COMMISSION IMPLEMENTING REGULATION (EU) 2025/848

of 6 May 2025

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties

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]), in particular Article 5b(11) thereof,

Whereas:

(1) For the purposes of registering relying parties that intend to rely on European Digital Identity Wallets ('wallets') for the provision of digital public or private services, as required by Regulation (EU) No 910/2014, Member States should establish and maintain national registers of wallet-relying parties established in their territory.

(2) The Commission regularly assesses new technologies, practices, standards and 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 under Commission Recommendation (EU) 2021/946 ([2]) 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 ([3]), the Commission should review and, if necessary, update this Regulation, to keep it in line with global developments, the Architecture and Reference Framework and to follow the best practices on the internal market.

(3) To ensure broad access to the registers and to achieve interoperability, Member States should set up both human and machine-readable interfaces that meet the technical specifications set out in this Regulation. Providers of wallet-relying party access certificates and wallet-relying party registration certificates, where available, should, for the purpose of issuing those certificates, also be able to rely upon these interfaces.

(4) As registration policies provide clear guidance to the wallet-relying parties on the registration process, Member States should set out and publish the registration policies applicable to the national registers established in their territory.

(5) The purpose of registering wallet-relying parties is to build trust in the use of the wallets through greater transparency. Therefore, Member States should make the relevant information available to the public in a manner that is both human and machine-readable. To this end, wallet-relying parties should provide the necessary information, including their entitlement or entitlements, to the national registers.

(6) Further, for the purpose of transparency, wallet-relying parties should declare, whether they intend to rely upon electronic identification of natural persons.

(7) To ensure that the registration process is cost-effective and proportionate to risk, registrars should set up online and, where applicable, automated registration processes for wallet-relying parties that are easy to use. Registrars should verify applications for registration without undue delay.

([1]) OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework (OJ L 210, 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (OJ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(8) Member States are to ensure that the wallets are able to authenticate wallet-relying parties, irrespective of where they are established in the Union. For this purpose, wallet-relying parties should use wallet-relying party access certificates when they identify themselves to wallet units. To guarantee interoperability of those certificates across all wallets provided within the Union, wallet-relying party access certificates should adhere to common requirements set out in the Annex. The Commission should develop harmonized certificate policies and certificate practice statements that should be implemented by the Member States. The Commission, in collaboration with Member States, should closely monitor the development of new or alternative standards on which relying-party access certificates could be implemented. In particular, trust models that have proven their efficacy and security in Member States should be assessed.

(9) As set out in Regulation (EU) No 910/2014, wallet-relying parties are not to request users to provide any data other than those indicated for the intended use of wallets during the registration process. Wallet users should be able to verify the registration data of wallet-relying parties. To enable wallet users to verify that the attributes being requested by the wallet-relying party are within the scope of their registered attributes, Member States may require the issuance of wallet-relying party registration certificates to registered wallet-relying parties. To ensure the interoperability of the wallet-relying party registration certificates, Member States should ensure that those certificates meet the requirements and standards set out in the Annex. In particular, wallet-relying parties should declare, whether they intend to rely upon electronic identification of natural persons to meet one of the requirements set out in paragraph 1 of Article 6 of Regulation (EU) 2016/679 of the European Parliament and of the Council ([4]) for the purpose of transparency. Further, relying parties are not to refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.

(10) To protect users against oversharing information with wallet-relying parties and warn them in such cases, Member States should include common access policies in their certificate policies that would enable a wallet solution to inform the wallet user whenever a wallet-relying party is asking for more information than what they have registered or been authorised to access.

(11) To protect wallet users, registrars should be able to suspend or cancel the registration of any wallet-relying party without prior notice where the registrars have reason to believe that the registration contains information which is inaccurate, out of date or misleading; that the wallet-relying party is not complying with the registration policy; or that the wallet-relying party is otherwise acting in breach of Union or national law or of the European Declaration on Digital Rights and Principles for the Digital Decade ([5]) in a way that relates to their role as a wallet-relying party, for example if the wallet-relying party has not rightfully minimised the set of attributes it requests access to. To safeguard the stability of the European Digital Identity Wallet ecosystem ('wallet ecosystem'), the decision to suspend or cancel a registration should be proportionate to the service disruption caused by the suspension or cancellation and the associated cost and inconvenience for the service provider and the user. Pursuant to Article 46a(4), point (f) of Regulation (EU) No 910/2014, supervisory bodies are also to be empowered to suspend and cancel the registration if required.

