Official Journal
of the European Union

EN
L series

2026/798

8.4.2026

COMMISSION IMPLEMENTING REGULATION (EU) 2026/798

of 7 April 2026

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards and specifications for the remote onboarding of users to the European Digital Identity Wallets by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures where the combination meets the requirements of assurance level high

THE EUROPEAN COMMISSION,

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(24) thereof,

Whereas:

(1) The onboarding of users to the European Digital Identity Wallets ('wallets') is a crucial step as regards the verification of the identity of the wallet users, the binding of the personal identification data of the users to their wallets and to the user device in which the wallet units are installed.

(2) To foster a high level of trust and security as well as a harmonised approach across Member States for the onboarding of wallet users with remote onboarding procedures in conjunction with the electronic identification means conforming to assurance level substantial, this implementing act establishes specifications and procedures in order to facilitate the onboarding of users to the European Digital Identity Wallet by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures that together meet the requirements of assurance level high.

(3) Those standards should reflect established practices and be widely recognised within the relevant sectors. Those standards should be adapted to include requirements ensuring the security and trustworthiness of the onboarding of users.

(4) Commission Implementing Regulation (EU) 2015/1502 ([2]) stipulates that where electronic identification means are issued at assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Therefore, in such a case, Member States should leverage on electronic identification means issued at assurance level high also for the onboarding process for the purpose of this Regulation.

(5) Where Member States onboard users to wallets by using an electronic identification means that has not been notified to the Commission, the assurance level of that means should be confirmed by a conformity assessment body defined in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council ([3]) or by an equivalent body and it should be demonstrated that the results of this previous issuance procedure of an electronic identification means remain valid.

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

([2]) 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).

([3]) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

(6) While the Annex sets out the requirements to fulfil for a specific level of identity proofing to be achieved, equivalence has not been established with regard to level of assurance as defined in Article 8 of Regulation (EU) No 910/2014. Therefore, requirements set out in the Annex should be considered as implementing those of Implementing Regulation (EU) 2015/1502 and to be fulfilled by the provider of person identification data or an entity providing identity proofing services on behalf of that provider.

(7) The Commission regularly assesses new technologies, practices, and technical specifications. In accordance with Recital 75 of Regulation (EU) 2024/1183 of the European Parliament and of the Council ([4]), the Commission should review and, if necessary, update this Implementing Regulation to keep it in line with global developments, new technologies, standards or technical specifications and to follow the best practices on the internal market in particular regarding the onboarding of users to the wallet.

(8) Regulation (EU) 2016/679 of the European Parliament and of the Council ([5]), and, where relevant, Regulation (EU) 2018/1725 of the European Parliament and of the Council ([6]), Directive 2002/58/EC of the European Parliament and of the Council ([7]) apply to the personal data processing activities under this Regulation.

(9) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered its opinion on 30 January 2026 ([8]).

(10) The committee established by Article 48 of Regulation (EU) No 910/2014 has not delivered an opinion within the time limit laid down by its Chair,

HAS ADOPTED THIS REGULATION:

Article 1

The reference standards and specifications referred to in Article 5a(24) of Regulation (EU) No 910/2014 are set out in the Annex to this Regulation.

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

([8]) EDPS Formal comments on the draft Commission Implementing Regulation as regards onboarding of users to the European Digital Identity Wallets.

Article 2

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, 7 April 2026.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

LIST OF REFERENCE STANDARDS AND SPECIFICATIONS

Conformance is assessed against the clauses of ETSI TS 119 461 V2.1.1 (2025-02) listed in section 1, subject to the adaptations listed in section 2.

Section 1 – Applicable clauses

— 5 Operational risk assessment;

— 6 Policies and practices;

— 7 Identity proofing service management and operation;

— 8 Identity proofing service requirements;

— 9.1 Introduction, compliance with the present document, general requirements for all use cases;

— 9.2.2 Use cases using an identity document for attended remote identity proofing;

— 9.2.3 Use cases using an identity document for unattended remote identity proofing;

— 9.2.4 Use case for identity proofing by authentication using eID means;

— 9.5 Use cases for additional identity proofing to enhance an identity proven by use of an eID from Baseline LoIP to Extended LoIP.

Section 2 – Adaptations

(1) 5 Operational risk assessment

— OVR-5-01: The requirements specified in ETSI EN 319 401 [1], clause 5 shall apply.

— *Note 1:* When the identity proofing is done by the provider of person identification data itself, the risk assessment of the provider of person identification data can cover the identity proofing.

(2) 6.1 Identity proofing service practice statement

— OVR-6.1-02: An IPSP shall identify in its practice statement the use cases for which compliance with the present document is claimed.

— *Note 1:* When the identity proofing is done by the provider of person identification data itself, the identity proofing service practice statement of the provider of person identification data can cover the information on the identity proofing and there is no need for a specific practice statement for identity proofing.

(3) 7.9 Vulnerabilities and incident management

— OVR-7.9-02: Reporting obligations according to ETSI EN 319401 [1] REQ-7.9.2-02X and clause 7.9.3 shall be fulfilled as required by the identity proofing context and the obligations of the provider of person identification data relying on the IPSP's service.

— EXAMPLE: Reporting to the supervisory authority supervising a provider of European Digital Identity Wallets established in the designating Member State can be done in cooperation between the IPSP and the provider of person identification data.

(4) 7.10 Collection of evidence

— OVR-7.10-01: The requirements specified in ETSI EN 319 401 [1], clause 7.10 shall apply.

