Official Journal
of the European Union

EN
L series

2024/2981

4.12.2024

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

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ([1]), and in particular Article 5c(6) thereof,

Whereas:

(1) Pursuant to Article 5c of Regulation (EU) No 910/2014, the certification of European Digital Identity Wallets ('wallets') is to be made in accordance with functional, cybersecurity, and data protection requirements to ensure a high level of security and trust in the wallets. Those certification requirements need to be harmonised across Member States in order to prevent market fragmentation and to build a robust framework.

(2) Regulation (EU) 2016/679 of the European Parliament and of the Council ([2]) and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ([3]) apply to the personal data processing activities under this Regulation.

(3) The Commission regularly assesses new technologies, practices, standards or technical specifications. To ensure the highest level of harmonisation among Member States for the development and certification of the wallets, the technical specifications set out in this Regulation rely on the work carried out on the basis of Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework ([4]) and in particular the Architecture and Reference Framework which is part of it. In accordance with recital 75 of Regulation (EU) 2024/1183 of the European Parliament and of the Council ([5]), the Commission should review and update this Implementing Regulation, if necessary, to keep it in line with global developments, the Architecture and Reference Framework and to follow the best practices on the internal market.

(4) In order to attest conformity to cybersecurity requirements included in the certification framework, the certification of wallet solutions should refer to, where available and relevant, European cybersecurity certification schemes established pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council ([6]). In the absence of such schemes, or when they partially cover cybersecurity requirements, this Regulation sets out the general requirements applying to national certification schemes, covering functional, cybersecurity, and data protection requirements.

([1]) OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).
([3]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).
([4]) OJ L 210, 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) 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 (OJ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).
([6]) 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) (OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Pursuant to Article 5a(11) of Regulation (EU) No 910/2014, the wallets are to be certified against assurance level high as set out in Regulation (EU) No 910/2014, as well as Commission Implementing Regulation (EU) 2015/1502 ([7]). That assurance level has to be reached by the overall wallet solution. Under this Regulation, some components of the wallet solution may be certified at a lower assurance level, provided this is duly justified and without prejudice to the assurance level high reached by the overall solution.

(6) All national certification schemes should assign a scheme owner who will be responsible for the development and maintenance of the certification scheme. The scheme owner may be a conformity assessment body, a governmental body or authority, a trade association, a group of conformity assessment bodies, or any appropriate body and can be different than the body operating the national certification scheme.

(7) The object of certification should include the software components of the wallet solution, such as the wallet instance. The wallet secure cryptographic application ('WSCA'), the wallet secure cryptographic device ('WSCD') and the platforms on which these software components are executed, while being part of the operating environment, should only be included in the object of certification when they are provided by the wallet solution. In other cases, and in particular when these devices and platforms are provided by end users, providers should establish assumptions on the wallet solution's operating environment, including on these devices and platforms, and implement measures to confirm that these assumptions are verified in practice. In order to ensure protection of critical assets through hardware and system software used to manage and protect cryptographic keys created, stored or processed by the WSCD, the WSCD needs to satisfy high standards of certification as reflected in international standards such as Common Criteria ('EUCC'), established in Commission Implementing Regulation (EU) 2024/482 ([8]), by EAL4 evaluation and advanced methodical vulnerability analysis, such as comparable to AVA_VAN.5. These certification standards should be used at the latest when certification of the conformity of wallets is carried out following a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881.

(8) Fully mobile, secure and user-friendly wallets are supported by the availability of standardised and certified tamper-resistant solutions, such as embedded secure elements, external devices such as smartcards, or embedded SIM platforms in mobile devices. It is important to ensure the timely access to embedded secure elements for national eID means and wallets and to coordinate efforts by Member States in this area. The European Digital Identity Cooperation Group established pursuant to Article 46e(1) of Regulation (EU) No 910/2014 ('Cooperation Group'), should therefore establish a dedicated subgroup for this purpose. Consulting relevant stakeholders, this subgroup should agree on a joint roadmap for access to embedded secure elements to be considered by the Commission for the review report on the Regulation (EU) No 910/2014. In order to facilitate the uptake of the wallet at national level, the Commission should furthermore, in cooperation with Member States, develop and continuously update a manual for use cases as part of the Architecture and Reference Framework.

(9) The object of certification of national certification schemes should also include the processes that are used to provide and operate the wallet solution, even if the definition or execution of those processes are subcontracted to third parties. In order to demonstrate that the processes satisfy the schemes' requirements, assurance information is allowed to be used as evidence, provided that a dependency analysis is used to determine if the assurance information is sufficient. Assurance information comes in many different forms, including reports and certificates of conformity, which can be private, national, European or international, based on standards or on technical specifications. The objective of the dependency analysis is to assess the quality of the assurance information available about a wallet's components.

([7]) Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 235, 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) 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) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Following procedures established for this purpose, the Cooperation Group should be able to provide opinions and recommendations on the draft national certification schemes submitted to it. These national certification schemes should be specific to the wallet architecture and there should be specific profiles for each specific architecture supported.

(11) In order to ensure a common understanding of, and harmonised approach to, the assessment of the most critical risks that might affect the provision and operation of wallets, a register of risks and threats that should be taken into consideration when designing wallet solutions independently of their specific architecture should be drawn-up. The cybersecurity objectives described in Regulation (EU) No 910/2014, such as confidentiality, integrity and availability of the wallet solution, as well as user and data privacy, should be borne in mind when identifying which risks should be included in the register. Due consideration of risks and threats included in this risk register should be part of the requirements of national certification schemes. To keep in line with the continuously evolving threat landscape, the risk register should be maintained and regularly updated in collaboration with the Cooperation Group.

(12) When establishing their certification schemes, scheme owners should perform a risk assessment to refine and complement the risks and threats listed in the register with risks and threats specific to the architecture or implementation of the wallet solution. The risk assessment should consider how the applicable risks and threats can be appropriately treated. Wallet providers should complement the scheme's risk assessment to identify any risks and threats specific to their implementation and propose appropriate treatment measures for evaluation by the certification body.

(13) To demonstrate that a wallet solution architecture meets the applicable security requirements, each architecture-specific scheme or profile should contain at least a description of the wallet solution architecture, a list of security requirements applicable to the wallet solution architecture, an evaluation plan to confirm that a wallet solution based on this architecture meets those requirements and a risk assessment. National certification schemes should require wallet providers to demonstrate how the design of the wallet solution that they provide matches the reference architecture and details the security controls and validation plans for the specific wallet solution. National certification schemes should also define a conformity assessment activity to verify that the wallet design properly reflects the selected profile's reference architecture. National certification schemes should comply with the requirements set out in Article 51 of Regulation (EU) 2019/881, except for its points (e) and (f), related to logging.

(14) Concerning the certification of products, certificates of conformity issued under the EU cybersecurity certification scheme on EUCC, and certificates of conformity issued under national certification schemes in the context of the SOG-IS Mutual Recognition Agreement, should be allowed to be used. Furthermore, other national certification schemes should be allowed to be used for less sensitive product components, such as those established following the standard CEN EN 17640 for fixed time cybersecurity evaluation methodology.

(15) The EU Digital Identity Wallet Trust Mark ('Trust Mark') should be used to indicate in a clear, simple and recognisable manner that a wallet has been provided in accordance with Regulation (EU) No 910/2014. Therefore, it should be considered as a mark of conformity for a wallet solution certified under national certification schemes. National certification schemes should not define any other marks of conformity.

(16) In order to discourage fraud, national certification schemes should define actions to be taken where certification under the scheme is being claimed fraudulently.

(17) To ensure an efficient management of vulnerability notifications, providers of wallet solutions and the electronic identification scheme under which they are provided should define and implement processes to evaluate the severity and potential impact of vulnerabilities. National certification schemes should set a threshold over which the certification body is to be notified. Such notification requirement should not affect the criteria established by data protection legislation and Member States' data protection authorities for notification on personal data breaches. Possible synergies could be established between the mandatory notification of breach or compromise of the wallet solutions and the notification of personal data breaches pursuant to Regulation (EU) 2016/679. The certification body's assessment of a vulnerability impact analysis report should be without prejudice to a data protection authority's assessment of a data protection impact assessment pursuant to Articles 35 and 36 of Regulation (EU) 2016/679.

(18) The providers of wallet solutions and the electronic identification scheme under which they are provided should notify the scheme owner of any justifications for exceptions to the vulnerability assessment required for the evaluation of the WSCD and WSCA, as set out in Annex IV.

(19) The cancellation of a certificate of conformity might have severe consequences such as the revocation of all deployed wallet units. Therefore, certification bodies should only consider cancellation if an unremedied vulnerability is likely to significantly affect the reliability of the wallet solution or the reliability of another wallet solution.

(20) A specific process for the update of national certification schemes should be put in place to manage the transition between successive releases of the schemes, in particular in relation to actions to be taken by the certificate holder regarding upcoming evaluations, maintenance, recertification and special evaluations.

(21) To facilitate transparency, wallet providers should publicly share security information about their wallet solution.

(22) Where national certification schemes rely on assurance information from other certification schemes or sources, a dependency analysis should be carried out to verify that the assurance documentation, for instance assurance reports and certificates of conformity, is available and adequate for the wallet solutions and the electronic identification scheme under which they are provided. The basis for this dependency analysis should be the risk assessment of the wallet solutions and the electronic identification scheme under which they are provided. The evaluation should determine whether the assurance documentation available for a given wallet solution and the electronic identification scheme under which it is provided is adequate to provide assurance corresponding to the targeted evaluation level. The evaluation should also update the dependency analysis, or entirely re-evaluate it, where necessary.

(23) Certification bodies should issue certificates of conformity in national certification schemes, together with a publicly available certification report, as referred to in Article 5d(2), point (a), of Regulation (EU) No 910/2014. The associated certification assessment report should be made available to the Cooperation Group.

(24) National certification schemes should set out yearly surveillance evaluation to ensure that the processes around the management and maintenance of the wallets are operating effectively, meaning that they operate as defined in the policies determining the processes. The biennial vulnerability assessment is a requirement stemming from Regulation (EU) No 910/2014, to ensure that the wallet solution continues to cover appropriately the cybersecurity risks and threats identified in the risk register, including any evolution of the threat landscape. The notions of surveillance evaluations, recertification evaluations and special evaluations should be in accordance with EN ISO/IEC 17021-1:2015.

(25) A certification cycle ends with the expiry of the certificate of conformity, or with the issuance of a new certificate of conformity following a successful recertification evaluation. The recertification evaluation should include an evaluation of all components of the object of certification, including an evaluation of the effectiveness and, where applicable, a vulnerability assessment. During recertification, it should be possible to reuse results from previous evaluations on components that have not changed.

(26) When a European cybersecurity certification scheme is adopted, national certification schemes with the same scope should cease issuing certifications after a defined transition period as referred to in Article 57(1) of Regulation (EU) 2019/881.

