NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

NATIONAL CERTIFICATION SCHEME

SLOVAK NATIONAL EUDIW CYBERSECURITY CERTIFICATION BASED ON V 0.4.614 OF EU CANDIDATE SCHEME

Title	National Certification Scheme Slovak National EUDIW Cybersecurity Certification based on v 0.4.614 of EU candidate scheme
Designation	NCS-02
Version	v.1.0
Issue date	25.5.2026
Date of effectiveness	22.6.2026
Approved by	JUDr. Roman Konečný

Národný bezpečnostný úrad | Budatínska 30 | 851 06 Bratislava | Slovenská republika
tel.: +421 2 6869 1111 | podatelna@nbu.gov.sk | www.nbu.gov.sk

Document History

Date	Version	Modification	Author
3.03.2026	0.1	Creation based on national templates	NBU
3.03.2026	0.2	Creation based on national templates and EU candidate scheme v 03	NBU
20.04.2026	0.3	Update to published EU draft candidate scheme	NBU
25.5.2026	1.0	First version	NBU

Content

Executive Summary (EU & Slovak Republic)

1. The present document establishes 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).
2. 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 compliance 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.
3. 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 is obvious at the national level, where certification will be tailored to a given architecture, defining precisely the schemes to be used for each component.
4. 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.
5. 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.
6. 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.
7. 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.
8. The scheme proposed below has been thought as an orchestrator, providing general guidelines for the evaluation and certification of the 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 suites 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.
9. Due to early stage of maturity of all certification ecosystem components and variability of approach, Slovak certification ecosystem circumstances are not too much different therefore we keep this summary as relevant for Slovak national scheme. We are addressing the deviations of Slovak approach comparing to original template in each chapter either by different color or under the original EU scheme draft text.

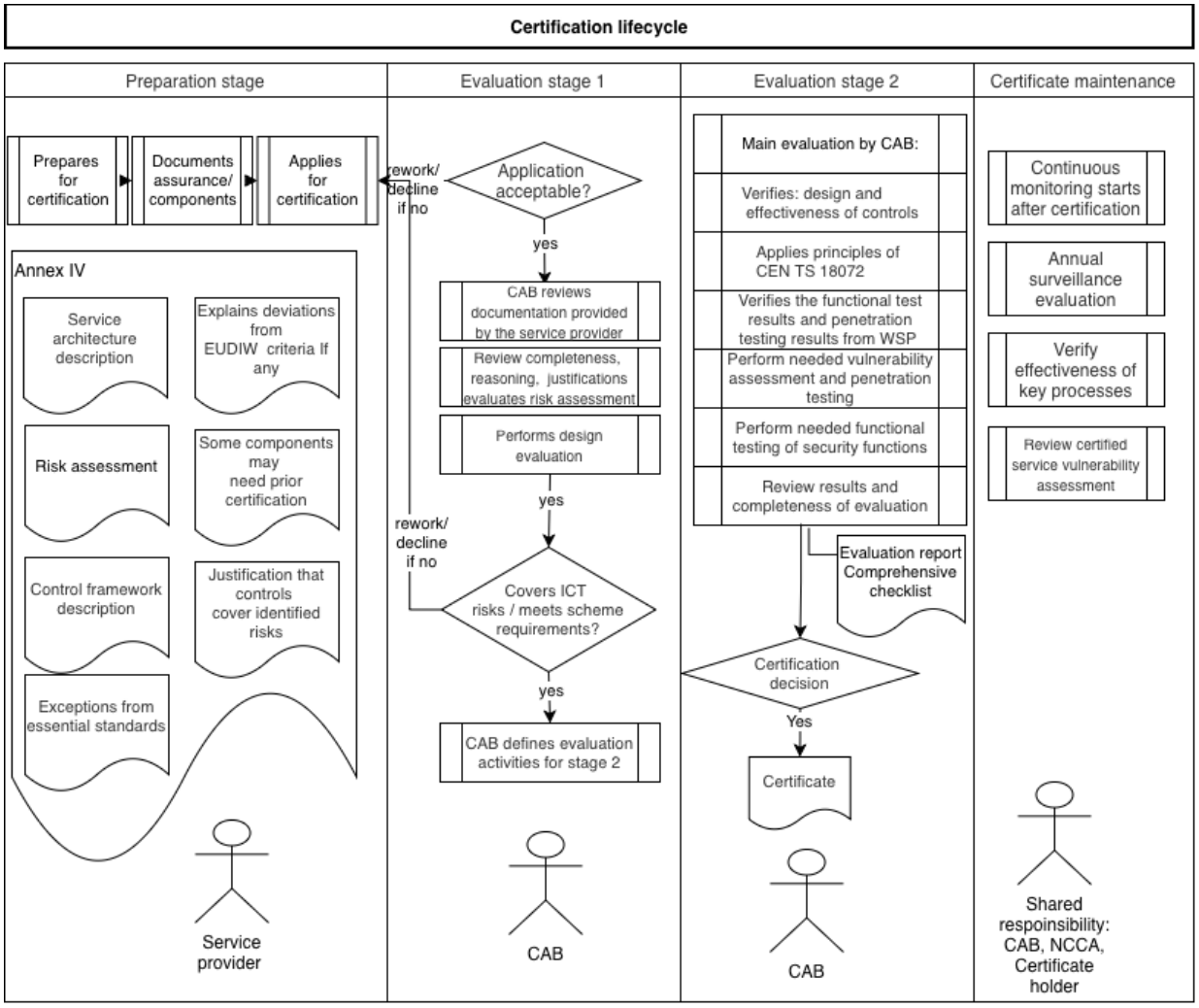
   There are differences due following reasons e.g.:

   a. missing information in template,
   b. open questions in the template/EU draft Scheme,
   c. different national background and circumstances,
   d. existing previous certification scheme for eIDAS in Slovakia,
   e. capability of existing CAB,
   f. specific Slovak law implementations or other constrains due to the aggressive timeline of this project.

Scheme Principles (informative)

The following table is included as an informative explanatory aid to preserve the certification-lifecycle logic described in the non-normative “Scheme Principles” chapter of the EU draft candidate EUDIW scheme; because the Slovak national scheme is drafted primarily on the basis of the normative structure and annexes of the EU draft scheme, the informative parts of the EU draft are not repeated in full in the main body of the Slovak national scheme, but their practical meaning is reflected here to explain how Annex I, Annex IV, Annex VIII, Annex X, Annex XI and the certificate-maintenance provisions operate together across the certification lifecycle.

The certification lifecycle shall be read together with the Slovak annexes that are following EU draft candidate EUDIW scheme structure aligned with Slovak national context. Annex I defines the certified object and its module boundaries. Annex IV defines the evidence package prepared by the service provider. Annex X defines the evaluation criteria. Annex XI defines the methods used by the CAB. Annex VIII defines CAB accreditation, authorisation, competence and permitted activities. Annex II governs certificate maintenance and surveillance after issuance.



Lifecycle phase	Diagram element	Explanation
Preparation stage	Prepares for certification	The service provider starts preparing the certification package before submitting the application. This is not only administrative preparation, but also preparation of

		architecture, risk, evidence, assurance documentation and scope justification.
Preparation stage	Documents assurance / components	The service provider identifies components, subservices, reusable assurance information and evidence for the certified ICT service. This includes component certificates, assurance reports, QTSP evidence, ISMS evidence, functional testing evidence and other conformity assessment outputs.
Preparation stage	Applies for certification	The provider submits the application and supporting package to the CAB. The application must identify the certified object, module(s), architectural profile(s), use-case modifier(s), dependencies and requested certificate boundary.
Preparation stage	Annex IV evidence package	The “Annex IV” box in the diagram represents the minimum information required for certification. It should be understood as the structured evidence package, not as a single document.
Preparation stage	Service architecture description	The provider describes the architecture of the certified service, including wallet solution, PID service, validation service, backend systems, WSCA/WSCD, interfaces, data flows, trust boundaries, assumptions and external dependencies.
Preparation stage	Risk assessment	The provider prepares an implementation-specific risk assessment, including risks from the Union risk register and Slovak implementation-specific risks.
Preparation stage	Control framework description	The provider explains the control framework and how controls are implemented across components, processes and modules.
Preparation stage	Exceptions from essential standards	The provider identifies where standards, technical specifications, essential standards, protection profiles or framework requirements are not fully applied, not applicable, still evolving or applied differently.
Preparation stage	Explains deviations from EUDIW criteria, if any	The provider must explain why any deviation does not reduce the required assurance level or leave a risk uncovered.
Preparation stage	Some components may need prior certification	Certain components may need prior certification, separate assessment or reusable assurance before they can support the overall certification conclusion. This is particularly relevant for WSCD, WSCA, wallet instance, backend ISMS, QTSP services or functional conformance testing.
Preparation stage	Justification that controls cover identified risks	The provider explains why the implemented controls and reusable assurance information cover the identified risks, including residual risks and compensating controls.
Evaluation stage 1	Application acceptable?	The CAB first checks whether the application is complete enough and within the scheme scope. This is an acceptability gate, not yet the full conformity assessment.
Evaluation stage 1	Rework / decline if no	If the application is incomplete, outside scope, inconsistent or insufficiently evidenced, the CAB does not proceed. The provider must correct the application or the case is declined.
Evaluation stage 1	CAB reviews documentation	The CAB reviews the submitted documentation to understand the service, scope, risk argument, evidence package, assumptions and reusable assurance.

