV.3.2: Paragraph (b) is due to the fact that the proposed requirement for independent testing is to base it on Common Criteria's ATE_IND.2, which only requires independent testing on a sample of tests.

2. An EUDIW certificate may be considered to fulfil the requirements for certification of privacy compliance of Article 5c(1), provided that the EUDIW criteria considered for the certificate include all the optional requirements from Annex X that include the "privacy" label.

NOTE XIV.3.3: There is a limited number of privacy requirements, which should then be included in the list of criteria as optional and appropriately labeled.

XV Terminology

Term	Definition
access control	means to ensure that physical and logical access to assets is authorised and restricted based on business and information security requirements [SOUCE: From ISO/IEC 27002:2022, 3.1.1]
access right	permission for a subject to access a particular object for a specific type of operation [SOURCE: From ISO/IEC 2382:2015, 2126298]
accreditation	third-party attestation related to a conformity assessment body, conveying formal demonstration of its competence, impartiality and consistent operation in performing specific conformity assessment activities [SOURCE: From ISO/IEC 17000:2020, 7.7]
accreditation body	conformity assessment body that performs accreditation Note 1 to entry: The authority of an accreditation body is generally derived from government. [SOURCE: From ISO/IEC 17000:2020, 2.6]
administration actions	set of actions for installing, deleting, modifying and consulting the configuration of a system participating in the service's information system and likely to modify its operation or security [SOURCE: From SecNumCloud Version 3.2, paragraph 1.3.2. Definitions (March 8, 2022)]
anonymisation	process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party [SOURCE: From ISO/IEC 29100:2011, 2.2]
application document	the document provided by a CSP to the CAB when applying for certification, which provides information about the cloud service to be certified
appropriate level of management	person or group of persons to whom top management has delegated a task or responsibility with the required mandate and authority Note 1 to entry: In security controls, the appropriate level of management would typically be responsible for topic-specific policies and procedures. [SOURCE: From CEN TS 18026:2024, 3.8]
appropriateness of evidence	The measure of the quality of evidence [SOURCE: From ISAE3000: 12.i.ii]

Term	Definition
asset	anything that has value to the organisation Note 1 to entry: In the context of information security, two kinds of assets can be distinguished: — the primary assets: — information; — business processes and activities; — the supporting assets (on which the primary assets rely) of all types, for example: — hardware; — software; — network; — personnel; — site; — organisation's structure. [SOURCE: From ISO/IEC 27002:2022, 3.1.2]
asset life	period from asset creation to asset end-of-life [SOURCE: From ISO 55000:2014, 3.2.2]
assumption	a factor in the conformity assessment process that is considered to be true, real, or certain, without proof or demonstration [From ISO/IEC/IEEE 24765:2017, 3.276]
assurance	grounds for justified confidence that a product, service or process meets specified requirements [SOURCES: Inspired from ISO/IEC 15408-1:3(2009).1.4 and from ISO/IEC/IEEE 15026-1(2019):3.1]
assurance information	information including a claim about a system, evidence supporting the claim, an argument showing how the evidence supports the achievement of the claim, and the context for these items [SOURCE: From ISO/IEC/IEEE 15026-1(2019):3.4]
assurance level	[CSA] a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned Note 1 to entry: A scheme often defines discrete assurance levels, and each such discrete level defines a degree of confidence in the fulfilment of requirements by the ICT product, ICT service, or ICT process. [SOURCE: From (EU) 2019/881, 2.21]
assurance level	[eIDAS] a basis for a defined level of confidence in the claimed or asserted identity of a person, characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate the risk of misuse or alteration of the identity at a defined level. Note 1 to entry: This definition includes the common elements of the three levels defined in Article 8. [SOURCE: From (EU) No 910/2014, Article 8]
attack	successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an asset or any attempt to expose, steal, or make unauthorized use of an asset. [SOURCE: From ISO/IEC 27002:2022, 3.1.3]

Term	Definition
attestation	issue of a statement, based on a decision, that fulfilment of specified requirements has been demonstrated Note 1 to entry: The resulting statement (…) is intended to convey the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, afford contractual or other legal guarantees. Note 2 to entry: First-party attestation and third-party attestation are distinguished by the terms declaration, certification, and accreditation, but there is no corresponding term applicable to second-party attestation. [SOURCE: From ISO/IEC 17000:2020, 7.3]
attribute	a characteristic, quality, right or permission of a natural or legal person or of an object [SOURCE: From Regulation (EU) No 910/2014, Article 3(43)]
audit	process for obtaining relevant information about an object of conformity assessment and evaluating it objectively to determine the extent to which specified requirements are fulfilled Note 1 to entry: The specified requirements are defined prior to performing an audit so that the relevant information can be obtained. Note 2 to entry: Examples of objects for an audit are management systems, processes, products and services. Note 3 to entry: For accreditation purposes, the audit process is called “assessment”. [SOURCE: From ISO 17000:2020, 6.4]
audit conclusion	outcome of an audit, after consideration of the audit objectives and all audit findings [SOURCE: From ISO 9000:2015, 3.13.10]
audit criteria	set of requirements used as a reference against which objective evidence is compared Note 1 to entry: Requirements may include policies, procedures, work instructions, legal requirements, contractual obligations, etc. [SOURCE: ISO 19011:2018, 3.7]
audit evidence	records, statements of fact or other information, which are relevant to the audit criteria and verifiable [SOURCE: FROM ISO/IEC 19011:2018, 3.9]
audit findings	results of the evaluation of the collected audit evidence against audit criteria [SOURCE: FROM ISO/IEC 19011:2018, 3.10]
audit plan	description of the activities and arrangements for an audit [SOURCE: From ISO 19011:2018, 3. 6]
audit programme	arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose [SOURCE: ISO 19011:2018, 3.4]
audit team	one or more persons conducting an audit, supported if needed by technical experts Note 1 to entry: One auditor of the audit team is appointed as the audit team leader. [SOURCE: ISO 9000:2015, 3.13.14]
audit time	time needed to plan and accomplish a complete and effective audit of the client’s service [SOURCE: From ISO/IEC 17021-1:2015, 3.16]
auditor	person who conducts an audit Note 1 to entry: In the schemes and related documents, 'the auditor' is typically used as the subject of requirements related to audit of the form "the auditor shall (...)". [SOURCE: From ISO/IEC 17021-1:2015, 3.6]