(27) National certification schemes should rely on existing frameworks and reuse evidence as appropriate in order to ensure harmonisation and interoperability. Member States may conclude agreements for the cross-border reuse of certification schemes or parts thereof. The European Commission and ENISA should, in cooperation with the Cooperation Group, support Member States in the development and maintenance of their national certification schemes ensuring knowledge-sharing and best practices.

(28) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([9]), and delivered its opinion on 30 September 2024.

(29) The measures provided for in this Regulation are in accordance with the opinion of the Committee referred to in Article 48(1) of Regulation (EU) No 910/2014,

HAS ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

This Regulation sets out reference standards and establishes specifications and procedures to build a robust framework for the certification of wallets to be updated on a regular basis to keep in line with technology and standards developments and with the work carried out on the basis of Recommendation (EU) 2021/946 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework, and in particular the Architecture and Reference Framework.

Article 2

Definitions

For the purpose of this Regulation, the following definitions apply:

(1) 'wallet solution' means a combination of software, hardware, services, settings, and configurations, including wallet instances, one or more wallet secure cryptographic applications and one or more wallet secure cryptographic devices;

(2) 'scheme owner' means an organisation which is responsible for developing and maintaining a certification scheme;

(3) 'object of certification' means products, processes and services or a combination thereof to which specified requirements apply;

(4) 'wallet secure cryptographic application' means an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device;

(5) 'wallet instance' means the application installed and configured on a wallet user's device or environment, which is part of a wallet unit, and that the wallet user uses to interact with the wallet unit;

([9]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(6) ‘wallet secure cryptographic device’ means a tamper-resistant device that provides an environment that is linked to and used by the wallet secure cryptographic application to protect critical assets and provide cryptographic functions for the secure execution of critical operations;

(7) ‘risk register’ means a record of information relevant to the certification process about identified risks;

(8) ‘wallet provider’ means a natural or legal person who provides wallet solutions;

(9) ‘certification body’ means a third-party conformity assessment body operating certification schemes;

(10) ‘wallet unit’ means a unique configuration of a wallet solution that includes wallet instances, wallet secure cryptographic applications and wallet secure cryptographic devices provided by a wallet provider to an individual wallet user;

(11) ‘critical assets’ means assets within or in relation to a wallet unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, this would have a very serious, debilitating effect on the ability to rely on the wallet unit;

(12) ‘wallet user’ means a user who is in control of the wallet unit;

(13) ‘incident’ means an incident as defined in point (6) of Article 6 of Directive (EU) 2022/2555 of the European Parliament and of the Council ([10]);

(14) ‘embedded disclosure policy’ means a set of rules, embedded in an electronic attestation of attributes by its provider, that indicates the conditions that a wallet-relying party has to meet to access the electronic attestation of attributes.

CHAPTER II

NATIONAL CERTIFICATION SCHEMES

Article 3

Establishment of national certification schemes

1. Member States shall assign a scheme owner for each national certification scheme.

2. The object of certification defined in national certification schemes shall be the provision and operation of wallet solutions and of the electronic identification schemes under which they are provided.

3. In accordance with Implementing Regulation (EU) 2015/1502, the object of certification in national certification schemes shall include the following elements:

(a) the software components, including settings and configurations of a wallet solution and of the electronic identification scheme under which the wallet solutions are provided;

(b) the hardware components and platforms on which the software components referred to in point (b) run on or rely upon for critical operations, in cases where they are provided directly or indirectly by the wallet solution and electronic identification scheme under which they are provided and when they are required to meet the desired level of assurance for those software components. When the hardware components and platforms are not provided by the wallet provider, national certification schemes shall formulate assumptions for evaluation of the hardware components and platforms, under which resistance against attackers with high attack potential in line with Implementing Regulation (EU) 2015/1502 can be provided, and specify the evaluation activities to confirm these assumptions as referred in Annex IV;

([10]) 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) (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(c) the processes that support the provision and operation of a wallet solution, including the user onboarding process as referred to in Article 5a of Regulation (EU) No 910/2014, covering at least enrolment, electronic means management and organisation pursuant to section 2.1, 2.2, and 2.4 of Annex I to Implementing Regulation (EU) 2015/1502.

4. National certification schemes shall include a description of the specific architecture of the wallet solutions and of the electronic identification scheme under which they are provided. When national certification schemes cover more than one specific architecture, they shall include a profile for each specific architecture.

5. For each profile, national certification schemes shall set out at least the following:

(a) the specific architecture of a wallet solution and of the electronic identification scheme under which they are provided;

(b) the security controls associated to assurance levels set out in Article 8 of Regulation (EU) No 910/2014;

(c) an evaluation plan drawn-up in accordance with section 7.4.1 of EN ISO/IEC 17065:2012;

(d) the security requirements necessary to address the cybersecurity risks and threats listed in the risk register set out in Annex I of this Regulation, up to the required assurance level, and to meet, where applicable, the objectives defined in Article 51 of Regulation (EU) 2019/881;

(e) a mapping of the controls referred to in point (b) of this paragraph to the components of the architecture;

(f) a description of how the security controls, the mapping, the security requirements and the evaluation plan referred to in points (b) to (c) allow providers of wallet solutions and the electronic identification scheme under which they are provided to adequately address the cybersecurity risks and threats identified in the risk register referred to in point (d), up to the required assurance level based on a risk assessment to refine and complement the risks and threats listed in the risk register with risks and threats specific to the architecture.

6. The evaluation plan referred to in paragraph 5, point (c) shall list evaluation activities to be included in the evaluation of wallet solutions and of the electronic identification scheme under which they are provided.

7. The evaluation activity referred to in paragraph 6 shall require providers of wallet solutions and the electronic identification scheme under which they are provided to provide information meeting the requirements listed in Annex II.

Article 4

General requirements

1. National certification schemes shall cover functional, cybersecurity and data protection requirements by using, when available and applicable, the following certification schemes:

(a) European cybersecurity certification schemes established pursuant to Regulation (EU) 2019/881, including the EUCC;

(b) national cybersecurity certification schemes covered by the EUCC, in accordance with Article 49 of Implementing Regulation (EU) 2024/482.

2. National certification schemes may, in addition, when available and applicable, refer to:

(a) other relevant national certification schemes;

(b) international, European, and national standards;

(c) technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([11]).

3. National certification schemes shall:

(a) specify the elements listed in section 6.5 of EN ISO/IEC 17067:2013;

(b) be implemented as a type 6 scheme, in accordance with section 5.3.8 of EN ISO/IEC 17067:2013.

4. National certification schemes shall comply with the following requirements:

(a) only providers referred to in Article 5a(2) of Regulation (EU) No 910/2014 are eligible to be issued certificates under the national certification schemes;

(b) only the Trust Mark is used as mark of conformity;

(c) providers of wallet solutions and the electronic identification scheme under which they are provided include references to Regulation (EU) No 910/2014 and this Regulation when referring to the scheme;

(d) providers of wallet solutions and the electronic identification scheme under which they are provided, complement the scheme's risk assessment as referred to in Article 3, paragraph 5 point (f), to identify risks and threats specific to their implementation and propose appropriate treatment measures for all relevant risks and threats;

(e) responsibilities and the legal action are established and include references to the applicable national legislation, which defines the responsibilities and possible legal action, where certification under the scheme is being used fraudulently.

5. The assessment referred to in paragraph 4, point (d) shall be shared with the certification body for evaluation.

Article 5

Incident and vulnerability management

1. National certification schemes shall contain incident and vulnerability management requirements in accordance with paragraphs 2 to 9.

2. The holder of a certificate of conformity of a wallet solution and of the electronic identification scheme under which it is provided shall notify their certification body without undue delay of any breach or compromise of the wallet solution, or of the electronic identification scheme under which it is provided, that is likely to impact its conformity with the requirements of the national certification schemes' requirements.

3. The holder of a certificate of conformity shall establish, maintain and operate a vulnerability management policy and procedures, taking into account the procedures set out in existing European and international standards, including EN ISO/IEC 30111:2019.

4. The holder of the certificate of conformity shall notify the issuing certification body of the vulnerabilities and changes affecting the wallet solution, based on defined criteria on the impact of these vulnerabilities and changes.

5. The holder of the certificate of conformity shall prepare a vulnerability impact analysis report for any vulnerability that affects the software components of the wallet solution. The report shall include the following information:

(a) the impact of the vulnerability on the certified wallet solution;

(b) possible risks associated with the proximity or likelihood of an attack;

([11]) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(c) whether the vulnerability can be remedied using available means;

(d) where the vulnerability can be remedied using available means, possible ways to remedy the vulnerability.

6. Where notification is required in paragraph 4, the holder of the certificate of conformity shall transmit, without undue delay, the vulnerability impact analysis report referred to in paragraph 5 to the certification body.

7. The holder of a certificate of conformity shall establish, maintain and operate a vulnerability management policy meeting the requirements set out in Annex I to the Cyber Resilience Act ([12]).

8. National certification schemes shall establish vulnerability disclosure requirements applicable to certification bodies.

9. The holder of a certificate of conformity shall disclose and register any publicly known and remediated vulnerability in the wallet solution or in one of the online repositories referred to in Annex V.

Article 6

Maintenance of national certification schemes

1. National certification schemes shall contain a process for reviewing their operation on a periodic basis. That process shall aim at confirming their adequacy and at identifying aspects requiring improvement, taking into account feedback from stakeholders.

2. National certification schemes shall include provisions concerning their maintenance. This process shall include at least the following requirements:

(a) rules for the governance of the national certification schemes' definition and requirements;

(b) the establishment of timelines for the issuance of certificates following the adoption of updated versions of the national certification schemes, both for new certificates of conformity and for previously issued ones;

(c) a periodic review of the national certification schemes, to ensure that the national certification schemes' requirements are being applied in a consistent manner, taking into account at least the following aspects:

— requests for clarification addressed to the scheme owner related to the national certification scheme requirements;

— feedback from stakeholders and other interested parties;

— responsiveness of the national certification scheme owner to requests of information.

(d) rules for monitoring reference documents and procedures for the evolution of national certification schemes' reference versions, including at least transition periods;

(e) a process to ensure the latest cybersecurity risks and threats as listed in the risk register set out in Annex I of this Regulation are covered;

(f) a process for managing other changes in national certification schemes.

([12]) 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) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. National certification schemes shall contain requirements for performing evaluations on currently certified products within a certain period after the revision of the scheme, or after the release of new specifications or standards, or new versions thereof, with which the wallet solutions and the electronic identification scheme under which they are provided shall comply.

CHAPTER III

REQUIREMENTS RELATING TO SCHEME OWNERS

Article 7

General requirements

1. Scheme owners shall develop and maintain national certification schemes and govern their operations.

2. Scheme owners may subcontract all or part of their tasks to a third party. When subcontracting to a private party, scheme owners shall set out the duties and responsibilities of all parties by contract. Scheme owners shall remain responsible for all subcontracted activities performed by their subcontractors.

