Official Journal
of the European Union

EN
L series

2024/2979

4.12.2024

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

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 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 the integrity and core functionalities of European Digital Identity Wallets.

([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 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 precise communication, technical differentiation, and clear assignment of responsibilities, it is necessary to distinguish between different components and configurations of wallets. A wallet solution should be understood as the complete system provided by a wallet provider that is necessary to operate a wallet. This should include the software and hardware components, as well as services, settings, and configurations needed to ensure the wallet functions properly. A wallet solution may be located on the users' devices and environments and the provider's backend structure. A wallet unit should be understood as a specific setup of the wallet solution for an individual user. It should include the application installed on a wallet user's device or environment that the wallet user interacts with directly (the 'wallet instance') and the necessary security features to protect the users' data and transactions. These security features should involve special software or hardware to encrypt and safeguard sensitive information. A wallet instance should be part of the wallet unit and allow the wallet user to access the functionalities of their wallet.

(6) 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. The use of common technical specifications may facilitate the access to embedded secure elements by wallet providers. Wallet secure cryptographic applications may be provided in various ways and to various kinds of wallet secure cryptographic devices. Where custom wallet secure cryptographic applications are provided by wallet providers as Java Card applets to embedded secure elements, wallet providers should follow the standards listed in Annex I or equivalent technical specifications.

(7) 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 to genuine wallet units of the wallet user.

(8) To ensure data protection by design and by default, the wallets should be provided with available state-of-the-art privacy enhancing techniques. These features should provide the possibility that wallets can be used without the wallet user being trackable across different wallet-relying parties, if applicable in the usage scenario. For instance, wallet providers should consider state-of-the-art privacy mitigating measures in relation to wallet unit attestations, such as using ephemeral wallet unit attestations or batch issuance. In addition, embedded disclosure policies should warn the wallet users against inappropriate or illegal disclosure of attributes from electronic attestations of attributes.

(9) Wallet unit attestations should make it possible for wallet-relying parties which request attributes from wallet units, to verify 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. To ensure the privacy and unlinkability, Member States should employ privacy preserving techniques also for the wallet unit attestation. This may include the usage of multiple wallet unit attestations for different purposes, disclosing only the minimally relevant information about the wallet necessary for a transaction, or to limit the lifetime of the wallet unit attestation as an alternative to the use of revocation identifiers.

([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) 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 and selective disclosure. As set out in Regulation (EU) No 910/2014 selective disclosure is a concept empowering the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only such information as is necessary for the provision of a service requested by a user. As the wallets are to enable the user to selectively disclose attributes, the standards listed in Annex II should be implemented in a way that enables this feature of the wallets. In addition, wallets may support other formats and functionalities to facilitate specific use cases.

(11) Logging transactions is an important tool to provide transparency, in the form of providing an overview of the transactions to the wallet user. Furthermore, logs should be used to enable the swift and easy sharing of certain information, at the request of the wallet user, with the competent supervisory authorities established pursuant Article 51 of Regulation (EU) 2016/679, in case of suspicious behaviour of wallet-relying parties.

(12) 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.

(13) Data export and portability objects can log the person identification data and electronic attestations of attributes that have been issued to a particular wallet unit. These objects allow wallet users to extract the relevant data from their wallet unit in order to strengthen their right to data portability. Wallet providers are encouraged to use the same technical solutions to also implement backup and recovery processes for wallet units, making it possible to recover lost wallet units or to transfer information from one wallet provider to another, where appropriate and insofar as this can be done without impairing the right to data protection and the security of the digital identity ecosystem.

(14) The generation of wallet-relying party specific pseudonyms should enable wallet users to authenticate themselves without providing wallet-relying parties with unnecessary information. As set out in Regulation (EU) No 910/2014, wallet users are not to be hindered from accessing services under a pseudonym, where there is no legal requirement for legal identity for authentication. Therefore, the wallets are to include a functionality to generate user-chosen and managed pseudonyms, to authenticate when accessing online services. The implementation of the specifications set out in Annex V should enable these functionalities accordingly. Further, wallet-relying parties are not to request users to provide any data other than those indicated for the intended use of wallets in the relying party register. Wallet users should be enabled to verify the registration data of relying parties at any point in time.

(15) As set out in Regulation (EU) 2024/1183, Member States are not, directly or indirectly, to limit access to public or private services to natural or legal persons not opting to use wallets and are to make available appropriate alternative solutions.

(16) 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.

([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).

(17) 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, 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 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;

(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) '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;

(4) '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;

(5) 'wallet user' means a user who is in control of the wallet unit;

(6) '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;

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

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

(9) '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;

(10) '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;

(11) '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;

(12) '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;

(13) ‘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;

(14) ‘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;

(15) ‘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.

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, except wallet user authentication to access the wallet unit, until the wallet unit has successfully authenticated the wallet user.

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) 2024/2980.

Article 4

Wallet instances

1. Wallet instances shall use at least one wallet secure cryptographic device to manage critical assets.

2. Wallet providers shall ensure integrity, authenticity and confidentiality of the communication between wallet instances and wallet secure cryptographic applications.

3. Where critical assets relate to performing electronic identification at assurance level high, the wallet cryptographic operations or other operations processing critical assets 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) 2015/1502 ([11]).

