EUROPEAN
COMMISSION

Brussels, XXX
[…](2024) XXX draft

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 registration of wallet-relying parties and the common mechanism for the identification and authentication of wallet-relying parties

ANNEX I

Information regarding wallet-relying parties

1. The name of the wallet-relying party as stated in an official record together with identification data of that official record.

2. Where applicable, one or more identifiers of the wallet-relying party, as stated in an official record together with identification data of that official record, expressed as:

   (a) an Economic Operators Registration and Identification (EORI) number as referred to in Commission Implementing Regulation (EU) No 1352/2013[1];

   (b) the registration number as registered in a national business register;

   (c) a Legal Entity Identifier (LEI) as referred to in Commission Implementing Regulation (EU) No 2022/1860[2];

   (d) a VAT registration number;

   (e) an excise number as specified in Article 2(12) of Council Regulation (EC) No 389/2012[3];

   (f) a tax reference number;

   (g) a European Unique Identifier (EUID) as referred to in Commission Implementing Regulation (EU) 2020/2244[4].

3. The physical address where the wallet-relying party is registered.

4. For the indication of the Member State in which the registering wallet-relying party is established, the ISO 3166-1 Alpha 2 codes shall be used, with the following exception: the Country Code for Greece shall be 'EL'.

5. Detailed contact information of the wallet-relying party, one or more, including:

   (a) a website for providing helpdesk and support;

   (b) a phone number where the wallet-relying party can be contacted for matters pertaining to its registration and intended use of the wallet units;

   (c) a digital address where the wallet-relying party can be contacted for matters pertaining to its registration and intended use of the wallet units;

[1] Commission Implementing Regulation (EU) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights, OJ L 341, 18.12.2013, p. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj.

[2] Commission Implementing Regulation (EU) 2022/1860 of 10 June 2022 laying down implementing technical standards for the application of Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to the standards, formats, frequency and methods and arrangements for reporting, OJ L 262, 7.10.2022, p. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj.

[3] Council Regulation (EU) No 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004, OJ L 121, 8.5.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj.

[4] Commission Implementing Regulation (EU) 2020/2244 of 17 December 2020 laying down rules for the application of Directive (EU) 2017/1132 of the European Parliament and of the Council as regards technical specifications and procedures for the system of interconnection of registers and repealing Commission Implementing Regulation (EU) 2015/884, OJ L 439, 29.12.2020, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2020/2244/oj.

(d) an e-mail address where the wallet-relying party can be contacted for matters pertaining to its registration and intended use of the wallet units;

6. A description of the type of services provided.

7. A list of the attributes that the relying party intends to request, expressed as a friendly name and a technical name including the namespace that the attributes are grouped under in a machine-readable format for automated processing, with an indication if they are mandatory or optional.

8. A description of the intended use of the attributes to be requested by the wallet-relying party from wallet units, including an indication if the intended use of the attribute are for purposes to fulfil specific rules of the Union or National law requiring the relying party to identify users.

9. An indication whether the wallet-relying party is a public sector body.

10. Where applicable, every entitlement of the wallet-relying party, that shall be expressed as follows:

(a) 'Service Provider' to express the entitlement of the wallet-relying party as a provider of services;

(b) 'QEAA_Provider' to express the entitlement of the wallet-relying party as a qualified trust service provider issuing qualified electronic attestations of attributes;

(c) 'Non_Q_EAA_Provider' to express the entitlement of the wallet-relying party as a Trust service provider issuing non-qualified electronic attestations of attributes;

(d) 'PUB_EAA_Provider' to express the entitlement of the wallet-relying party as a provider of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source;

(e) 'PID_Provider' to express the entitlement of the wallet-relying party as a provider of person identification data;

(f) 'QCert_for_ESeal_Provider' to express the entitlement of the wallet-relying party as a qualified trust service provider issuing qualified certificates for electronic seals;

(g) 'QCert_for_ESig_Provider' to express the entitlement of the wallet-relying party as a qualified trust service provider issuing qualified certificates for electronic signatures;

(h) 'rQSealCDs_Provider' to express the entitlement of the wallet-relying party as a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device;

(i) 'rQSigCDs_Provider' to express the entitlement of the wallet-relying party as a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic seal creation device;

(j) 'ESig_ESeal_Creation_Provider' to express the entitlement of the wallet-relying party as a (non-qualified) trust service provider of remote creation of electronic signatures or electronic seals as a non-qualified trust service;

(k) ‘WAC_Provider’ to express the entitlement of the wallet-relying party as a qualified trust service provider issuing qualified certificate for web authentication.