3. Scheme owners shall perform their monitoring activities, if applicable, at least on the basis of the following information:

(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 and appeals received pursuant to Article 15.

4. Scheme owners shall inform the Cooperation Group of revisions to the national certification schemes. That notification shall provide adequate information for the Cooperation Group to issue recommendations to scheme owners and opinions about the updated national certification schemes.

CHAPTER IV

REQUIREMENTS RELATING TO PROVIDERS OF WALLET SOLUTIONS AND THE ELECTRONIC IDENTIFICATION SCHEME UNDER WHICH THEY ARE PROVIDED

Article 8

General requirements

1. National certification schemes shall contain cybersecurity requirements based on a risk assessment of each specific supported architecture. Those cybersecurity requirements shall aim to treat the identified cybersecurity risks and threats, as established in the risk register set out in Annex I.

2. In line with Article 5a(23) of Regulation (EU) No 910/2014, national certification schemes shall require wallet solutions, and the electronic identification schemes under which they are provided, to be resistant against attackers with high attack potential for assurance level high, as referred to Implementing Regulation (EU) 2015/1502.

3. National certification schemes shall establish security criteria, which shall include the following requirements:

(a) Cyber Resilience Act where applicable, or requirements meeting the security objectives set out in Article 51 of Regulation (EU) 2019/881;

(b) the establishment and implementation of policies and procedures concerning the management of risks associated with the operation of a wallet solution, including the identification and assessment of risks and the mitigation of the identified risks;

(c) the establishment and implementation of policies and procedures related to the management of changes and to the management of vulnerabilities in accordance with Article 5 of this Regulation;

(d) the establishment and implementation of human resource management policies and procedures, including requirements on expertise, reliability, experience, security training, and qualifications of personnel involved in the development or operation of the wallet solution;

(e) requirements relating to the wallet solution's operating environment, including in the form of assumptions on the security of the devices and platforms on which the software components of the wallet solution run, including WSCDs and where applicable and relevant, conformity assessment requirements to confirm that those assumptions are verified on the relevant devices and platforms;

(f) for each assumption that is not backed by a certificate of conformity or other acceptable assurance information, a description of the mechanism that the wallet provider uses to enforce the assumption, as well as a justification that the mechanism is sufficient to ensure that the assumption is verified;

(g) the establishment and implementation of measures to ensure the use of a currently certified version of the wallet solution.

4. National certification schemes shall contain functional requirements relating to update mechanisms for every software component of the wallet solutions and the electronic identification scheme under which they are provided for the operations listed in Annex III.

5. National certification schemes shall require that the following information and documentation is provided or otherwise made available to the certification body by the applicant for certification:

(a) evidence related to the information referred to in Annex IV, point 1, including where necessary details on the wallet solution and its source code, including:

— *architecture information:* for every component of the wallet solution (including product, process and service components), a description of its essential security properties, including its external dependencies;

— *controls and assurance levels:* for every security control of the wallet solution, a description of the control and the required assurance level, based on the Annex to Implementing Regulation (EU) 2015/1502, which sets out a number of technical specifications and procedures that apply to the various controls implemented by the electronic identification means;

— *mapping the controls to architecture components:* a description of how the controls of the wallet are implemented using the different components of the wallet solution, based on a rationale explaining why a given assurance level is required, and how the control is implemented with all required security aspects at the appropriate level;

— *rationale and justification of risk coverage:* a justification of:

  — the mapping of controls to components;

  — the suitability of the proposed evaluation plan to appropriately cover all controls;

  — the coverage provided by the controls of the cybersecurity risks and threats identified in the risk register, complemented by controls of risks and threats specific to the implementation, at the appropriate assurance level;

(b) the information listed in Annex V;

(c) a complete list of the certificates of conformity and other assurance information used as evidence during the evaluation activities;

(d) any other information relevant for the evaluation activities.

CHAPTER V

REQUIREMENTS RELATING TO CERTIFICATION BODIES

Article 9

General requirements

1. Certification bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008 of the European Parliament and of the Council ([13]) in accordance with EN ISO/IEC 17065:2012, provided that they comply with the requirements set out in national certification schemes in accordance with paragraph 2.

2. For the purposes of accreditation, certification bodies shall comply with all the following competence requirements:

(a) detailed and technical knowledge of the relevant architectures of a wallet solution and of the electronic identification scheme under which they are provided, as well as of the threats and risks relevant to those architectures;

(b) knowledge of available security solutions and of their properties pursuant to the Annex of Implementing Regulation (EU) 2015/1502;

(c) knowledge of the activities performed in virtue of certificates of conformity applied to components of the wallet solution and the electronic identification scheme under which they are provided, as being the object of certification;

(d) detailed knowledge of the applicable national certification scheme as established in accordance with Chapter II.

3. Certification bodies shall perform their surveillance activities in particular on the basis of the following information:

(a) information coming from national accreditation bodies, and relevant market surveillance authorities;

(b) information resulting from their own or another authority's audits and investigations;

(c) complaints and appeals received pursuant to Article 15.

Article 10

Subcontracting

Certification bodies may subcontract the evaluation activities, as set out in Article 13, to third parties. Where evaluation activities are subcontracted, national certification schemes shall establish the following:

(1) all subcontractors of the certification body performing evaluation activities shall, as applicable and appropriate for the activities to be performed, meet the requirements of harmonised standards like EN ISO/IEC 17025:2017 for testing, EN ISO/IEC 17020:2012 for inspection, EN ISO/IEC 17021-1:2015 for audit, and EN ISO/IEC 17029:2019 for validation and verification;

(2) certification bodies shall take responsibility for all evaluation activities outsourced to other bodies and demonstrate that they have taken appropriate measures during their accreditation, including by relying on their subcontractors' own accreditation, when applicable;

(3) the degree to which prior agreement to outsourcing needs shall be obtained from scheme owners or the client whose wallet solution is being certified under the certification scheme.

([13]) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Article 11

Notification to the supervisory body

Certification bodies shall notify the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014 of the issuance, suspension and cancellation of certificates of conformity of wallet solutions and the electronic identification scheme under which they are provided.

Article 12

Incident and vulnerability management

1. Certification bodies shall suspend, without undue delay, the certificate of conformity of the wallet solutions and the electronic identification scheme under which they are provided after they confirm that the notified security breach or compromise impacts the conformity with the national certification schemes' requirements, of the wallet solution or of the electronic identification scheme under which they are provided.

2. Certification bodies shall cancel the certificate of conformity that has been suspended following a security breach or compromise that has not been remedied in a timely manner.

3. Certification bodies shall cancel certificates of conformity where an identified vulnerability has not been remedied commensurately with its severity and potential impact in a timely manner, in accordance with Articles 5c(4) and 5e(2) of Regulation (EU) No 910/2014.

CHAPTER VI

CONFORMITY ASSESSMENT ACTIVITIES

Article 13

Evaluation activities

1. National certification schemes shall contain methods and procedures to be used by the conformity assessment bodies when conducting their evaluation activities in accordance with EN ISO/IEC 17065:2012, which shall cover at least the following aspects:

(a) the methods and procedures to conduct evaluation activities, including those related to WSCD, as set out in Annex IV;

(b) the audit of the implementation of the wallet solution and the electronic identification scheme under which they are provided, based on the risk register, set out in Annex I and complemented where necessary by implementation-specific risks;

(c) functional testing activities, based, when available and appropriate, on test suites that are defined according to technical specifications or standards;

(d) assessment of the existence and suitability of maintenance processes, including at least version management, update management and vulnerability management;

(e) assessment of the operating effectiveness of the maintenance processes, including at least version management, update management and vulnerability management;

(f) dependency analysis provided by the wallet provider, including a methodology to assess the acceptability of assurance information, which shall include the elements set out in Annex VI;

(g) vulnerability assessment, at the appropriate level, including:

— a review of the design of the wallet solution, and where applicable, of its source code;

— testing of the resistance of the wallet solution against attackers with high attack potential for assurance level 'high' pursuant to Section 2.2.1 of the Annex to Implementing Regulation (EU) 2015/1502;

(h) assessment of the evolution of the threat environment and its impact on the coverage of the risks by the wallet solution, to determine which evaluation activities are required on the various components of the wallet solution.

2. National certification schemes shall contain an evaluation to determine whether the implementation of wallet solutions and the electronic identification scheme under which those wallet solutions are provided match the architecture set out in Article 3 paragraph 5, point (a), as well as an evaluation to determine whether the evaluation plan proposed together with the implementation matches the evaluation plan referred to in Article 3 paragraph 5, point (c).

3. National certification schemes shall set out sampling rules, in order to avoid the repetition of identical evaluation activities and to focus on activities that are specific to a given variant. Those sampling rules shall allow functional and security tests to be performed only on a sample of variants of a target component of a wallet solution and the electronic identification scheme under which they a provided and on a sample of target devices. National certification schemes shall require all certification bodies to justify their use of sampling.

4. National certification schemes shall require the evaluation, by the certification body, of the WSCA based on the methods and procedures set out in Annex IV.

Article 14

Certification activities

1. National certification schemes shall set out an attestation activity for the purpose of issuing a certificate of conformity, in accordance with section V(a) of EN ISO/IEC 17067:2013, Table 1, including the following aspects:

(a) the content of the certificate of conformity as set out in Annex VII;

(b) how the results of the evaluation are to be reported in the public certification report, including at least a summary of the preliminary audit and validation plan, as set out in Annex VIII;

(c) the content of the evaluation results reported in the certification assessment report, including the elements set out in Annex VIII.

2. The certification assessment report may be made available to the Cooperation Group and to the Commission.

Article 15

Complaints and appeals

National certification schemes shall contain procedures or references to the applicable national legislation, which define the mechanism to effectively lodge and handle complaints and appeals in relation to their implementation of the certification scheme or to a certificate of conformity issued. These procedures shall include the provision of information to the complainant of the progress of the proceedings and on the decision taken, and information to the complainant on the right to an effective judicial remedy. National certification schemes shall require that all complaints and appeals that have not been or cannot be resolved by the certification body are sent to the scheme owner for assessment and resolution.

Article 16

Surveillance activities

1. National certification schemes shall require certification bodies to implement surveillance activities consisting of surveillance evaluation of processes combined with random tests or inspections.

2. National certification schemes shall contain requirements for scheme owners to monitor the compliance of certification bodies with their obligations pursuant to Regulation (EU) No 910/2014 and pursuant to national certification schemes, if applicable.

3. National certification schemes shall contain requirements for certification bodies to monitor the following:

(a) compliance by holders of a certificate of conformity issued under national certification schemes with their obligations concerning certification pursuant to Regulation (EU) No 910/2014 and pursuant to national certification schemes;

(b) compliance of the certified wallet solution with the requirements set out in national certification schemes.

