Official Journal
of the European Union

EN
L series

2025/1943

30.9.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/1943

of 29 September 2025

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for qualified certificates for electronic signatures and qualified certificates for electronic seals

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 28(6) and Article 38(6) thereof,

Whereas:

(1) Qualified certificates for electronic signatures and qualified certificates for electronic seals play a crucial role in the digital business environment by promoting the transition from traditional paper-based processes to electronic equivalent ones. By linking electronic signature validation data or electronic seal validation data to a natural or legal person respectively and by confirming the name of that person, qualified certificates enhance the certainty regarding the identity of the signatory and of the seal creator.

(2) The presumption of compliance laid down in Article 28(6) and Article 38(6) of Regulation (EU) No 910/2014 should only apply where qualified trust services for the issuance of qualified certificates for electronic signatures and qualified trust services for the issuance of qualified certificates for electronic seals comply with the standards set out in this Regulation. These standards should reflect established practices and be widely recognised within the relevant sectors. They should be adapted to include additional controls ensuring the security and trustworthiness of the qualified trust services and of the content of the qualified certificates.

(3) If a trust service provider adheres to the requirements set out in the Annex to this Regulation, supervisory bodies should presume compliance with the relevant requirements of Regulation (EU) No 910/2014 and duly consider such presumption for granting or confirming the qualified status of the trust service. However, a qualified trust services provider may still rely on other practices to demonstrate compliance with the requirements of the Regulation (EU) No 910/2014.

(4) The Commission regularly assesses new technologies, practices, standards or technical specifications. In accordance with recital 75 of Regulation (EU) 2024/1183 of the European Parliament and of the Council ([2]), the Commission should review and update this Regulation, if necessary, to keep it in line with global developments, new technologies, standards or technical specifications and to follow the best practices on the internal market.

(5) Regulation (EU) 2016/679 of the European Parliament and of the Council ([3]) and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ([4]) apply to the personal data processing activities under this Regulation.

([1]) OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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).

([3]) 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).

([4]) 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).

(6) 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 ([5]) and delivered its opinion on 6 June 2025.

(7) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS REGULATION:

Article 1

Reference standards and specifications for qualified certificates for electronic signatures and electronic seals

1. The reference standards and specifications referred to in Article 28(6) of Regulation (EU) No 910/2014 are set out in Annex I to this Regulation.

2. The reference standards and specifications referred to in Article 38(6) of Regulation (EU) No 910/2014 are set out in Annex II to this Regulation.

Article 2

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, 29 September 2025.

For the Commission
The President
Ursula VON DER LEYEN

([5]) 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).

ANNEX I

List of reference standards and specifications for qualified certificates for electronic signatures

The standards ETSI EN 319 411-2 V2.6.1 ('ETSI EN 319 411-2'), ETSI EN 319 412-1 V1.6.1 ('ETSI EN 319 412-1'), ETSI EN 319 412-2 V2.4.1 ('ETSI EN 319 412-2'), and ETSI EN 319 412-5 V2.5.1 ('ETSI EN 319 412-5') apply with the following adaptations:

1. For ETSI EN 319 411-2

(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] ETSI EN 319 411-1 V1.5.1 (2025-04) 'Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements', with the following adaptations:

Clause 2.1 Normative references of ETSI EN 319 411-1 V1.5.1 shall be amended as follows:

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

— [10] ETSI EN 319 412-2 V2.4.1 'Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons'.

— [14] ETSI EN 319 412-1 V1.6.1 'Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures'.

— [3] ETSI EN 319 412-5 V2.5.1 'Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements'.

— [5] ETSI EN 319 412-1 V1.6.1 'Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures'.

— [6] CEN/TS 419261:2015 'Security requirements for trustworthy systems managing certificates and time-stamps'.

— [7] European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms' published by the European Union Agency for Cybersecurity ('ENISA') ([1]).

— [8] Commission Implementing Regulation (EU) 2024/482 ([2]) 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).

— [9] Commission Implementing Regulation (EU) 2024/3144 ([3]) amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation.