	provided by service provider	
Evaluation stage 1	Review completeness, reasoning, justifications, evaluates risk assessment	The CAB checks whether the evidence package is complete, whether the provider's reasoning is coherent, and whether the risk assessment is sufficiently linked to controls and components.
Evaluation stage 1	Performs design evaluation	The CAB evaluates whether the service design, architecture, dependencies, assumptions and controls are suitable to meet the evaluation criteria.
Evaluation stage 1	Covers ICT risks / meets scheme requirements?	The CAB determines whether, if implemented and operated as described, the service would cover ICT risks and meet scheme requirements. This is the key stage 1 decision gate.
Evaluation stage 1	CAB defines evaluation activities for stage 2	The CAB prepares the evaluation plan for the main evaluation stage. This plan identifies audits, inspections, tests, dependency checks, sampling, vulnerability assessment, functional testing and residual activities.
Evaluation stage 2	Main evaluation by CAB	The CAB performs the main evaluation activities according to the evaluation plan. This is the evidence-gathering and verification stage.
Evaluation stage 2	Verifies design and effectiveness of controls	The CAB verifies both that controls are properly designed and that they operate effectively, or for initial certification, that operating effectiveness can be demonstrated through pilots, tests or controlled operation. The evaluation goes beyond a simple documentation audit.
Evaluation stage 2	Applies principles of CEN TS 18072	The CAB uses audit, inspection and, where needed, testing logic suitable for high-assurance ICT services and composite evaluation.
Evaluation stage 2	Verifies functional test results and penetration testing results from WSP	The CAB reviews testing already performed or provided by the wallet solution provider, including functional conformance testing and penetration testing. The CAB does not blindly accept results; it verifies suitability, scope and reliability.
Evaluation stage 2	Perform needed vulnerability assessment and penetration testing	Where existing evidence is insufficient, or where risk requires direct validation, the CAB performs or requires additional vulnerability assessment and penetration testing.
Evaluation stage 2	Perform needed functional testing of security functions	The CAB performs or requires functional testing of security-relevant functions, especially where functional conformance is necessary to demonstrate that security functions are correctly implemented.
Evaluation stage 2	Review results and completeness of evaluation	The CAB reviews whether all required activities were completed, whether evidence is sufficient and whether findings have been resolved.

Evaluation stage 2	Evaluation report / comprehensive checklist	The CAB prepares the evaluation report and a comprehensive checklist showing how evidence, criteria, methods and conclusions are linked.
Evaluation stage 2	Certification decision	The certification decision is made based on the evaluation results, review and conclusion that requirements are met without unresolved blocking nonconformities.
Evaluation stage 2	Certificate	The certificate records the certified scope, modules, profiles, assumptions, dependencies, assurance level, certificate holder and validity.
Certificate maintenance	Continuous monitoring starts after certification	After certification, the certified service must remain under monitoring. This is a shared responsibility of the certificate holder, CAB and NCCA.
Certificate maintenance	Annual surveillance evaluation	The certified service is periodically reassessed, normally annually, to confirm continued conformity.
Certificate maintenance	Verify effectiveness of key processes	Maintenance checks whether key processes such as vulnerability management, change management, incident management, fraud management and certified-version control remain effective.
Certificate maintenance	Review certified service vulnerability assessment	The CAB reviews whether the vulnerability assessment remains current in light of new vulnerabilities, component changes, threat evolution and dependency changes.
Cross-cutting	Service provider actor	The service provider owns preparation, documentation, risk assessment, evidence collection and maintenance of the certified service.
Cross-cutting	CAB actor	The CAB checks acceptability, evaluates documentation, performs or coordinates evaluation activities, reviews results and supports the certification decision.
Cross-cutting	Shared responsibility: CAB, NCCA, certificate holder	Maintenance is not only CAB activity. The certificate holder monitors changes and vulnerabilities, the CAB performs surveillance and special evaluations, and the NCCA performs oversight.

Foreword

(EU, informative)

1. CONSTRAINTS

a) 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 Standardization Organisations (ESOs) for their subsequent maintenance.

b) 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.

2. MENTIONS OF REGULATIONS

a) The scheme makes few direct mentions to Regulation (EU) 2024/1183, commonly referred to the European Digital Identity Framework (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.

b) 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) won't be suitable for presumption of conformity.

c) Regulation 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.

Initial Context of the Slovak National Certification Scheme for EUDI Wallet (informative)

Initial Context and Background

1. At the time of finalizing this draft of the Slovak National Certification Scheme, guidance for the national implementation of the EUDI Wallet certification scheme became available. This guidance was prepared with the objective of establishing a credible, repeatable and mutually compatible certification framework at EU level, with the ambition that national schemes could be transformed as smoothly as possible into a future EU level candidate scheme.
2. This development confirmed the original strategic intention of the derive the national scheme to the greatest extent possible from existing materials, frameworks and standards, and to align it as closely as possible with the future common European certification scheme.
3. **The Slovak National Scheme therefore:**
   a) Builds extensively on existing EU documents and reference materials,
   b) Relies on applicable international standards, some even in draft stage
   c) Anticipates future alignment with the evolving EU candidate scheme,
   d) Minimizes national deviations from EU draft scheme unless strictly necessary.
   e) This approach is intended to ensure long-term compatibility, reduce rework, and facilitate a potential transition to an EU level certification scheme.

4. **Uncertainty and Evolving Environment**
   - The EUDI WALLET National Certification Scheme project is inherently complex due to:
     1) Ambiguity in certain regulatory and technical requirements,
     2) Ongoing development of relevant standards,
     3) Evolving architecture of the national EUDI Wallet solution,
     4) Evolving Architecture reference framework (ARF)
     5) Incomplete or draft level functional conformance frameworks,
     6) The dynamic evolution of EU level certification concepts,
     7) Lack of experience and experts for audit, certification and scheme preparation of the EUDIW topic, which is the complex of product, service, process certification
     8) Aggressive timeline for national solution certification under scheme that is just being developed
   - Additionally, the timeline for certification of a national solution remains uncertain as the solution is still being developed and adjusted to changing ARF. As a result, some referenced standards and frameworks may still be under development at the time of conformity assessment, and the auditor will need to take decisions and justify deviation from the drafts standards during the certification audit.
5. **Bridge-building approach:**

   - The Slovak national certification scheme does not aim to create added value by repeating regulatory requirements or restating paragraphs from existing standards. Instead, the purpose of the scheme is to present a structured way of thinking about the requirements, connect related requirements across different frameworks, identify

overlaps and gaps, and explain how gaps are to be temporarily mitigated until a European certification scheme becomes fully available. The scheme is therefore intentionally designed as a bridge between the current national implementation phase and the future European certification framework.

- This bridging role is driven by practical constraints. There is a significant shortage of qualified experts, and the same experts are already required across multiple certification schemes and overlapping domains including eIDAS, national cybersecurity regulation, ETSI-based QTSP assessments, future EUCC-related activities, and emerging EUDI Wallet conformity work. The Slovak scheme therefore seeks to minimize duplication of effort, maximize reuse of assessment outputs, and avoid a structure that would force the same work to be repeated during later transition to an EU scheme.

6. **Under these circumstances:**

a) Auditors are expected to apply professional judgement and due care when assessing requirements derived from draft or evolving standards.

b) Certification bodies will need to clearly document which provisions are fully applicable and which are conditional or transitional.

c) Solution providers are expected to identify and address gaps where standards are incomplete or evolving, particularly in relation to Level High assurance requirements and provide justification how certified ecosystem of EUDIW comply with requirements of legislation and certification requirements at the LoA “high”.

d) Issuing this draft at this stage serves an important purpose: it establishes a direction for all involved stakeholders and provides transparent expectations regarding certification processes, documentation, input materials, and anticipated timelines for current and future wallet solution providers.

7. **Four practical pillars of the Slovak approach**

The Slovak scheme is built on four practical pillars.

(a) The first pillar is the already established cybersecurity audit ecosystem under national law, including compulsory cybersecurity audit requirements and a regulated qualification framework for cybersecurity auditors.

(b) The second pillar is the long-standing experience from eIDAS and trust service provider auditing, where reliable outcomes have historically depended not only on prescriptive text but also on the competence and professional judgment of auditors operating under ETSI-based and previously ISACA-influenced frameworks.

(c) The third pillar is a deliberately auditor-centric approach, which accepts that in a transitional and principle-based environment expert auditors must bridge the gap between legal obligations, technical standards, architectural realities and available evidence.

(d) The fourth pillar is systematic reuse of existing European and international outputs, including ENISA materials, ETSI standards, ISO standards, the Functional Conformance Assessment Framework, elements of the Architecture Reference Framework and other essential standards and technical specifications.

This means that the Slovak scheme does not redefine or replicate available requirements. Rather, it treats available materials as authoritative inputs and integrates them into the evaluation process in a structured and traceable manner. The Architecture Reference Framework is not treated as a standalone source of obligations, but as a structured

expression of legal and technical requirements that must be interpreted and mapped into evaluation criteria, controls and evidence.

