EUROPEAN
COMMISSION

Brussels, 28.11.2024
C(2024) 8495 final

ANNEXES 1 to 5

ANNEXES

to the

Commission Implementing Regulation

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

ANNEX I

List of standards referred to in Article 5

- SAM.01 Secured Applications for Mobile - Requirements for supporting 3rd party Applets on eSIM and eSE via SAM. v1.1 2023, GSMA;
- GPC_GUI_ 217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM v1.0 2024-04;
- GPC_SPE_0 34 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03;
- GPC_SPE_0 07 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07;
- GPC_SPE_0 13 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04;
- GPC_SPE_0 93 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03;
- GPD_SPE_0 75 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.

ANNEX II

List of standards referred to in Article 8

- ISO/IEC.18013-5:2021
- ‘Verifiable Credentials Data Model 1.1’, W3C Recommendation, 03 March 2022.

ANNEX III

List of common embedded disclosure policies referred to in Article 10

1. ‘No policy’ indicating that no policy applies to the electronic attestations of attributes.

2. ‘Authorised relying parties only policy’, indicating that wallet users may only disclose electronic attestations of attributes to authenticated relying parties which are explicitly listed in the disclosure policies.

3. ‘Specific root of trust’ indicating that wallet users should only disclose the specific electronic attestation of attributes to authenticated wallet-relying parties with wallet-relying party access certificates derived from a specific root (or list of specific roots) or intermediate certificate(s).

ANNEX IV

Signature and seal formats referred to in Article 12

1. Mandatory signature or seal format:

   (a) PAdES (PDF Advanced Electronic Signature) as specified in ETSI EN 319 142-1 V1.1.1 (2016-04); Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures.

2. List of optional signature or seal formats:

   (a) XAdES as specified in 'ETSI EN 319 132-1 V1.2.1 (2022-02) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures (XAdES)' for signing of XML format;

   (b) JAdES as specified in 'ETSI TS 119 182-1 V1.2.1 (2024-07) Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures' for signing of JSON format;

   (c) CAdES (CMS Advanced Electronic Signature) as specified in 'ETSI EN 319 122-1 V1.3.1 (2023-06) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures' for the signing of CMS format;

   (d) ASiC (Associated Signature Container) as specified in 'ETSI EN 319 162-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers and ETSI EN 319 162-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers' for the signing of containers.

3. Application programming interface:

   – Cloud Signature Consortium (CSC) specification v2.0 (20 April 2023).

ANNEX V

Technical specifications for pseudonym generation referred to in Article 14

Technical specifications:

- WebAuthn – W3C Recommendation, 8 April 2021, Level 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.