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

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

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) OJ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

(2) 5.2 Certification Practice Statement Requirements

— OVR-5.2-02 The CP(s) identified by the TSP's documentation shall specify the requirements on certificate profiles to be used.

(3) 5.3 Certificate Policy name and identification

— OVR-5.3-01 If any changes are made to a CP as described in clause 4.2.2 which affects the applicability, then the policy identifier shall be changed.

(4) 6.1 Publication and repository responsibilities

— OVR-6.1-02 The information identified in DIS-6.1-04 of ETSI EN 319 411-1 [2] shall be publicly and internationally available.

(5) 6.2.2 Initial identity validation

— REG-6.2.2-01A The collection of attributes and evidence on the subject's identity as well as their validation shall be as specified in accordance with the implementing acts adopted pursuant to Article 24(1c) of Regulation (EU) No 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] and [QCP-n-qscd] The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified in accordance with the implementing acts adopted pursuant to Article 24(1c) of Regulation (EU) No 910/2014 [i.1].

— NOTE 1 void.

(6) 6.3.3 Certificate issuance

— GEN-6.3.3-01 The requirements GEN-6.3.3-01 to GEN-6.3.3-10 identified in ETSI EN 319 411-1 [2], clause 6.3.3 shall apply.

— GEN-6.3.3-02 [CONDITIONAL] If a certificate is issued to a natural person identified in association with the legal person, then the subject attributes identifying the organisation in the certificate shall represent the legal person or sub-entity of that legal person and the subject identifier in the certificate shall be the natural person.

— GEN-6.3.3-03 The CP identifier shall be [CHOICE]:

(a) [QCP-n]

— as specified in clause 5.3, item (a), and/or

— an OID, allocated by the TSP, other relevant stakeholder or further standardisation for a certificate policy enhancing the corresponding applicable policy requirements defined in the present document.

(b) [QCP-n-qscd]

— as specified in clause 5.3, item (c), and/or

— an OID, allocated by the TSP, other relevant stakeholder or further standardisation for a certificate policy enhancing the corresponding applicable policy requirements defined in the present document.

(7) 6.3.5 Key Pair and Certificate Usage

— SDP-6.3.5-02A [CONDITIONAL] If the TSP manages the QSCD for the subject, the TSP shall be a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device, in accordance with Regulation (EU) No 910/2014 [i.1].

— SDP-6.3.5-11A The subscriber's obligations (see clause 6.3.4) shall include, if the subscriber or subject generates the subject's keys:

(a) an obligation to generate the subject keys using an algorithm compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group [7] and published by ENISA for the uses of the certified key as identified in the CP;

(b) an obligation to use key length and algorithm compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group [7] and published by ENISA for the uses of the certified key as identified in the CP during the validity time of the certificate.

(8) 6.3.10 Certificate Status Services

— CSS-6.3.10-08 [CONDITIONAL] If CRLs are provided, the TSP shall preserve the integrity and the availability of the last CRL at least for the period specified in the CPS as requested in CSS-6.3.10-12.

(9) 6.4.4 Personnel Controls

— OVR-6.4.4-02 TSP's personnel in trusted roles, and if applicable its subcontractors in trusted roles, 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.

— OVR-6.4.4-03 Compliance with OVR-6.4.4-02 shall include regular (at least every 12 months) updates on new threats and current security practices.

— OVR-6.4.4-04 In addition to the trusted roles identified in ETSI EN 319 401 [1], (clause 7.2-15), the trusted roles of the registration and revocation officers with responsibilities as defined in TS 419261 [6] shall be supported. In cases where the QTSP is directly managed by or operated on behalf of a Member State or public sector body, those additional trusted roles may be fulfilled by one or more formal representatives acting for and on behalf of the registration and revocation officers officiating in local or regional administrations.

(10) 6.4.9 CA or RA Termination

— OVR-6.4.9-02 The TSP's termination plan shall comply with the requirements set out in the implementing acts adopted pursuant to Article 24(5) of Regulation (EU) No 910/2014 [i.1].