Term	Definition
authentic source	a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice [SOURCE: From Regulation (EU) No 910/2014, Article 3(47)]
authentication	[cybersecurity] provision of assurance that a claimed characteristic of an entity is correct [SOURCE: From ISO/IEC 27022:2022, 3.1.4 [identity] an electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form [SOURCE: From Regulation (EU) No 910/2014, Article 3(5)]
authenticity	property that an entity is what it claims to be [SOURCE: From ISO/IEC 27000:2018, 3.6]
authorisation	activity performed by a NCCA to verify that an accredited CAB meets the specific or additional requirements define in a European cybersecurity certification scheme [SOURCE: From EUCSA, Article 60(3)]
bridge letter	A document made available by a service organisation to cover a period of time between the reporting period end date of the current ISAE report and the release of a new ISAE report. Note to entry: bridge letters are needed in complements to ISAE reports that do not make forward-looking statements, to provide some guarantee that the vendor still operates the controls that have been audited in the previous reports, and declares any changes to its control framework [SOURE: ISAE]
business continuity	capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption [SOURCE: From ISO 22301:2019, 2019, 3.3]
business continuity plan	documented information that guides an organisation to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives [SOURCE: From ISO 22301:2019, 2019, 3.4]
business impact analysis	process of analysing the impact over time of a disruption on the organisation Note 1 to entry: The outcome is a statement and justification of business continuity requirements. [SOURCE: From ISO 22301:2019, 2019, 3.5]
capacity management	process for monitoring, analysis, reporting and improvement of capacity [SOURCE: From ISO/IEC TS 22237-7:2018, 3.1.2]
certification	third-party attestation related to an object of conformity assessment, with the exception of accreditation [SOURCE: From ISO/IEC 17000:2020, 7.6]

Term	Definition
certification audit **joint audit** **combined audit** **integrated audit**	audit carried out by an auditing organisation independent of the client and the parties that rely on certification, for the purpose of certifying the client's service Note 1 to entry: Unless specifically qualified (e.g., “internal audit”), in the definitions which follow, the term “audit” has been used for simplicity to refer to third-party certification audit. Note 2 to entry: Certification audits include initial, surveillance, re-certification audits, and can also include special audits. Note 3 to entry: A joint audit is when two or more auditing organisations cooperate to audit a single client. Note 4 to entry: A combined audit is when a client is being audited against the requirements of two or more standards together. Note 5 to entry: An integrated audit is when a client has integrated the application of requirements of two or more standards into a single service and is being audited against more than one standard. Note 6 to entry: Removed references to management systems and the original Note 3. [SOURCE: From ISO/IEC 17021-1:2015, 3.4]
certification body	third-party conformity assessment body operating certification schemes Note 1 to entry: A certification body can be non-governmental or governmental (with or without regulatory authority). Note to entry: In the present document, the term certification body is used specifically to refer to a conformity assessment body that issues certificates, and conformity assessment body is used when referring to evaluation tasks that may be delegated to other bodies. [SOURCE: From ISO/IEC 17065:2012, 3.12, Note added]
certification report	document that accompanies the certificate, and provides a simple presentation of the certified service and a summary of the conformity assessment activities
certification requirement	specified requirement, including service requirements, that is fulfilled by the client as a condition of establishing or maintaining certification Note to entry: This is the most high-level definition, which covers all kinds of requirements that need to be met in order to be certified. [SOURCE: From ISO/IEC 17065:2012, definition 3.7]
certification scheme	conformity assessment scheme that includes a certification activity Note 1 to entry: In a certification scheme, a successful assessment leads to the issuance of a certificate.
change management	process for recording, coordination, approval and monitoring of all changes [SOURCE: From ISO/IEC TS 22237-7:2018, 3.1.3]
characteristic	distinguishing feature Note 1 to entry: A characteristic can be inherent or assigned. Note 2 to entry: A characteristic can be qualitative or quantitative. [SOURCE: From ISO 9000:2015, 3.10.1]
claim	information declared by the client (3.13) Note 1 to entry: The claim is the object of conformity assessment by validation (3.2)/verification (3.3). Note 2 to entry: The claim can represent a situation at a point in time or could cover a period of time. Note 3 to entry: The claim should be clearly identifiable and capable of consistent evaluation or measurement against specified requirements by a validation body (3.4)/verification body (3.5). Note 4 to entry: The claim can be provided in the form of a report, a statement, a declaration, a project plan, or consolidated data. [SOURCE: From ISO/IEC 17029:2019, 3.1]

Term	Definition
client	organisation whose service is being audited for certification purposes Note 1 to entry: “management system” has been replaced by “service” [SOURCE: Adapted from ISO/IEC 17021-1:2015, 3.5]
code of conduct	document specifying the ethical or personal behaviour required by a CSP from its employees [SOUCE: Adapted from ISO/IEC TS 17027:2014, 2.23]
compensating control	an internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions [SOURCE: SOC2]
competence	ability to apply knowledge and skills to achieve intended results [SOURCE: From ISO/IEC 17021:2015, 3.7]
complaint	expression of dissatisfaction by any person or organisation to a CAB or accreditation body or to the CAB’s NCCA, relating to the activity of that CAB, where a response is expected [SOURCE: Adapted from ISO/IEC 17000:2020, 8.7]
compliance	conformity in the context of the rules and requirements defined in a certification scheme that apply to the provider of the certified product, service or process Note 1 to entry: This is a refinement of ISO19011, which defines compliance as conformity in the context of a statutory requirement or regulatory requirement. In this case, compliance is conformity in the context of a given scheme. Note 2 to entry: The term is used to differentiate between compliance of a cloud service provider to the requirements defined in the scheme and conformity of a cloud service to the requirements on controls defined in the scheme. [SOURCE: Inspired from ISO 19011:2018, 3.7]
component	smallest selectable set of elements on which requirements may be based [SOURCE: From ISO/IEC 15408-1:2022, 3.17]
compromise	loss of confidentiality, integrity, or availability of information, including any resultant impairment of (1) processing integrity or availability of systems or (2) the integrity or availability of system inputs or outputs [SOURCE: TSC]
configuration management	management activity that applies technical and administrative direction over the life cycle of a product and service, its configuration identification and status, and related product and service configuration information [SOURCE: From ISO/IEC TS 10007:2017, Introduction]
conformity	fulfilment of a requirement Note 1 to entry: when used in opposition with compliance, conformity relates to the requirements related to the object of conformity assessment rather than to the requirements related to the certification scheme. [SOURCE: From ISO/IEC 19011:2018, 3.20]
conformity assessment	demonstration that specified requirements are fulfilled Note 1 to entry: The process of conformity assessment (…) can have a negative outcome, i.e. demonstrating that the specified requirements are not fulfilled. Note 2 to entry: The subject field of conformity assessment includes selection activities, determination activities such as testing, inspection and audit, review activities, and attestation activities such as certification, as well as the accreditation of conformity assessment bodies. Note 3 to entry: EN ISO/IEC 17000 does not include a definition of “conformity”. “Conformity” does not feature in the definition of “conformity assessment”. Nor does EN ISO/IEC 17000 address the concept of compliance. [SOURCE: From ISO/IEC 17000:2020, 4.1, some modifications in notes]

