



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 protocols and interfaces to be supported by the 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 protocols and interfaces to be supported by the 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 ('the 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') being the cornerstone of the framework. The framework aims at facilitating access to services across Member States, for natural and legal persons, 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 protocols and interfaces.
- (3) In order to ensure transparency and trustworthiness of wallet relying parties towards wallet users, the protocols and interfaces used by the wallet solutions should provide wallet users with a reliable mechanism to authenticate wallet relying parties and other wallet units. Inversely, wallet providers should provide a mechanism to authenticate and validate relying parties receive assurances with respect to trustworthiness and authenticity of the wallet units.
- (4) In order to facilitate the issuance of person identification data and electronic attestations of attributes, all wallet solutions should support a minimum set of protocols and interfaces.

-

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

² OJ..., ELI:

³ OJ..., ELI:

⁴ OJ..., ELI:

⁵ OJ..., ELI:

- (5) When person identification data and electronic attestations of attributes are presented via the wallets to relying parties, both in remote and proximity scenarios, all wallet solutions should support common technical specifications as this is the most efficient way to ensure their usability by all wallets across Member States. Additionally, wallet units may support other protocols and interfaces for specific use cases.
- (6) In order to protect the data of wallet users, wallet providers should ensure that wallet units validate requests from wallet relying parties or other wallet units prior to making any data available. For the same reason, in accordance with Article 5a(4)(d)(ii) of Regulation (EU) No 910/2014, wallet providers should ensure that wallet units allow wallet users to make data erasure requests.
- (7) In order to enable swift reactions in the case of any data protection concerns related to Article 5a(4)(d)(iii) of Regulation (EU) No 910/2014, wallet providers should ensure that wallet solutions provide mechanisms for the easy reporting of a relying party to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received. Appropriate flexibility should be left to wallet providers and data protection authorities in establishing suitable mechanisms for interacting with the data protection authorities of the Member State that issued the electronic identification scheme under which the relevant wallet is provided.
- (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 on the interfaces and protocols of the wallet solutions. .

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 provider’ means a natural or legal person who provides wallet solutions;
- (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;

- (6) 'wallet secure cryptographic application' means an application that manages critical assets by using the cryptographic functions provided by the wallet secure cryptographic device;
- (7) 'wallet secure cryptographic device' means an environment that hosts the wallet secure cryptographic application and provides cryptographic functions;
- (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) '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;
- (11) '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;
- (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 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;
- (14) '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;
- (15) '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;
- (16) 'cryptographic binding' means the method to link person identification data or electronic attestations of attributes to wallet units through cryptographic means.

Article 3

General provisions

- 1. Wallet providers shall ensure that wallet units support protocols and interfaces that enable the following:
 - (a) issuance of person identification data and electronic attestations of attributes to wallet units in accordance with Article 4;
 - (b) presentation of attributes of person identification data or electronic attestations of attributes, to wallet relying parties and other wallet units in accordance with Article 5;
 - (c) communication of data erasure requests to wallet relying parties in accordance with Article 6;

- (d) reporting of wallet relying parties to supervisory authorities established under Article 51 of Regulation (EU) 2016/679⁶ in accordance with Article 7.
2. Regarding the protocols and interfaces referred to in paragraph 1, points (a) and (b), wallet providers shall ensure that wallet units:
 - (a) where interacting with wallet relying parties, authenticate and validate the wallet relying party access certificates;
 - (b) where interacting with other wallet units, authenticate and validate the wallet unit attestations of other wallet units,
 - (c) where applicable, authenticate and validate requests made using wallet relying party access certificates or wallet unit attestations from other wallet units;
 - (d) display to wallet users information contained in the wallet relying party access certificates or in case of other wallet units, the wallet unit attestations, including, where applicable, the attributes that wallet users are being requested to present;
 - (e) present wallet unit attestations of the wallet unit to wallet relying parties or wallet units that request it;
 - (f) do not present any requested attributes to wallet relying parties or wallet units until the following requirements are met:
 3. the wallet secure cryptographic application has authenticated the identity of the wallet user;
 4. embedded disclosure policies have been processed within the wallet unit in accordance with Article 11 of Implementing Regulation 2024/XXX regards integrity and core functionalities, where applicable;
 5. wallet users have approved the presentation.

