



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 the integrity and core functionalities of 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 the integrity and core functionalities 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 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') being the cornerstone of the framework, it 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 relevant specifications and procedures. This is achieved by means of four implementing Regulations, dealing with protocols and interfaces [Commission Implementing Regulation 2024/XXX²], integrity and core functionalities [Commission Implementing Regulation 2024/XXX³], person identification data and electronic attestation of attributes [Commission Implementing Regulation 2024/XXX⁴], as well as the trust framework [Commission Implementing Regulation 2024/XXX⁵]. This Regulation lays down the relevant requirements for integrity and core functionalities.
- (3) Before citizens, residents, and businesses can use wallet units, specific components and functionalities for wallet providers should be set up.
- (4) Wallet secure cryptographic applications [as separate specialised components within a wallet unit] are necessary not only for the protection of critical assets, such as cryptographic private keys, but also for the provision of crucial functionalities, such as the presentation of electronic attestations of attributes.
- (5) Wallet units are to enable providers of person identification data or electronic attestations of attributes to verify that they are issuing this data or attestations genuine wallet units. After issuance, those providers should be able to continue to monitor

—

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.

whether the wallet unit used for issuance is still valid, so that they may revoke issued person identification data or electronic attestations of attributes when wallet units are no longer valid.

- (6) To ensure data protection by design and by default, the wallets should be provided with several privacy enhancing features. These features should ensure that the wallets are to be used without the wallet user being trackable across different wallet relying parties. In addition, embedded disclosure policies should warn the wallet users against inappropriate disclosure of identity information. Wallet providers should ensure that the implementation of these features do not affect interoperability between wallets. The generation of pseudonyms should enable wallet users to authenticate themselves without providing wallet relying parties with unnecessary information.
- (7) Wallet unit attestations should make it possible for wallet relying parties that request attributes from wallet units to certify the validity status of the wallet unit that they are communicating with, as wallet unit attestations are to be revoked when a wallet unit is no longer considered valid. The information regarding the validity status of the wallet units should be made available in an interoperable manner, to ensure that it can be used by all wallet relying parties. Moreover, for cases where wallet users lost their wallet units or no longer have control over it, wallet providers should enable wallet users to request the revocation of their wallet unit.
- (8) In order to ensure that all wallets are technically capable of receiving and presenting person identification data and electronic attestations of attributes in cross-border scenarios without impairing interoperability, wallets should support predetermined types of data formats. In addition, wallets may support other formats and functionalities to facilitate specific use cases.
- (9) Logging of transactions is an important tool to provide transparency, in the form of an overview of all transactions to the wallet user. Furthermore, logs should be used to enable the swift and easy sharing of certain information, at the wallet user's request, with the competent supervisory authorities established pursuant Article 51 of Regulation (EU) 2016/679⁶, in case of suspicious behavior of wallet relying parties.
- (10) For a wallet user to be able to sign electronically, a qualified certificate, which is bound to a qualified electronic signature creation device should be issued to the wallet user. The wallet user should have access to a signature creation application. While the issuance of qualified certificates is a service of qualified trust service providers, wallet providers or other entities should be able to provide the other components. For instance, qualified electronic signature creation devices may be managed by qualified trust service providers as a service or they may be local to the wallet user's device, for example, as a smartcard. Similarly, signature creation applications may be integrated in the wallet instance, be a separate app on the wallet user's device or be provided remotely.
- (11) Backup and recovery objects log the person identification data and electronic attestations of attributes that have been issued to a particular wallet unit. This function is needed to enable wallet users to request attestation providers to re-issue the relevant data to another wallet unit, for example, making it possible to recover lost wallet units or to transfer information from one wallet provider to another to exercise the user's right to data portability.

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

- (12) 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:

CHAPTER I GENERAL PROVISIONS

Article 1

Subject matter and scope

This Regulation lays down rules for the integrity and core functionalities of the wallets.