Term	Definition
conformity assessment body **CAB**	body that performs conformity assessment services, excluding accreditation Note to entry: The term conformity assessment body is used to refer to bodies that perform conformity assessment tasks in general, and the term certification body to refer to bodies that issue certificates. [SOURCE: From ISO/IEC 17000:2020, 4.6, note added]
conformity assessment scheme	set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing conformity assessment Note 1 to entry: A conformity assessment scheme can be managed within a conformity assessment system. Note 2 to entry: A conformity assessment scheme can be operated at an international, regional, national sub-national, or industry sector level. Note 3 to entry: A scheme can cover all or part of the conformity assessment functions. [SOURCE: From ISO/IEC 17000:2020, 4.9]
conformity assessment system	set of rules and procedures for the management of similar or related conformity assessment schemes Note 1 to entry: A conformity assessment system can be operated at an international, regional, national, sub-national, or industry sector level. [SOURCE: From ISO/IEC 17000:2020, 4.8]
conformity self-assessment	first-party conformity assessment activities, which evaluate whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme Note 1 to entry: The original definition from EC 881-2019 has been reworded to make the link with the definition of a first-party conformity assessment activity, but the meaning remains unchanged. [SOURCE: From (EU) 2019/881:2.22]
consultancy	participation in a) the designing, manufacturing installing, maintaining or distributing of a certified product or a product to be certified, or b) the designing, implementing, operating or maintaining of a certified process or a process to be certified, or c) the designing, providing or maintaining of a certified service or a service to be certified [SOURCE: From ISO/IEC 17065:2012, 3.2]
control	measure that maintains and/or modifies risk Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice or other conditions and/or actions which maintain and/or modify risk. Note 2 to entry: Controls may not always exert the intended or assumed modifying effect. [SOURCE: From ISO 31000:2018, 3.8 / ISO/IEC 27002:2022, 3.1.8]
control objective	statement describing what is to be achieved as a result of implementing controls [SOURCE: ISO/IEC 27000:2018, 3.15]
control risk	the risk that an event that prevents a security requirement from being met will not be prevented or detected and corrected on a timely basis by the controls [Adapted from ISAE]

Term	Definition
credential	representation of an identity Note 1 to entry: A credential is typically made to facilitate data authentication of the identity information in the identity it represents. Note 2 to entry: The identity information represented by a credential can be printed on paper or stored within a physical token that typically has been prepared in a manner to assert the information as valid. EXAMPLE: A credential can be a username, a username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc. [SOURCE: From ISO/IEC 24760-1:2011, 3.3.5]
criteria	rules on which a judgment or decision can be based, or by which a product, service, result, or process can be evaluated [SOURCE: From ISO/IEC/IEEE 15289:2019, 3.1.6]
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, 2.11, note added]
cybersecurity	the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats [SOURCE: From Regulation (EU) 2019/881, Article 2(1)]
Cybersecurity Act **EUCSA**	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
cyber threat	any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons [SOURCE: From Regulation (EU) 2019/881, Article 2(8)]
data at rest	data recorded on stable, non-volatile storage [SOURCE: From ISO/IEC 27040:2024, 3.2.3]
data centre	structure, or group of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network telecommunications equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control together with the necessary levels of resilience and security required to provide the desired service availability Note 1 to entry: A structure can consist of multiple buildings and/or spaces with specific functions to support the primary function. Note 2 to entry: The boundaries of the structure or space considered the data centre, which includes the information and communication technology equipment and supporting environmental controls, can be defined within a larger structure or building. [SOURCE: From ISO/IEC 30134-1:2016, 3.6]
data in motion **data in transit**	data being transferred from one location to another Note 1 to entry: These transfers typically involve interfaces that are accessible and do not include internal transfers (i.e., never exposed to outside of an interface, chip, or device). [SOURCE: From ISO/IEC 27040:2015, 3.8]
data record	electronic data recorded with related meta- data supporting the processing of the data [SOURCE: From Regulation (EU) No 910/2014, Article 3(56)]

Term	Definition
decision	conclusion, based on the results of review, that fulfilment of specified requirements has or has not been demonstrated [SOURCE: From ISO/IEC 17000:2020, 7.2]
declaration	first-party attestation [SOURCE: From ISO/IEC 17000:2020, 7.5]
de-identification process	process of removing the association between a set of identifying attributes and the data principal [SOURCE : From ISO/IEC 20889:2018, 3.6]
design effectiveness	Refers to the suitability of the control as of a specified date or for a specified period (typically 6 to 12 months), based on the auditor's conclusion on whether (i) the risks that threaten the achievement of the control objectives have been identified by management; (ii) the controls would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives from being achieved. [SOURCE: Inspired from ISAE3402]
detective control	A control that detects and reports when errors, omissions and unauthorised uses or entries occur [SOURCE: SOC2]
determination	activities undertaken to develop complete information regarding fulfilment of the specified requirements by the object of conformity assessment or its sample [SOURCE: From ISO/IEC 17000:2020, A.3.1]
development environment	The environment in which changes to software are developed NOTE: The environment may be local to an individual developer's workstation or distributed, possibly based on external services
disruption	incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organisation's objectives [SOURCE: From ISO 22301:2019, 2019, 3.10]
document	recorded information or material object, which can be treated as a unit [SOURCE: From ISO 5127:2001, 1.2.02]
effectiveness	extent to which planned activities are realised and planned results achieved [SOURCE: ISO Supplement:3.6]
electronic attestation of attributes **EAA**	an attestation in electronic form that allows attributes to be authenticated [SOURCE: From Regulation (EU) No 910/2014, Article 3(44)]
electronic identification **eID**	the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person [SOURCE: From Regulation (EU) No 910/2014, Article 3(1)]
electronic identification means **eID means**	a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service [SOURCE: From Regulation (EU) No 910/2014, Article 3(2)]
electronic identification scheme **eID scheme**	a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons [SOURCE: From Regulation (EU) No 910/2014, Article 3(4)]