8. **Alignment with the National Accreditation Body**
   a) The development of the Slovak National Certification Scheme for the EUDI Wallet was carried out in close alignment with the Slovak NAB SNAS (Slovak National Accreditation Service). During a series of analytical workshops and consultations, potential structural approaches have been evaluated.
   b) In cooperation with Slovak NAB SNAS we analyzed the existing potential inspirational resources for choosing the approach for national scheme e.g.:
      1) **CASCO toolbox** https://www.iso.org/committee/54998/x/catalogue/p/1/u/0/w/0/d/0.
      2) **ISO/IEC 17011: 2017** Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies
      3) **ISO/IEC 17029:2019** Conformity assessment — General principles and requirements for validation and verification bodies
      4) **ISO/IEC DIS 17007:2026**
      5) Conformity assessment — Guidance for drafting normative documents suitable for use for conformity assessment
      6) **ISO/IEC DRT 17032:2019**
      7) **Conformity assessment** — Guidelines and examples of a certification scheme for processes
   c) A critical milestone in preparing this draft was reaching agreement with the Slovak National Accreditation Body on how to manage:
      1) Ambiguity in regulatory and technical requirements,
      2) Changes resulting from unfinished or evolving standards,
      3) Modifications to product architecture,
      4) Future updates to EU level candidate schemes,
      5) The evolving concept of conformity assessment.
9. **This agreement established a structured approach to:**
   a) Updating and maintaining the national scheme,
   b) Managing changes within the accreditation and certification ecosystem,
   c) Preventing regulatory paralysis caused by uncertainty,
   d) Ensuring progress despite evolving external inputs.
   e) The scheme therefore includes a defined change management logic for accreditation and certification workflows - see the flowchart.

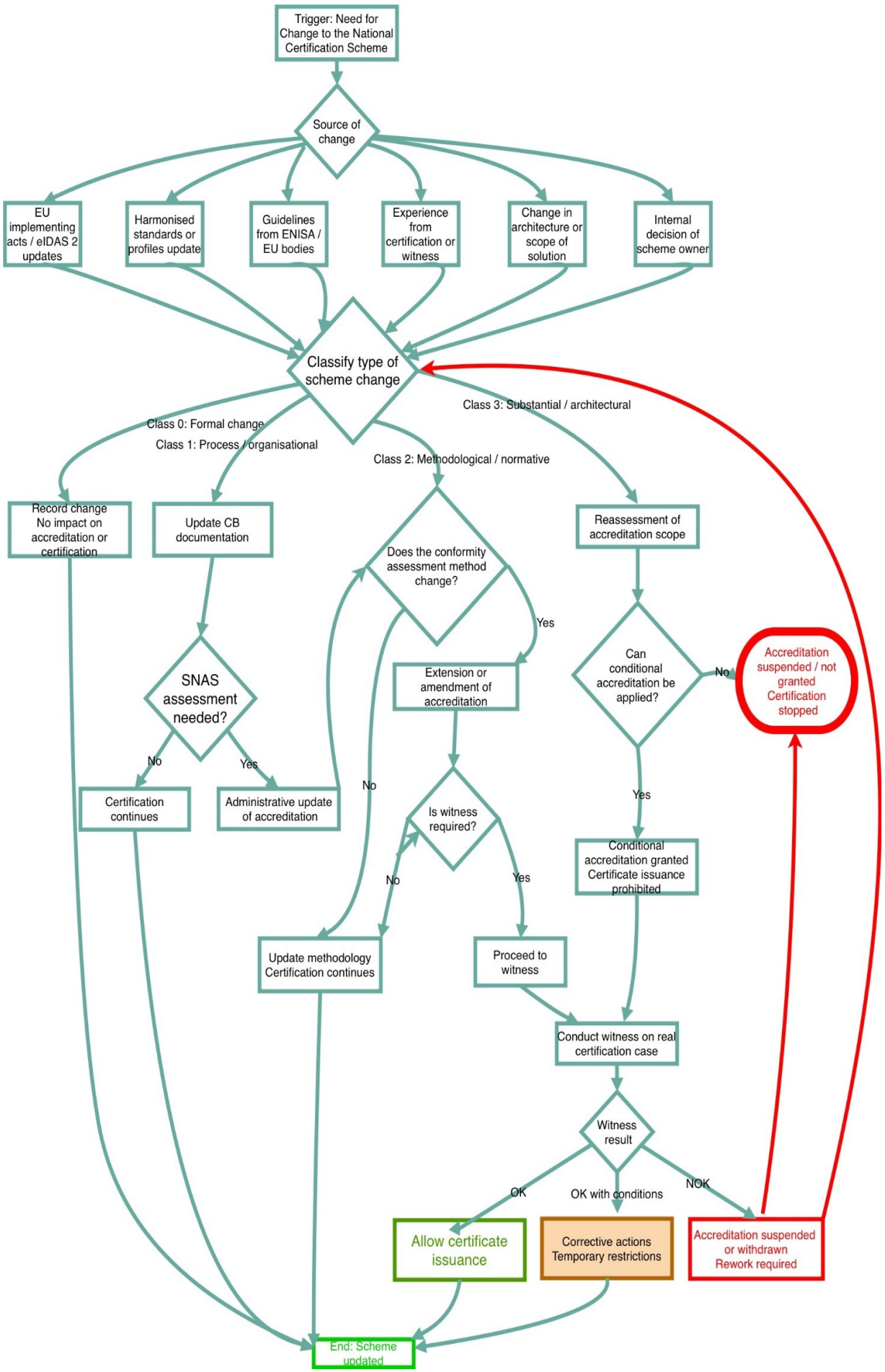

Trigger: Need for Change to the National Certification Scheme
Source of change
EU implementing acts / eIDAS 2 updates
Harmonised standards or profiles update
Guidelines from ENISA / EU bodies
Experience from certification or witness
Change in architecture or scope of solution
Internal decision of scheme owner
Classify type of scheme change
Class 0: Formal change
Class 1: Process / organisational
Class 2: Methodological / normative
Class 3: Substantial / architectural
Record change No impact on accreditation or certification
Update CB documentation
Does the conformity assessment method change?
Reassessment of accreditation scope
SNAS assessment needed?
Yes
No
Extension or amendment of accreditation
Can conditional accreditation be applied?
No
Accreditation suspended / not granted Certification stopped
No
Certification continues
Administrative update of accreditation
No
Is witness required?
Yes
Yes
Conditional accreditation granted Certificate issuance prohibited
No
Yes
Update methodology Certification continues
Proceed to witness
Conduct witness on real certification case
Witness result
OK
OK with conditions
NOK
Allow certificate issuance
Corrective actions Temporary restrictions
Accreditation suspended or withdrawn Rework required
End: Scheme updated

Diagram step	Explanation	Rationale in the scheme context
Trigger: need for change to the National Certification Scheme	A change need is identified.	The Slovak scheme is designed as a controlled, forward-looking baseline that must evolve with EU guidance, standards, architecture and accreditation practice.
Source of change	Identify why the scheme may need to change.	Change must be traceable to a concrete driver, not handled informally.
EU implementing acts / eIDAS 2 updates	Legal or regulatory change at EU level.	May require mandatory adaptation of the national scheme to preserve legal conformity.
Harmonised standards or profiles update	New or revised technical standards, protection profiles or harmonised documents.	The scheme relies on EU and international outputs and should integrate them where relevant.
Guidelines from ENISA / EU bodies	New interpretative or technical guidance.	Such guidance may affect evaluation criteria, methods, or assurance expectations.
Experience from certification or witness	Lessons from real certification, pilot evaluation or accreditation witness.	Accreditation and certification are interdependent; witness experience may reveal practical gaps.
Change in architecture or scope of solution	The wallet architecture, modules, profiles or certification scope changes.	Architecture/profile changes can affect risk, dependencies, evaluation plan and accreditation scope.
Internal decision of scheme owner	NBÚ/scheme owner decides to refine the scheme.	The scheme owner periodically reassesses the need for updates.
Classify type of scheme change	Determine the impact category of the change.	This is the core control point: the response must be proportional to the materiality of the change.
Class 0: Formal change	Editorial, formatting, numbering, terminology or non-substantive correction.	No impact on certification or accreditation because requirements and methods remain unchanged.
Record change — no impact on accreditation or certification	Register the change and keep the existing scheme effective.	Maintains traceability without triggering unnecessary reassessment.
Class 1: Process / organisational change	Change affects procedures, responsibilities, documentation, reporting or administrative workflows.	May affect CAB documentation or accreditation records but does not necessarily change technical requirements.
Update CB documentation	Certification body updates procedures, templates, checklists, competence records or operating documents.	Required to ensure the CAB continues operating consistently with the updated scheme.
SNAS assessment needed?	Decide whether the change affects accredited activities or competence assumptions.	Accreditation scope and CAB capability must remain aligned with the scheme.
No → certification continues	If accreditation scope is unaffected, certification may continue.	Avoids regulatory paralysis where the change is administrative only.
Yes → administrative	SNAS updates or confirms accreditation documentation.	Keeps accreditation records aligned without requiring a full technical reassessment.

update of accreditation		
Class 2: Methodological / normative change	Change affects evaluation criteria, methods, standards, normative references, evidence expectations or assessment logic.	These changes may affect how conformity is demonstrated, but not necessarily the architecture or accreditation scope.
Does the conformity assessment method change?	Decide whether the actual evaluation method, competence, testing, inspection or audit approach changes.	The document distinguishes audit, inspection and testing activities; method changes may affect accreditation.
No → update methodology, certification continues	Update interpretation, guidance, checklists or evaluation matrices without interrupting certification.	Appropriate where the change clarifies existing requirements but does not change the method or assurance basis.
Yes → extension or amendment of accreditation	Accreditation scope or methods may need amendment before certificates can rely on the updated method.	Required where the CAB needs new competence, method, testing or inspection capability.
Is witness required?	Decide whether SNAS must observe a real certification case.	The document states that accreditation may require a witness audit during a real certification process.
No → update methodology, certification continues	Accreditation update can be completed administratively or by document review.	Used where competence has already been demonstrated.
Yes → proceed to witness	SNAS observes the CAB in a real certification case.	Necessary where competence must be demonstrated in practice.
Conduct witness on real certification case	Accreditation witness is performed during an actual certification activity.	This reflects the scheme's parallel accreditation/certification model.
Witness result: OK	CAB competence and method application are confirmed.	Certificate issuance may proceed.
Allow certificate issuance	Certification can continue under the updated scheme/method.	Assurance remains valid and accreditation basis is confirmed.
Witness result: OK with conditions	Minor issues or limitations are identified.	Certification may continue only with corrective actions or temporary restrictions.
Corrective actions / temporary restrictions	CAB must correct issues; scope or issuance may be temporarily limited.	Proportional response to non-critical findings.
Witness result: NOK	CAB cannot demonstrate required competence or method application.	Certification cannot continue safely under the changed method.
Accreditation suspended or withdrawn / rework required	Accreditation is suspended/withdrawn or the CAB must repeat preparation.	Prevents issuance of certificates without demonstrated competence.
Class 3: Substantial / architectural change	Change affects fundamental architecture, certification scope, assurance model, module boundaries, critical components, or risk coverage.	The document treats architectural and critical-component changes as material.

