



EUROPEAN
COMMISSION

Brussels, XXX
[...] (2024) XXX draft

COMMISSION IMPLEMENTING REGULATION (EU) .../...

of XXX

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

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

COMMISSION IMPLEMENTING REGULATION (EU) .../...

of **XXX**

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

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/EC¹, and in particular Article 5a(23) thereof,

Whereas:

- (1) The European Digital Identity Framework established by Regulation (EU) No 910/2014, is a crucial component in the establishment of a secure and interoperable digital identity ecosystem across the Union. With the European Digital Identity Wallets ('wallets') as the cornerstone of the framework, it aims at facilitating access to services across Member States, for citizens, residents, and businesses, while ensuring the protection of personal data and privacy.
- (2) Article 5a(23) of Regulation (EU) No 910/2014 mandates the Commission, where necessary, to establish the relevant specifications and procedures. This is achieved by means of four Implementing Regulations, dealing with protocols and interfaces [Commission Implementing Regulation (EU) 2024/XXX²], integrity and core functionalities [Commission Implementing Regulation (EU) 2024/XXX³], person identification data and electronic attestation of attributes [Commission Implementing Regulation (EU) 2024/XXX⁴], as well as the trust framework [Commission Implementing Regulation (EU) 2024/XXX⁵]. This Regulation lays down the relevant requirements for person identification data and electronic attestations of attributes.
- (3) To ensure harmonisation, certain common functionalities should be available for all wallets, including the ability to securely request, obtain, select, combine, store, delete, share, and present, under the sole control of the wallet user, person identification data and electronic attestations of attributes. To ensure that person identification data and electronic attestations of attributes can be processed via every wallet unit, technical specifications concerning person identification data attributes, the data format, and the trust infrastructure for person identification need to be supported by all wallet solutions. Further, common specifications in relation to attributes of person

¹ OJ L 257, 28.8.2014, p.73, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>.

² OJ XXX, ELI: XXX

³ OJ XXX, ELI: XXX

⁴ OJ XXX, ELI: XXX

⁵ OJ XXX, ELI: XXX

identification data aims at ensuring that they can be used for identity matching as required.

- (4) To ensure transparency towards wallet users, providers of person identification data should publish information indicating which wallet solutions they support. A common assurance level high is imposed on the verification of the identity of wallet users prior to the issuance of person identification data, equivalent to the assurance level high laid down for electronic means of identification under Regulation (EU) No 910/2014. In this manner, the wallet units ensure the highest available degree of trustworthiness for means of identification across the Union.
- (5) In order to support interoperability, electronic attestations of attributes should comply with harmonised requirements on the format and, where applicable, in relation to embedded disclosure set out in Implementing Regulation (EU) 2024/XXX regards integrity and core functionalities.
- (6) To protect the data of wallet users and to ensure the authenticity of electronic attestations of attributes, mechanisms for the authentication of providers of electronic attestations of attributes, and for the verification of the authenticity and validity of wallet units by that provider should apply prior to the issuance of the attestations to wallet units.
- (7) In order to avoid the use of, and the reliance on, person identification data and electronic attestations of attributes that have lost their legal validity after being issued to a wallet unit, providers of person identification data and of electronic attestations of attributes should publish a policy outlining the circumstances and procedures for revocation.
- (8) The measures provided for in this Regulation are in accordance with the opinion of the committee referred to in 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 issuance of person identification data and electronic attestations of attributes to wallet units.

Article 2

Definitions

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

- (1) ‘wallet user’ means a natural or legal person who is the subject of the person identification data associated with the wallet unit that they are in control of;
- (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, and which is managed and operated by a wallet provider;

- (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 using the cryptographic functions provided by the wallet secure cryptographic device;
- (6) 'wallet secure cryptographic device' means an environment that hosts the wallet secure cryptographic application and provides cryptographic functions;
- (7) 'wallet provider' means a natural or legal person who provides wallet solutions;
- (8) 'critical assets' means information that would put a wallet unit in a critical state in case the assets get compromised and therefore needs protection against duplication and tampering;
- (9) 'wallet cryptographic operation' means a cryptographic mechanism necessary in the context of authentication of the wallet user and the issuance or presentation of person identification data or electronic attestations of attributes;
- (10) '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;
- (11) '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;
- (12) 'provider of person identification data' means a natural or legal person responsible for ensuring that the person identification data of a user is cryptographically bound to a wallet unit;
- (13) 'wallet unit attestation' means a data object that describes the components of the wallet unit, allow authentication and validation of those components and are cryptographically bound to wallet secure cryptographic devices;
- (14) '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;
- (15) 'provider of wallet relying party access certificates' means a natural or legal person mandated by a Member State to issue relying party access certificates to wallet relying parties registered in that Member State;
- (16) 'cryptographic binding' means the method to link person identification data or electronic attestations of attributes to wallet units through cryptographic means.