Term	Definition
electronic signature	data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign [SOURCE: From Regulation (EU) No 910/2014, Article 3(10)]
employee	a person under contract with the provider to whom human resource management controls apply
EU statement of conformity	declaration produced by a vendor of ICT product, ICT process, or ICT service after performing a conformity self-assessment in the context of a European cybersecurity certification scheme, that states that a specific ICT product, ICT service or ICT process complies with the requirements of the European cybersecurity certification scheme [SOURCE: Inspired from Regulation (EU) 2019/881, recital (81)]
European Cybersecurity Certification group **ECCG**	A group composed of representatives of national cybersecurity certification authorities or other relevant national authorities [SOURCE: Adapted from Cybersecurity Act, Article 62]
European cybersecurity certification scheme	a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes Note 1 to entry: This definition is a refinement of the definition of a certification scheme. [SOURCE: From (EU) 2019/881:2.9]
European Digital Identity Framework **EDIF**	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
European Digital Identity Wallet **EUDI Wallet** **wallet**	an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals [SOURCE: From Regulation (EU) No 910/2014, Article 3(42)]
EU Digital Identity Wallet Trust Mark	a verifiable, simple and recognisable indication which is communicated in a clear manner that a European Digital Identity Wallet has been provided in accordance with the eIDAS regulation [SOURCE: From Regulation (EU) No 910/2014, Article 3(50), slightly modified]
evaluation	combination of the selection and determination functions of conformity assessment activities [SOURCE: From ISO/IEC 17065:2012, 3.3]
evaluation technical report **ETR**	[CC] documentation of the overall verdict and its justification, produced by the evaluator, and submitted to an evaluation authority [SOURCE: From ISO 15408-1: 2022, 3.43]
events log	log which records audit trail data related to the system operations [SOURCE: From ISO 14641:2018, 3.2]
expiry	ending of the validity of the statement of conformity after a specified period [SOURCE: From ISO/IEC 17000:2020, 8.4]
fair presentation	accurate, truthful and transparent description Note: This is typically applied to the client's description of its service [SOURCE: Inspired from AICPA SOC2]

Term	Definition
feature	abstract functional characteristic of a system of interest that end-users and other stakeholders can understand Note 1 to entry: In systems engineering, features are syntheses of the needs of stakeholders. These features will be used, amongst others, to build the technical requirement baselines. [SOURCE: From ISO/IEC 26550:2015, 3.14]
first-party	the person or organisation that provides the object of conformity assessment [SOURCE: From ISO/IEC 17000:2020, 2.2]
first-party conformity assessment activity	conformity assessment activity that is performed by the person or organisation that provides the object of conformity assessment [SOURCE: From ISO/IEC 17000:2020, 4.3]
fraud	intentional dishonest act causing actual or potential gain or loss that creates social or economic harm Note 1 to entry: Fraud also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit. Note 2 to entry: Fraudulent conduct need not necessarily represent a breach of law. Note 3 to entry: Fraud can involve fraudulent conduct by internal and/or external parties targeting the organization or fraudulent conduct by the organization itself targeting external parties. Note 4 to entry: Fraud can include loss of moneys or other property by persons internal and external to the organization and where deception is used at the time, immediately before or immediately following the activity. Note 5 to entry: Fraud can be external or internal or both. External fraud is where no perpetrator is employed by or has a close association with the target organization. Internal fraud is where at least one perpetrator is employed by or has a close association with the target organization and has detailed internal knowledge of the organization's operations, systems and procedures. [SOURCE: From ISO/IEC 37003:2025, 3.1]
fraud event	instance of fraud against or by an organization [SOURCE: From ISO/IEC 37003:2025, 3.2]
functional component	functional building block needed to engage in an activity, backed by an implementation [SOURCE: From ISO/IEC 22123-1:2023, 3.3.9]
guide	person appointed by the client to assist the audit team [SOURCE: From ISO/IEC 17021-1:2015, 3.8]
ICT process	a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service Note 1 to entry: This term is to be used when a process is intended to be the object of a cybersecurity certification. The term 'process' is more general and should be used in other situations. [SOURCE: From EUCSA, Article 2(14)]
ICT product	an element or a group of elements of a network or information system Note 1 to entry: In the definition of certification schemes, the use of 'ICT product' follows this definition from EC 881-2019, and will mostly be used to refer to certification schemes and products certified using such schemes. It is a subset of the more general term product, whose definition originates in ISO9000. [SOURCE: From EUCSA, Article 2(12)]

Term	Definition
ICT service	a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems Note 1 to entry: In the definition of certification schemes, the use of 'ICT service' follows this definition from EC 881-2019, and will mostly be used to refer to certification schemes and products certified using such schemes. For a more general use, it is preferable to use the term 'service'. [SOURCE: From EUCSA, Article 2(13)]
identity matching	a process where person identification data, or electronic identification means are matched with or linked to an existing account belonging to the same person [SOURCE: From Regulation (EU) No 910/2014, Article 3(55)]
impact	outcome of a disruption affecting objectives [SOURCE: From ISO 22301:2019, 3.10]
impartiality	presence of objectivity [SOURCE: From ISO/IEC 17065:2012, 3.13]
incident	any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. [SOURCE: EN 319 401]
incident handling	actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents [SOURCE: From ISO/IEC 27035-1:2023, 3.1.8]
incident response	actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it [SOURCE: From ISO/IEC 27035-1:2023, 3.1.9]
information	meaningful data [SOURCE: ISO 9000:2015, 3.8.2]
information security	preservation of confidentiality, integrity and availability of information [SOURCE: From ISO/IEC 27000:2016, 2.33]
information security breach	compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed. [SOURCE: From ISO/IEC 27002:2022, 3.1.13]
information security event **security event**	occurrence indicating a possible breach of information security or failure of controls [SOURCE: From ISO/IEC 27035-1:2023, 3.1.4]
information security incident **security incident** **incident**	one or multiple related and identified information security events that can harm an organisation's assets or compromise its operations [SOURCE: From ISO/IEC 27035-1:2023, 3.1.5]
information security incident management **incident management**	exercise of a consistent and effective approach to the handling of information security incidents [SOURCE: From ISO/IEC 27002:2022, 3.1.16]
information security management system **ISMS**	part of the overall management system, based on a business risk approach, used to establish, implement, operate, monitor, review, maintain and improve information security [SOURCE: From ISO/TS 12812-2:2017, 3.11]
inquiry	activity consisting of seeking information of knowledgeable persons, within the entity or outside the entity [SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]