— *Note 1:* Long-term requirements for retention of evidence can be fulfilled by the provider of person identification data requesting the identity proofing instead of by the IPSP when the two are different entities.

— *Note 2:* The requirements of clause 8.5.2 of the present document apply.

(5) 7.11 Business continuity management

— OVR-7.11-02: Processes for crisis management according to ETSI EN 319401 [1], REQ-7.11.3-01X shall be as required by the identity proofing context and the obligations of the provider of person identification data relying on the IPSP's service.

(6) 7.12 Termination and termination plans

— OVR-7.12-01: The requirements specified in ETSI EN 319401 [1], clause 7.12, excluding REQ-7.12-11, shall apply.

— *Note:* When the IPSP and the provider of person identification data requesting the identity proofing are different entities, they can agree mutual or unilateral assistance in establishing termination plans.

(7) 8.1 Initiation

— INI-8.1-05: In the event that the remote identity proofing process is aborted or fails, the IPSP shall ensure that individuals are provided with sufficient explanations and remedies particularly in the case of unattended remote identity proofing. The information should ensure that individuals can effectively contribute to the prompt resolution of the problem and, if needed, exercise their data subject rights – such as the right to rectification or the ability to contest the decision – against the relevant controller.

(8) 8.2.1 General requirements

— COL-8.2.1-08: The IPSP shall implement measures to ensure compliance with the requirements of data protection by design and by default in accordance with Article 25 of Regulation (EU) 2016/679 during the onboarding process especially as regards to the processing of biometric data. Relevant measures may consist of adequate privacy-enhancing cryptographic controls, devices and organisational measures. Those measures should limit the data collection to what is strictly necessary for the processing of biometric data and any other personal data to be collected from the physical and digital sources of identification for the binding of the User's personal identification data to their wallets and to the User's device in which the Wallet Unit is installed.

(9) 8.2.4 Use of existing eID means as evidence

— [CONDITIONAL] COL-8.2.4-02X: If the Baseline LoIP is targeted, the eID means shall have been notified at least at eIDAS LoA substantial or its assurance level shall have been confirmed by an accredited conformity assessment body defined in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body, and, if all applicable requirements are fulfilled, the assessment shall result in a certificate of compliance based on a certification audit. This formal certification process shall be based on a security evaluation process that refers to the levels of assurance defined for notified electronic identification means or for certified European Digital Identity Wallets under Regulation (EU) No 910/2014 [i.25].

— COL-8.2.4-02A: void

(10) 8.3.1 General requirements

— VAL-8.3.1-11X: The identity proofing process shall verify that the evidence is valid at the time of the identity proofing.

(11) 8.3.3 Validation of physical identity document

— VAL-8.3.3-21: The effectiveness of the measures for complying with the requirements VAL-8.3.3-05X, VAL-8.3.3-05A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07A and VAL-8.3.3-07X, shall be confirmed by an accredited conformity assessment body defined in Article 2(13) of Regulation (EC) no 765/2008 or an equivalent body.

— VAL-8.3.3-22: The reference face image from the physical identity document shall be collected using near field communication and the process shall perform passive or active authentication of the chip on the physical identity document.

(12) 9.1 Introduction, compliance with the present document, general requirements for all use cases

— USE-9.1-01X: To be compliant with the present document, an identity proofing process shall conform to use case in clause 9.5 of the present document for Extended LoIP.

— USE-9.1-03X: void.

(13) 9.2.3.4 Use case for automated operation

— USE-9.2.3.4-04: The IPSP shall establish target values for the FAR and FRR, based on a risk analysis and its threats intelligence procedure, by following the methodology established in the ENISA report 'Methodology for sectoral cybersecurity assessments' [i.28] or an equivalent methodology, in fully automated identity proofing processes. The target values used by the IPSP shall be equal to or lower than those set for hybrid use cases, when they exist. The IPSP shall maintain these target values for FAR and FRR consistently, supported by a risk analysis and its threats intelligence procedure.

(14) 9.5.1 General requirements

— First paragraph: Where the applicant is a natural person, including a natural person representing a legal person, and the identity of the applicant has been proven to Baseline LoIP by means of authentication using an eID, and an enhancement to Extended LoIP is required, the following requirements shall apply.

— USE-9.5.1-08: The additional identity proofing required to strengthen the reliability of an identity is only applicable for eID that have not been issued with a reliance on automated comparison between face images for the initial issuance process.

(15) 9.5.2 Use case for enhancing identity proofing to Extended LoIP by a full identity proofing using an identity document

— USE-9.5.2-01: The identity proofing to enhance from Baseline to Extended LoIP shall be according to the requirements for Extended LoIP from one of the use cases described in clauses 9.2.2, or 9.2.3 of the present document for Extended LoIP.

(16) 9.5.3 Use case for enhancing identity proofing to Extended LoIP by use of a previously captured reference face image

— USE-9.5.3-01: An identity proofing process fulfilling the requirements for Extended LoIP from one of the use cases described in clauses 9.2.2, or 9.2.3 of the present document, or the identity proofing process has been peer reviewed or certified by an accredited conformity assessment body defined in Article 2(13) of Regulation (EC) No 765/2008 or an equivalent body to comply with assurance level high in accordance with Regulation (EU) No 910/2014 [i.25] shall be used to capture a reference face image and to bind the necessary identity attributes to this reference face image.