Official Journal
of the European Union

EN
L series

2024/2982

4.12.2024

COMMISSION IMPLEMENTING REGULATION (EU) 2024/2982

of 28 November 2024

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ([1]), and in particular Article 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) Regulation (EU) 2016/679 of the European Parliament and of the Council ([2]), and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ([3]) apply to all personal data processing activities under this Regulation.

(3) 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) 2024/2982 ([4]), integrity and core functionalities: Commission Implementing Regulation (EU) 2024/2979 ([5]), person identification data and electronic attestation of attributes: Commission Implementing Regulation (EU) 2024/2977 ([6]), as well as the notifications to the Commission: Commission Implementing Regulation (EU) 2024/2980 ([7]). This Regulation lays down the relevant requirements for protocols and interfaces.

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

([2]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

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

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

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

([7]) Commission Implementing Regulation (EU) 2024/2980 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem (OJ L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) The Commission regularly assesses new technologies, practices, standards or technical specifications. To ensure the highest level of harmonisation among Member States for the development and certification of the wallets, the technical specifications set out in this Regulation rely on the work carried out on the basis of Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework ([8]) and in particular the architecture and reference framework. In accordance with Recital 75 of Regulation (EU) 2024/1183 of the European Parliament and of the Council ([9]), the Commission should review and update this Implementing Regulation, if necessary, to keep it in line with global developments, the architecture and reference framework, and to follow the best practices on the internal market.

(5) 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 wallet units so that relying parties can receive assurances with respect to trustworthiness and authenticity of the wallet units. Further, the technical infrastructure of the wallets should also be designed to ensure that only the minimal necessary amount of data is transferred only to the authorised relying parties, while keeping unlinkability between the different transactions. 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.

(6) To ensure the usability of wallet solutions across Member States, all wallet solutions should support common technical specifications when person identification data and electronic attestations of attributes are presented via the wallets to relying parties, both in remote and proximity scenarios. Additionally, wallet units may support other protocols and interfaces for specific use cases.

(7) To ensure data protection by design and by default, the wallets should be provided with several privacy enhancing features to prevent providers of electronic identification means and electronic attestation of attributes from combining personal data obtained when providing other services with the personal data processed to provide the services falling within the scope of Regulation (EU) No 910/2014. As set out in Regulation (EU) No 910/2014, 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 enabled to verify the registration data of relying parties at any point in time. Further, wallet units should be able to display wallet relying party registration certificates to users, when available, as part of an attribute request. This should enable wallet users to verify that the attributes being requested by the wallet relying party are within the scope of their registered attributes, providing assurance that the request is legitimate and trustworthy.

(8) 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 and 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 to wallet-relying parties.

(9) 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 reporting of a relying party to the competent national data protection authority. Appropriate flexibility should be left to wallet providers and data protection authorities in establishing suitable mechanisms for interacting with data protection authorities of the Member States.

(10) 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 ([10]), and delivered its opinion on 30 September 2024.

([8]) OJ L 210, 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 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).

([10]) 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).

(11) 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 protocols and interfaces of wallet solutions for:

(1) the issuance of person identification data and electronic attestations of attributes to wallet units;

(2) the presentation of attributes of person identification data and electronic attestations of attributes, to wallet-relying parties and other wallet units;

(3) the communication of data erasure requests to wallet-relying parties;

(4) the reporting of wallet-relying parties to supervisory authorities established under Article 51 of Regulation (EU) 2016/679;

to be updated on a regular basis to keep in line with technology and standards developments and with the work carried out on the basis of Recommendation (EU) 2021/946, and in particular the Architecture and Reference Framework.

Article 2

Definitions

For the purpose 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 user' means a user who is in control of the wallet unit;

(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 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;

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

(6) '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;

(7) '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;

(8) '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;

(9) '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;

(10) ‘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;

(11) ‘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;

(12) ‘wallet unit attestation’ means a data object that describes the components of the wallet unit or allows authentication and validation of those components;

(13) ‘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;

(14) ‘wallet-relying party registration certificate’ means a data object that indicates the attributes the relying party has registered to intend to request from users;

(15) ‘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;

(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

Regarding the protocols and interfaces referred to in Articles 4 and 5, wallet providers shall ensure that wallet units:

(1) authenticate and validate the wallet-relying party access certificates where interacting with wallet-relying parties;

(2) authenticate and validate the wallet unit attestations of other wallet units where interacting with other wallet units;

(3) authenticate and validate requests made using wallet-relying party access certificates or wallet unit attestations from other wallet units, where applicable;

(4) authenticate and validate the wallet-relying party registration certificate, where applicable;

(5) display to wallet users information contained in the wallet-relying party access certificates or in the wallet unit attestations;

(6) display to wallet users, where applicable, the attributes that wallet users are requested to present;

(7) display to wallet users, where applicable, information contained in the wallet-relying party registration certificate;

(8) present wallet unit attestations of the wallet unit to wallet-relying parties or wallet units that request it;

(9) do not present any requested attributes to wallet-relying parties or wallet units until the following requirements are met:

(a) verify the wallet secure cryptographic application has authenticated the identity of the wallet user;

(b) verify embedded disclosure policies have been processed within the wallet unit in accordance with Article 11 of Implementing Regulation (EU) 2024/2979, where applicable;

(c) verify wallet users have partially or in full approved the presentation.

(10) enable privacy preserving techniques which ensure unlinkability where the electronic attestations of attributes do not require the identification of the wallet user, when presenting attestations or person identification data across different wallet-relying parties.

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 units request issuance of person identification data and electronic attestations of attributes only from parties having an authentic and valid wallet-relying party access certificate attesting them as:

(a) a provider of person identification data;

(b) a provider of a qualified electronic attestation of attributes;

(c) a provider of an electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source; or

(d) a provider of non-qualified electronic attestations of attributes.

3. 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 from providers of person identification data or providers of electronic attestations of attributes that enable issuance of person identification data or electronic attestations in more than one format, the wallet unit shall request it in all formats referred to in Article 8 of Implementing Regulation (EU) 2024/2979 laying down rules for the application of Regulation (EU) No 910/2014 as regards the integrity and core functionalities of European Digital Identity Wallets;

(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 upon their request;

(c) wallet solutions shall support mechanisms that enable providers of person identification data to verify issuance, delivery and activation in compliance with assurance level high requirements set out in Commission Implementing Regulation (EU) 2015/1502 ([11]);

(d) wallet units shall verify the authenticity and validity of person identification data and electronic attestations of attributes.

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 where appropriate in proximity, in accordance with the standards set out in the Annex.

2. Wallet providers shall ensure that, at the request of users, wallet units respond to successfully authenticated and validated requests from wallet-relying parties referred to in Article 3, in accordance with the standards set out in the Annex.

3. Wallet providers shall ensure that wallet units support proving the possession of private keys corresponding to public keys used in cryptographic bindings.

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

4. Wallet providers shall ensure that wallet solutions support the selective disclosure of attributes of personal identification data and of electronic attestations of attributes.

5. Paragraphs 1 to 4 shall apply *mutatis mutandis* to interactions between two wallet units in proximity.

Article 6

Communication of data erasure requests

1. Wallet providers shall ensure that wallet units 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.

2. Wallet providers shall implement the protocols and interfaces for reporting wallet-relying parties in compliance with national procedural laws of the Member States.

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, 28 November 2024.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

STANDARDS REFERRED TO IN ARTICLE 5(1) AND (2)

— ISO/IEC 18013-5:2021

— ISO/IEC TS 18013-7:2024