Term	Definition
Inspection	[CASCO] examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements Note 1 to entry: Examination can include direct or indirect observations, which can include measurements or the output of instruments. Note 2 to entry: Conformity assessment schemes or contracts can specify inspection as examination only. [SOURCE: From ISO/IEC 17000:2020, 6.3]
inspection	[IAASB] an activity involving the examination of records or documents, whether internal or external, in paper form, electronic form, or on other media, or a physical examination of evidence [SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]
interested party **stakeholder**	person or organisation that can affect, be affected by, or perceive itself to be affected by a decision or activity [SOURCE: ISO Supplement:3.2]
internal audit	audit conducted by, or on behalf of, an organisation itself for management review and other internal purposes, and which can form the basis for an organisation's self-declaration of conformity Note 1 to entry: In many cases, particularly in smaller organisations, independence can be demonstrated by the freedom from responsibility for the activity being audited. [SOURCE: From ISO 22300:2021, 3.1.134]
large scale cybersecurity incident	incident whose disruption exceeds a Member State's capacity to respond to it or with a significant impact on at least two Member States [SOURCE: From Directive (EU) 2022/2555]
life cycle	stages involved in the management of an asset Note 1 to entry: The naming and number of the stages and the activities under each stage usually vary in different industry sectors and are determined by the organisation. [SOURCE: From ISO 55000:2014, 3.2.3]
limited assurance	assurance type where the nature and extent of the evaluation activities have been designed to provide a reduced level of assurance. Note 1 to entry: The evaluator's conclusion is expressed in a form that conveys whether, based on the evaluation activities performed and evidence obtained, a matter(s) has come to the evaluator's attention to cause the evaluator to believe the object of conformity assessment presents nonconformities. Note 2 to entry: The evaluator's conclusion in a limited assurance engagement is framed in a negative sense, for instance: " Based on the procedures performed, nothing came to our attention to indicate that the cloud service XYZ does not satisfy the certification requirements of the **Error! Unknown document property name.** at assurance level LLL." [SOURCE: Inspired from ISO 14064-3:2019, 3.6.7]
major nonconformity	nonconformity that affects the capability of the management system to achieve its intended results Note 1 to entry: Nonconformities could be classified as major in the following circumstances: - if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements; - a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity. [SOURCE: Adapted from ISO/IEC 17021-1:2015, 3.12]

Term	Definition
malware **malicious software**	Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability Note 1 to entry: Viruses and Trojan horses are examples of malware. [SOURCE: ISO/IEC 27033-1:2015, 3.22]
management system	set of interrelated or interacting elements of an organisation to establish policies and objectives, and processes to achieve those objectives Note 1 to entry: A management system can address a single discipline or several disciplines. Note 2 to entry: The system elements include the organisation's structure, roles and responsibilities, planning and operation. Note 3 to entry: The scope of a management system may include the whole of the organisation, specific and identified functions of the organisation, specific and identified sections of the organisation, or one or more functions across a group of organisations. [SOURCE: From ISO/IEC 27000:2018, 3.41]
material	significant to intended users Note 1 to entry: Materiality is the concept that misstatements, individually or aggregated, can influence the reliability of the claim or decisions made by the intended user. Note 2 to entry: Materiality can be qualitative or quantitative. [SOURCE: From ISO/IEC 17029:2019, 3.16]
minor nonconformity	nonconformity that does not affect the capability of the management system to achieve its intended results [SOURCE: Adapted from ISO/IEC 17021-1:2015, 3.12]
monitoring	determining the status of a system, a process or an activity Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe. [SOURCE: ISO/IEC 27000:2018, 3.46]
multifactor authentication	authentication mechanism consisting of two or more of the independent categories of credentials (knowledge, possession, and inherence factor) to verify the user's identity for a login or other transaction [SOURCE: EN 319 401
national cybersecurity certification scheme **national scheme**	a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme Note 1 to entry: This definition is a refinement of the definition of a certification scheme. [SOURCE: From Regulation (EU) 2019/881, 2.10]
national accreditation body **NAB**	the sole body in a Member State that performs accreditation with authority derived from the State [SOURCE: From Regulation (EC) No 765/2008, 2.1]
near miss	event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but was successfully prevented from transpiring or did not materialize. [SOURCE: From Directive (EU) 2022/2555, Article 6(5)]
non-compliance	nonconformity in the context of the rules and requirements defined in a certification scheme Note 1 to entry: This is a refinement of ISO19011, which defines non-compliance as nonconformity in the context of a statutory requirement or regulatory requirement. Here, compliance is conformity in the context of a given scheme. [SOURCE: Inspired from ISO 19011:2018, 3.7]

Term	Definition
nonconformity	non-fulfilment of a requirement Note 1 to entry: when used in opposition with non-compliance, conformity relates to the requirements related to the object of conformity assessment rather than to the requirements related to the certification scheme. [SOURCE: From ISO/IEC 17021-1:2015, 3.11]
object of conformity assessment **object**	entity to which specified requirements apply EXAMPLE: Product, process, service, system, installation, project, data, design, material, claim, person, body or organisation, or any combination thereof. [SOURCE: From ISO/IEC 17000:2020, 4.2, Note 2]
objective	result to be achieved Note 1 to entry: An objective can be strategic, tactical, or operational. Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, organisation-wide, project, product and process]. Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an information security objective or by the use of other words with similar meaning (e.g. aim, goal, or target). Note 4 to entry: In the context of information security management systems, information security objectives are set by the organisation, consistent with the information security policy, to achieve specific results. [SOURCE: From ISO/IEC 27000:2018, 3.49]
objective evidence **evidence**	data supporting the existence or verity of something Note 1 to entry: Objective evidence can be obtained through observation, measurement, test, or by other means. Note 2 to entry: Objective evidence for the purpose of audit generally consists of records, statements of fact or other information which are relevant to the audit criteria and verifiable. [SOURCE: From ISO 9000:2015, 3.8.3]
observation	activity consisting of looking at a process or procedure being performed by others [SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]
observer	person who accompanies the audit team but does not audit [SOURCE: From ISO/IEC 17021-1:2015, 3.9]
offline mode	as regards the use of European Digital Identity Wallets, an interaction between a user and a third party at a physical location using close proximity technologies, whereby the European Digital Identity Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction [SOURCE: From Regulation (EU) No 910/2014, Article 3(57)]
operating effectiveness	A control is operating effectively, if (i) it was consistently applied as designed throughout the specified period, and (ii) in case of manual controls, they were applied by individuals who have the appropriate competence and authority. [SOURCE: Inspired from ISAE3402]
operational requirement	requirement that relates directly to the operation of a service, specified in standards or in other normative documents identified by the certification scheme [SOURCE: Inspired from ISO/IEC 17065:2012, 3.8]