Article 17

Consequences of non-compliance

National certification schemes shall set out the consequences of non-conformity of a certified wallet solution and of the electronic identification scheme under which they are provided, with the requirements set out in this Regulation. Those consequences shall include the following aspects:

(1) the obligation on the certification body to inform the holder of the certificate of conformity and to request the holder of the certificate of conformity to apply remedial actions;

(2) the obligation on the certification body to inform other relevant market surveillance authorities where the non-conformity concerns relevant Union legislation;

(3) the conditions for carrying out remedial actions by the holder of the certificate of conformity;

(4) the conditions for the suspension of a certificate of conformity by the certification body and for restoration of the certificate of conformity after the non-conformity has been remediated;

(5) the conditions for cancellation of a certificate of conformity by the certification body;

(6) the consequences of non-compliance by the certification body with the requirements of the national certification scheme.

CHAPTER VII

CERTIFICATION LIFECYCLE

Article 18

Certification lifecycle

1. The validity of certificates of conformity issued under national certification schemes shall be subject to regular evaluation activities by the certification body carried out in accordance with the requirements set out in Annex IX.

2. National certification schemes shall contain a process for the recertification of wallet solutions and the electronic identification scheme under which they are provided, upon request of the holder of the certificate of conformity before the expiry of the initial certificate of conformity. That process for recertification shall include a full evaluation of the wallet solution and of the electronic identification scheme under which they are provided, including a vulnerability assessment, following the principles set out in Annex IX.

3. National certification schemes shall contain a process for managing changes in a certified wallet solution and the electronic identification scheme under which they are provided. That process shall include rules for determining whether a change is to be covered by a special evaluation as referred to in paragraph 4 or by the verification of the operating effectiveness of the maintenance processes as referred to Annex IV.

4. National certification schemes shall contain a process for special evaluations in accordance with EN ISO/IEC 17065:2012. That process for special evaluations shall include a selection of activities to be performed to address the specific issue that triggered the special evaluation.

5. National certification schemes shall set out rules related to the cancellation of a certificate of conformity.

CHAPTER VIII

RECORDKEEPING AND PROTECTION OF INFORMATION

Article 19

Retention of records

1. National certification schemes shall contain requirements for certification bodies concerning a record system for all relevant information produced in connection with the conformity assessment activities that they perform, including data issued and received by providers of wallet solutions and the electronic identification schemes under which they are provided. The records of such information shall be stored in a secure manner. The records may be kept electronically and shall remain accessible for as long as required by Union law or national law, and for at least five years, after the cancellation or expiry of the relevant certificate of conformity.

2. National certification schemes shall set out requirements for the holder of the certificate of conformity to store the following information securely for the purpose of this Regulation, and for at least five years after the cancellation or expiry of the relevant certificate of conformity:

(a) records of the information provided to the certification body or any of its sub-contractors during the certification process;

(b) specimens of hardware components that have been included in the scope of certification for the wallet solution.

3. National certification schemes shall require the holder of the certificate of conformity to make the information referred to in paragraph 1 available to the certification body or the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014 upon request.

Article 20

Protection of information

Under national certification schemes, all persons or organisations that are granted access to information in the execution of activities under the national certification scheme shall be required to ensure the security and protection of trade secrets and other confidential information, as well as preserving intellectual property rights, and take the necessary and appropriate technical and organisational measures to ensure this confidentiality.

CHAPTER IX

FINAL PROVISIONS

Article 21

Transition to a European cybersecurity certification scheme

This Regulation shall be subject to review, on the adoption of the first European cybersecurity certification scheme for wallet solutions and the electronic identification schemes under which they are provided, with the objective of taking into account the contribution of such a European cybersecurity certification scheme to the overall certification of wallet solutions and the electronic identification schemes under which they are provided.

Article 22

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 28 November 2024.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

RISK REGISTER FOR EUROPEAN DIGITAL IDENTITY WALLETS

Introduction

The risk register describes the main security and privacy risks and threats that apply to wallets, and which shall be properly addressed in every architecture and implementation of wallets. The **high-level risks** (Section I) are related to the use of wallets by users and relying parties, and they are associated to direct threats targeting the assets of wallets. In addition, a few **system-level risks** (Section II) to wallets are identified, which would typically result from a combination of threats applying to the entire wallet system.

Risk type	Risk ID	Related risk titles
High-level risks to the wallets	R1	Creation or use of an existing electronic identity
	R2	Creation or use of a fake electronic identity
	R3	Creation or use of fake attributes
	R4	Identify theft
	R5	Data theft
	R6	Data disclosure
	R7	Data manipulation
	R8	Data loss
	R9	Unauthorised transaction
	R10	Transaction manipulation
	R11	Repudiation
	R12	Transaction data disclosure
	R13	Service disruption
	R14	Surveillance
System-related risks	SR1	Wholesale surveillance
	SR2	Reputational damage
	SR3	Legal non-compliance

The register also identifies **technical threats** (Section III) targeting the implementation of the wallet solution. These threats are related to the high-level risks in the sense that each one of them could be used to trigger many high-level risks.

Threat type	Threat ID	Related threat titles	Subcategories of threats
Technical threat	TT1	Physical attacks	1.1 *Theft*
			1.2 *Information leakage*
			1.3 *Tampering*
	TT2	Errors and misconfigurations	2.1 *Errors made when managing an IT system*
			2.2 *Application-level errors or usage errors*
			2.3 *Development-time errors and system misconfigurations*

Threat type	Threat ID	Related threat titles	Subcategories of threats
	TT3	Use of unreliable resources	3.1 *Erroneous use or configuration of wallet components*
	TT4	Failure and outages	4.1 *Failure or dysfunction of equipment, devices or systems*
			4.2 *Loss of resources*
			4.3 *Loss of support services*
	TT5	Malicious actions	5.1 *Interception of information*
			5.2 *Phishing and spoofing*
			5.3 *Replay of messages*
			5.4 *Brute-force attack*
			5.5 *Software vulnerabilities*
			5.6 *Supply chain attacks*
			5.7 *Malware*
			5.8 *Random number prediction*

Finally, the register **lists direct threats to the wallets**, and each one is associated to a (non-exhaustive) selection of risks (Section IV).

SECTION I

High-level risks to the wallets

R1. Creation or use of an existing electronic identity

Creation or use of an existing electronic identity is defined as the creation of an electronic identity in a wallet that exists in the real world and is assigned to another user. By essence, this risk leads to the risks of Identity theft (R4), and Unauthorised transactions (R9).

R2. Creation or use of a fake electronic identity

Creation or use of a fake electronic identity is defined as the creation of an electronic identity in a wallet that does not exist in the real world.

R3. Creation or use of fake attributes

Creation or use of fake attributes is defined as the creation or use of attributes that cannot be validated to be issued by the claimed provider and cannot be trusted.

R4. Identify theft

Identity theft is defined as the unauthorised acquisition of the wallet unit or loss of authentication factors enabling to impersonate a person.

R5. Data theft

Data theft is defined as the unauthorised extraction of data. Data theft is also associated to threats, such as data interception (unauthorised capture of data in transit) and data decryption (unauthorised decoding of encrypted data), which are likely to lead in some cases to Data disclosure (R6).

R6. Data disclosure

Data disclosure is defined as the unauthorised exposure of personal data including special categories of personal data. The privacy breach risk is very similar when considered from a privacy rather than security viewpoint.

R7. Data manipulation

Data manipulation is defined as the unauthorised alteration of data.

R8. Data loss

Data loss is defined as the situation where data stored in the wallet is lost through misuse or malicious action. This risk is often a secondary risk of Data manipulation (R7) or Service disruption (R13), where all or part of the data cannot be restored.

R9. Unauthorised transaction

Unauthorised transactions are defined as operational activities conducted without the permission or knowledge of the wallet user. In many cases, an unauthorised transaction can lead to Identity theft (R4) or Data disclosure (R6). It is also related to unauthorised transactions, such as the misuse of cryptographic keys.

R10. Transaction manipulation

Transaction manipulation is defined as the unauthorised alteration of operations in the wallet. Transaction manipulation is an attack on integrity, and it is related to a data integrity breach.

R11. Repudiation

Repudiation is defined as a situation where a stakeholder can deny performing an action or being involved in a transaction, and other stakeholders do not have proper evidence to contradict them.

R12. Transaction data disclosure

Transaction data disclosure is defined as the disclosure of information related to information on a transaction between stakeholders.

R13. Service disruption

Service disruption is defined as an interruption or degradation in the normal operation of the wallet. A specific kind of service disruption is user lock-out, defined as the inability of a user to access their account or their wallet.

R14. Surveillance

Surveillance, or monitoring, is defined as the unauthorised tracking or observation of a wallet user's activities, communication, or data. Surveillance is often related to inference, which is defined as the deduction of sensitive or personal information from seemingly innocuous data.

SECTION II

System-related risks

These risks are not used in the list of threats, as they are usually the consequence of multiple threats, repeated in a way that threatens the full system.

SR1. Wholesale surveillance

Wholesale surveillance is defined as the tracking or observation of the activities of many users through their wallet's communication or data. Wholesale surveillance is often associated to surveillance (R14) and inference at a global scale, where information about many users is combined to deduce sensitive or personal data about users or to identify statistical trends that can be used to design further attacks.

SR2. Reputational damage

Reputational damage is defined as the harm caused to an organisation's or governmental body's reputation. Reputational damage will also stem from other risks when a breach or incident is covered by media and paints the organisation under an unfavourable light. Reputational damage can lead to further risks, such as loss of trust, stemming from the user's reasonable doubts, and loss of ecosystem, when the full ecosystem collapses.

SR3. Legal non-compliance

Legal non-compliance is defined as a situation when relevant laws, regulations or standards cannot be adhered to. In the context of the wallet, as security and privacy of the solution are legal requirements, all threats are likely to lead to some kind of legal non-compliance.

SECTION III

Technical threats

The technical threats are not all linked to specific risks on the wallets, because many of them are means that could be used to implement attacks corresponding to many different risks.

TT1. Physical attacks

1.1 *Theft*

Theft is defined as the theft of devices that may alter the wallet's proper functioning (in case the device is stolen and the wallet unit is not adequately protected). This may contribute to many risks, including Identity theft (R4), Data theft (R5), and Unauthorised transactions (R9).

1.2 *Information leakage*

Information leakage is defined as unauthorised access, information exposure, or sharing after physical access to the wallet. This may contribute in particular to Data Disclosure (R6) and Data theft (R5).

1.3 *Tampering*

Tampering is defined as violating the integrity of one or multiple components of the wallet unit, or of the components the wallet unit relies on, e.g., the user device or its operating system. This may contribute in particular to Data manipulation (R7), Data loss (R8) and Transaction manipulation (R10). When tampering targets software components, it may contribute to many risks.

TT2. Errors and misconfigurations

2.1 *Errors made when managing an IT system*

Errors made when managing an IT system are defined as information leakage, sharing or damage caused by misuse of IT assets by users (lack of awareness of application features) or by improper configuration or management of IT assets.