(12) For the purpose of *ex post* monitoring, investigations by law enforcement and dispute handling, registrars should keep records of all the information provided by wallet-relying parties established in their national register for 10 years.

(13) Regulation (EU) 2016/679 and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ([6]) apply to the personal data processing activities under this Regulation.

([4]) 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).

([5]) OJ C 23, 23.1.2023, p. 1.

([6]) 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).

(14) 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 ([7]), and delivered its opinion on 31 January 2025.

(15) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter and scope

This Regulation lays down rules for the registration of wallet-relying parties.

Article 2

Definitions

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

(1) 'wallet-relying party' means a relying party that intends to rely upon wallet units for the provision of public or private services by means of digital interaction;

(2) '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;

(3) '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;

(4) '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;

(5) '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;

(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) '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;

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

(9) 'wallet user' means a user who is in control of the wallet unit;

(10) 'national register of wallet-relying parties' means a national electronic register used by a Member State to make information on wallet-relying parties registered in that Member State publicly available as set out in Article 5b(5) of Regulation (EU) No 910/2014;

(11) 'provider of wallet-relying party access certificates' means a natural or legal person mandated by a Member State to issue wallet-relying party access certificates to wallet-relying parties registered in that Member State;

([7]) 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).

(12) ‘wallet-relying party access certificate’ means a certificate for electronic seals or signatures authenticating and validating the wallet-relying party issued by a provider of wallet-relying party access certificates;

(13) ‘provider of person identification data’ means a natural or legal person responsible for issuing and revoking the person identification data and ensuring that the person identification data of a user is cryptographically bound to a wallet unit;

(14) ‘registrar of wallet-relying parties’ means the body responsible for establishing and maintaining the list of registered wallet-relying parties established in their territory and who has been designated by a Member State;

(15) ‘wallet-relying party registration certificate’ means a data object that describes the intended use of the relying party and indicates the attributes the relying party has registered to intend to request from users;

(16) ‘provider of wallet-relying party registration certificates’ means a natural or legal person mandated by a Member State to issue wallet-relying party registration certificates to wallet-relying parties registered in that Member State.

Article 3

National registers

1. Member States shall establish and maintain at least one national register of wallet-relying parties with information regarding registered wallet-relying parties established in that Member State.

2. The register shall include at least the information set out in Annex I.

3. Member States shall designate at least one registrar to manage and operate at least one national register of wallet-relying parties.

4. Member States shall make the information set out in Annex I on registered wallet-relying parties publicly available online, both in human-readable form and in a form suitable for automated processing.

5. The information referred to in paragraph 2 shall be available through a single common application programming interface (‘API’) and through a national website. It shall be electronically signed or sealed by or on behalf of the registrar, in accordance with the common requirements for a single API set out in Section 1 of Annex II.

6. Member States shall ensure that the API referred to in paragraph 5 complies with the common requirements set out in Section 2 of Annex II.

7. Member States shall ensure that the registers comply with the relevant common registration policies set out in Article 4.

Article 4

Registration policies

1. Member States shall lay down and publish one or more national registration policies applicable to the national registers established in their territory.

2. Member States may include or reuse existing sectoral or national registration policies.

3. The national registration policy shall include at least information on:

(a) the identification and authentication procedures applicable to wallet-relying parties during the registration process;

(b) the required supporting documentation, regarding the identity, business registration, applicable entitlement or entitlements, and other relevant information on the wallet-relying party;

(c) the authentic sources or other official electronic records and where those sources or records can be relied upon to provide accurate data;

(d) any other information or other evidence required as part of the registration process;

(e) where applicable, the automated means of enabling wallet-relying parties to register or to update an existing registration;

(f) the redress mechanism available to wallet-relying parties under the laws and procedures of the Member State where the national register is established;

(g) the rules and procedures for the verification of the identity of the registered wallet-relying parties and of any other relevant information provided by that party.

4. The procedures and documentation referred to in paragraph 3, points (a) and (b), shall enable the wallet-relying parties to indicate which specific entitlement or entitlements it is acting under, as set out in Annex I.

5. Where appropriate, the requirements set out in the national registration policy shall not impede an automated registration process.

