EUROPEAN
COMMISSION

Brussels, XXX
[…](2026) XXX draft

ANNEXES 1 to 3

**ANNEXES**

**to the**

**COMMISSION IMPLEMENTING REGULATION**

**amending Implementing Regulation (EU) 2025/1569 as regards applicable standards and specifications**

## ANNEX I

‘*ANNEX I*

**List of reference standards and specifications referred to in Article 3**

ETSI TS 119 471 V1.1.1 (2025-05) shall apply with the following adaptations:

(1) 2.1 Normative references:

[1] ETSI EN 319 401 V3.1.1 (2024-06): "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[2] European Cybersecurity Certification Group, Sub-group on Cryptography: "Agreed Cryptographic Mechanisms" published by the European Union Agency for Cybersecurity (‘ENISA’).

[3] FIPS PUB 140-3 (2019) "Security Requirements for Cryptographic Modules".

[4] Commission Implementing Regulation (EU) 2024/482[1] of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[5] Commission Implementing Regulation (EU) 2024/3144[2] of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation[3].

[6] ISO/IEC 15408:2022 (parts 1 to 5): “Information security, cybersecurity and privacy protection – Evaluation criteria for IT security”.

(2) 3.1 Terms:

Following term is added:

– secure cryptographic device: device which holds the user’s private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

(3) 4. EAA trust services

This clause 4 shall not apply.

(4) 6.1 EAAS practice statement:

– REQ-EAASP-6.1-02: EAASP shall document the revocation mechanism in the EAAS practice statement

(5) 6.2 Terms and conditions:

REQ-EAASP-6.2.4-07: Subscribers and parties relying on the trust service shall be informed, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually, of precise terms and conditions, including the items listed above, before entering into a contractual relationship.

6.3 Information security policy:

[1] OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

[2] OJ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

REQ-EAASP-6.3-02: The EAASP shall establish procedures to notify the supervisory body of any changes in the provision of the electronic archiving trust service and on the intention to cease those activities, in accordance with business requirements and relevant laws and regulations, including in accordance with the requirements of the implementing acts adopted pursuant to Article 24(5) of Regulation (EU) No 910/2014. The EAASP shall notify the supervisory body at least:

– one month before implementing any change;

– three months before the planned cessation of a trust service provision.

(6) 7.2 Human resources:

REQ-EAASP-7.2-02: EAASP's personnel in trusted role shall be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.REQ-EAASP-7.2-03: This shall include regular (at least every 12 months) updates on new threats and current security practices.

(7) 7.5 Cryptographic controls:

– REQ-EAASP-7.5.2-05: void

– REQ-EAASP-7.5.2-06: void

– REQ-EAASP-7.5.3-01A: Appropriate security controls shall be in place for the management of any cryptographic keys, cryptographic algorithms, and cryptographic devices throughout their lifecycle, following, where appropriate, a cryptographic agility approach.

– REQ-EAASP-7.5.3-01B: For the purpose of the provision of its trust services, the EAASP shall select and use suitable cryptographic techniques compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [2].

– REQ-EAASP-7.5.3-02: The EAASP shall ensure that this secure cryptographic device is either is a qualified signature or seal creation device or is a trustworthy system certified in accordance with:

  (a) Common Criteria for Information Technology Security Evaluation, as set out in ISO/IEC 15408 [6] or in Common Criteria for Information Technology Security Evaluation, version CC:2002, Parts 1 through 5, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security, and certified to EAL 4 or higher; or

  (b) the European Common Criteria-based cybersecurity certification scheme (EUCC) [4][5], and certified to EAL 4 or higher; or

  (c) until 31.12.2030, FIPS PUB 140-3 [3] level 3.

  This certification shall be to a security target or protection profile, or to a module design and security documentation, which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

If the secure cryptographic device benefits from an EUCC [4][5] certification, then this device shall be configured and used in accordance with that certification.

(8) 7.8 Network security:

– REQ-EAASP-7.8-05: The vulnerability scan requested by REQ-7.8-13 of ETSI EN 319 401 [1] shall be performed at least once per quarter.

– REQ-EAASP-7.8-06: The penetration test requested by REQ-7.8-17X of ETSI EN 319 401 [1] shall be performed at least once per year.

– REQ-EAASP-7.8-07: Firewalls shall be configured to prevent all protocols and accesses not required for the operation of the EAASP.

(9) 7.9 Vulnerabilities and Incident management:

– REQ-EAASP-7.9-02: Monitoring activities shall take account of the sensitivity of any information collected or analysed. 7.12 EAASP and EAAS termination and termination plans

(10) 7.12 EAASP and EAAS termination and termination plans

– REQ-EAASP-7.12-04: The EAASP's termination plan shall comply with the requirements set out in the implementing acts adopted pursuant to Art.24(5) of Regulation (EU) No 910/2014 [i.1].'

## ANNEX II

*'ANNEX II*

**Technical specifications referred to in Article 3 and Article 4**

Providers of qualified electronic attestations of attributes and providers of electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall issue their attestations in compliance with the list of standards set out in Annex II of Commission Implementing Regulation (EU) 2024/2979[3] and apply the revocation techniques also set out in Annex II of Commission Implementing Regulation (EU) 2024/2979[4].

[3] 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).

[4] 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).

## ANNEX III

*'ANNEX IV*

**List of standards and technical specifications referred to in Article 9**

The verification mechanisms referred to in Article 9 shall comply with either one or both of the following:

(a) the technical specifications set out in [TBC clause 6.1.1 of ETSI TS 119 478 V0.0.10][5] - Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources;

(b) the technical specifications set out in [TBC clause 6.2.2 and in clause 6.2.3 of ETSI TS 119 478 V0.0.10][6]- Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources.'

[5] Pending adoption.

[6] Pending adotpion.