2.2 *Application-level errors or usage errors*

Application-level errors or usage errors are defined as dysfunctions of the application due to an error in the application itself or to an error by one of the users (wallet users and relying parties).

2.3 *Development-time errors and system misconfigurations*

Development-time errors and system misconfigurations are defined as dysfunction or vulnerabilities caused by improperly developed or configured IT assets or business processes (inadequate specifications of IT products, inadequate usability, insecure interfaces, improper policy and procedure flows, design errors).

TT3. Use of unreliable resources

The use of unreliable resources is defined as an activity leading to unintentional damage due to ill-defined trust relationships, such as trusting a third-party provider without sufficient assurance.

3.1 *Erroneous use or configuration of wallet components*

An erroneous use or configuration of wallet components is defined as unintentional damage to wallet components due to an erroneous use or misconfiguration by wallet users or by insufficiently trained developers, or due to lack of adaptation to changes in the threat landscape, typically the use of vulnerable third-party components or runtime platforms.

TT4. Failure and outages

4.1 *Failure or dysfunction of equipment, devices or systems*

A failure or dysfunction of equipment is defined as unintentional damage to IT assets due to a failure or dysfunction of equipment, including the provider's infrastructure and the user devices.

4.2 *Loss of resources*

The loss of resources is defined as an outage or dysfunction due to unavailability of such resources, e.g., as maintenance parts.

4.3 *Loss of support services*

The loss of support services is defined as an outage or dysfunction due to unavailability of support services required for proper operation of the system, including network connectivity of the provider's infrastructure and of the user device.

TT5. Malicious actions

5.1 *Interception of information*

The interception of information is defined as the capture of information improperly secured in transmission, including man-in-the-middle attacks.

5.2 *Phishing and spoofing*

Phishing is defined as the capture of information provided by the user following a deceptive interaction, often associate to the spoofing of legitimate communication means and websites. These threats target the user and typically contribute to Identity theft (R4) and Unauthorised transactions (R9), often through Data theft (R5) or Data disclosure (R6).

5.3 *Replay of messages*

Replay of messages is defined as the reuse of previously intercepted messages to perform unauthorised transactions, often at protocol level. This technical threat mainly contributes to unauthorised transactions, which may then lead to other risks, depending on the transaction.

5.4 *Brute-force attack*

Brute-force attack is defined as a breach of security, often confidentiality, by performing a large number of interactions until the responses provide valuable information.

5.5 *Software vulnerabilities*

The threat related to software vulnerabilities is a breach of security through exploitation of a software vulnerability in the components of the wallet or in the software and hardware components used in the implementation of the wallet, including published vulnerabilities and unpublished (0-day) vulnerabilities.

5.6 *Supply chain attacks*

A supply chain attack is defined as a breach of security through attacks perpetrated on the supplier of the wallet provider or of its users to enable further attacks on the wallet itself.

5.7 *Malware*

Malware is defined as a breach of security through malicious applications performing unwanted and illegitimate actions on the wallet.

5.8 *Random number prediction*

Random number prediction is defined as the enablement of brute-force attacks through partial or complete prediction of generated random numbers.

SECTION IV

Threats to the wallets

This last section presents a selection of typical threat scenarios specific to the wallets, which are mapped to the key related high-level risks, as listed above. This list indicates threats that need to be covered, but it does not constitute an exhaustive list of threats, which depends greatly on the architecture of the selected wallet solution and on the evolution of the threat environment. Additionally, in the risk assessment and proposed measures, the wallet provider can only be responsible for those components in scope of certification (*).

ID *Identifier*	Threat description *Description of the identified threat* (*)	Risk title *Related risks*
TR1	An attacker can revoke pseudonyms without justified reason.	Creation or use of a fake electronic identity (R2)
TR2	An attacker can issue fabricated electronic identities that do not exist.	Creation or use of a fake electronic identity (R2)
TR3	An attacker can start to issue unauthorised PIDs.	Creation or use of a fake electronic identity (R2)
TR4	An attacker can get an administrator to enter a wrong PID provider into the PID provider trusted list.	Creation or use of a fake electronic identity (R2)
TR5	An attacker can bypass the remote identity proofing service.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR6	An attacker can bypass the physical identity proofing service.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR7	An attacker can bypass the identity proofing services related to the use of a remote (qualified) certificate.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR8	An attacker can get access to a wallet that is not bound to a person.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR9	An attacker can defeat technical and procedural controls to create wrong PIDs.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR10	An attacker can activate a new wallet on an invalid WSCD.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR11	An attacker can bypass the identity proofing service related to the use of existing eID means.	Creation or use of an existing electronic identity (R1) / Identify theft (R4) / Unauthorised transaction (R9)
TR12	An attacker can circumvent the verification by the PID provider that the wallet is controlled by the user and have a PID issued into a compromised wallet under the attacker's control.	Creation or use of an existing electronic identity (R1) / Identify theft (R4) / Unauthorised transaction (R9)

ID *Identifier*	Threat description *Description of the identified threat (*)*	Risk title *Related risks*
TR13	An attacker can get a valid PID into an invalid wallet unit.	Creation or use of an existing electronic identity (R1) / Identify theft (R4) / Unauthorised transaction (R9)
TR14	A PID provider can issue fabricated identities where the identity is related to an existing person.	Creation or use of an existing electronic identity (R1) / Identity theft (R4) / Unauthorised transaction (R9)
TR15	An attacker can link a PID with the wrong wallet because the PID provider is not able to link the PID to the correct wallet.	Creation or use of an existing electronic identity (R1) / Identify theft (R4) / Unauthorised transaction (R9)
TR16	An attacker can make the user approving the activation of a new wallet unit/instance under the attacker's control – with subsequent control of attestations as well.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2) / Identify theft (R4) / Unauthorised transaction (R9)
TR17	An attacker can issue a PID of another state to access data / digital assets of targeted citizens.	Creation or use of an existing electronic identity (R1) / Identity theft (R4) / Unauthorised transaction (R9)
TR18	An attacker can defeat technical and procedural controls to create fake (Q)EAAs.	Creation or use of fake attributes (R3)
TR19	An attacker can present (Q)EAAs that are not validly issued to them.	Creation or use of fake attributes (R3)
TR20	An attacker can attack the cryptographic linking mechanism of the wallet between the PID and a (Q)EAA that should not be issued to them.	Creation or use of fake attributes (R3)
TR21	An attacker can use a (Q)EAA in a wallet, although the physical counterpart of the (Q)EAA is expired or invalid.	Creation or use of fake attributes (R3)
TR22	An attacker can circumvent the verification by the (Q)EAA provider that the wallet is in control of the user and have a (Q) EAA issued into a compromised wallet under the attacker's control.	Creation or use of fake attributes (R3)
TR23	An attacker can forge electronic attestations of attributes.	Creation or use of fake attributes (R3)
TR24	An attacker can inject forged electronic attestations of attributes into a wallet.	Creation or use of fake attributes (R3)
TR25	The wallet can present attributes to a relying party without the approval of a user.	Data disclosure (R6)
TR26	PID, (Q)EAAs or pseudonyms can be presented to a wrong relying party.	Data disclosure (R6)
TR27	An attacker can initiate a malicious renewal of EAA.	Data disclosure (R6)
TR28	An attacker can get a user into wrongfully approving a request for electronic attestations of attributes (phishing or other).	Data disclosure (R6)

ID *Identifier*	Threat description *Description of the identified threat (*)*	Risk title *Related risks*
TR29	An attacker can leak attributes from the wallet and identify the wallet user where identification is not required/allowed.	Data disclosure (R6)
TR30	An attacker can defeat technical and procedural controls to extract data.	Data disclosure (R6)
TR31	A request can be leaked to an attacker.	Data disclosure (R6)
TR32	An attacker can obtain knowledge on the embedded disclosure policy for attributes and present attributes contained in the current request by wallet units.	Data disclosure (R6)
TR33	An attacker can extract logs, or parts of them.	Data disclosure (R6)
TR34	An attacker can know whether a wallet is installed on the same device he is using, or on another one, and get information on it.	Data disclosure (R6)
TR35	An attacker can obtain a knowledge factor used for user authenticating to the WSCA.	Data disclosure (R6)
TR36	The electronic attestation of attributes about a person that is presented in multiple transactions with a relying party, or across different relying parties, unintentionally allows to link multiple transactions to the relevant person.	Data disclosure (R6)
TR37	A public attestation/relying party revocation list can contain information about the user's usage of their attestation (e.g. location, IP address …).	Data disclosure (R6)
TR38	Not being able to prove user's consent for shared attributes, relying parties can affect the integrity of logs.	Data disclosure (R6)
TR39	An attacker can unlawfully trace wallet users using unique/traceable identifiers.	Data disclosure (R6) / Surveillance (R14)
TR40	A relying party that consists of multiple units/entities that each have a different scope of what they are allowed to request/process, can request and process data for which they do not have lawful grounds for.	Data disclosure (R6) / Unauthorised transaction (R9)
TR41	An attacker can subvert the integrity and authenticity checks by the wallet of PIDs to always return success.	Data manipulation (R7)
TR42	An attacker can bypass or subvert the performance of checks by the wallet that verify the integrity and authenticity of requested attributes to always return success.	Data manipulation (R7)
TR43	An attacker can bypass or subvert the performance of checks by the wallet that verify all requested attributes belonging to the same user to always return success.	Data manipulation (R7)
TR44	An attacker can bypass or subvert the performance of checks by the wallet that verify the PID is valid and issued by a trusted PID provider to always return success.	Data manipulation (R7)

ID *Identifier*	Threat description *Description of the identified threat (*)*	Risk title *Related risks*
TR45	An attacker can bypass or subvert the performance of checks by the wallet that verify that a QEAA is valid and issued by a qualified TSP, who is registered to issue the QEAA, to always return success.	Data manipulation (R7)
TR46	An attacker can bypass or subvert the performance of checks by the wallet that verify whether the PID has been revoked by the PID provider to always return success.	Data manipulation (R7)
TR47	An attacker can bypass or subvert the performance of checks by the wallet that verify whether the (Q)EAA has been revoked by the (Q)EAA provider to always return success.	Data manipulation (R7)
TR48	An attacker can modify the content of backup and recovery data that should be exclusively under the user's control.	Data manipulation (R7) / Data loss (R8)
TR49	An attacker can modify the transaction history for a given wallet instance from the activity logs.	Data manipulation (R7) / Data loss (R8)
TR50	An attacker can eavesdrop during the connection from the wallet to relying parties.	Data theft (R5) / Data disclosure (R6)
TR51	An attacker can convince a user to share personal data (i.e. PID, EAA-s, pseudonyms, electronic signatures, logs and other data) with the attacker or with a third party that the user did not intend to do so.	Data theft (R5) / Data disclosure (R6)
TR52	An attacker can read the transaction history for a given wallet instance from the activity logs.	Data theft (R5) / Data disclosure (R6)
TR53	An attacker can export or extract cryptographic key material outside of the WSCD.	Data theft (R5) / Data disclosure (R6) / Unauthorised transaction (R9)
TR54	An attacker can read the content of backup and recovery data that should be exclusively under the user's control.	Data theft (R5) / Data disclosure (R6)
TR55	An attacker can bypass the user authentication method to use a pseudonym generated by a wallet unit.	Identity theft (R4)
TR56	An attacker can propose an application that mimics a specific legitimate wallet to users.	Identity theft (R4)
TR57	An attacker can export wallet data, including PID, (Q)EAAs or logs.	Identity theft (R4)
TR58	An attacker can export cryptographic binding material.	Identity theft (R4)
TR59	An attacker can take over identities through the cryptographic keys of the wallet.	Identity theft (R4)
TR60	An attacker can duplicate another user's personal wallet unit on their personal device and use it.	Identify theft (R4) / Creation or use of an existing electronic identity (R1)