Article 5

Information to be provided to the national registers

1. Wallet-relying parties shall at least provide the information set out in Annex I to national registers.

2. Wallet-relying parties shall ensure that the information provided is accurate at the time of registration.

3. Wallet-relying parties shall update any information previously registered in the national register of wallet-relying parties without undue delay.

Article 6

Registration processes

1. Registrars shall establish easy to use electronic, and where possible, automated registration processes for wallet-relying parties.

2. Registrars shall process applications for registration without undue delay and provide a response to the application for registration to the applicant within the timeframe defined in the applicable registration policy, using appropriate means and in accordance with the laws and procedures of the Member State where the national register is established.

3. Where possible, registrars shall verify in an automated manner:

(a) the accuracy, validity, authenticity and integrity of the information required under Article 5;

(b) where applicable, the power of attorney of representatives of the wallet-relying parties drawn up and submitted in accordance with the laws and procedures of the Member State where the national register is established;

(c) the type of entitlement or entitlements of the wallet-relying parties as set out in Annex I;

(d) the absence of an existing registration in another national register.

4. Registrars shall verify the information set out in paragraph 3 against the supporting documentation provided by the wallet-relying parties or against appropriate authentic sources or other official electronic records in the Member State where the national register is established and to which the registrars have access in accordance with the applicable national laws and procedures.

5. The verification of entitlements of wallet-relying parties referred to in paragraph 3, point (c) shall be carried out in accordance with Annex III.

6. Where the registrar cannot verify the information in accordance with paragraphs 3 to 5, the registrar shall reject the registration.

7. When a wallet-relying party no longer intends to rely upon wallet units for the provision of public or private services under a specific registration, it shall notify the relevant registrar without undue delay and request the cancellation of that registration.

Article 7

Wallet-relying party access certificates

1. Member States shall authorise at least one certificate authority to issue wallet-relying party access certificates.

2. Member States shall ensure that providers of wallet-relying party access certificates issue wallet-relying party access certificates exclusively to registered wallet-relying parties.

3. Member States shall implement in a syntactically and semantically harmonised manner the certificate policies and certificate practice statements for the wallet-relying party access certificates, in accordance with the requirements set out in Annex IV.

Article 8

Wallet-relying party registration certificates

1. Member States may authorise at least one certificate authority to issue wallet-relying party registration certificates.

2. Where a Member State authorised the issuance of a wallet-relying party registration certificate, that Member State shall;

(a) require providers of wallet-relying party registration certificates to issue wallet-relying party registration certificates exclusively to registered wallet-relying parties;

(b) ensure that each intended use is expressed in the wallet-relying party registration certificates;

(c) ensure that wallet-relying party registration certificates include a general access policy, being syntactically and semantically harmonised across the Union, informing users that the wallet-relying party is only allowed to request the data specified in the registration certificates for the intended use registered in the registration certificates;

(d) ensure that providers of wallet solutions established in that Member State comply with the general access policy by informing users when a wallet-relying party requests data that is not specified in the registration certificates;

(e) implement wallet-relying party registration certificates in a syntactically and semantically harmonised manner and in line with the requirements set out in Annex V;

(f) implement dedicated certificate policies and certificate practice statements for the wallet-relying party registration certificates in accordance with the requirements set out in Annex V;

(g) ensure that wallet-relying parties provide a URL to the privacy policy regarding the intended use.

3. The policy referred to in point (g) shall be expressed in the wallet-relying party registration certificate.

Article 9

Suspension and cancellation of registration

1. Registrars shall suspend or cancel a registration of a wallet-relying party where such a suspension or cancellation is requested by a supervisory body pursuant to Article 46a(4), point (f) of Regulation (EU) No 910/2014.

2. Registrars may suspend or cancel a registration of a wallet-relying party where the registrars have reasons to believe one of the following:

(a) the registration contains information, which is inaccurate, out of date or misleading;

(b) the wallet-relying party is not compliant with the registration policy;

(c) the wallet-relying party is requesting more attributes than they have registered in accordance with Article 5 and Article 6;

(d) the wallet-relying party is otherwise acting in breach of Union or national law in a manner related to their role as wallet-relying party.

3. Registrars shall suspend or cancel a registration of a wallet-relying party where the request for cancellation or suspension is made by the same wallet-relying party.