Reassessment of accreditation scope	SNAS/NBÚ reassess whether the current accreditation can still cover the scheme.	Needed because the change may require different competence, methods, or scope.
Can conditional accreditation be applied?	Determine whether certification can continue under controlled conditions.	Supports progress despite evolving requirements, while preserving assurance.
No → accreditation suspended / not granted / certification stopped	If conditions cannot ensure reliable assessment, certification stops.	Protects credibility of the scheme and prevents invalid certificates.
Yes → conditional accreditation granted; certificate issuance prohibited	CAB may continue preparatory/evaluation work, but may not issue certificates yet.	Useful where witness or additional evidence is needed before final accreditation.
Conduct witness on real certification case	Real case is used to confirm competence under the changed architecture or scope.	Aligns with the document's requirement that accreditation and certification may need to progress in parallel.
End: scheme updated	The updated scheme, documentation, accreditation status and certification logic are aligned.	Final state: the scheme remains current, traceable and usable without undermining assurance.

10. **Interdependency of Certification and Accreditation and WS development**
    a) Under accreditation rules, the accreditation of a certification body requires the performance of a "witness audit". A witness audit must be conducted during a real certification process. Consequently:
        1) Accreditation cannot be finalized without an active certification case.
        2) The certification scheme cannot be considered operational without alignment to accreditation requirements.
        3) At least one pilot or real certification client is required.
        4) Same time WS cannot be used in production without certification therefore it is evident that certification needs to be executed at the stage of prototype and in stage environment.
    b) Given the specific scope of EUDI Wallet validation certification in Slovakia, it is anticipated that there will be only one national wallet solution subject to certification with a phased approach when certifying specific profiles. Therefore, the accreditation and certification processes must be conducted in parallel, with the certification process forming an integral part of the accreditation witness audit.
    c) Both streams are expected to progress concurrently and conclude in a coordinated manner alongside the first phases of WS development.
11. **Rationale for Using the EU Template**
    a) EU guidance recommends a staged and evolutionary approach to the development of the national EUDI Wallet ecosystem. The full range of use cases, functionalities and interoperability layers is expected to mature over several years.
    b) At the same time, the European certification framework may reach operational clarity sooner than the complete national functional evolution of the wallet solution.
    c) The anticipated validity of a national certificate (e.g. five years) must be viewed considering the expected development of a European-level certification scheme.

d) It is highly probable that transition to an EU certification framework will occur before the expiry of the first national certificate. As a result:
    1) The Slovak national scheme is expected to operate within a transitional timeframe.
    2) A fully independent national structural model would likely create unnecessary future transformation costs.
e) Based on the considerations above, the Slovak National Scheme adopts the EU candidate scheme template as its structural foundation in order to:
    1) Ensure maximum alignment with future EU certification requirements,
    2) Enable smooth and easy review by EDICG
    3) Minimize structural deviations and transformation effort,
    4) Avoid duplication and unnecessary national-specific constructs,
    5) Facilitate smoother later peer review and EU-level comparability,
    6) Provide predictability to accreditation bodies and certification personnel,
    7) Clearly distinguish genuinely Slovak-specific elements from common EU baseline requirements.
f) The Slovak National Scheme therefore serves both as:
    1) A national operational certification framework, and
    2) A structured bridge toward a future European certification scheme.
g) This approach ensures regulatory continuity, proportionality of effort, and strategic coherence within the evolving European digital identity ecosystem.

12. **Parallel Evolution of Standards and Architecture**

a) The accreditation and certification processes are expected to require several months (estimated 6–9 months or longer – subject to architecture components). During this period:
    1) Relevant international standards may reach more mature stages.
    2) Protection profiles and certified component according EUCC might be available.
    3) Additional EU guidance and documents may be issued.
    4) The national wallet architecture will evolve and become more precisely defined .
b) The scheme therefore must be sufficiently flexible to accommodate evolving technical and regulatory inputs without requiring structural redesign.

13. **The accompanying process flowchart describes how:**

a) External changes (e.g., new standards, EU guidance, architectural updates) are evaluated, their impact on the national scheme is assessed, and necessary modifications are implemented in a controlled and transparent manner.
b) This approach ensures forward movement without creating circular dependencies or deadlocks caused by regulatory uncertainty within timeline pressure.

14. **Use of EU Templates and Version Alignment**

a) The draft of the Slovak National Scheme was initially prepared using a template for national schemes version 0.2 from 08/2025. Shortly before finalization, Template of EU candidate scheme Version 0.3.609 and updated EU guidelines became available and public consultation of the version 0.4.614.
b) In response, the drafting process transitioned to align with the EU candidate scheme version No. 04.614, with the following objectives:

1) Use the most recent available alignment baseline,
2) Facilitate smooth transformation into a future EU candidate scheme,
3) Minimize national deviations,
4) Simplify peer review and EU level assessment,
5) Avoid unnecessary reinvention of existing structures,
6) Clearly identify and justify any Slovak specific differences.

c) This deliberate alignment strategy reduces long-term regulatory friction and supports interoperability at EU level. Later updates of European draft scheme will be considered according to the logic described in the flow chart.

15. **Functional Conformance Assessment Framework**

a) An additional enabling factor for progressing with this draft was the publication of Version 0.1 of the Functional Conformance Assessment Framework.

b) Although preliminary, this framework provided:
1) A structured methodology for approaching functional testing,
2) Guidance for selecting appropriate testing procedures,
3) An interpretative framework for assessing functional requirements of digital identity solutions,
4) A reference point in situations where architectural profiles were not yet fully defined.

c) Given the evolving nature of this framework:
1) Auditors may need to determine which parts are applicable at the time of evaluation.
2) The most advanced available version of the framework should be used for functional testing, unless explicitly justified otherwise.
3) Deviations or nonapplicable sections must be clearly documented and justified in conformity assessment reports.

16. **Purpose of Issuing This Draft**

a) Despite the evolving regulatory and technical landscape, this draft is issued to:
1) Establish clear expectations for certification,
2) Enable accreditation bodies and certification personnel to prepare qualification frameworks,
3) Provide predictability for current and future solution providers,
4) Define a structured pathway towards LoA “High” certification,
5) Avoid stagnation due to regulatory uncertainty.

b) This document therefore represents a controlled, forward-looking baseline that is designed to evolve in a managed and transparent manner alongside EU developments.

17. **Regulatory and Strategic Context of Slovak National Scheme**

The Slovak framework for the European Digital Identity Wallet is built on Act No. 272/2016 Coll. on trust services, as amended, which implements eIDAS requirements in Slovak law, and on the related EU legal framework governing EUDI Wallet certification, accreditation, supervision and assurance level requirements.

The national scheme operates at the intersection of several layers of obligations: eIDAS and its implementing acts for the EUDI Wallet ecosystem; the Cybersecurity Act and its implementing regulations for national cybersecurity governance and compulsory audit obligations; ETSI and ISO-based conformity assessment and management-system requirements; and, where relevant, product-oriented schemes and technical requirements such as EUCC, Common Criteria-derived assurance, functional conformance frameworks and emerging technical profiles.

18. National Legal Foundation and stakeholder roles

Within the Slovak ecosystem, NBÚ acts as scheme owner and key supervisory authority in the trust services and national certification environment, while the Ministry of Interior is expected to act as the public authority responsible for ensuring provision of the European Wallet and the related eID scheme and PID linkage functions. SNAS acts as the national accreditation body, and the conformity assessment body must operate within the accreditation and authorization logic foreseen by the scheme.

From the perspective of national law, the provider of the wallet solution must be a Qualified Trust Service Provider or demonstrate that it has concluded a valid contract with a Qualified Trust Service Provider for this purpose. This legal condition is not merely administrative; it is a structural prerequisite that directly affects admissibility of the provider, reuse of existing trust-service assurance, CAB dependency analysis and the scope of supervision by NBÚ.

Under the Slovak national certification scheme, the wallet solution and its operational environment must comply not only with eIDAS and the implementing acts, but also with all applicable obligations arising from Slovak cybersecurity legislation. This includes information systems, networks, supporting infrastructure and organizational measures used for the provision and operation of the wallet solution.