ID *Identifier*	Threat description *Description of the identified threat (*)*	Risk title *Related risks*
TR61	Authorities of another state can ask the user to show and/or share all the wallet data in a situation of proximity, such as when crossing the border of that state.	Identify theft (R4) / Surveillance (R14)
TR62	Users cannot transfer their transaction logs after failure of a user device, resulting in a loss of traceability of previous transactions on the new wallet.	Repudiation (R11)
TR63	Users cannot recover their transaction logs after failure of a user device, resulting in a loss of traceability on the new wallet.	Repudiation (R11)
TR64	Relying parties can have difficulties proving consent for remote electronic signatures.	Repudiation (R11)
TR65	An attacker can flood the connection(s) with requests during the connection to relying parties.	Service disruption (R13)
TR66	An attacker can flood a status provisioning service with connections to relying parties.	Service disruption (R13)
TR67	An attacker can make the attribute presentation appearing as contested/denied, despite the attribute presentation stating its validity.	Service disruption (R13)
TR68	An attacker can revoke a PID without justified reason.	Service disruption (R13)
TR69	An attacker can revoke a PID without user consent.	Service disruption (R13)
TR70	An attacker can revoke a (Q)EAA without justified reason.	Service disruption (R13)
TR71	An attacker can revoke a (Q)EAA without user consent.	Service disruption (R13)
TR72	An attacker can trigger multiple identification requests without them being recognised as intentional orphan requests.	Service disruption (R13)
TR73	An attacker can send multiple requests with no follow-up transaction.	Service disruption (R13)
TR74	An attacker can allow a relying party to request identification without a matching identification (response) and full control.	Service disruption (R13)
TR75	An attacker can send a response to a request after its timeout, or similar situations leading to a service disruption.	Service disruption (R13)
TR76	A relying party can send multiple invalid requests.	Service disruption (R13)
TR77	An attacker can send multiple invalid requests to a wallet provider.	Service disruption (R13)
TR78	An attacker can make a Member State unable to revoke an untrusted PID provider from the trusted PID provider trusted list.	Service disruption (R13)
TR79	An attacker can prevent suspension or revocation of a wallet.	Service disruption (R13)

ID *Identifier*	Threat description *Description of the identified threat (*)*	Risk title *Related risks*
TR80	An attacker can block transactions by relying parties, users and/or PID provider.	Service disruption (R13)
TR81	An attacker can disable or make a WSCD unavailable.	Service disruption (R13)
TR82	An attacker can make the PID provider unable to revoke or suspend PIDs.	Service disruption (R13) / Unauthorised transaction (R9)
TR83	A relying party can derive the user's identity data beyond data shared with them.	Surveillance (R14)
TR84	A group of colluding relying parties or PID providers can derive the user's identity data beyond data known to them.	Surveillance (R14)
TR85	An attacker can track and trace a user by using person identification data of the user where identification of the user is not required.	Surveillance (R14)
TR86	An attacker can combine a 'forged' presentation of (Q)EAA combinations.	Transaction manipulation (R10)
TR87	An attacker can activate/take over the wallet remotely (e.g., a bank app embedding an authentication or attestation request) without the explicit consent or sole control of the user, in situations where the user is unaware of (e.g., asleep), or cannot see the relying party.	Transaction manipulation (R10)
TR88	Attackers can make changes to a request's metadata (service name, usages, etc.).	Transaction manipulation (R10)
TR89	Attackers can make changes to response information (service state, nonce, etc.).	Transaction manipulation (R10)
TR90	Attackers can make changes to a request's attribute information (over asking, etc.).	Transaction manipulation (R10)
TR91	A relying party can replay elements from a previous session in another session.	Transaction manipulation (R10)
TR92	An attacker can replace or modify the PID during its transfer from the PID provider to the wallet unit.	Transaction manipulation (R10)
TR93	An attacker can replace or modify the PID during its transfer from the wallet unit to the online relying party.	Transaction manipulation (R10)
TR94	An attacker can replace or modify the PID during its transfer from the wallet unit to the offline relying party.	Transaction manipulation (R10)
TR95	An attacker can issue a PID without the user's consent.	Unauthorised transaction (R9)
TR96	An attacker can use revoked or invalid embedded disclosure policies, possibly without the relying parties' knowledge.	Unauthorised transaction (R9)
TR97	An attacker can trick the wallet into verifying wrong electronic signatures.	Unauthorised transaction (R9)
TR98	An attacker can use the wallet outside of the user's control.	Unauthorised transaction (R9)

ID *Identifier*	Threat description *Description of the identified threat (*)*	Risk title *Related risks*
TR99	An attacker can convince a user to authenticate and approve transactions with an attacker or unauthorised third party.	Unauthorised transaction (R9)
TR100	An attacker can make a user electronically sign without presenting the content to the user or after presenting wrong content.	Unauthorised transaction (R9)
TR101	An attacker can bypass access control of the user's account with the wallet provider.	Unauthorised transaction (R9)
TR102	An attacker can impersonate relying parties during the connection to relying parties.	Unauthorised transaction (R9) / Data disclosure (R6)
TR103	The user behind the relying party – browser connection can be different from the user behind the relying party – wallet connection.	Unauthorised transaction (R9) / Data disclosure (R6) / Identity theft (R4)
TR104	An attacker can convince the user to revoke the user's wallet without reason.	Unauthorised transaction (R9) / Service disruption (R13)
TR105	An attacker can perform man-in-the-middle attacks.	Unauthorised transaction (R9) / Data disclosure (R6) / Surveillance (R14)
TR106	An attacker can present invalid or revoked attributes from a wallet that does not regularly connect to the network.	Effect on various risks
TR107	An attacker can steal information from a user by spoofing a wallet.	Effect on various risks
TR108	An attacker can impersonate the user by replaying/imitating a data request (e.g., authentication), which would appear as valid.	Effect on various risks
TR109	An attacker can replay an embedded disclosure policy towards a user, to imitate an approved request.	Effect on various risks
TR110	An attacker can exploit the lack of information of wallet users, or undue delays, after a security breach or compromise.	Effect on various risks
TR111	An attacker can modify a previously installed legitimate wallet instance to add malicious features.	Effect on various risks
TR112	An attacker can modify a legitimate wallet instance and propose it to users as a legitimate one.	Effect on various risks
TR113	An attacker can defeat the user authentication mechanism itself to bypass the authentication of the wallet user.	Effect on various risks
TR114	An attacker can introduce malicious code or backdoors into the wallet code during its deployment to the user device.	Effect on various risks
TR115	An attacker can introduce malicious code or backdoors into the wallet code during its development.	Effect on various risks
TR116	An attacker can tamper with the generation of random numbers to reduce their entropy sufficiently to enable attacks.	Effect on various risks

ID *Identifier*	Threat description *Description of the identified threat (*)*	Risk title *Related risks*
TR117	An attacker can tamper with user devices in the supply chain to include code or configurations that do not meet the conditions of use of the wallet.	Effect on various risks
TR118	An attacker can activate a wallet unit while using a spoofed WSCD controlled by the attackers.	Effect on various risks
TR119	An attacker can read information sent to the WSCA and/or the WSCD.	Effect on various risks
TR120	An attacker can send arbitrary information to the WSCA.	Effect on various risks
TR121	An attacker can steal information by intercepting the exchanges between the WSCA and the WSCD.	Effect on various risks
TR122	An attacker can send arbitrary information to the WSCD.	Effect on various risks
TR123	An attacker can send information to the WSCD, circumnavigating the WSCA.	Effect on various risks
TR124	An attacker can use phishing to get users to a fake wallet and PID management web application.	Effect on various risks
TR125	An attacker can replace a wallet's keys with other keys to create messages to be used in another attack.	Effect on various risks
TR126	An attacker can modify or destroy a wallet's keys, making some functions of the wallet unusable.	Effect on various risks
TR127	An attacker can control a malware to access data stored in the wallet.	Effect on various risks
TR128	An attacker can access evidence generated in the wallet.	Effect on various risks
TR129	Wallet providers can access objects in the wallet.	Effect on various risks
TR130	Wallet providers can access evidence generated in the wallet.	Effect on various risks
TR131	An attacker can steal an unlocked wallet device.	Effect on various risks
TR132	An attacker can manipulate the system to prevent certain events from being logged.	Effect on various risks
TR133	An attacker can intercept communication between the wallet instance and the WSCA, or replay/imitate a user (e.g. by hijacking authentication mechanism).	Effect on various risks

ANNEX II

CRITERIA TO ASSESS THE ACCEPTABILITY OF ASSURANCE INFORMATION

Name	Object	Points of attention
EUCC	ICT Products	About the issuer: none (accredited certification bodies) About the scope: — Check the protection profile and security target — Check the evaluation assurance level and augmentations About the assurance: — Check restrictions in the user documentation — For composition, may require access to evaluation technical report
EUCS (when available)	Cloud services	About the issuer: none (accredited certification bodies) About the scope: — Check the cloud service description — Check the evaluation level and extension profiles About the assurance: — Check the transparency information and, if needed, the composition information
Common Criteria schemes operated in the EU, including SOG-IS schemes	ICT products	About the issuer: none (Member States) About the scope: — Check the protection profile and security target — Check the evaluation assurance level and augmentations About the assurance: — Check restrictions in the user documentation — For composition, may require access to evaluation technical report
EN 17640:2018 (FITCEM, including CSPN, BSZ, LINCE, BSZA)	ICT products	About the issuer: — Check the scheme and the requirements for certification bodies About the scope: — Check the product description — Check the security claims — Check the assurance level About the assurance: — Check the activities performed and the findings in the report
Certification schemes of qualified signature creation devices in accordance with Art. 30 of Regulation (EU) No 910/2014	QSCD	About the issuer: — Check the scheme and the requirements for certification bodies About the scope: — Check the product description — Check the security claims — Check the assurance level About the assurance: — Check the activities performed

Name	Object	Points of attention
EN ISO/IEC 27001:2022	ISMS	About the issuer: none (Accredited certification bodies) About the scope: — Check the management system description — Check the statement of applicability About the assurance: — Check the activities performed
SOC2	Organisations	About the issuer: — Check their public accountant status About the scope: — Check the Management Statement and the description of the controls — Check the statement of applicability About the assurance: — Check the findings in the report — Check bridge letters if needed
MDSCert (GSMA) (when available)	Mobile Devices	About the issuer: — Check the requirements for certification bodies About the scope: — Check the security assurance level — Check the scheme requirements About the assurance: — Check the activities and findings in the report
Other schemes	Any component	About the scheme: — Check the relevance and provisions of the scheme About the issuer: — Check the requirements for certification bodies About the scope: — Check the scheme requirements — Check the security target or similar document describing the security functional and assurance requirements — Check the product description and selected security functional requirements About the assurance: — Check the activities and findings in the report

ANNEX III

FUNCTIONAL REQUIREMENTS FOR WALLET SOLUTIONS

Under Article 5a(4), (5), (8), and (14) of Regulation (EU) No 910/2014, the functional criteria to be met by a certified wallet solution and the electronic identification scheme under which it is provided shall include the functional requirements for the operations listed in the following:

(1) Commission Implementing Regulation (EU) 2024/2979 ([1]) laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities;

(2) Commission Implementing Regulation (EU) 2024/2982 ([2]) laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework;

(3) Commission Implementing Regulation (EU) 2024/2977 ([3]) laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets.