(11) 6.5.1 Key Pair Generation and Installation

— OVR-6.5.1-01A CA key pair generation shall be performed using an algorithm compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [7] for the CA's signing purposes.

— OVR-6.5.1-01B The selected key length and algorithm for CA signing key shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [7] for the CA's signing purposes.

— OVR-6.5.1-01C [CONDITIONAL] If the CA generates the subject's keys, CA-generated subject keys shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [7] for the purposes stated in the CP during the validity time of the certificate.

(12) 6.5.2 Private key protection and cryptographic module engineering controls

— GEN-6.5.2-01 All requirements identified in ETSI EN 319 411-1 [2], clause 6.5.2 shall apply, except requirements OVR-6.5.2-01, OVR-6.5.2-03 and OVR-6.5.2-04.

— GEN-6.5.2-02 TSP's key pair generation, including keys used by revocation and registration services, shall be carried out within a secure cryptographic device which is a trustworthy system certified in accordance with:

— Common Criteria for Information Technology Security Evaluation, as set out in ISO/IEC 15408 [10] 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

— the European Common Criteria-based cybersecurity certification scheme (EUCC) [8][9] and certified to EAL 4 or higher; or

— until 31.12.2030, FIPS PUB 140-3 [11] 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 [8][9] certification, then this device shall be configured and used in accordance with that certification.

— GEN-6.5.2-03 The CA private signing key shall be held and used within a secure cryptographic device meeting the requirements of GEN-6.5.2-01 and GEN-6.5.2-02.

(13) 6.5.7 Network Security Controls

— OVR-6.5.7-02 The vulnerability scan requested by REQ-7.8-13 of ETSI EN 319 401 [1] shall be performed at least once per quarter.

— OVR-6.5.7-03 The penetration test requested by REQ-7.8-17X of ETSI EN 319 401 [1] shall be performed at least once per year.

— OVR-6.5.7-04 Firewalls shall be configured to prevent all protocols and accesses not required for the operation of the TSP.

(14) 6.6.1 Certificate Profile

— GEN-6.6.1-05 The certificate shall include one of the policy identifiers identified in GEN-6.3.3-03 [CHOICE]. The certificate may include other OIDs allocated by the TSP.

2. For ETSI EN 319 412-2

(1) 2.1 Normative references

— [2] ETSI EN 319 412-5 V2.5.1 'Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements'.

— [9] European Cybersecurity Certification Group, Sub-group on Cryptography 'Agreed Cryptographic Mechanisms' published by ENISA.

(2) 4.2.2 Signature

— GEN-4.2.2-2 Signature algorithm shall be selected in accordance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [9].

— NOTE void.

(3) 4.2.3.1 Legal person issuers

— GEN-4.2.3.1-3 If an appropriate registration number is known to exist, then the identity of the issuer shall contain organizationIdentifier with a value of that registration number as stated in the corresponding official record establishing that registration number.

(4) 4.2.5 Subject public key info

— GEN-4.2.5-2 The subject public key shall be selected in accordance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [9].

— NOTE void.

(5) 4.2.6 Serial number

— GEN-4.2.6-01 The certificate serialNumber (as specified in IETF RFC 5280 [1] clause 4.1.2.2) shall be unique for each certificate issued by the TSP.

ANNEX II

List of reference standards and specifications for qualified certificates for electronic seals

The standards ETSI EN 319 411-2 V2.6.1 ('ETSI EN 319 411-2'), ETSI EN 319 412-1 V1.6.1 ('ETSI EN 319 412-1'), ETSI EN 319 412-3 V1.3.1 ('ETSI EN 319 412-3'), ETSI EN 319 412-2 V2.4.1 ('ETSI EN 319 412-2'), and ETSI EN 319 412-5 V2.5.1 ('ETSI EN 319 412-5') apply with the following adaptations:

1. For ETSI EN 319 411-2

(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] ETSI EN 319 411-1 V1.5.1 (2025-04) 'Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements', with the following adaptations:

Clause 2.1 Normative references of ETSI EN 319 411-1 V1.5.1 shall be amended as follows:

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

— [10] ETSI EN 319 412-2 V2.4.1 'Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons'.