4. When considering the suspension or cancellation in accordance with paragraph 2, the registrar shall conduct a proportionality assessment, taking into account the impact on the fundamental rights, security and confidentiality of the users in the ecosystem, as well as the severity of the disruption envisaged to be caused by the suspension or cancellation and the associated costs, both for the wallet-relying party and the user. Based on the result of this assessment, the registrar may suspend or cancel the registration with or without prior notice to the affected wallet-relying party.

5. Where the registration of a wallet-relying party is suspended or cancelled, the registrar shall inform the provider of the relevant wallet-relying party access certificates, the provider of the relevant wallet-relying party registration certificates, and the affected wallet-relying party of this action without undue delay and not later than 24 hours after the suspension or cancellation. This notification shall include information on the reasons for the suspension or cancellation and on the available means of redress or appeal.

6. The provider of wallet-relying party access certificates and the provider of wallet-relying registration certificates, shall, where applicable, revoke without undue delay the wallet-relying party access certificates, and the wallet-relying party registration certificates, respectively, of the wallet-relying party for which registration has been suspended or cancelled.

Article 10

Record keeping

Registrars shall keep records of the information provided by wallet-relying parties and registered in accordance with Annex I for the registration of a wallet-relying party and the issuance of the wallet-relying party access certificates and the wallet-relying party registration certificates, and of any subsequent changes to this information, for 10 years.

Article 11

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*.

It shall apply from the 24 December 2026.

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

Done at Brussels, 6 May 2025.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

Information regarding wallet-relying parties

1. Where applicable, the name of the wallet-relying party, as stated in an official record together with identification data of that official record.

   (a) if none are applicable, paragraph 2 shall be used.

2. Where applicable, a user-friendly name of the wallet-relying party that can be either a trade name or service name that is recognisable to the user.

3. Where applicable, one or more identifiers of the wallet-relying party, as stated in an official record together with identification data of that official record, expressed as:

   (a) an economic operators registration and identification ('EORI') number as referred to in Commission Implementing Regulation (EU) No 1352/2013 ([1]);

   (b) a registration number as registered in a national business register;

   (c) a legal entity identifier ('LEI') as referred to in Commission Implementing Regulation (EU) 2022/1860 ([2]);

   (d) a value-added tax ('VAT') registration number;

   (e) an excise number as referred to in Article 2(12) of Council Regulation (EU) No 389/2012 ([3]);

   (f) a tax reference number;

   (g) an european unique identifier ('EUID') as referred to in Commission Implementing Regulation (EU) 2021/1042 ([4]);

   (h) other national identifier or identifiers.

4. The physical address where the wallet-relying party is established.

5. Where applicable, a uniform resource locator ('URL') belonging to the wallet-relying party.

6. Where the identifier is expressed in accordance with points 3(a), (d), (f) or (h), the country indicator of the Member State where the wallet-relying party is established shall be prefixed using ISO 3166-1 Alpha 2 codes, with the exception of the country indicator for Greece which shall be 'EL'.

7. Contact information of the wallet-relying party, at least one of the following:

   (a) a website where the wallet-relying party can be contacted for matters pertaining to provision of helpdesk and support;

   (b) a phone number where the wallet-relying party can be contacted for matters pertaining to its registration and intended use of the wallet units;

   (c) an email address where the wallet-relying party can be contacted for matters pertaining to its registration and intended use of the wallet unit.

8. A description of the type of services the wallet-relying party provides.

([1]) Commission Implementing Regulation (EU) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights (OJ L 341, 18.12.2013, p. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([2]) Commission Implementing Regulation (EU) 2022/1860 of 10 June 2022 laying down implementing technical standards for the application of Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to the standards, formats, frequency and methods and arrangements for reporting (OJ L 262, 7.10.2022, p. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Council Regulation (EU) No 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004 (OJ L 121, 8.5.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

([4]) Commission Implementing Regulation (EU) 2021/1042 of 18 June 2021 laying down rules for the application of Directive (EU) 2017/1132 of the European Parliament and of the Council as regards technical specifications and procedures for the system of interconnection of registers and repealing Commission Implementing Regulation (EU) 2020/2244 (OJ L 225, 25.6.2021, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2021/1042/oj).

9. For each intended use, a list of the data, including attestations and attributes, that the relying party intends to request, a user-friendly name and a technical name, the attestation type and any other syntaxes that the data is grouped under, in a machine-readable format for automated processing.

10. For each intended use, a description of intended use of the data that the wallet-relying party intends to request from wallet units.