([1]) Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities (OJ L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework (OJ L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets (OJ L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

ANNEX IV

METHODS AND PROCEDURES FOR EVALUATION ACTIVITIES

1. Audit of the implementation of a wallet solution

A conformity assessment activity shall consist of selecting specific evaluation activities.

National certification schemes shall specify an evaluation activity to assess the information provided, covering at least the following:

(a) an analysis of the information provided to confirm that it is suited for one of the architectures specified in national certification schemes;

(b) an analysis of the coverage of the cybersecurity risks and threats identified in the risk register of Annex I by the described security controls.

The analysis mentioned in points (a) to (b) shall rely on the rationale and justification provided by the wallet provider.

2. Evaluation activities related to the wallet secure cryptographic device

(1) Critical operations, including cryptographic computations, are not required to be fully implemented in the WSCD. However, the part implemented in the WSCD, when operating as part of the wallet solution, shall guarantee the protection of the critical operations it performs against attacks by attackers with high attack potential in accordance with Commission Implementing Regulation (EU) 2015/1502 ([1]).

(2) The WSCD or part thereof may be within the object of certification when it is provided by the certificate holder or applicant, or outside of its scope when it is embedded in a device provided by the end user. In addition, national certification schemes shall specify the evaluation activities to verify the suitability of the WSCD, in the two following cases:

   (a) if the WSCA depends on the particular WSCD (i.e. if it needs to be evaluated as a composite product based on the WSCD) then the evaluation of the WSCA shall require access to additional information related to the WSCD's certification, including, in particular, its evaluation technical report;

   (b) if an architecture considered in the scheme uses several WSCDs, or if some of the operations on critical assets are performed outside of the WSCD, then national certification schemes shall include evaluation activities to ensure that the overall solution offers the expected level of security.

(3) As a prerequisite to the certification under national certification schemes, the WSCD shall be assessed against the requirements of assurance level high as set out in Implementing Regulation (EU) 2015/1502.

When the conditions in Article 3(3), point (b) are fulfilled, the evaluation of the WSCD or part thereof shall include a vulnerability assessment as set out in EN ISO/IEC 15408-3:2022 at level AVA_VAN.5, as set out in Annex I of the Commission Implementing Regulation (EU) 2024/482 ([2]), unless it is duly justified to the certification body that the security characteristics of the WSCA make it possible to use a lower assessment level while keeping the same overall assurance level high as set out in Implementing Regulation (EU) 2015/1502.

([1]) Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 235, 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([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) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(4) In addition, in the documentation related to each specific architecture, national certification schemes shall formulate assumptions for this evaluation of the WSCD under which resistance against attackers with high attack potential in accordance with Implementing Regulation (EU) 2015/1502 can be provided and specify the evaluation activities to confirm these assumptions and to confirm after issuance of the certificate that the assumptions are still verified. The national schemes shall also require the candidates to certification to refine these assumptions for their specific implementation, and to describe the measures in place to guarantee that the assumptions are verified throughout the certification lifecycle.

(5) In all cases, national certification schemes shall include an evaluation activity to verify that the assurance information available for the WSCD is suitable for the purpose of the wallet solution, through an analysis of the assurance information, such as the security target for EUCC certificates, including the following activities:

(a) verifying that the scope of the evaluation is suitable, which for EUCC certificates, for instance, means verifying that the security target claims conformity to one of the protection profiles recommended in the EUCC;

(b) verifying that the assumptions on the operating environment are compatible with the wallet solution, which for EUCC certificates, for instance, means that these assumptions can be found in the security target;

(c) verifying that the recommendations in the user guidance or documentation are compatible with the conditions on which the WSCD is to be used in the wallet solution;

(d) verifying that the assumptions made in the national certification scheme about WSCDs are verified and covered in the assurance information.

(6) In cases where some of the verifications are not fully conclusive, national certification schemes shall require certification bodies to specify compensating requirements for the wallet secure cryptographic application (WSCA) based on the WSCD, to be included in the evaluation of the WSCA. If this is not possible, national certification schemes shall deem the WSCD unsuitable, meaning that the wallet solution shall not be issued a certificate of conformity.

3. **Evaluation activities related to the wallet secure cryptographic application (WSCA)**

(1) National certification schemes shall require that a WSCA, as part of a wallet solution, is evaluated against the requirements of at least assurance level high as set out in Implementing Regulation (EU) 2015/1502.

(2) This evaluation shall include a vulnerability assessment, as set out in EN ISO/IEC 15408-3:2022 at level AVA_VAN.5, as set out in Annex I of Implementing Regulation (EU) 2024/482, unless it is duly justified to the certification body that the security characteristics of the WSCA make it possible to use a lower assessment level while keeping the same overall assurance level high as set out in Implementing Regulation (EU) 2015/1502.

(3) When the WSCA is not provided by the wallet provider, national certification schemes shall formulate assumptions for this evaluation of the WSCA under which resistance against attackers with high attack potential in accordance with Implementing Regulation (EU) 2015/1502 can be provided and specify the evaluation activities to confirm these assumptions and to confirm after issuance of the certificate that the assumptions are still verified. The national schemes shall also require the candidates to certification to refine these assumptions for their specific implementation, and to describe the measures in place to guarantee that the assumptions are verified throughout the certification lifecycle.

(4) In all cases, national certification schemes shall include an evaluation activity to verify that the assurance information available for the WSCA is suitable for the purpose of the wallet solution, through an analysis of the assurance information, such as the security target for EUCC certificates, including the following activities:

(a) verifying that the scope of the evaluation is suitable, which for EUCC certificates, for instance, means verifying that the security target claims conformity to one of the protection profiles recommended in the EUCC;

(b) verifying that the assumptions on the operating environment are compatible with the wallet solution, which for EUCC certificates, for instance, means that these assumptions can be found in the security target;

(c) verifying that the recommendations in the user guidance or documentation are compatible with the conditions on which the WSCA is to be used in the wallet solution;

(d) verifying that the assumptions made in the national certification scheme about WSCAs are verified and covered in the assurance information.

(5) National certification schemes shall require that the evaluation of the WSCA covers all security controls implemented by this WSCA.

4. **Evaluation activities related to the end user device**

Since the risk register, as set out in Annex I of this Regulation, identifies risks that are directly linked to the security of the end user device, national certification schemes shall specify security requirements for end user devices. However, as these devices are provided by the end user and not by the wallet provider, these requirements shall be covered by assumptions.

For each assumption, the wallet solution shall include a mechanism to verify for every wallet unit that the underlying end user device satisfies the assumption. Such mechanisms shall be considered as security controls and covered by evaluation activities to demonstrate both their suitability and their effectiveness at the appropriate assurance level.

Two examples are set out below:

(a) an end user device may include a certified WSCD, which needs to be demonstrated. Typically, this would be done by using a cryptographic mechanism to verify the presence in the certified WSCD of a cryptographic secret that is only available in the certified WSCD. In this case, this cryptographic secret should be considered as a critical asset and be covered by the certification of the WSCD and/or of the WSCA;

(b) a typical requirement for end user devices would be that the devices must receive security updates. Since this requirement is related to the wallet instance, the mechanism used to verify the availability of security updates only needs to be covered by evaluation activities at an assurance level suitable for the wallet instance, especially as it is likely to be integrated into the wallet instance.

5. **Evaluation activities related to the wallet instance**

(1) The evaluation of the wallet instance shall consider the following two main challenges:

(a) the wallet instance is likely to exist in a set of variants of the same base application, with each variant specialised for a specific category of end user devices;

(b) the different variants of the wallet instance will likely need frequent updates in order to follow the development of the underlying security platform, for instance when vulnerabilities are identified that require changes to applications.

(2) The evaluation of the wallet instance shall take into consideration these specific challenges. One of the immediate consequences is that the Common Criteria framework may not be suitable in all cases. Therefore, alternative evaluation methodologies shall be considered where necessary. National certification schemes shall consider the use of the EN 17640:2018 methodology for the following:

(a) as part of the scheme itself;

(b) through national schemes based on the methodology;

(c) through national schemes based on similar principles but created before the development of the EN 17640:2018 methodology.

(3) In addition, as there may be limited added value in performing a full dedicated evaluation of each variant, national certification schemes shall consider specifying criteria allowing sampling to be performed, in order to avoid repetition of identical evaluation activities and to focus on activities that are specific to a given variant. National certification schemes shall require all certification bodies to justify their use of sampling.

(4) National certification schemes shall include updates of the wallet instance in the overall change management process specified for the wallet solution. They shall also lay down rules on the procedures that shall be performed by the wallet provider for every update (e.g. analysing the impact of the changes on the security controls), and on the evaluation activities that shall be performed by the certification body on updates under specified conditions (e.g. assessing the operating effectiveness of a modified security control). The change management process is one of the processes whose operating effectiveness is required to be checked annually in accordance with Article 18(3).

6. **Evaluation activities related to the services and processes used for the provision and operation of the wallet solution**

(1) For the evaluation of services and processes that play a role in the provision and operation of the wallet solution and the electronic identification scheme under which they are provided, the evaluation team shall gather evidence by conducting evaluation activities that may include audit, inspection, verification and validation activities.

(2) The certification body shall confirm the sufficiency and appropriateness of the evidence to provide sufficient assurance that the services and processes meet the certification requirements, by confirming the following:

(a) the accuracy of the information presented in the description of the processes and services;

(b) the suitability of the design and the controls of the processes and services to meet the evaluation criteria;

(c) the operating effectiveness of an implementation of these controls throughout a specified period before the evaluation.