ANNEX II

1. REQUIREMENTS ON ELECTRONIC SIGNATURES OR SEALS APPLIED TO THE INFORMATION MADE AVAILABLE ON REGISTERED WALLET-RELYING PARTIES

Electronic signatures and electronic seals referred to in Article 3(2) shall be JSON advanced electronic signatures at conformance level B-B, B-T or B-LT, and comply with the following ETSI technical specifications:

– ETSI TS 119 182-1 V1.2.1 (JAdES baseline signatures).

2. REQUIREMENTS ON THE SINGLE API

1. The API shall:

(1) be a REST API, supporting JSON as format with JAdES or ASIC signature format in accordance with the relevant requirements specified in Section 1 of this Annex;

(2) allow any requestor, without prior authentication, to make (search/read) requests to the register, for information about a wallet-relying party, based on defined parameters including the wallet-relying party official or business registration number, or the name of the wallet-relying party or any information referred to in Annex II Paragraph 1, 2 and 8;

(3) ensure that replies to requests referred to in paragraph 2 include one or more statements on information about registered wallet-relying parties;

(4) be published as an OpenAPI version 3, together with the appropriate documentation.

2. The statements referred to in point (3) shall be expressed under the form of electronically signed or sealed JSON files, with format and structure in accordance with the requirements on electronic signatures or seals set out Section 1.

ANNEX III

Source of evidentiary documentation for the verification of entitlements of wallet-relying parties

1. The verification that a wallet-relying party is a provider of qualified electronic attestations of attributes, a provider of qualified certificate for electronic signatures or seals, or a provider of a qualified trust service for the management of a remote qualified electronic signature or seal creation device, shall be based on the national trusted lists issued in accordance with Article 22 of Regulation (EU) No 910/2014.

2. The verification that a wallet-relying party is a provider of non-qualified electronic attestations of attributes or a provider of remote creation of electronic signatures or seals as a non-qualified trust service shall be based on the national trusted lists issued in accordance with Article 22 of Regulation (EU) No 910/2014 of the European Parliament and of the Council[5].

3. The verification that a wallet-relying party is a provider of person identification data shall be based on the list of providers of person identification data published by the Commission in accordance with Article 5a(18) of Regulation (EU) No 910/2014.

4. The verification that a wallet-relying party is a provider of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be based on the list published by the Commission in accordance with Article 45f(3) of Regulation (EU) No 910/2014.

ANNEX IV

Requirements for wallet-relying party access certificates

1. The certificate policy applicable to the provision of wallet-relying party access certificates shall describe the security requirements that apply to, and the rules that indicate the applicability of, a wallet-relying party access certificate for their issuance to and use by wallet-relying parties in their interactions with wallet solutions.

2. The certificate practice statement applicable to the provision of wallet-relying party access certificates shall describe the practices that a provider of wallet-relying party access certificates employs in issuing, managing, revoking, and re-keying wallet-relying party access certificates. The re-issuance of wallet-relying party access certificates for the same signature or seal activation data shall not be permitted.

3. The certificate policy and certificate practice statement applicable to the provision of wallet-relying party access certificates shall comply with IETF RFC 3647, and shall in particular include:

   (a) a clear description of the public key infrastructure hierarchy and certification paths from the end-entity wallet-relying party access certificates up to the top

[5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

of the hierarchy used for issuing them, while indicating the expected trust anchor(s) in such hierarchy and paths;

(b) a comprehensive description of the procedures for the issuance of wallet-relying party access certificates, including for the verification of the identity and of any certified attribute of the wallet-relying party to which a wallet-relying party certificate is to be issued;

(c) the obligation for the provider of wallet-relying party access certificates, when issuing a wallet-relying party certificate, to verify that:

- the wallet-relying party is included, with a valid registration status, in a register of the Member State in which that wallet-relying party is established;
- any information in the wallet-relying party access certificate is accurate and consistent with the registration information available from that register.

(d) a comprehensive description of the procedures for revocation of wallet-relying party access certificates;

(e) the obligation for the provider of wallet-relying party access certificates to implement measures and processes to:

- continuously monitor any changes in the relying party registers in which wallet-relying parties to whom they have issued wallet-relying party access certificates are registered;
- when such changes so require, revoke any wallet-relying party certificate that they issued to the corresponding wallet-relying party, in particular when the content of the certificate is no longer accurate and consistent with the information registered, or when the registration of the relying party is suspended or cancelled.