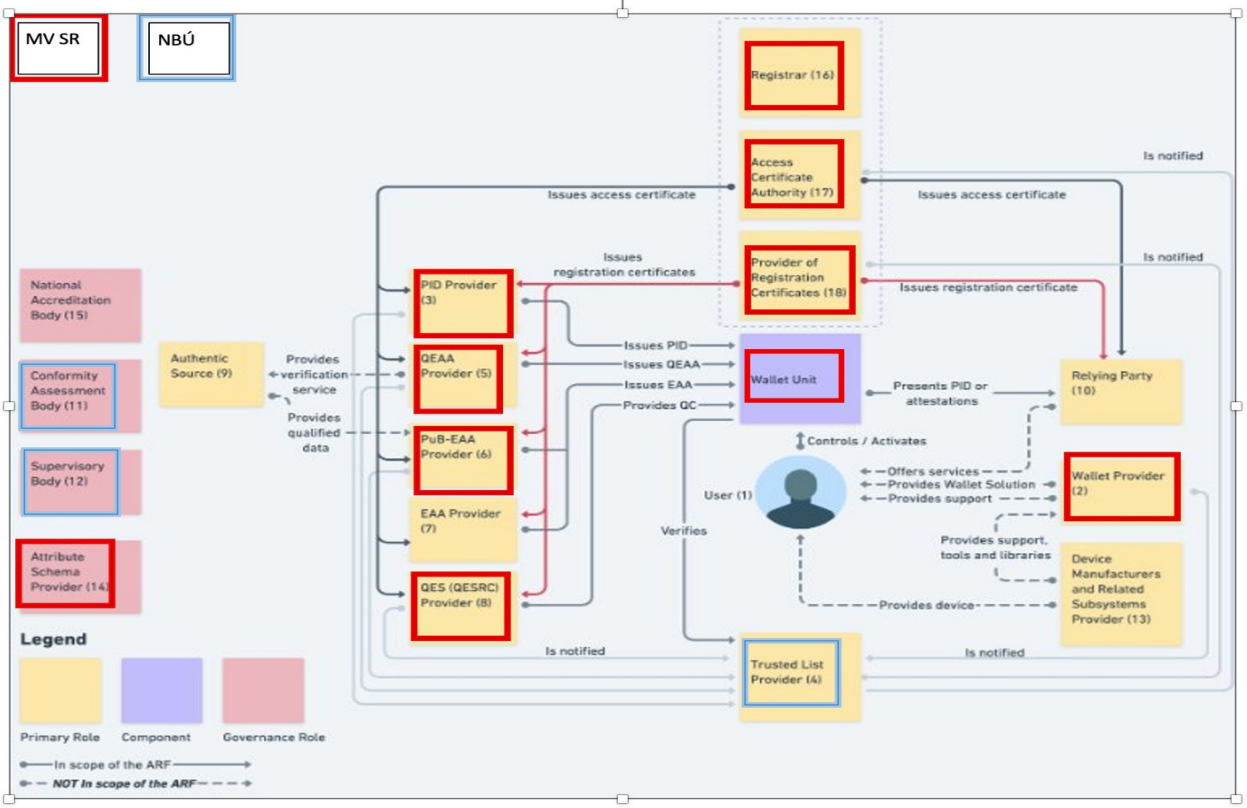
The provider must ensure that the wallet solution is designed, implemented and operated in accordance with the security measures prescribed for relevant categories under Act No. 69/2018 Coll. on cybersecurity and its implementing regulation, including establishment of an information security management framework, risk analysis and treatment, implementation of technical and organizational measures, incident detection and handling, continuity planning, security monitoring and, where required, compulsory cybersecurity audit. Compliance with national cybersecurity law forms an integral part of the overall certification assessment and may provide reusable assurance information, but only after the CAB has assessed its suitability and relevance through dependency analysis.

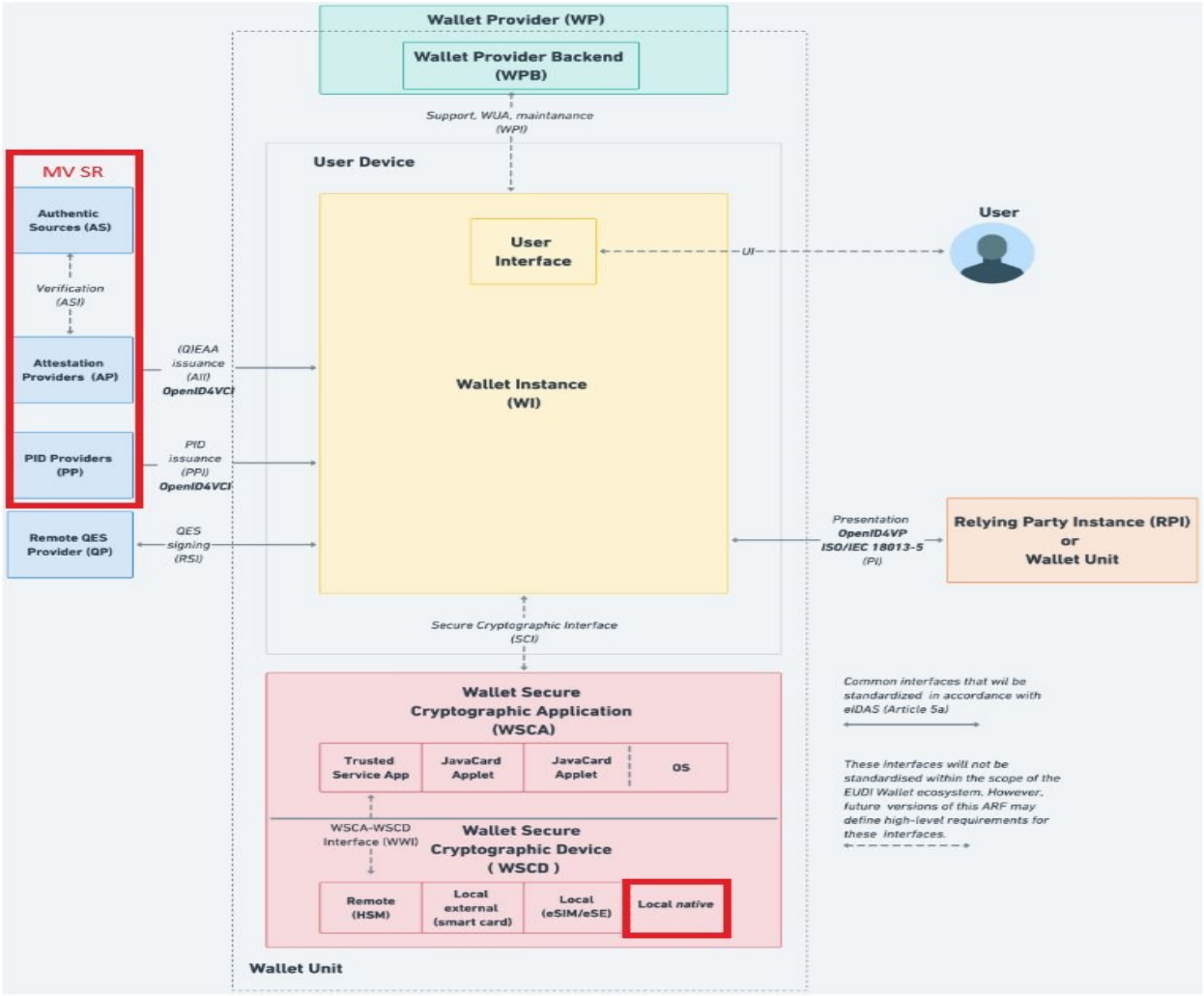
1. The Slovak framework for the European Digital Identity Wallet (EUDIW) is built on Act No. Slovak **Trust Services Act** (as amended), which implements the eIDAS Regulation within the Slovak law with mandatory compliance with LoA ”High”.
2. **Key Stakeholders and Their Roles**

   Main Slovak actors within the certification ecosystem:

Member State	Slovakia (SK)
Scheme owner	NBÚ (NOKC)
Supervisory body	NBÚ (SRD)
National accreditation body	SNAS
CAB	NBÚ (SAC)
Wallet provider	MV SR (Ministry of Interior)

eID scheme provider	MV SR (Ministry of Interior)





3. **NBÚ (National Security Authority):**
   a) Acts as the **Supervisory Body** for trust services and the European wallet framework [Slovak **Trust Services Act** No. 272/2016, § 11(a), § 12(3)].
   b) Serves as the **Single Point of Contact** for trust services, European wallets, and electronic identification schemes [Slovak **Trust Services Act** No. 272/2016, § 11(b)].
   c) Responsible for the **Certification** of cybersecurity of information and communication technologies under the Cybersecurity Act [Slovak **Trust Services Act** No. 272/2016, § 11(d)].
   d) Maintains the **Trusted List** and the national infrastructure for certificate validation [Slovak **Trust Services Act** No. 272/2016, § 11(i), § 11(g)].
4. **Ministry of Interior of the Slovak Republic:**
   a) The public authority responsible for **ensuring the provision** of the European Wallet [Slovak **Trust Services Act** No. 272/2016, § 10a(1)(b)].
   b) Compiles and maintains the list of **Relying Parties** [Slovak **Trust Services Act** No. 272/2016, § 10a(1)(a)].
   c) Ensures the linkage of **Person Identification Data (PID)** with the wallet [Slovak **Trust Services Act** No. 272/2016, § 10a(1)(c)].
   d) Acts as the issuer of public sector body responsible for an authentic source **Electronic Attestation of Attributes (PubEAA)** based on data from national **Authentic Sources** [Slovak **Trust Services Act** No. 272/2016, § 10a(2), eIDAS Art 3(46)].
5. **European Wallet Provider:**

a) Must be a **Qualified Trust Service Provider (QTSP)** or demonstrate a contract with one for this purpose [Slovak **Trust Services Act** No. 272/2016, § 10(1)].

b) Required to submit a **Notification of Intent** to provide the wallet and a valid **Wallet Certificate** to the NBÚ [Slovak **Trust Services Act** No. 272/2016, § 10(2)].

c) Must register **Relying Parties** after verifying their identity and ensuring their consent to the wallet's rules [Slovak **Trust Services Act** No. 272/2016, § 10(5)].

d) Obligated to report any suspicion of **unlawful or fraudulent use** to the NBÚ without delay [Slovak **Trust Services Act** No. 272/2016, § 10(6)(e)].