(3) The accuracy of the description and the operating effectiveness of an implementation of controls may be considered as verification objectives, in the sense of ISO/IEC 17000:2020, of the corresponding claims by the wallet provider (i.e. confirmation of fairness of events that have already occurred or results that have already been obtained), whereas the suitability of the design and the controls of the services and processes to meet the evaluation criteria may be considered as a validation objective, in the sense of ISO/IEC 17000:2020, of the corresponding claim by the wallet provider (i.e. confirmation of plausibility regarding an intended future use or projected outcome).

(4) Considering that a wallet solution is not allowed to operate before being certified, operating effectiveness cannot be confirmed on the basis of the actual operation of the solution. Therefore, this shall be confirmed using evidence gathered during tests or pilots.

(5) National certification schemes may already exist for specific services and processes, for instance for the onboarding of users. The use of such schemes shall be considered by national certification schemes, if applicable.

7. **Evaluation activities related to the ICT services used for the provision and operation of the wallet solution**

(1) Some wallet architectures may rely on dedicated ICT services, including cloud services for the provision and operation of a wallet solution, and these services may host sensitive data as well as sensitive operations. In such a case, national certification schemes shall specify security requirements for these ICT services.

(2) Many certification schemes already exist for ICT services, cloud services, and other sources of assurance information, including those listed in Annex II. National certification schemes shall rely, when available and applicable, on those existing mechanisms, through one of the following mechanisms:

(a) mandating the use of a specific scheme or of a selection of schemes, by specifying the conditions under which the ICT or cloud services is to be assessed using these schemes;

(b) leaving the choice of the assessment to the wallet provider and use the dependency analysis activity to analyse the suitability of the assurance information obtained through these assessments.

(3) In both cases, national certification schemes shall specify additional evaluation activities as needed to analyse or supplement the information obtained through these schemes.

ANNEX V

LIST OF PUBLICLY AVAILABLE INFORMATION ABOUT WALLETS

1. The information that shall be made public pursuant to Article 8(5) shall include at least the following:
   (a) any limitations on the use of a wallet solution;
   (b) guidance and recommendations by the wallet provider to assist end users with the secure configuration, installation, deployment, operation and maintenance of wallets;
   (c) the period during which security support will be offered to end users, in particular as regards to the availability of cybersecurity related updates;
   (d) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;
   (e) a reference to online repositories listing publicly disclosed vulnerabilities related to wallets and to any relevant cybersecurity advisories.

2. The information referred to in paragraph 1 shall be made available in a clear, comprehensive and easily accessible manner, in a publicly accessible space, to any person seeking to use a wallet solution.

ANNEX VI

METHODOLOGY TO ASSESS THE ACCEPTABILITY OF ASSURANCE INFORMATION

1. Assessing the availability of assurance documentation

Evaluators shall list the assurance documentation available for every relevant component of the wallet solution and the electronic identification scheme under which they are provided. Then, evaluators shall assess the overall relevance of each piece of assurance documentation for the dependency review.

The following aspects shall be considered in the analysis:

(1) about the assurance documentation itself:

(a) the type of assurance documentation, with all required details,

(examples of such documents are certificates of conformity according to EN ISO/IEC 27001:2022 or Type 1 or Type 2 for ISAE reports);

(b) the period covered or period of validity,

(this period may be supplemented with a bridge letter (a document to cover a period of time between the end date of the reporting period of the current ISAE report and the release of a new ISAE report) or similar a statement);

(c) the applicable framework (e.g. existing standard);

(d) whether the assurance documentation includes a mapping to the scheme's requirements;

(2) about the assurance report issuer's professional competence and impartiality:

(a) name of the certification body and, if available, name of the lead evaluator;

(b) evidence of the certification body's and the evaluator's competence (e.g. accreditation, personal certification, etc.);

(c) evidence of the certification body's and the evaluator's impartiality (e.g. accreditation, etc.).

2. Assessing assurance related to individual requirements

Evaluators shall verify that the assurance documentation available for the wallet solution and the electronic identification scheme under which they are provided is adequate to determine that the wallet solution meets the expectations relative to the certification scheme's individual requirements.

This assessment shall be performed for every relevant component of the wallet solution and the electronic identification scheme under which they are provided, by formulating an assumption on the wallet solution's security controls.

For each such assumption, the evaluation team shall determine whether or not the assurance provided in the available assurance documentation is adequate.

The determination that the assurance is adequate shall be based on the following:

(1) the required information is available, with the expected assurance level, in the assurance documentation;

(2) the information available in the assurance documentation does not cover the full scope of the requirement, but additional controls or compensating controls (i.e., internal controls that reduce the risk of existing or potential control weakness) implemented in the wallet solution or in the electronic identification scheme under which they are provided allow the evaluators to determine that the information is adequate;

(3) the information available in the assurance documentation does not offer the expected assurance level but the controls implemented to assess and monitor the wallet provider allow the evaluators to determine that the information is adequate;

(4) if the assurance documentation mentions nonconformities on the design or implementation of the controls used to meet an assumption, the remedial actions proposed and implemented by the wallet provider and reviewed by its evaluators shall be adequate to guarantee that the assumption is indeed met.

ANNEX VII

CONTENT OF THE CERTIFICATE OF CONFORMITY

1. A unique identifier allocated by the certification body issuing the certificate of conformity.

2. Information related to the certified wallet solution and the electronic identification schemes under which they are provided, and about the holder of the certificate of conformity, including the following:
   (a) name of the wallet solution;
   (b) name of the electronic identification schemes under which the wallet solution is provided;
   (c) version of the wallet solution that was evaluated;
   (d) name, address and contact information of the holder of the certificate of conformity;
   (e) link to the website of the holder of the certificate of conformity containing the information that is required to be made publicly available.

3. Information related to the evaluation and certification of the wallet solution and the electronic identification schemes under which they are provided, including the following:
   (a) name, address and contact information of the certification body that issued the certificate of conformity;
   (b) where different from the certification body, name of the conformity assessment body that performed the evaluation, together with information on its accreditation;
   (c) name of the scheme owner;
   (d) references to Regulation (EU) No 910/2014 and to this Regulation;
   (e) a reference to the certification report associated with the certificate of conformity;
   (f) a reference to the certification assessment report associated with the certificate of conformity;
   (g) a reference to the standards used for the evaluation, including their versions;
   (h) the date of issuance of the certificate of conformity;
   (i) the period of validity of the certificate of conformity.

ANNEX VIII

CONTENT OF THE PUBLIC CERTIFICATION REPORT AND THE CERTIFICATION ASSESSMENT REPORT

1. The public certification report shall contain at least the following aspects:
   (a) executive summary;
   (b) identification of the wallet solution and of the electronic identification scheme under which they are provided;
   (c) a description of the wallet solution and of the electronic identification scheme under which they are provided;
   (d) the security information to be made publicly available, as described in Annex V, or a pointer to this information;
   (e) a summary of the preliminary audit and validation plan;
   (f) a summary of the review and the certification decision.

2. The certification assessment report shall at least contain:
   (a) a description of the wallet solution's design, the identification system and the onboarding process, together with the risk assessment and the specific validation plan;
   (b) a description of how the wallet solution meets the requirements of assurance level high and of how this is demonstrated by the results of the certification assessment of the wallet solution conducted in accordance with this Regulation;
   (c) a description of the result of assessment of the conformity of the wallet solution and of the electronic identification scheme under which the corresponding wallet units are provided with, in particular the conformity with the following:
      — the requirements set out in Article 5a(4), (5), and (8) of Regulation (EU) No 910/2014;
      — the requirement for logical separation set out in Article 5a(14) of Regulation (EU) No 910/2014;
      — where applicable, the standards and technical specifications referred to in Article 5a(24) of Regulation (EU) No 910/2014, while describing how these requirements relate to the corresponding normative requirements specified by national certification schemes;
   (d) a summary of the result of the performance of the validation plan, including all identified nonconformities.

ANNEX IX

SCHEDULE FOR MANDATORY SURVEILLANCE EVALUATIONS

1. Article 18 specifies requirements for the certification lifecycle, in particular the performance of regular evaluation activities. These activities shall include at least the following:

   (a) a full evaluation of the object of conformity assessment in the initial evaluation and at every recertification evaluation, including an update feature of any product component;

   (b) a vulnerability assessment in the initial evaluation and at every recertification evaluation, and at least every two years in surveillance evaluations, covering at least the changes in the object of conformity assessment and the changes in the threat environment since the last vulnerability assessment;

   (c) additional activities such as penetration testing in case of an increased risk level or the emergence of new threats;

   (d) an evaluation of the operating effectiveness of maintenance processes at least every year in surveillance and recertification evaluations, covering at least version control, update and vulnerability management processes;

   (e) following a successful review and certification decision, the issuance of a certificate of conformity after the initial evaluation and after every recertification evaluation.

2. A reference schedule is set out in Table 1 based on a 4-year cycle, where:

   (a) year 1 starts when the certificate of conformity is first issued; and

   (b) all evaluation activities shall be performed within 12-months from the evaluation of the previous year.

3. The schedule set out in Table 1 is a recommendation to ensure timely recertification and to avoid disruptions in the provision of the wallet solution. Other schedules may be possible, as long as the validity of the certificate of conformity does not exceed five years, as laid down in Article 5c(4) of Regulation (EU) No 910/2014.

4. In addition to the regular evaluations, a special evaluation might be triggered at the demand of the certification body or of the holder of the certificate of conformity, following a significant change to the object of certification or to the threat environment.

5. Any evaluation, including surveillance evaluations and special evaluations, might lead to the issuance of a new certificate of conformity, in particular in case of significant changes to the object of certification, but with the same date of expiry as the original certificate of conformity.

Table 1

A full 4-year evaluation cycle

Time	Eval. type	Activities
Year 0	Initial	— Full evaluation of the object of certification, including vulnerability assessment — Including a feature to perform updates on each software component — Evaluation of the maintenance processes, excluding their operating effectiveness — Issuance of the certificate of conformity and start of the 4-year cycle
Year 1	Surveillance	— Evaluation of the operating effectiveness of the maintenance processes — At least version check, update, vulnerability management — Evaluation of changes impacting the security of the product

Time	Eval. type	Activities
Year 2	Surveillance	— Vulnerability assessment of the full solution — Evaluation of the operating effectiveness of the maintenance processes — At least version control, update, vulnerability management — Evaluation of changes impacting the security of the product
Year 3	Surveillance	— Evaluation of the operating effectiveness of the maintenance processes — At least version check, update, vulnerability management — Evaluation of changes impacting the security of the product
Year 4	Recertification	(1) Full evaluation of the object of certification, including vulnerability assessment (2) Simplified evaluation for features/processes that have not changed (3) Including a feature to perform updates on each software component (4) Evaluation of the maintenance processes, including their operating effectiveness (5) Issuance of a new certificate of conformity