Term	Definition
organisation	person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives Note 1 to entry: The concept of organisation includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private. [SOURCE: From ISO/IEC 27000:2018, 3.50]
output	result of a process Note 1 to entry: Whether an output of the organisation is a product or a service depends on the preponderance of the characteristics involved, e.g. a painting for sale in a gallery is a product whereas supply of a commissioned painting is a service, a hamburger bought in a retail store is a product whereas receiving an order and serving a hamburger ordered in a restaurant is part of a service. [SOURCE: From ISO 9000:2015, 5.6]
outsourcing	acquisition of services (with or without products) in support of a business function for performing activities using supplier's resources rather than the acquirer's Note 1 to entry: For the purposes of this document the terms "outsourcing" and "subcontracting" are considered to be synonyms. [SOURCE: From ISO/IEC 27036-1:2015, 3.6] [SOURCE Note 1: From ISO/IEC 17065:2012, $ 6.2.2.1]
peer assessment	assessment of a body against specified requirements by representatives of other bodies in, or candidates for, an agreement group Note 1 to entry: This entry is not satisfactory for several reasons, and in particular because it refers to concepts that are not currently defined (agreement group) and have little interest for us, and also mentions of a "body", which is unclear. Note 2 to entry: On the other hand, this could cover both CABs at level 'high' and NCCAs, but some rewriting is required. [SOURCE: From ISO/IEC 17000:2020, 4.5]
penetration testing	Authorised simulated cyberattack on a computer system, performed to evaluate the security of the system. [SOURCE: Adapted from Wikipedia]
persistent data	data which is retained in the information system for more than one data management session [SOURCE: From ISO/IEC TR 10032: 2003, 2.54]
person identification data	a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person [SOURCE: Regulation (EU) No 910/2014, Article 3(3)]
personnel	persons doing work under the CSP's direction Note 1 to entry: The concept of personnel includes the CSP's members, such as the governing body, top management, employees, temporary staff, contractors and volunteers. [SOURCE: Adapted from ISO/IEC 27002:2022, 3.1.20]
point of contact	defined organisational function or role serving as the coordinator or focal point of information concerning incident management activities [SOURCE: From ISO/IEC 27035-1:2023, 3.1.10]
policy	intentions and direction of an organisation, as formally expressed by its top management [SOURCE: From ISO/IEC 27000:2018, 3.53]
pre-production environment	Mirror of production environment used for final testing or debugging

Term	Definition
preventive control	An internal control that is used to avoid undesirable events, errors and other occurrences that an enterprise has determined could have a negative material effect on a process or end product [SOURCE: SOC2]
procedure	specified way to carry out an activity or a process Note 1 to entry: In this context, a process is defined as a set of interrelated or interacting activities that use inputs to deliver an intended result. [SOURCE: From ISO/IEC 17000:2020, 5.2]
process	set of interrelated or interacting activities which transforms inputs into outputs [SOURCE: From ISO Supplement:3.12]
product	result of a process Note 1 to entry: Four generic product categories are noted in ISO 9000:2005: — services (e.g. transport) (see definition in 3.6); — software (e.g. computer program, dictionary); — hardware (e.g. engine, mechanical part); — processed materials (e.g. lubricant). Many products comprise elements belonging to different generic product categories. Whether the product is then called service, software, hardware or processed material depends on the dominant element. Note 2 to entry: Products include results of natural processes, such as growth of plants and formation of other natural resources. Note 3 to entry: Adapted from ISO/IEC 17000:2004, definition 3.3. [SOURCE: From ISO/IEC 17065:2012, 3.4]
production environment	The environment that serves customers
qualified electronic attestation of attributes	an electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V of eIDAS [SOURCE: From Regulation (EU) No 910/2014, Article 3(45)]
qualified electronic signature	an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures [SOURCE: From Regulation (EU) No 910/2014, Article 3(12)]
qualified trust service	a trust service that meets the applicable requirements laid down in the eIDAS regulation [SOURCE: From Regulation (EU) No 910/2014, Article 3(17)]
qualified trust service provider	a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body [SOURCE: From Regulation (EU) No 910/2014, Article 3(20)]
reasonable assurance	assurance type where the nature and extent of the evaluation activities have been designed to provide a high but not absolute level of assurance. Note 1 to entry: The evaluator's conclusion is expressed in a form that conveys the evaluator's opinion on the outcome of the evaluation of the object of evaluation against applicable criteria. Note 2 to entry: The evaluator's conclusion in a reasonable assurance engagement is framed in a positive sense, for instance: "Based on the activities performed, in our opinion, the cloud service XYZ satisfies the certification requirements of the **Error! Unknown document property name.** at evaluation level LLL." [SOURCE: Inspired from ISO 14064-3:2019, 3.6.6]

Term	Definition
relying party	a natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service [SOURCE: From Regulation (EU) No 910/2014, Article 3(6)]
reperformance	The auditor's independent execution of procedures or controls that were originally performed as part of the customer's internal controls [SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]
requirement	need or expectation that is stated, generally implied or obligatory Note 1 to entry: "Generally implied" means that it is custom or common practice for the organisation and interested parties that the need or expectation under consideration is implied. Note 2 to entry: A specified requirement is one that is stated, for example in documented information. Note 3 to entry: A qualifier can be used to denote a specific type of requirement, e.g. product requirement, service requirement, customer requirement. [SOURCE: From ISO/IEC 27000:2018, 3.56]
residual risk	risk remaining after risk treatment Note 1 to entry: Residual risk can contain unidentified risk. Note 2 to entry: Residual risk can also be known as "retained risk". [SOURCE: From ISO Guide73:2009, 3.8.1.6]
restoration	reinstatement of the full or partial statement of conformity [SOURCE: From ISO/IEC 17000:2020, 8.5]
review	determination of the suitability, adequacy or effectiveness of an object to achieve established objectives EXAMPLE: Management review, design and development review, review of customer requirements, review of corrective action and peer review. Note 1 to entry: Review can also include the determination of efficiency. [SOURCE: From EN ISO 9000:2015, 3.11.2]
review	<certification> consideration of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to fulfilment of specified requirements by an object of conformity assessment [SOURCE: From ISO/IEC 17000:2020, 7.1]
review report	the document written by the CAB after performing the review of the evaluation performed by the audit team
risk	effect of uncertainty on objectives Note 1 to entry: An effect is a deviation from the expected — positive and/or negative. Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process). Note 3 to entry: Risk is often characterised by reference to potential events and consequences, or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. [SOURCE: From ISO 31073:2022, 3.1.1]