19. **The Certification Framework in Slovak Law**

1. **Object of Certification:** The certification must cover the integrated provision and operation of both the **Wallet Solution** and the **eID scheme** under which it is provided [IA 2024/2981, Art 3(2)].
2. **Granting Qualified Status:** The NBÚ grants "Qualified Status" based on a **Conformity Assessment Report** issued by an accredited **Conformity Assessment Body (CAB)** [Slovak **Trust Services Act** No. 272/2016, § 3(1) and § 11(a)].
3. **Notify the Commission of information:** The NBÚ notify the Commission based on a **Conformity Assessment Report** issued by an accredited **Conformity Assessment Body (CAB)** [Slovak **Trust Services Act** No. 272/2016, § 11(e), eIDAS Art 5a(18) a), b) and c) and Art 5c(3); IA 2024/2981, Art 14(2)].
4. **Accreditation Standards:** Certification bodies must be accredited in accordance with **EN ISO/IEC 17065:2012** [IA 2024/2981, Art 9(1)].
5. **Cybersecurity Audits:** Wallet providers must submit a final report on the results of a **Cybersecurity Audit** to the NBÚ [Slovak **Trust Services Act** No. 272/2016, § 3(1)(c)].
6. **Assurance Level High:** The national scheme requires wallet solutions to be resistant against attackers with **high attack potential**, verifying compliance with **Assurance Level High** as set out in **Regulation (EU) 2015/1502** [IA 2024/2981, Art 8(2)].

20. **Verification and Oversight Process**

1. **Submission:** The provider submits their intention and technical certificates to the NBÚ [Slovak **Trust Services Act** No. 272/2016, § 10(2)].
2. **Verification:** The NBÚ verifies if the provider complies with the **Act on Trust Services** and eIDAS requirements [Slovak **Trust Services Act** No. 272/2016, § 10(3)].
3. **Remediation:** If deficiencies are found, the NBÚ suspends proceedings and requires the provider to remedy them within a set time limit [Slovak **Trust Services Act** No. 272/2016, § 10(3)].
4. **Surveillance:** Once operational, the NBÚ carries out ongoing **inspections** and monitoring to ensure continuous compliance [Slovak **Trust Services Act** No. 272/2016, § 12(1)].
5. From a certification perspective, NBÚ:
   a) grants Qualified Status based on a Conformity Assessment Report,
   b) verifies compliance with national and eIDAS requirements,
   c) conducts ongoing supervision and inspections.

21. **Conformity Assessment and Qualified Status for QTSP**

1. The process follows a structured path:
   a) A Conformity Assessment Body (CAB), accredited under EN ISO/IEC 17065:2012, performs the assessment.
   b) The CAB issues a Conformity Assessment Report.
   c) NBÚ grants Qualified Status based on that report.
   d) The provider must also submit the final report from a Cybersecurity Audit.
2. According to the § 10 (1) of Slovak **Trust Services Act** No. 272/2016, Wallet solution provider must fulfil the requirement:
3. "A provider of the European wallet is a person who is a qualified trust service provider or demonstrates that they have concluded a contract with a qualified trust service provider for this purpose and meet the requirements laid down in a Article 5a of Regulation (EU) No 910/2014 as amended."
4. Pursuant to Slovak **Trust Services Act** No. 272/2016, a CAB's certification decision is a critical input for the NBÚ. A trust service provider without qualified status must submit the certificate and the final report to the NBÚ to be granted qualified status and included in the trusted list. Any CAB that fails to maintain its accreditation or identified non-conformities must immediately notify the NBÚ.

22. **Slovak Regulatory NIS2 Integration into Act No. 69/2018 Coll. on Cybersecurity.**

1. **Conformance to NIS2 implementation – compulsory audit and security requirements for the Public sector.**
   a) Under the Slovak national certification scheme for the European Digital Identity Wallet, the Ministry of Interior, as the solution provider for the public sector wallet, is required to ensure full compliance not only with the requirements of eIDAS and the implementing acts, but also with all applicable obligations arising from Slovak cybersecurity legislation.
   b) In particular, the wallet solution and its operational environment shall comply with the requirements of Act No. 69/2018 Coll. on Cybersecurity and on Amendments to Certain Acts (hereinafter also referred to as the **"Act No. 69/2018 Coll. on Cybersecurity")**, including all implementing regulations issued thereunder. This obligation applies to the information systems, networks, supporting infrastructure, and organizational measures used for the provision and operation of the wallet solution.
   c) The Ministry of Interior shall ensure that the wallet solution is designed, implemented and operated in accordance with the security measures prescribed for operators of essential services or other relevant categories under the Cybersecurity Act, as applicable. This includes the establishment of an information security management framework, risk analysis and risk treatment processes, implementation of technical and organizational security measures, incident detection and handling capabilities, continuity planning, and regular security monitoring.
   d) Where required by law, the Ministry shall undergo cybersecurity audits performed by authorized auditors and shall submit the final audit report to the National Security Authority. Identified non-conformities shall be remedied within the prescribed timeframes, and corrective measures shall be demonstrably implemented and documented.
   e) Compliance with the Cybersecurity Act forms an integral part of the overall certification assessment. The conformity assessment body and the National Security Authority shall take into account the results of cybersecurity supervision and audits when evaluating whether the wallet solution meets the requirements for

certification at Assurance Level High.

f) By embedding the full set of national cybersecurity obligations into the certification framework, the Slovak scheme ensures that the European Digital Identity Wallet is not assessed in isolation as a technical product, but as a critical public digital infrastructure operating under a comprehensive and enforceable security regime.

23. **Relationship to other European frameworks and standards**

a) The current Slovak scheme draws inspiration from and, where relevant, makes use of Regulation (EU) 2019/881, Commission Implementing Regulation (EU) 2024/2981, Commission Implementing Regulation (EU) 2025/2162, the eIDAS framework as amended, Directive (EU) 2022/2555, the national transposition of NIS2, ETSI EN 319 401, ETSI EN 319 403-1, ISO/IEC 17065, ISO/IEC 17000, ISO/IEC 17029, ISO/IEC 15408 and related technical materials. These references do not mean that every listed document automatically becomes a direct normative requirement for every certificate. Rather, they form the evaluated corpus from which the scheme structure, CAB competence expectations, evaluation logic and evidence-reuse rules are derived.

b) The scheme is intentionally careful not to over-prescribe standards in a way that would unnecessarily constrain accreditation or force premature commitment to technical frameworks that are still evolving. The preferred approach is to use eIDAS, the implementing acts, the structure of the Architecture Reference Framework and the concept of essential standards as the normative umbrella, while leaving room for justified and well-documented selection of the most suitable technical standards and evidence sources in each profile or module.

24. **Applicability of CRA and product-oriented evidence**

Where the Cyber Resilience Act or other product-oriented obligations are applicable to one or more products integrated into the wallet ecosystem, the wallet provider, acting as global solution manager, should provide documented mapping showing how existing certificates or technical evidence correspond to the applicable product requirements and where residual gaps remain. If existing certificates do not fully cover applicable requirements, the provider must provide additional evidence so that the CAB can assess conformity of the integrated solution without prejudice to the responsibilities of the actual manufacturer or supplier.

25. **Strategic positioning of the Slovak scheme**

Strategically, the Slovak scheme positions itself as a transitional yet defensible national framework that maximizes reuse of existing mature assurance ecosystems rather than attempting to rebuild them. Its objective is not to restate all rules already contained in European law or detailed standards, but to connect them into an auditable and nationally operable scheme structure. This positioning is especially important for future peer review, future European comparability, and long-term maintainability of certificates, reports and reused evidence.

REFERENCES (original EU scheme)

a) The current scheme makes references to the following regulations:

1) 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)

2) 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)

3) 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

4) 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

5) 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

6) 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)

7) 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

8) 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)

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

1) ISO/IEC 17000:2020 - Conformity assessment – Vocabulary and general principles,

2) ISO/IEC 17065:2012 - Conformity assessment – Requirements for bodies certifying products, processes and services,

3) ISO/IEC 17021-1:2015 - Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements,

4) ISO/IEC 17025:2017 - Conformity assessment – General requirements for the competence of testing and calibration laboratories,

5) ISO/IEC 17029:2019 - Conformity assessment – General principles and requirements for validation and verification bodies,

6) ISO/IEC 15408:2022, Parts 1 to 5 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security (Common Criteria),

7) CEN TS 18072 - Requirements for Conformity Assessment Bodies certifying ICT Services,
8) EN 17640:2022, “Fixed-time cybersecurity evaluation methodology for ICT products”
9) ETSI EN 319 401 - Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers. The latest applicable published version shall be used, with version 3.2.1 / January 2026 treated as the baseline considered during preparation of this scheme unless updated through the scheme maintenance process.
10) EN ETSI 319 403-1: “Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers”.

c) Related Slovak legislative regulations:

1) **Act No. 69/2018 Coll. on Cybersecurity**
2) Act No. 272/2016 Coll. on Trust Services for Electronic Transactions in the Internal Market and on Amendments to Certain Acts (**Trust Services Act**)
3) **Executive order No. 227/2025 Coll.** to **Act No. 69/2018 Coll. on Cybersecurity** (security requirements – NIS 2 implementation)
4) **Act No. 71/1967 Coll. on Administrative Procedure, as amended.**
5) **Act No. 9/2010 Coll. on Complaints, as amended.**
6) **Act No. 18/2018 Coll. on personal data protection and on amendments to certain acts.**
7) **Act No. 215/2004 Coll. on the protection of classified information and on amendments to certain acts.**
8) Additional resources evaluated:
    a. ISO/IEC 17011: 2017 Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies
    b. ISO/IEC 17029: 2019 Conformity assessment — General principles and requirements for validation and verification bodies
    c. ISO/IEC DIS 17007: 2026 - Conformity assessment — Guidance for drafting normative documents suitable for use for conformity assessment
    d. ISO/IEC DRT 17032:2019 - Conformity assessment — Guidelines and examples of a certification scheme for processes

9) ENISA, *Wallet-Related Service Provider Security Requirements, Version 0.5.614, March 2026, based on EN 319 401*. Used as an external technical reference for interpreting wallet-related security requirements, risk-register mappings, standards mappings and CIR (EU) 2015/1502 mappings. The document is not reproduced in the Slovak national scheme and shall be used in its original version, subject to applicability assessment by the CAB.
10) FCAF available at Github (https://github.com/eu-digital-identity-wallet/eudi-doc-functional-conformance-assessment) or https://conformance.eudi.dev/latest-draft/

1. General requirements (normative)

1.1. Subject matter and scope

1. This document sets out the Slovak national certification scheme based on the European draft 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) services for the provision and operation of a wallets solutions and the electronic identification ('eID') schemes under which it is provided;
    b) services for the provision and operation of a wallet solutions;
    c) services 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) services used to verify the validity of wallet units and relying parties;
    e) Requirements of Slovak national laws for operation of EUDIW Solution Providers (SP).
3. 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, namely the European Cybersecurity Act (CSA).

1.2. Definitions

1. For the purpose of this scheme, the definitions in Regulation (EU) 2019/881, Regulation (EU) No 910/2014, Commission Implementing Regulation (EU) 2024/2981 and Annex XV of this scheme apply.
2. The following terms are highlighted for consistent interpretation in the Slovak national scheme:
    - wallet solution, wallet instance, wallet unit, Wallet Secure Cryptographic Application (WSCA), Wallet Secure Cryptographic Device (WSCD), critical assets, wallet user and wallet provider have the meaning assigned to them in Commission Implementing Regulation (EU) 2024/2981;
    - scheme owner means the Slovak authority responsible for maintaining this national certification scheme and coordinating its future updates;
    - national cybersecurity certification authority / NCCA means NBÚ when acting in the role assigned by Regulation (EU) 2019/881 and Slovak cybersecurity law;
    - certification body or CAB means a conformity assessment body accredited and, where applicable, authorised to perform certification activities under this scheme;
    - certificate holder means the legal entity responsible for the certified ICT service and for maintaining the certified state during the validity of the certificate;
    - incident, vulnerability, nonconformity, material change, reusable assurance information, dependency and operating-environment assumption shall be interpreted consistently with Chapters 5 to 8 and Annexes II, IX, X and XI;
    - Qualified Trust Service Provider (QTSP) prerequisite means the Slovak legal condition that the wallet solution provider must be a QTSP or must demonstrate

a valid contractual arrangement with a QTSP where required by Slovak law.

3. 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.

1.3. Assurance level

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

1.4. Conformity self-assessment

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 (normative)

2.1. Evaluation criteria for EUDIW ICT services

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.
   c) External technical reference: Wallet-Related Service Provider Security Requirements, Version 0.5.614, March 2026, based on EN 319 401, including its mappings to standards, reference documents, the EUDIW risk register and CIR (EU) 2015/1502[1]. The purpose of this reference is to support interpretation of Annex X evaluation criteria, especially where wallet-specific, PID-provider-specific, validation-service-specific or risk-register-related requirements need to be mapped to concrete controls, evidence and evaluation activities. Where the referenced document contains requirements, mappings or conformity-assessment notes that are relevant to the Slovak certified scope, the CAB shall use them as technical input to the evaluation plan, risk assessment review and criteria-to-evidence mapping. The Slovak scheme does not incorporate the referenced document by full textual reproduction, because the document is long, evolving and intended to be used as a technical baseline that may be updated independently.

2. 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.

2.2. Methods for evaluating EUDIW ICT services

[1] Or last available version

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.
4. Provider of EUDIW ICT services shall be according to Slovak law evaluated as QTSP.
5. The methodology for the evaluation of EUDIW ICT services is based on standard ETSI EN 319 403-1 (builds on EN ISO/IEC 17065), 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.
6. The methodology for the evaluation of EUDIW ICT services is based on ETSI EN 319 403-1, which itself builds on EN ISO/IEC 17065 for certification of services, and is complemented by process requirements and methods derived from CEN TS 18072 and by scheme-specific methods defined in Annex XI. This combination is necessary because the scheme relies on high-level requirements, composite and modular evaluation, reuse of assurance information from diverse origins, and assurance level High.
7. The CAB shall therefore be prepared to perform not only audit activities, but also inspection and, where required, testing activities. Audit activities are used primarily to assess the governance, organizational and operational processes of the provider. Inspection activities are used to verify technical architecture, configuration, integration logic, design assumptions and enforcement mechanisms. Testing activities are used where functional conformity, vulnerability resistance, or residual gaps in reused assurance information require direct technical validation.
8. The CAB shall apply a three-step evaluation logic for all in-scope services and processes: first, confirmation of the accuracy of the information presented by the provider; second, confirmation of the suitability of the design and controls to meet the applicable evaluation criteria; and third, confirmation of the operating effectiveness of those controls during a specified period or, for initial certification, through evidence gathered directly during tests, pilots or controlled operation.
9. Where the certification relies on composition within the scheme, or on evidence from other schemes such as EUCC, ETSI-based audits, ISO/IEC 27001 or national cybersecurity audits, the CAB shall perform a dependency and admissibility analysis before such evidence is reused. This analysis shall verify the scope, assurance level, issuer competence, validity, assumptions, nonconformities and the need for compensating controls or residual CAB activities. Reuse of evidence is encouraged, but only where its relevance and adequacy have been demonstrated.
10. Functional conformance assessment shall be treated as distinct from cybersecurity assurance evaluation. Functional tests, whether based on Functional Conformity Assessment Framework (FCAF)[2], designated national integration test suites or equivalent technical specifications, shall not be used as a substitute for security evaluation activities required for assurance level High. Likewise, vulnerability

[2] Last version of FCAF should be used in the time of certification

assessment and penetration testing shall be planned and executed in a manner appropriate to the architectural profile, criticality of the component and the residual exposure after reuse of other assurance information.

11. Provider of EUDIW ICT services shall, in accordance with Slovak law, be evaluated also in the context of trust-service and national cybersecurity obligations where relevant to the scope. The CAB shall therefore consider not only the direct product or service artefacts, but also the surrounding lifecycle, change management, incident management, vulnerability management, version management, update mechanisms and other operating controls necessary to sustain the certified state of the service over time.
12. The CAB shall use the external technical reference document on wallet-related service provider security requirements as a supporting source when selecting evaluation activities under Annex XI. The document shall not replace Annex XI methods. Instead, it shall help the CAB determine which requirements can be assessed by audit, inspection, functional testing, specific testing, interactive testing, vulnerability assessment, penetration testing or dependency analysis. Where the referenced document proposes conformity-assessment notes, these notes shall be treated as guidance unless made mandatory by this scheme, by Annex X, by Annex XI or by applicable Union or Slovak law.

2.3. Subcontracting of evaluation activities

Where the CAB subcontracts evaluation activities, it SHALL comply with Article 10 of Commission Implementing Regulation (EU) 2024/2981 and retain full responsibility for all subcontracted activities and their results. Subcontractors performing testing, inspection, audit or validation/verification activities SHALL meet the applicable competence standards, including EN ISO/IEC 17025 for testing, EN ISO/IEC 17020 for inspection, EN ISO/IEC 17021-1 for audit activities and EN ISO/IEC 17029 for validation or verification activities, where relevant to the subcontracted task.

The CAB SHALL identify all subcontracted evaluation activities in the evaluation plan, assess and document subcontractor competence, impartiality, confidentiality and information-protection arrangements, and ensure that subcontracted results are reviewed before being relied upon. The CAB SHALL notify NBÚ / the scheme owner before subcontracting security-sensitive evaluation activities, unless a stricter approval requirement is defined by accreditation, authorization or Slovak law.

3. Issuance, renewal and withdrawal of EUDIW certificates (normative)

3.1. Information necessary for certification

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) Slovak Cybersecurity Law compulsory audit according to **Act No. 69/2018 Coll. on Cybersecurity**;
    g) Slovak **Trust Services Act** - QTSP audit and qualified status.
4. After confirming the authenticity of the evaluation results, and after analyzing 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 contains 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.
7. 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.

8. The information referred to above shall include, as a minimum, the categories of information listed in Annex IV. The list in Annex IV is intentionally comprehensive but not exhaustive. The applicant remains responsible for providing any additional information, access, technical artefact, justification or explanatory material necessary for the CAB to conclude without objection on the sufficiency, suitability and effectiveness of the evidence provided.
9. Applicants for certification may provide to the certification body appropriate evaluation results from prior conformity assessments, including results under the present scheme, European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881, qualification and certification by conformity assessment bodies accredited according to CIR (EU) 2025/2162, assessments of trust service providers, conformity assessment under other accredited schemes, compulsory audits under the Slovak Cybersecurity Act, and audit and supervision outputs related to qualified trust service provider status.
10. After confirming the authenticity of the evaluation results and analysing their suitability, maturity, relevance, scope, assumptions and conformity to applicable requirements, the certification body may reuse such results only to the extent justified by the dependency analysis defined in the scheme. The CAB shall determine whether the evidence can be accepted without residual activity, accepted with compensating controls, accepted with

additional CAB testing or inspection, or rejected for the purpose of the current certification.