11. An indication whether the wallet-relying party is a public sector body.

12. The entitlement or entitlments of the wallet-relying party, that shall be expressed as follows:

    (a) 'Service_Provider' to express the entitlement of the wallet-relying party as a provider of services;

    (b) 'QEAA_Provider' to express the entitlement of the wallet-relying party as a qualified trust service provider issuing qualified electronic attestations of attributes;

    (c) 'Non_Q_EAA_Provider' to express the entitlement of the wallet-relying party as a trust service provider issuing non-qualified electronic attestations of attributes;

    (d) 'PUB_EAA_Provider' to express the entitlement of the wallet-relying party as a provider of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source;

    (e) 'PID_Provider' to express the entitlement of the wallet-relying party as a provider of person identification data;

    (f) 'QCert_for_ESeal_Provider' to express the entitlement of the wallet-relying party as a qualified trust service provider issuing qualified certificates for electronic seals;

    (g) 'QCert_for_ESig_Provider' to express the entitlement of the wallet-relying party as a qualified trust service provider issuing qualified certificates for electronic signatures;

    (h) 'rQSigCDs_Provider' to express the entitlement of the wallet-relying party as a qualified trust service provider providing qualified trust services for the management of a remote qualified electronic signature creation device;

    (i) 'rQSealCDs_Provider' to express the entitlement of the wallet-relying party as a qualified trust service provider providing qualified trust services for the management of a remote qualified electronic seal creation device;

    (j) 'ESig_ESeal_Creation_Provider' to express the entitlement of the wallet-relying party as a non-qualified trust service provider providing a non-qualified trust service for remote creation of electronic signatures or electronic seals.

13. With regard to paragraph 12, point (c), Member States may provide additional sub-entitlements to state which attestations a specific non-qualified issuer of electronic attestation of attributes shall issue.

14. Where applicable, an indication that the wallet-relying party relies upon an intermediary acting on behalf of the relying party who intends to rely upon the wallet.

15. Where applicable, an association to the intermediary that the wallet-relying party is relying upon that is acting on behalf of the relying party who intends to rely upon the wallet.

ANNEX II

1. REQUIREMENTS FOR ELECTRONIC SIGNATURES OR SEALS APPLIED TO THE INFORMATION MADE AVAILABLE ON REGISTERED WALLET-RELYING PARTIES REFERRED TO IN ARTICLE 3

— JavaScript Object Notation ('JSON');

— IETF 7515 for JSON Web Signatures.

2. REQUIREMENTS ON THE SINGLE COMMON API REFERRED TO IN ARTICLE 3

(1) The single common API shall:

(a) be a REST API, supporting JSON as a format and signed in accordance with the relevant requirements specified in Section 1;

(b) allow any requestor, without prior authentication, to search and request complete lists to the register, for information about registered wallet-relying parties, allowing for partial matches based on defined parameters including, where applicable, the official or business registration number of the wallet-relying party, the name of the wallet-relying party or the information referred to in Article 8, paragraph 2, point (g) and Annex I points 12, 13, 14 and 15;

(c) ensure that replies to requests referred to in point (b) that match at least one wallet-relying party shall include one or more statements on information about registered wallet-relying parties and information according to Annex I, current and historic wallet-relying party access certificates and wallet-relying party registration certificates but exclude the contact information in Annex I point 4;

(d) be published as an OpenAPI version 3, together with the appropriate documentation and technical specifications ensuring interoperability across the Union;

(e) provide security functions, including security by default and by design, to ensure the availability and integrity of the API and the availability of information through it.

(2) The statements referred to in point (c) shall be expressed under the form of electronically signed or sealed JSON files, with a format and structure in accordance with the requirements on electronic signatures or seals set out Section 1.

ANNEX III

Source of documentary evidence for the verification of entitlements of wallet-relying parties referred to in Article 6

1. The verification that a wallet-relying party is a provider of qualified electronic attestations of attributes, a provider of qualified certificates for electronic signatures or seals, or a provider of a qualified trust service for the management of remote qualified electronic signature or seal creation devices, shall be based on the national trusted lists published in accordance with Article 22 of Regulation (EU) No 910/2014.
2. The verification that a wallet-relying party is a provider of non-qualified electronic attestations of attributes or a provider of remote creation of electronic signatures or seals as a non-qualified trust service shall be based, where applicable, on the national trusted lists published in accordance with Article 22 of Regulation (EU) No 910/2014, or, for non-qualified trust service providers who are not registered in the national trusted lists, on verification procedures that Members States have set out in their registration policies as laid out in Article 4.
3. The verification that a wallet-relying party is a provider of person identification data shall be based on the list of providers of person identification data published by the Commission in accordance with Article 5a(18) of Regulation (EU) No 910/2014.
4. The verification that a wallet-relying party is a provider of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be based on the list published by the Commission in accordance with Article 45f(3) of Regulation (EU) No 910/2014.