Term	Definition
risk analysis	process to comprehend the nature of risk and to determine the level of risk Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Note 2 to entry: Risk analysis includes risk estimation. [SOURCE: From ISO 31073:2022, 3.3.1]
risk assessment	overall process of risk identification, risk analysis and risk evaluation [SOURCE: From ISO 31073:2022, 3.3.8]
risk evaluation	process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable Note 1 to entry: Risk evaluation assists in the decision about risk treatment. [SOURCE: From ISO 31073:2022, 3.3.2]
risk identification	process of finding, recognising and describing risks Note 1 to entry: Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs. [SOURCE: From ISO 31073:2022, 3.3.9]
risk management	coordinated activities to direct and control an organisation with regard to risk [SOURCE: From ISO 31073:2022, 3.2.1]
risk of material misstatement	The risk that the subject matter information is materially misstated prior to the start of the engagement [SOURCE: From ISAE3000: 12.w]
risk owner	person or entity with the accountability and authority to manage a risk [SOURCE: From ISO 31073:2022, 3.3.14]
risk treatment	process to modify risk (1.1) Note 1 to entry: Risk treatment can involve: • avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; • taking or increasing risk in order to pursue an opportunity; • removing the risk source; • changing the likelihood; • changing the consequences; • sharing the risk with another party or parties [including contracts and risk financing]; and • retaining the risk by informed decision. Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”. Note 3 to entry: Risk treatment can create new risks or modify existing risks. [SOURCE: From ISO 31073:2022, 3.3.32]
role	set of activities that serves a common purpose [SOURCE: From ISO/IEC 22123-1:2023, 3.3.10]

Term	Definition
role-based access control **RBAC**	security technique for authentication that authorises operations or allows access to resources based upon the user's identity and his/her relationship to other users and entities EXAMPLE 1: A teacher has read/write access to the grades for his/her students (role: "the teacher of the student"), but no access to other students' grades EXAMPLE 2: A principal has read-only access to the grades of all of his/her teachers' students (role: "the principal of the teachers of the students"), but the principal is not permitted to change any grades [SOURCE: From ISO/IEC 20944-1:2013, 3.21.20.2]
sampling	selection and/or collection of material or data regarding an object of conformity assessment Note 1 to entry: Selection can be on the basis of a procedure, an automated system, professional judgement etc. Note 2 to entry: Selection and collection can be performed by the same or different persons or organisations. [SOURCE: From ISO/IEC 17000:2020, 6.1]
scope of certification	identification of — the service(s) for which the certification is granted, — the applicable certification scheme and scheme options, and — the standard(s) and other normative document(s), including their date of publication, to which it is judged that the service(s) comply Note to entry: The definition has been altered to include “scheme options”, which may in the context of the EUCS cover in particular the selected evaluation level and extension profiles. [SOURCE: Adapted from ISO/IEC 17065:2012, 3.10]
security assurance	grounds for justified confidence that a claim about meeting security objectives has been or will be achieved [SOURCE: From ISO/IEC/IEEE 15026-1(2019):3.4]
security problem	statement which in a formal manner defines the nature and scope of the security that the object of conformity assessment is intended to address Note 1 to entry: This statement consists of a combination of: — threats to be countered by the object of conformity assessment, — the OSPs enforced by the object of conformity assessment, and — the assumptions that are upheld for the object of conformity assessment and its operational environment. [SOURCE: Adapted from ISO/IEC 15408-1:2009, 3.1.61]
security zone	area of a network in which limited data exchange with areas outside is allowed [SOURCE: From ISO/TR 11636:2009, 2.13]
selection	planning and preparation activities in order to collect or produce all the information and input needed for the subsequent determination function Note 1 to entry: Selection activities vary widely in number and complexity. In some instances, very little selection activity may be needed. [SOURCE: From ISO/IEC 17000:2020, A.2.1]
service	output of an organisation with at least one activity necessarily performed between the organisation and the customer Note 1 to entry: This definition from ISO9000 echoes the definition of a product, and is refined into the notion of information service from European Regulation 1535/2015. [SOURCE: From ISO 9000:2000, 3.7.7]
service requirement	requirement that relates directly to a service, specified in standards or in other normative documents identified by the certification scheme [SOURCE: Adapted from ISO/IEC 17065:2012, 3.8]

Term	Definition
specified requirement	need or expectation that is stated Note 1 to entry: Specified requirements may be stated in normative documents such as regulations, standards and technical specifications. Note 2 to entry: Specified requirements can be detailed or general Note 3 to entry: In the context of a European cybersecurity certification scheme, the specified requirements typically correspond to the requirements specified in the scheme, either directly or indirectly (in normative documents referred to in the scheme). [SOURCE: From ISO/IEC 17000:2020, 5.1]
Stakeholder Cybersecurity Certification Group SCCG	Advisory group composed of members selected from among recognised experts representing the relevant stakeholders [SOURCE: Adapted from Cybersecurity Act, Article 22]
state-of-the-art	developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience Note 1 to entry: The state of the art embodies what is currently and generally accepted as good practice in technology and medicine. The state of the art does not necessarily imply the most technologically advanced solution. The state of the art described here is sometimes referred to as the "generally acknowledged state of the art". [SOURCE: From ISO/IEC Guide 63:2019, 3.18]
state-of-the-art document	a document which specifies evaluation methods, techniques and tools that apply to the certification of ICT services, or any other requirements necessary for certification, in order to harmonise evaluation [SOURCE: Adapted from (EU) 2024/482 (EUCC), Article (2)(14)]
strategy	planned activities to achieve a long term or overall objective [SOURCE: ISO 9000:2015, 3.5.12]
strong	not easily defeated, having strength or power greater than average or expected, able to withstand attack or solidly built [SOURCE: From ISO/IEC 19790:2012, 3.123]
strong user authentication	an authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data [SOURCE: From Regulation (EU) No 910/2014, Article 3(51)]
subsystem	a set of elements, which is a system itself, and a component of a larger system [SOURCE: Wikipedia]
sufficiency of evidence	The measure of the quantity of evidence [SOURCE: From ISAE3000: 12.i.i]
supplementary cybersecurity information	Information related to cybersecurity to be made publicly available by any manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU statement of conformity has been issued NOTE: The information includes guidance and recommendations, the period during which security support will be offered, contact information for receiving vulnerability information and a reference to online repositories listing vulnerabilities. [From Regulation (EU) 2019/881, Article 55]