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) ‘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;
- (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) ‘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;
- (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) ‘cryptographic binding’ means the method to link person identification data or electronic attestations of attributes to wallet units through cryptographic means.

CHAPTER II

INTEGRITY OF EUROPEAN DIGITAL IDENTITY WALLETS

Article 3

Wallet unit integrity

1. Wallet units shall not perform any functionality listed in Article 5a(4) of Regulation (EU) No 910/2014 until the wallet unit has successfully authenticated the wallet users.
2. Wallet providers shall, for each wallet unit, sign or seal, at least one wallet unit attestation compliant with the requirements laid down in Article 6. The certificate used to sign or seal the wallet unit attestation shall be issued under a certificate listed in the trusted list referred to in Implementing Regulation (EU) 2024/XXX regards notifications to the Commission concerning European Digital Identity Wallets.

Article 4

Wallet instances

1. Wallet instances shall use at least one wallet secure cryptographic device to securely store and manage critical assets.
2. The communication between wallet instances and wallet secure cryptographic applications shall utilise secure channels.
3. Where critical assets relate to performing electronic identification at assurance level high, the wallet cryptographic operations shall be performed in accordance with the requirements for the characteristics and design of electronic identification means at assurance level high, as set out in Commission Implementing Regulation (EU) 2015/1502⁷.

Article 5

Wallet secure cryptographic applications

Wallet providers shall ensure that:

—

⁷ OJ L 235, 9.9.2015, ELI: https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj9.

- (1) wallet secure cryptographic applications perform wallet cryptographic operations involving critical assets only in cases where those applications have successfully authenticated wallet users;
- (2) where wallet secure cryptographic applications authenticate wallet users in the context of performing electronic identification at assurance level high, the processing is carried out in accordance with the requirements for the characteristics and design of electronic identification means at assurance level high, as set out in Implementing Regulation (EU) 2015/1502;
- (3) wallet secure cryptographic applications are able to generate new cryptographic keys;
- (4) wallet secure cryptographic applications are able to perform secure erasure of critical assets;
- (5) wallet secure cryptographic applications are able to generate a proof of possession of private keys;
- (6) wallet secure cryptographic applications protect the private keys generated by those wallet secure cryptographic applications during the entire lifetime of the keys;
- (7) wallet secure cryptographic applications complying with the requirements for the characteristics and design of electronic identification means at assurance level high, as set out in Implementing Regulation (EU) 2015/1502; are the only component able to execute wallet cryptographic operations and any other operation with related critical assets in the context of performing electronic identification at assurance level high.

Article 6

Wallet unit authenticity and validity

1. Wallet providers shall ensure that each wallet unit contains wallet unit attestations that:
 - (a) describe the components of the wallet unit;
 - (b) allow authentication and validation of those components;
 - (c) are cryptographically bound to wallet secure cryptographic devices.
2. Wallet providers shall ensure that the wallet unit attestations referred to in paragraph 1 contain a public key, and that the corresponding private key is protected by the wallet secure cryptographic application.
3. Wallet providers shall:
 - (a) establish accounts for wallet users;
 - (b) disclose to wallet users their rights and obligations in relation to their wallet unit;
 - (c) ensure wallet users have the right to request revocation of their wallet unit;
 - (d) provide suitable mechanisms for the secure authentication of wallet users;
 - (e) ensure that the authentication mechanisms referred to in point (d) are independent of wallet units.

Article 7

Revocation of wallet units

1. Wallet providers shall be the only entity capable of revoking wallet unit attestations for wallet units that they have provided.
2. Wallet providers shall establish a publicly available policy specifying the conditions and the timeframe for the revocation of data objects relating to wallet units that they have provided.
3. Where the value of one or more attributes in wallet unit attestations have changed, wallet providers shall revoke the wallet unit attestations without delay and re-issue the wallet unit attestations with correct values.
4. Where wallet providers have revoked wallet unit attestations, they shall inform affected wallet users without delay, in a manner that is concise, easily accessible, and easy to understand, and using clear and plain language, of the revocation of their wallet units, including the reason or reasons for the revocation.
5. Where wallet providers have revoked wallet unit attestations, they shall make publicly available the validity status of the wallet unit attestation and describe the location of that information in the wallet unit attestation.