ANNEX IV

Requirements for wallet-relying party access certificates referred to in Article 7

1. The wallet-relying party access certificate policy applicable to the provision of wallet-relying party access certificates shall describe the security requirements that apply to, and the rules that indicate the applicability of, a wallet-relying party access certificate so that wallet-relying parties can be issued with and use those certificates in their interactions with wallet solutions.

2. The wallet-relying party access certificate practice statement applicable to the provision of wallet-relying party access certificates shall describe the practices that a provider of wallet-relying party access certificates employs in issuing, managing, revoking, and re-keying wallet-relying party access certificates.

3. The certificate policy and certificate practice statement applicable to the provision of wallet-relying party access certificates shall be syntactically and semantically harmonised across the Union and shall, as applicable, comply with at least the normalised certificate policy ('NCP') requirements as specified in standard ETSI EN 319411-1 version 1.4.1 (2023-10), and shall include:

   (a) a clear description of the public key infrastructure hierarchy and certification paths from the end-entity wallet-relying party access certificates up to the top of the hierarchy used for issuing them, indicating the expected trust anchor(s) in such hierarchy and paths which should rely on the trust framework established in accordance with Article 5a(18) of Regulation (EU) No 910/2014;

   (b) a comprehensive description of the procedures for the issuance of wallet-relying party access certificates, including for the verification of the identity and any other attributes of the wallet-relying party to which a wallet-relying party certificate is to be issued;

   (c) the obligation for the providers of wallet-relying party access certificates, when issuing a wallet-relying party access certificate, to verify that:

      — the wallet-relying party is included, with a valid registration status, in a national register of wallet-relying parties of the Member State in which that wallet-relying party is established;

      — any information in the wallet-relying party access certificate is accurate and consistent with the registration information available from that register.

   (d) a comprehensive description of the procedures for revocation of wallet-relying party access certificates;

   (e) the obligation for the providers of wallet-relying party access certificates to implement measures and processes on:

      — continuously monitoring any changes in the national register for wallet-relying parties in which wallet-relying parties to whom they have issued wallet-relying party access certificates are registered;

      — revoking, when changes require, any wallet-relying party certificate that the provider issued to the corresponding wallet-relying party, in particular when the content of the certificate is no longer accurate and consistent with the information registered, or when the registration of the wallet-relying party is suspended or cancelled.

   (f) a comprehensive description of the procedures and mechanisms for the harmonised validation of wallet-relying party access certificates across the Union;

   (g) the obligation for the providers of wallet-relying party access certificates to allow relevant stakeholders, including wallet-relying parties as regards their own certificates, competent supervisory bodies and data protection authorities, to request the revocation of wallet-relying party access certificates;

   (h) the obligation for the providers of wallet-relying party access certificates to register all such revocations in its certificate database and to publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after receipt of the revocation request;

(i) the obligation for the providers of wallet-relying party access certificates to provide information on the validity or revocation status of wallet-relying party certificates issued by that provider;

(j) a description, where relevant, on how a provider of wallet-relying party access certificates logs all wallet-relying party access certificates they have issued, in compliance with internet engineering task force ('IETF') request for comments ('RFC') 9162 Certificate Transparency version 2.0;

(k) the obligation for the wallet-relying party access certificates to include:

— the location where the certificate supporting the advanced electronic signature or advanced electronic seal on that certificate is available, for the entire certification path to be built up to the expected trust anchor in the public key infrastructure hierarchy used by the provider;

— a machine processable reference to the applicable certificate policy and certificate practice statement;

— the information referred to in Annex I, points 1, 2, 3, 5, 6 and 7, (a), (b) and (c).

4. The revocation set out in point 3(g) shall become effective immediately upon its publication.

5. The information set out in point 3(h) shall be made available at least on a per certificate basis at any time and at least beyond the validity period of the certificate in an automated manner that is reliable, free of charge and effectively in accordance with the certificate policy.