Article 3

Issuance of person identification data to wallet units

1. Providers of person identification data shall issue the person identification data to wallet users in accordance with the electronic identification schemes under which their wallet solutions are provided.
2. Providers of person identification data shall ensure that person identification data issued to wallet units contains the information required for authentication and validation of the person identification data.

3. Providers of person identification data shall ensure that person identification data issued to wallet units comply with the technical specifications set out in the Annex.
4. Member States shall ensure that the set of person identification data attributes issued to a given wallet user is unique.
5. Providers of person identification data shall ensure that person identification data that they issue apply cryptographically binding to the wallet unit to which they are issued.
6. Member States shall make publicly available a list of wallet solutions that they support for issuing person identification data.
7. Member States shall enroll wallet users in accordance with the requirements relating to enrolment, as set out in Commission Implementing Regulation (EU) 2015/1502⁶.
8. Providers of person identification data shall identify themselves to wallet units using their wallet relying party access certificate when issuing person identification data to wallet units.
9. Before issuing person identification data to wallet units, providers of person identification data shall authenticate and validate the wallet unit attestations of those wallet units using the wallet provider trusted list established in accordance with Implementing Regulation (EU) 2024/XXX regards notifications to the Commission concerning European Digital Identity Wallets and verify that the wallet unit belongs to a wallet solution the provider of person identification data accepts.

Article 4

Issuance of electronic attestations of attributes to wallet units

1. Electronic attestations of attributes issued to wallet units shall comply with the list of standards set out in Annex I of Implementing Regulation (EU) 2024/XXX regards integrity and core functionalities.
2. Providers of electronic attestations of attributes shall identify themselves to wallet units using their wallet relying party access certificate.
3. Providers of electronic attestations of attributes shall ensure that electronic attestations of attributes issued to wallet units contain the information required for authentication and validation of those electronic attestations of attributes.

Article 5

Revocation of person identification data and electronic attestations of attributes

1. Providers of person identification data or electronic attestation of attributes issued to a wallet unit shall have written and publicly accessible policies for validity status management, including, where applicable, the conditions under which such person identification data or electronic attestation of attributes can be revoked.
2. Providers of person identification data or electronic attestation of attributes shall be the only entities able to revoke the person identification data or electronic attestations of attributes that they issued.

—

⁶ OJ L 235, 09.09.2015, ELI: https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj.

3. Where providers of person identification data or electronic attestations of attributes have revoked person identification data or electronic attestations of attributes, they shall inform wallet users subject of those person identification data or electronic attestations of attributes without delay of the revocation and of the reasons for the revocation. This shall be done in a manner that is concise, easily accessible and using clear and plain language.
4. Providers of person identification data or electronic attestation of attributes issued to a wallet unit shall revoke that data or attestation, in each of the following circumstances:
 - (a) upon the explicit request of the wallet user on whose wallet unit the person identification data or electronic attestation of attributes are stored;
 - (b) where it is known to the providers that the security or trustworthiness of the person identification data or electronic attestation of attributes has been compromised;
 - (c) upon becoming aware of the death or dissolution of the wallet user;
 - (d) upon becoming aware that the value of one or more attributes in the person identification data or the electronic attestation of attributes have changed;
 - (e) where the wallet unit to which the person identification data or electronic attestation of attributes was issued to has been revoked;
 - (f) in other situations determined by the providers of person identification data or electronic attestations of attributes in their policies referred to in paragraph 1.
5. Providers of person identification data or of electronic attestation of attributes issued to a wallet unit shall ensure that revocations cannot be reverted.
6. Where providers of person identification data or electronic attestations of attributes revoke person identification data and electronic attestations of attributes issued to wallet units, they shall make publicly available the validity status of person identification data or electronic attestations of attributes they issue and indicate the location of that information in the person identification data or electronic attestations of attributes.

Article 6

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,

For the Commission
The President
Ursula VON DER LEYEN