Article 5

Wallet secure cryptographic applications

1. Wallet providers shall ensure that wallet secure cryptographic applications:

(a) perform wallet cryptographic operations involving critical assets other than those needed for the wallet unit to authenticate the wallet user only in cases where those applications have successfully authenticated wallet users;

([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).

(b) where they authenticate wallet users in the context of performing electronic identification at assurance level high; perform authentication of wallet users, 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;

(c) are able to securely generate new cryptographic keys;

(d) are able to perform secure erasure of critical assets;

(e) are able to generate a proof of possession of private keys;

(f) protect the private keys generated by those wallet secure cryptographic applications during the existence of the keys;

(g) comply 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;

(h) are the only components able to execute wallet cryptographic operations and any other operation with critical assets in the context of performing electronic identification at assurance level high.

2. Where wallet providers decide to provide a wallet secure cryptographic application to an embedded secure element these wallet providers shall base their technical solution on the technical specifications listed in Annex I or on other equivalent technical specifications.

Article 6

Wallet unit authenticity and validity

1. Wallet providers shall ensure that each wallet unit contains wallet unit attestations.

2. Wallet providers shall ensure that the wallet unit attestations referred to in paragraph 1 contain public keys and that the corresponding private keys are protected by a wallet secure cryptographic device.

3. Wallet providers shall:

(a) inform wallet users of their rights and obligations in relation to their wallet unit;

(b) provide mechanisms, independent of wallet units, for the secure identification and authentication of wallet users;

(c) ensure wallet users have the right to request revocation of their wallet unit attestations, using the authentication mechanisms referred to in point (b).

Article 7

Revocation of wallet unit attestations

1. Wallet providers shall be the only entities 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 wallet unit attestations.

3. Where wallet providers have revoked wallet unit attestations, they shall inform affected wallet users within 24 hours of the revocation of their wallet units, including the reason for the revocation and the consequences for the wallet user. This information shall be provided in a manner that is concise, easily accessible and using clear and plain language.

4. Where wallet providers have revoked wallet unit attestations, they shall make publicly available the validity status of the wallet unit attestation in a privacy preserving manner 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 II.

Article 9

Transaction logs

1. Irrespective of whether or not a transaction is successfully completed, wallet instances shall log all transactions with wallet-relying parties and other wallet units, including electronic signing and sealing.

2. The logged information shall at least contain:

(a) the time and date of the transaction;

(b) the name, contact details, and the unique identifier of the corresponding wallet-relying party and the Member State in which that wallet-relying party is established, or in case of other wallet units, relevant information from the wallet unit attestation;

(c) the type or types of data requested and presented in the transaction;

(d) in the case of non-completed transactions, the reason for such non-completion.

3. Wallet providers shall ensure integrity, authenticity and confidentiality of the logged information.

4. Wallet instances shall log reports sent by the wallet user to the data protection authorities via their wallet unit.

5. The logs referred to in paragraphs 1 and 2 shall be accessible to the wallet provider, where it is necessary for the provision of wallet services, on the basis of explicit prior consent by the wallet user.

6. The logs referred to in paragraphs 1 and 2 shall remain accessible for as long as they are required by Union law or national law.

7. Wallet providers shall enable wallet users to export the logged information referred to in paragraph 2.

Article 10

Embedded disclosure

1. Wallet providers shall ensure that electronic attestations of attributes with common embedded disclosure policies set out in Annex III can be processed by the wallet units that they provide.

2. Wallet instances shall be able to process and present such embedded disclosure policies referred to in paragraph 1 in conjunction with data received from the requesting wallet-relying party.

3. 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 securely interface with one of the following types of qualified signature or seal creation devices: local, external, or remotely managed 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, at least for non-professional purposes, free-of-charge access to signature creation applications which allow the creation of free-of-charge qualified electronic signatures using the certificates referred to in paragraph 1.

Article 12

Signature creation applications

1. The signature creation applications used by wallet units may be provided either by wallet providers, by providers of 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) creating signatures or seals in accordance with at least the mandatory formats referred to in Annex IV;

(d) informing wallet users about the result of the signature or seal creation process.

3. The signature creation applications may either be integrated into or be external to wallet instances. Where signature creation applications rely on remote qualified signature creation devices and where they are integrated into wallet instances, they shall support the application programming interface referred to in Annex IV.

Article 13

Data export and portability

Wallet units shall, where technically feasible and excepting cases of critical assets, support secure export and portability of personal data of the wallet user, to allow the wallet user to migrate to a wallet unit of a different wallet solution in a way that ensures level of assurance high as set out in Implementing Regulation (EU) 2015/1502.

Article 14

Pseudonyms

1. Wallet units shall support the generation of pseudonyms for wallet users in compliance with the technical specifications set out in Annex V.

2. Wallet units shall support the generation, upon the request of a wallet-relying party, of a pseudonym which is specific and unique to that wallet-relying party and provide this pseudonym to the wallet-relying party, either standalone or in combination with any person identification data or electronic attribute attestation requested by that wallet-relying party.

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, 28 November 2024.

For the Commission
The President
Ursula VON DER LEYEN

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, 3 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:

   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 3191 22-1 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/.