Term	Definition
supplier	organisation or an individual that enters into agreement with the acquirer for the supply of a product or service Note 1 to entry: Other terms commonly used for supplier are contractor, producer, seller, or vendor. Note 2 to entry: the term “service provider” is typically used in this scheme for suppliers of services Note 3 to entry: when opposed to “service provider”, the term “supplier” refers to a supplier of products [SOURCE: Adapted from ISO/IEC 27036:1-2014, 3.9]
support	set of activities necessary to ensure that an operational system or component fulfils its original requirements and any subsequent modifications to those requirements. NOTE: Examples include software or hardware maintenance, user training. [SOURCE: From ISO/IEC/IEEE 24756:2017, 3.4054]
surveillance	systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity Note 1 to entry: We may not want to keep this term, because of possible confusion with market surveillance, but it is kept for now, as some term needs to cover that concept. [SOURCE: From ISO/IEC 17000:2020, 8.1]
suspension	temporary restriction of the statement of conformity by the body that issued the statement, for all or part of the specified scope of attestation [SOURCE: From ISO/IEC 17000:2020, 8.2]
system	A distinct entity that consists of a number of interacting parts such that the removal or failure of one part may incapacitate the entity as a whole [SOURCE: From www.oxfordreference.com]
system component	a functional component required for the information security of the cloud service during the creation, processing, storage, transmission, deletion or destruction of information in the cloud service provider's area of responsibility NOTE: system components may include software, hardware, or both. EXAMPLES: firewalls, load balancers, web servers, application servers, database servers. [Source: Adapted from C5:2020]
technical expert	person who provides specific knowledge or expertise to the audit team [SOURCE: From ISO/IEC 17021-1:2015, 3.14]
test environment	The environment in which new and changed code is tested
test	<development>activity in which a system or component is executed under specified conditions, the results are observed or recorded, and an evaluation is made of some aspect of the system or component [SOURCE: IEEE Std 610.12-1990]
testing	<conformity assessment>determination of one or more characteristics of an object of conformity assessment, according to a procedure Note 1 to entry: The procedure can be intended to control variables within testing as a contribution to the accuracy or reliability of the results. Note 2 to entry: The results of testing can be expressed in terms of specified units or objective comparison with agreed references. Note 3 to entry: The output of testing can include comments (e.g. opinions and interpretations) about the test results and fulfilment of specified requirements. [SOURCE: From ISO/IEC 17000:2020, 6.2]

Term	Definition
third-party	a person or body that is independent of the person or organisation that provides the object of conformity assessment, and of user interests in that object [SOURCE: From ISO/IEC 17000:2020, 2.2]
third-party conformity assessment activity	conformity assessment activity that is performed by a person or organisation that is independent of the provider of the object of conformity assessment, and has no user interest in the object [SOURCE: From ISO/IEC 17000:2020, 4.5]
threat	potential cause of an unwanted incident, which can result in harm to a system or organisation [SOURCE: From ISO/IEC 27000:2018, 3.74]
top management	person or group of people who directs and controls an organisation at the highest level Note 1 to entry: Top management has the power to delegate authority and provide resources within the organisation. Note 2 to entry: If the scope of the management system covers only part of an organisation, then top management refers to those who direct and control that part of the organisation. [SOURCE: ISO Supplement:3.5]
trust service	an electronic service normally provided for remuneration which consists of: (a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (c) the creation of electronic signatures or electronic seals; (d) the validation of electronic signatures or electronic seals; (e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals; (f) the management of remote electronic signature creation devices or remote electronic seal creation devices; (g) the issuance of electronic attestations of attributes; (h) the validation of electronic attestation of attributes; (i) the creation of electronic timestamps; (j) the validation of electronic timestamps; (k) the provision of electronic registered delivery services; (l) the validation of data transmitted through electronic registered delivery services and related evidence; (m) the electronic archiving of electronic data and electronic documents; (n) the recording of electronic data in an electronic ledger; [SOURCE: From Regulation (EU) No 910/2014, Article 3(16)]
trust service provider	a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider [SOURCE: From Regulation (EU) No 910/2014, Article 3(19)]
tunnel	data path between networked devices which is established across an existing network infrastructure Note 1 to entry: Tunnels can be established using techniques such as protocol encapsulation, label switching, or virtual circuits [SOURCE: From ISO/IEC 27033-1:2015, 3.40]
user	a natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with the eIDAS regulation [SOURCE: Regulation (EU) No 910/2014, Article 3(5a)]

Term	Definition
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 wallet user may use one or more user devices to support a wallet unit
user environment	part of the wallet unit that is hosted in the wallet provider's remote environment NOTE: Although all user environments are part of the same remote environment, a user only has access to their own user environment
validation	[conformity assessment] confirmation of plausibility for a specific intended use or application through the provision of objective evidence that specified requirements (5.1) have been fulfilled Note 1 to entry: Validation can be applied to claims to confirm the information declared with the claim regarding an intended future use. [SOURCE: From ISO/IEC 17000:2020, 6.5]
validation	[eIDAS] the process of verifying and confirming that data in electronic form are valid in accordance with the eIDAS regulation [SOURCE: From Regulation (EU) No 910/2014, Article 3(41)]
verification	confirmation of truthfulness through the provision of objective evidence that specified requirements (5.1) have been fulfilled Note 1 to entry: Verification can be applied to claims to confirm the information declared with the claim regarding events that have already occurred or results that have already been obtained. [SOURCE: From ISO/IEC 17000:2020, 6.6]
version control	establishment and maintenance of baselines and the identification and control of changes to baselines that make it possible to return to the previous baseline [SOURCE: From ISO/IEC/IEEE 24765:2017, 3.4546]
vulnerability	weakness of an asset or control that can be exploited by one or more threats [SOURCE: From ISO/IEC 27000:2018, 2018, 3.77]
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: the wallet instance is an instance of one or more wallet user interface applications, possibly split between the wallet user's device and the wallet provider's remote environment [SOURCE: From CIR (EU) 2024/2981, Article 2(5), note added]
wallet provider	natural or legal person who provides wallet solutions NOTE: Because of the composite nature of a wallet solution, the wallet provider produces or procures the hardware and software for the wallet solution, manages their configurations or settings, and makes them available to wallet users. The wallet provider also provides the services from the wallet solution, and operates the processes required to manage the wallet units. [SOURCE: From CIR (EU) 2024/2981, Article 2(8)]

Term	Definition
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, 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, 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, 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 wallet secure cryptographic devices may not be actually provided to the user, as they may 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 3: 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, Article 2(10), notes added]
wallet user	user who is in control of the wallet unit [SOURCE: From CIR (EU) 2024/2981, Article 2(12)]
withdrawal **cancellation**	revocation of the statement of conformity by the body that issued the statement [SOURCE: From ISO/IEC 17000:2020, 8.3]

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