— [14] ETSI EN 319 412-1 V1.6.1 'Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures'.

— [3] ETSI EN 319 412-5 V2.5.1 'Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements'.

— [5] ETSI EN 319 412-1 V1.6.1 'Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures'.

— [6] CEN/TS 419261:2015 'Security requirements for trustworthy systems managing certificates and time-stamps', (produced by CEN).

— [7] European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms' published by ENISA.

— [8] Implementing Regulation (EU) 2024/482 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).

— [9] Implementing Regulation (EU) 2024/3144 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation.

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

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

(2) 5.2 Certification Practice Statement Requirements

— OVR-5.2-02 The CP(s) identified by the TSP's documentation shall specify the requirements on certificate profiles to be used.

(3) 5.3 Certificate Policy name and identification

— OVR-5.3-01 If any changes are made to a CP as described in clause 4.2.2 which affects the applicability, then the policy identifier shall be changed.

(4) 6.1 Publication and repository responsibilities

— OVR-6.1-02 The information identified in DIS-6.1-04 of ETSI EN 319 411-1 [2] shall be publicly and internationally available.

(5) 6.2.2 Initial identity validation

— REG-6.2.2-01A The collection of attributes and evidence on the subject's identity as well as their validation shall be as specified in accordance with the implementing acts adopted pursuant to Article 24(1c) of Regulation (EU) No 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] and [QCP-l-qscd] The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified in accordance with the implementing acts adopted pursuant to Article 24(1c) of Regulation (EU) No 910/2014 [i.1].

— NOTE 3 See note 2.

(6) 6.3.3 Certificate issuance

— GEN-6.3.3-01 The requirements GEN-6.3.3-01 to GEN-6.3.3-10 identified in ETSI EN 319 411-1 [2], clause 6.3.3 shall apply.

— GEN-6.3.3-02 The CP identifier shall be [CHOICE]:

(a) [QCP-l]

— as specified in clause 5.3, item (b), and/or

— an OID, allocated by the TSP, other relevant stakeholder or further standardisation for a certificate policy enhancing the corresponding applicable policy requirements defined in the present document.

(b) [QCP-l-qscd]

— as specified in clause 5.3, item (d), and/or

— an OID, allocated by the TSP, other relevant stakeholder or further standardisation for a certificate policy enhancing the applicable policy requirements defined in the present document.

(7) 6.3.5 Key Pair and Certificate Usage

— SDP-6.3.5-02A [CONDITIONAL] If the TSP manages the QSCD for the subject, the TSP shall be a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic seal creation device, in accordance with Regulation (EU) No 910/2014 [i.1]

— SDP-6.3.5-11A The subscriber's obligations (see clause 6.3.4) shall include, if the subscriber or subject generates the subject's keys:

(a) an obligation to generate the subject keys using an algorithm compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [7] for the uses of the certified key as identified in the CP; and

(b) an obligation to use key length and algorithm compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA[7] for the uses of the certified key as identified in the CP during the validity time of the certificate.

(8) 6.3.10 Certificate Status Services

— CSS-6.3.10-08 [CONDITIONAL] If CRLs are provided, the TSP shall preserve the integrity and the availability of the last CRL at least for the period specified in the CPS as requested in CSS-6.3.10-12.

(9) 6.4.4 Personnel Controls

— OVR-6.4.4-02 TSP's personnel in trusted roles, and if applicable its subcontractors in trusted roles, 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.

— OVR-6.4.4-03 Compliance with OVR-6.4.4-02 shall include regular (at least every 12 months) updates on new threats and current security practices.

— OVR-6.4.4-04 In addition to the trusted roles identified in ETSI EN 319 401 [1], (clause 7.2-15), the trusted roles of the registration and revocation officers with responsibilities as defined in TS 419261 [6] shall be supported. In cases where the QTSP is directly managed by or operated on behalf of a Member State or public sector body, those additional trusted roles may be fulfilled by one or more formal representatives acting for and on behalf of the registration and revocation officers officiating in local or regional administrations.

