



Brussels, XXX
[...] (2024) XXX draft

ANNEXES 1 to 4

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 qualified electronic attestations of attributes and electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source

ANNEX I

Technical specifications for the issuance of qualified electronic attestations of attributes and electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source referred to in Article 3

- (1) Providers of qualified electronic attestation 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 to natural or legal persons according to the specifications established in the standard listed below:
 - (a) ETSI TS 119 471 V0.0.10. (2024-11) Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services
- (2) Providers of qualified electronic attestation 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 one of the following common formats:
 - (a) One of the standards in the list set out in Annex I of Commission Implementing Regulation (EU) 2024/XXX¹ 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.

¹ Commission Implementing Regulation (EU) 2024/XXX 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 II

Requirements for the secure electronic notification system referred to in Article 5(1)

- (1) The interface of the secure electronic notifications system shall be at least in English.
- (2) The secure electronic notifications system provided by the Commission shall be designed to:
 - (a) allow the Member States to submit the same information only once, by re-using prior submitted information where appropriate;
 - (b) enable the submission of information via both machine processable interfaces and human usable interfaces;
 - (c) support appropriate access controls and access control management, delegating to the Member States the power to grant access to competent representatives as regards the notifications;
 - (d) support notifications of the information specified in Annex III;
 - (e) allow Member States to view notified information;
 - (f) acknowledge receipt of notifications of information by electronic means;
 - (g) retain, and allow Member States to view, a historical record of any changes in any notified information.

ANNEX III

Information to be submitted, through the secure electronic notification system, by the Member States, as referred to in Article 5(2)

The information to be notified about public sector bodies responsible for an authentic source that act as providers of electronic attestation of attributes, or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources, shall include at least:

- (1) the name of the issuer and the public sector body responsible for the authentic source, as used in official records;
- (2) the registration number of the issuer and the public sector body responsible for the authentic source, where applicable, as used in official records;
- (3) the Member State in which the issuer and the public sector body responsible for the authentic source are established;
- (4) an identification of the Union or national law under which the issuing body is established as the responsible for the authentic source on the basis of which the electronic attestation of attributes is issued or as the body designated to act on its behalf;
- (5) the contact email and contact phone number of the issuer, for matters related to the electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source of attributes;
- (6) the URL of the webpage for additional information about the issuer and the public sector body responsible for the authentic source, where applicable;
- (7) one or more certificates which can be used to verify the signature or seal created by issuers of electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source on the electronic attestation of attributes that they provide;
- (8) a conformity assessment report as specified in paragraph 3 of Article 45f of Regulation (EU) 910/2014.

ANNEX IV

Requirements for the verification of attributes as referred to in Article 9

- (1) Member States shall ensure that their public sector bodies responsible for an authentic source, or their designated intermediaries, shall make available interfaces that enable qualified trust service providers of electronic attestations of attributes to confirm the accuracy of an attribute value, from the applicable an authentic source, about a specific natural or legal person.
- (2) Member States may impose access controls or other verification mechanisms that provide integrity, authenticity and confidentiality on the interfaces referenced in paragraph 1, to:
 - (a) determine whether a verification request for attributes against an authentic source was made by a qualified trust service provider of electronic attestations of attributes;
 - (b) determine whether a provider of electronic attestations of attributes or a provider of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source is in the process of issuing an electronic attestation of attributes containing the requested attributes, and whether those attributes rely on an authentic source;
 - (c) identify the user of the interface through which the verification request is submitted;
 - (d) determine whether the verification request for attributes was made by the user of the interface through which the verification request is submitted.
- (3) In all other respects, the verification of attributes shall comply with the specifications established in the standard listed below:
 - (a) ETSI TS 119 471 V0.0.10. (2024-11) Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services.