11. The applicant shall structure the submission so that the CAB can trace requirements to implemented controls, implemented controls to system components and operational processes, and those components and processes to concrete evidence. In particular, the applicant should provide a coherent package covering legal and organizational context, architecture and assumptions, security controls and assurance levels, reusable assurance information, risk assessment and evaluation planning, implementation artefacts, vulnerability and incident management artefacts, and public-information obligations.
12. Where the provider relies on essential standards, draft standards, architecture frameworks or component certificates as part of its justification of conformity, the provider shall explain how the requirements were interpreted and applied, how deviations or non-applicable parts were handled, and how residual risks are mitigated. Where certain relevant evidence is missing or insufficient, the certification body may suspend or pause the process until the missing information is provided.
13. Given the scope and expected depth of assessment at assurance level High, applicants should in general initiate preparation of certification evidence well in advance of the expected certification deadline. As a rule of good practice, the provider should plan for a lead time of at least six months before the assumed date of the required certification decision, without counting delays caused by incomplete or insufficient submissions.

3.2. Conditions for issuance of an EUDIW 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 authorization, 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.

3. 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.

3.3. Issuance of an EUDIW certificate

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.
7. Any certificate issued under EUDIW needs to be accompanied by a certification report, their respective contents being defined in Annexes, and which 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).

3.4. Mark and label

Transitional applicability note: *This section and Annex XII are included to preserve the structure of the EU draft candidate scheme. They shall not be used operationally in the Slovak national scheme before the European EUDIW scheme becomes applicable, or before the competent Slovak authority expressly establishes or activates a national mark and label mechanism.*

Slovak alignment note: *Until such activation, public transparency shall be based on the certificate, the certification report and the publicly available information package defined in Annex III, Annex V and Annex VI. The EUDI Wallet Trust Mark remains separate from any cybersecurity certification mark or label.*

The holder of a certificate, component providers, subcontractors and other parties involved in the certified ICT service shall not claim that an individual component, module, product, process or service is certified under this scheme unless such component, module, product, process or service is explicitly identified as the certified ICT service or as part of the certified scope in the EUDIW certificate and certification report. Any public reference to certification shall accurately reflect the scope, limitations and version covered by the certificate.

3.5. Period of validity of an EUDIW certificate

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.
3. A vulnerability assessment SHALL be carried out at least every two years during the period of validity of the certificate, in accordance with Article 5c(4) of Regulation (EU) No 910/2014 and the applicable requirements of Commission Implementing Regulation (EU) 2024/2981. The schedule in Annex II SHALL reflect this minimum frequency. The biennial vulnerability assessment MAY be incorporated into annual surveillance, recertification or a special evaluation, provided that a full vulnerability assessment is documented at least every two years.

4. Rationale
    a) 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.
    b) 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.
5. 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.

3.6. Maintenance of an EUDIW 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.
4. 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.

3.7. Withdrawal of an EUDIW certificate

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.
5. 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.

4. Conformity assessment bodies (normative)

4.1. Requirements for accreditation of a conformity assessment body

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.

4.2. Additional or specific requirements for a conformity assessment body

Transitional applicability note: *This section is included to preserve the structure of the EU draft candidate scheme. It shall not be used operationally in the Slovak national scheme before the European EUDIW scheme becomes applicable, or before the competent Slovak authority expressly establishes or activates a national mark and label mechanism. Authorisation mechanism is not applied unti l EUDIW scheme comes into force. Slovak NCCA is cooperating and being informed about the CAB accreditation by Slovak NAB.*

4.3. Notification of certification bodies

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 authorization 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 authorization:
1) date of the authorization;
2) reference number of the authorization;
3) duration of validity of the authorization;
4) scope of the authorization.

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

4.4. Termination of a certification body

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:
1) 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;
2) 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.

5. Compliance monitoring (normative)

5.1. Monitoring activities by the NCCA

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.
    d) The scheme owner SHALL also monitor the operation of this national certification scheme on the basis of information from CABs, the national accreditation body, supervisory bodies, complaints, appeals, surveillance results and certification experience. This scheme-owner monitoring supports scheme maintenance and is distinct from case-specific NCCA compliance monitoring.
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 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.
9. Rationale
    a) 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.
    b) 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 bodies so they can launch if required a special evaluation to determine how the threat is mitigated by the ICT services that they have certified.

5.2. Monitoring activities by the certification body

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; complaints and appeals received;
    c) vulnerability information that could impact the ICT services it has certified.
3. 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.

5.3. Monitoring activities by the holder of the certificate

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.
4. Rationale
    a) 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.
5. 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.

5.4. Complaints and appeals

1. The scheme owner and each CAB operating under this scheme SHALL establish, maintain and apply documented procedures for lodging, receiving, assessing and resolving complaints and appeals relating to certification activities, including certification decisions, suspension, withdrawal, monitoring activities and alleged misuse of certification claims, in accordance with Article 15 of Implementing Regulation (EU) 2024/2981. Procedures SHALL ensure impartial review by persons independent from the original decision, acknowledgement of receipt, and retention of records.
2. The CAB SHALL handle complaints and appeals in accordance with Metodické usmernenie NCCA – Pre podávanie sťažností a odvolaní (reference: 02620/2025/OBC-002), published on the NBÚ website.
3. Where a complaint or appeal falls within administrative or supervisory competence of a Slovak authority, the procedure SHALL be applied consistently with applicable Slovak law, including Act No. 71/1967 Coll. on Administrative Procedure and Act No. 9/2010 Coll. on Complaints, as amended. The right to judicial remedy under applicable law is not affected. Unresolved or material complaints or appeals that may affect scheme integrity, CAB competence or certificate validity SHALL be escalated to NBÚ / the scheme owner without undue delay.

6. Non-conformities and non-compliance (normative)

6.1. Consequences of nonconformity of a certified service

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.
3. 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.
4. 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.
5. 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.
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.
7. Rationale
    a) 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.
    b) 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.
    c) 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.
    d) 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

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;

c) 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.

6.3. Suspension of the EUDIW certificate

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 910/2014about 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.

6.4. Consequences of non-compliance by the certification body

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 authorized certification body that may be in a better technical position to perform these activities;

c) analyze 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 or any other accredited and authorized 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

c) accredited and authorized 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:

d) where necessary, report the non-compliance of the certification body to the national accreditation body;

e) where applicable, assess the potential impact on the authorization.

6. Non-compliance by the certification body of course may impact its accreditation, authorization 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 organize a review of impacted certificates by another certification body, and if issues are identified, require some conformity assessment activities to be performed again.

7. Vulnerability management (normative)

7.1. Vulnerability management procedures

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.
8. 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.

7.2. Vulnerability impact analysis

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.
3. Rationale
    a) 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.
    b) 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.
4. 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 analyzed by the certification body during regular maintenance conformity assessments.

7.3. Vulnerability impact analysis report

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 the changes in the operational environment.
8. Rationale
    a) 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.
    b) 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.
    c) 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.
9. 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.

7.4. Vulnerability remediation

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 EUDIW 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.
3. Rationale
    a) 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.
    b) 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 (normative)

8.1. Coordinated vulnerability disclosure

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.
3. Rationale
    a) 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.
    b) 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.
    c) The Article is extremely simple, and it also requires the policy to be made publicly available.

8.2. Information shared with the supervisory authorities

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 910/2014shall share the relevant information received in accordance with Section 7.2 with the national supervisory bodies established in other Member States.
6. 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.

8.3. Publication of the vulnerability

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.

9. Retention, disclosure and protection of information (normative)

9.1. Retention of records by conformity assessment bodies

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.

9.2. Information made available by the holder of a 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.
5. In addition to 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.

9.3. Information made available by ENISA

Transitional applicability note: This section is included to preserve the structure of the EU draft candidate scheme. It shall not be used operationally in the Slovak national scheme before the European EUDIW scheme becomes applicable.

9.4. Protection of information

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 organizational measures.

10. Mutual recognition

Transitional applicability note: This section is included to preserve the structure of the EU draft candidate scheme. It shall not be used operationally in the Slovak national scheme before the European EUDIW scheme becomes applicable.

11. Peer assessment

Transitional applicability note: This section is included to preserve the structure of the EU draft candidate scheme. It shall not be used operationally in the Slovak national scheme before the European EUDIW scheme becomes applicable.

12. Maintenance and final requirements

Transitional applicability note: This section is included to preserve the structure of the EU draft candidate scheme. It shall not be used operationally in the Slovak national scheme before the European EUDIW scheme becomes applicable. Annex XII covers context for adjustments of Slovak national scheme to European certification scheme.

Normative requirement: NBÚ / the scheme owner SHALL maintain this national certification scheme, review its continued adequacy and update it when required by changes in Union law, Slovak law, European guidance, standards, technical specifications, risk registers, functional conformance frameworks, architecture profiles or certification experience. Scheme changes SHALL be handled through the change-management logic described in the informative context and reflected in the applicable annexes.

Normative requirement: NBÚ / the scheme owner SHALL transmit the draft national certification scheme and any material revision to the Cooperation Group with adequate information for opinions and recommendations, in accordance with Regulation (EU) No 910/2014 and Commission Implementing Regulation (EU) 2024/2981. EU-scheme-specific final requirements shall apply when the European EUDIW scheme becomes applicable.