ANNEX V

Requirements for wallet-relying party registration certificates referred to in Article 8

1. The wallet-relying party registration certificate policy applicable to the provision of wallet-relying party registration certificates shall describe the security requirements that apply to, and the rules that indicate the applicability of, a wallet-relying party registration certificate for their issuance to and use by wallet-relying parties in their interactions with wallet solutions. The wallet relying party registration certificate policy shall be published in human-readable.

2. The wallet-relying party registration certificate practice statement applicable to the provisioning of wallet-relying party registration certificates shall describe the practices that a provider of wallet-relying party registration certificates employs in issuing, managing, revoking, and re-keying wallet-relying party registration certificates, and, where applicable, how they relate to wallet-relying party access certificates issued to wallet-relying parties. The wallet relying party registration certificate practice statement shall be published in human-readable.

3. The wallet-relying party registration certificate policy and certificate practice statement applicable to the provisioning of wallet-relying party registration certificates shall be syntactically and semantically harmonised across the Union and shall comply with at least the applicable NCP requirements as specified in standard ETSI EN 319411-1 version 1.4.1 (2023-10), and shall include:

   (a) a clear description of the public key infrastructure hierarchy and certification paths from the end-entity wallet-relying party registration certificates up to the top of the hierarchy used for issuing them, while indicating the expected trust anchor(s) in such hierarchy and paths;

   (b) a comprehensive description of the procedures for the issuance of wallet-relying party registration certificates, including for the verification of the identity and of any attribute of the wallet-relying party to which a wallet-relying party certificate is to be issued;

   (c) the obligation for the provider of wallet-relying party registration certificates, when issuing a wallet-relying party registration certificate, to verify that:

      — the wallet-relying party is included, with a valid registration status, in a national register for wallet-relying parties of the Member State in which that wallet-relying party is established;

      — the information in the wallet-relying party registration certificate is accurate and consistent with the registration information available from that register;

      — the wallet-relying party access certificate is valid;

      — the description of the procedures for revocation of wallet-relying party registration certificates is comprehensive.

   (d) the obligation for the provider of wallet-relying party registration certificates implements measures and processes on:

      — continuously monitoring in an automated manner any changes in the national register for wallet-relying parties in which wallet-relying parties to whom they have issued wallet-relying party registration certificates are registered;

      — reissue the wallet-relying party registration certificate;

      — revoking any wallet-relying party registration certificate that they issued to the corresponding wallet-relying party, when such changes so require, in particular when the content of the certificate is no longer accurate and consistent with the information registered, or when the registration of the wallet-relying party is modified, suspended or cancelled.

   (e) a comprehensive description of the procedures and mechanisms for the harmonised validation of wallet-relying party registration certificates;

(f) the obligation for the provider of wallet-relying party registration certificates to allow relevant stakeholders, including wallet-relying parties as regards their own certificates, competent supervisory bodies and data protection authorities, to request the revocation of wallet-relying party registration certificates;

(g) the obligation for the provider of wallet-relying party registration certificates to register all such revocations in its certificate database and to publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request for revocation;

(h) the obligation for the providers of wallet-relying party registration certificates to provide information on the validity or revocation status of wallet-relying party registration certificates issued by that provider;

(i) a description, where relevant, on how a provider of wallet-relying party registration certificates logs all wallet-relying party registration certificates they have issued;

(j) the obligation for the wallet-relying party registration certificates:

— to include the location where the validation data of the advanced electronic signature or advanced electronic seal for the certificate used to sign or seal the registration certificate is available, for the entire trust chain to be built up to the expected trust anchor;

— to include a machine-readable reference to the applicable certificate policy and certificate practice statement;

— to include the information referred to in Annex I, points 1, 2, 3, 5, 6 and 8, 9, 10, 11, 12, 13, 14 and 15;

— to include the URL to the privacy policy referred to in Article 8(2)g;

— to include a general access policy as referred to in Article 8(3);

4. The data exchange format for the relying party registration certificate shall be signed JSON Web Tokens (IETF RFC 7519) and CBOR Web Tokens (IETF RFC 8392).

5. The revocation referred to in point 3(g) shall become effective immediately upon its publication.

6. The information referred to in point 3(h) shall be made available at least on a per certificate basis at any time and at least beyond the validity period of the certificate in an automated manner that is reliable, free of charge and effectively in accordance with the certificate policy.