(f) a comprehensive description of the procedures and mechanisms for the validation of wallet-relying party access certificates;

(g) the obligation for the provider of wallet-relying party access certificates to allow relevant stakeholders, including wallet-relying parties and competent supervisory bodies, to request the revocation of wallet-relying party access certificates;

(h) the obligation for the provider of wallet-relying party access certificates to register all such revocations in its certificate database and to publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request for revocation. The revocation shall become effective immediately upon its publication;

(i) the obligation for the providers of wallet-relying party access certificates to provide information on the validity or revocation status of wallet-relying party certificates issued by that provider. This information shall be made available at least on a per certificate basis at any time and at least beyond the validity period of the certificate in an automated manner that is reliable, free of charge and effectively in accordance with the certificate policy;

(j) the obligation for the providers of wallet-relying party access certificates to log all wallet-relying party access certificates they have issued to ensure certificate transparency, in compliance mutatis mutandis with IETF RFC 9162;

(k) the obligation for the wallet-relying party access certificates to include:

– the location where the certificate supporting the advanced electronic signature or advanced electronic seal on that certificate is available, for the entire certification path to be built up to the expected trust anchor in the public key infrastructure hierarchy used by the provider;

– a machine processable reference to the applicable certificate policy and certificate practice statement;

– the information referred to in Annex I, points (1) to (3), 5(b) and 5(d).

ANNEX V

Requirements for wallet-relying party registration certificates

1. The certificate policy applicable to the provision of wallet-relying party registration certificates shall describe the security requirements that apply to, and the rules that indicate the applicability of, a wallet-relying party registration certificate for their issuance to and use by wallet-relying parties in their interactions with wallet solutions.

2. The certificate practice statement applicable to the provision of wallet-relying party registration certificates shall describe the practices that a provider of wallet-relying party registration certificates employs in issuing, managing, revoking, and re-keying wallet-relying party registration certificates, and where applicable how they relate to wallet-relying party access certificates issued to wallet-relying parties.

3. The certificate policy and certificate practice statement applicable to the provision of wallet-relying party registration certificates shall comply with IETF RFC 3647 and IETF RFC 5755, and shall in particular include:

(a) a clear description of the public key infrastructure hierarchy and certification paths from the end-entity wallet-relying party registration certificates up to the top of the hierarchy used for issuing them, while indicating the expected trust anchor(s) in such hierarchy and paths;

(b) a comprehensive description of the procedures for the issuance of wallet-relying party registration certificates, including for the verification of the identity and of any certified attribute of the wallet-relying party to which a wallet-relying party certificate is to be issued;

(c) the obligation for the provider of wallet-relying party registration certificates, when issuing a wallet-relying party registration certificate, to verify that:

– the wallet-relying party is included, with a valid registration status, in a register of the Member State in which that wallet-relying party is established;

– any information in the wallet-relying party registration certificate is accurate and consistent with the registration information available from that register.

(d) a comprehensive description of the procedures for revocation of wallet-relying party registration certificates;

(e) the obligation for the provider of wallet-relying party registration certificates to implement measures and processes to:

- continuously monitor any changes in the relying party registers in which wallet-relying parties to whom they have issued wallet-relying party registration certificates are registered;

- when such changes so require, revoke any wallet-relying party registration certificate that they issued to the corresponding wallet-relying party, in particular when the content of the certificate is no longer accurate and consistent with the information registered, or when the registration of the relying party is suspended or cancelled.

(f) a comprehensive description of the procedures and mechanisms for the validation of wallet-relying party registration certificates;

(g) the obligation for the provider of wallet-relying party registration certificates to allow relevant stakeholders, including wallet-relying parties and competent supervisory bodies, to request the revocation of wallet-relying party registration certificates;

(h) the obligation for the provider of wallet-relying party registration certificates to register all such revocations in its certificate database and to publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request for revocation. The revocation shall become effective immediately upon its publication;

(i) the obligation for the providers of wallet-relying party registration certificates to provide information on the validity or revocation status of wallet-relying party registration certificates issued by that provider. This information shall be made available at least on a per certificate basis at any time and at least beyond the validity period of the certificate in an automated manner that is reliable, free of charge and effectively in accordance with the certificate policy;

(j) the obligation for the providers of wallet-relying party registration certificates to log all wallet-relying party registration certificates they have issued to ensure certificate transparency, in compliance mutatis mutandis with IETF RFC 9162;

(k) the obligation for the wallet-relying party registration certificates:

- to include the location where the certificate supporting the advanced electronic signature or advanced electronic seal on that certificate is available, for the entire certification path to be built up to the expected trust anchor in the public key infrastructure hierarchy used by the provider;

- to include a machine processable reference to the applicable certificate policy and certificate practice statement;

- to include the information referred to in Annex I, points 1, 2 and 8;

- to comply with IETF RFC 5755 to express attributes in relation to wallet-relying party registration certificates.