(10) 6.4.9 CA or RA Termination

— OVR-6.4.9-02 The TSP's termination plan shall comply with the requirements set out in the implementing acts adopted pursuant to Article 24(5) of Regulation (EU) No 910/2014 [i.1]].

(11) 6.5.1 Key Pair Generation and Installation

— OVR-6.5.1-01A CA key pair generation shall be performed using an algorithm compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group published by ENISA [7] for the CA's signing purposes.

— OVR-6.5.1-01B The selected key length and algorithm for CA signing key shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group published by ENISA [7] for the CA's signing purposes.

— OVR-6.5.1-01C [CONDITIONAL] If the CA generates the subject's keys, CA-generated subject keys shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group published by ENISA [7] for the purposes stated in the CP during the validity time of the certificate.

(12) 6.5.2 Private key protection and cryptographic module engineering controls

— GEN-6.5.2-01 All requirements identified in ETSI EN 319 411-1 [2], clause 6.5.2 shall apply, except requirements OVR-6.5.2-01, OVR-6.5.2-03 and OVR-6.5.2-04.

— GEN-6.5.2-02 TSP's key pair generation, including keys used by revocation and registration services, shall be carried out within a secure cryptographic device which is a trustworthy system certified in accordance with:

  — Common Criteria for Information Technology Security Evaluation, as set out in ISO/IEC 15408 [10] 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

  — the European Common Criteria-based cybersecurity certification scheme (EUCC) [8][9] and certified to EAL 4 or higher; or

  — until 31.12.2030, FIPS PUB 140-3 [11] 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 [8][9] certification, then this device shall be configured and used in accordance with that certification.

— GEN-6.5.2-03 The CA private signing key shall be held and used within a secure cryptographic device meeting the requirements of GEN-6.5.2-01 and GEN-6.5.2-02.

(13) 6.5.7 Network Security Controls

— OVR-6.5.7-02 The vulnerability scan requested by REQ-7.8-13 of ETSI EN 319 401 [1] shall be performed at least once per quarter.

— OVR-6.5.7-03 The penetration test requested by REQ-7.8-17X of ETSI EN 319 401 [1] shall be performed at least once per year.

— OVR-6.5.7-04 Firewalls shall be configured to prevent all protocols and accesses not required for the operation of the TSP.

(14) 6.6.1 Certificate Profile

— GEN-6.6.1-05 The certificate shall include one of the policy identifiers identified in GEN-6.3.3-02 [CHOICE].

2. For ETSI EN 319 412-3

(1) 2.1 Normative references

— [2] ETSI EN 319 412-2 V2.4.1 ‘Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons’.

(2) 4.2.1 Subject

— LEG-4.2.1-6 The organizationIdentifier attribute shall contain an identification of the subject organization different from the organization name. If an appropriate registration number is known to exist, then the organizationIdentifier attribute shall contain a value of that registration number as stated in the corresponding official record establishing that registration number.

3. For ETSI EN 319 412-2:

(1) 2.1 Normative references

— [2] ETSI EN 319 412-5 V2.5.1 ‘Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements’.

— [9] European Cybersecurity Certification Group, Sub-group on Cryptography: ‘Agreed Cryptographic Mechanisms’ published by ENISA.

(2) 2.2 Informative references

— [i.7] void.

(3) 4.2.2 Signature

— GEN-4.2.2-2 Signature algorithm shall be selected in accordance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [9].

— NOTE void.

(4) 4.2.3.1 Legal person issuers

— GEN-4.2.3.1-3 If an appropriate registration number is known to exist, then the identity of the issuer shall contain organizationIdentifier with a value of that registration number as stated in the corresponding official record establishing that registration number.

(5) 4.2.5 Subject public key info

— GEN-4.2.5-2 The subject public key shall be selected in accordance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [9].

— NOTE void.

(6) 4.2.6 Serial number

— GEN-4.2.6-01 The certificate serialNumber (as specified in IETF RFC 5280 [1] clause 4.1.2.2) shall be unique for each certificate issued by the TSP.