Article 4

Issuance of person identification data and electronic attestations of attributes to wallet units

1. Wallet providers shall ensure that wallet solutions support protocols and interfaces for the issuance of person identification data and electronic attestations of attributes to wallet units.
2. Wallet providers shall ensure that wallet solutions request person identification data and electronic attestations of attributes only from parties having an authentic and valid wallet relying party access certificate issued to a provider of person identification data or provider of electronic attestations of attributes.
3. Wallet providers shall ensure that wallet units authenticate and validate wallet relying party access certificates using only the trusted list of providers of wallet relying party access certificates referred to in Article 18 of Implementing Regulation (EU) 2024/XXX regards notifications to the Commission, before requesting issuance of person identification data, as well as verify that the

—

⁶ OJ L 119, 4.5.2016, p.1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>.

wallet relying party access certificate is issued to a provider of person identification data.

4. Wallet providers shall ensure that wallet units:
 - (a) authenticate and validate the wallet relying party access certificates before requesting the issuance of electronic attestations of attributes,
 - (b) verify whether the wallet relying party access certificate is issued to:
 - a provider of person identification data;
 - a provider of a qualified electronic attestation of attributes;
 - a provider of an electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source; or
 - a provider of non-qualified electronic attestations of attributes.
5. In relation to the issuance of person identification data and electronic attestations of attributes to a wallet unit, wallet providers shall ensure that the following requirements are complied with:
 - (a) where wallet users use their wallet unit to request the issuance of person identification data or of electronic attestations of attributes, the wallet unit shall request it in all formats supported by the wallet solution;
 - (b) where wallet users use their wallet unit to interact with providers of person identification data or electronic attestations of attributes, wallet units shall enable authentication and validation of the wallet unit components by presenting the wallet unit attestations to those providers;
 - (c) wallet solutions shall support mechanisms that enable providers of person identification data to verify issuance, delivery and activation in compliance with the requirements set out in Commission Implementing Regulation (EU) 2015/1502⁷;
 - (d) wallet instances shall verify the authenticity and validity of person identification data.

Article 5

Presentation of attributes to wallet relying parties

1. Wallet providers shall ensure that wallet solutions support protocols and interfaces for the presentation of attributes to wallet relying parties, remotely and in proximity, in accordance with standard set out in the Annex.
2. Wallet providers shall ensure that wallet units respond to successfully authenticated and validated requests from wallet relying parties, as set out in Article 3, in accordance with the standard set out in the Annex.
3. Wallet providers shall ensure that wallet solutions support proving the possession of private keys corresponding to public keys used in cryptographic bindings.
4. Wallet providers shall ensure that wallet solutions support the selective disclosure of attributes of personal identification data and of electronic attestations of attributes.

–

⁷ OJ L 235, 9.9.2015, p. 7, ELI: https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj.

5. Paragraphs 1 to 4 shall apply mutatis mutandis to interactions between two wallet units in proximity. Where wallet providers intend to enable interactions between two wallet units remotely, they shall implement mechanisms that ensure an equivalent level of trustworthiness to that set out in paragraphs 1 to 4 of this Article.

Article 6

Communication of data erasure requests

1. Wallet providers shall ensure that wallet solutions support protocols and interfaces allowing wallet users to request from wallet relying parties with whom they have interacted through those wallet units, the erasure of their personal data provided through those wallet units, in accordance with Article 17 of Regulation (EU) 2016/679.
2. The protocols and interfaces referred to in paragraph 1 shall allow wallet users to select the wallet relying parties to which data erasure requests are to be submitted.
3. Wallet units shall display to the wallet user previously submitted data erasure requests made through those wallet units.

Article 7

Reporting of wallet relying parties to supervisory authorities established under Article 51 of Regulation (EU) 2016/679

1. Wallet providers shall ensure that wallet units allow wallet users to easily report wallet relying parties to supervisory authorities established under Article 51 of Regulation (EU) 2016/679 of the Member State that issued the electronic identification scheme under which the relevant wallet is provided.
2. Wallet providers shall implement the protocols and interfaces for reporting wallet relying parties in compliance with national procedural laws of the Member State that issued the electronic identification scheme under which the relevant wallet is provided.
3. Wallet providers shall ensure that wallet units allow wallet users to substantiate the reports, including by attaching relevant information to identify the wallet relying parties, and the wallet users' claims in machine-readable format.

Article 8

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

DRAFT