CHAPTER III

CORE FUNCTIONALITIES AND FEATURES OF EUROPEAN DIGITAL IDENTITY WALLETS

Article 8

Formats for person identification data and electronic attestations of attributes

Wallet providers shall ensure that wallet solutions support the usage of person identification data and electronic attestations of attributes issued in compliance with the list of standards set out in Annex I.

Article 9

Transaction logs

1. Irrespective of whether or not a transaction is successfully completed, wallet units shall log at least the following information on all transactions with wallet relying parties and other wallet units:
 - (a) the time and date of the transaction;
 - (b) the name of the corresponding wallet relying party;
 - (c) the personal data presented in the transaction;
 - (d) in the case of non-completed transactions, the reason for such non-completion.
2. Wallet solutions shall keep log files relating to reports sent by the wallet user to the data protection authorities via their wallet unit. These log files shall be accessible to the wallet users of the wallet unit concerned.

3. Wallet providers shall provide wallet users with information enabling them to access the stored transaction logs referred to in paragraph 1.
4. Wallet providers shall enable wallet users to export the records referred to in paragraphs 1 and 2 from the wallet unit.

Article 10

Embedded disclosure

1. Wallet providers shall ensure that electronic attestations of attributes with common embedded disclosure policies set out in Annex II can be stored in the wallet units that they provide. Wallet instances shall be able to process and present such embedded disclosure policies in conjunction with data received from the requesting wallet relying party.
2. Wallet instances shall verify whether the wallet relying party complies with the requirements of the embedded disclosure policy and inform the wallet user of the result.

Article 11

Qualified electronic signatures and seals

1. Wallet providers shall ensure that wallet users are able to receive qualified certificates for qualified electronic signatures or seals which are linked to qualified signature or seal creation devices that are either local, external, or remote in relation to the wallet instances.
2. Wallet providers shall ensure that wallet solutions are able to interface with local, external, or remote qualified signature or seal creation devices for the purposes of using the qualified certificates referred to in paragraph 1.
3. Wallet providers shall ensure that wallet users who are natural persons have, for non-professional purposes, free-of-charge access to integrated or external signature creation applications which allow the creation of free-of-charge qualified electronic signatures using the certificates referred to in paragraph 1.
4. Wallet providers shall ensure that wallet instances are able to verify the qualified status of qualified trust service providers providing signing or sealing services in the context of remote signature or seal creation through the wallet instance.

Article 12

Signature creation applications

1. The signature creation applications used by wallet units may be provided either by wallet providers, by providers of qualified trust services or by wallet relying parties.
2. Signature creation applications shall have the following functions:
 - (a) signing or sealing wallet user-provided data;
 - (b) signing or sealing relying party-provided data;
 - (c) supporting signatures or seals in at least one of the formats referred to in Annex III;
 - (d) informing wallet users about the result of the signature or seal creation process.

3. The signature creation applications may be either integrated into the wallet instances or be provided externally. Where signature creation applications are integrated into wallet instances, they shall support the application programming interface referred to in Annex III.

Article 13

Data recovery and portability

1. Wallet solutions shall support backup and recovery of the data of the wallet user to allow the wallet user to migrate free of charge to another wallet unit of the same wallet solution provided under the same electronic identification scheme. The data backed up and restored shall include the logs referred to in Article 9 as well as any data needed to restore or re-issue person identification data and any electronic attestations of attributes to the new wallet unit.
2. Wallet solutions shall support portability of the data of the wallet user to allow the wallet user to migrate to a different wallet solution.

Article 14

Pseudonyms

Wallet solutions shall support the generation of wallet relying party specific pseudonyms for wallet users in compliance with the technical specifications set out in Annex IV.

CHAPTER IV FINAL PROVISIONS

Article 15

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*