



2025/1943

30.9.2025

**DURCHFÜHRUNGSVERORDNUNG (EU) 2025/1943 DER KOMMISSION**

**vom 29. September 2025**

**zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards für qualifizierte Zertifikate für elektronische Signaturen und qualifizierte Zertifikate für elektronische Siegel**

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG<sup>(1)</sup>, insbesondere auf Artikel 28 Absatz 6 und Artikel 38 Absatz 6,

in Erwägung nachstehender Gründe:

- (1) Qualifizierte Zertifikate für elektronische Signaturen und qualifizierte Zertifikate für elektronische Siegel haben im digitalen Geschäftsumfeld eine große Bedeutung, weil sie den Übergang von herkömmlichen papiergestützten Verfahren zu entsprechenden elektronischen Verfahren fördern. Durch die Verknüpfung elektronischer Signaturvalidierungsdaten oder elektronischer Siegelvalidierungsdaten mit einer natürlichen bzw. juristischen Person und durch die Bestätigung des Namens dieser Person verbessern qualifizierte Zertifikate die Gewissheit in Bezug auf die Identität des Unterzeichners und des Siegelerstellers.
- (2) Die Konformitätsvermutung gemäß Artikel 28 Absatz 6 und Artikel 38 Absatz 6 der Verordnung (EU) Nr. 910/2014 sollte nur gelten, wenn qualifizierte Vertrauensdienste für die Ausstellung qualifizierter elektronischer Signaturen und qualifizierte Vertrauensdienste für die Ausstellung qualifizierter elektronischer Siegel den in der vorliegenden Verordnung festgelegten Standards bzw. Normen entsprechen. Diese Standards bzw. Normen sollten bewährte Verfahren widerspiegeln und in den betreffenden Sektoren weithin anerkannt sein. Sie sollten so angepasst werden, dass sie zusätzliche Kontrollen umfassen, um die Sicherheit und Vertrauenswürdigkeit der qualifizierten Vertrauensdienste sowie den Inhalt der qualifizierten Zertifikate zu gewährleisten.
- (3) Erfüllt ein Vertrauensdiensteanbieter die im Anhang der vorliegenden Verordnung festgelegten Anforderungen, so sollten die Aufsichtsstellen davon ausgehen, dass die einschlägigen Anforderungen der Verordnung (EU) Nr. 910/2014 erfüllt sind, und diese Vermutung bei der Gewährung oder Bestätigung des Status des qualifizierten Vertrauensdienstes gebührend berücksichtigen. Ein qualifizierter Vertrauensdiensteanbieter kann sich jedoch weiterhin auf andere Verfahren stützen, um die Erfüllung der Anforderungen der Verordnung (EU) Nr. 910/2014 nachzuweisen.
- (4) Die Kommission bewertet regelmäßig neue Technologien, Praktiken, Standards bzw. Normen oder technische Spezifikationen. Nach Erwägungsgrund 75 der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates<sup>(2)</sup> sollte die Kommission die vorliegende Verordnung überprüfen und erforderlichenfalls aktualisieren, um sie mit globalen Entwicklungen, neuen Technologien, Standards oder technischen Spezifikationen in Einklang zu halten und den bewährten Verfahren im Binnenmarkt zu folgen.
- (5) Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates<sup>(3)</sup> und, sofern anwendbar, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates<sup>(4)</sup> gelten für die Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung.

<sup>(1)</sup> ABl. L 257 vom 28.8.2014, S. 73, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>.

<sup>(2)</sup> Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität (ABl. L, 2024/1183, 30.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/1183/oj>).

<sup>(3)</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

<sup>(4)</sup> Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37, ELI: <http://data.europa.eu/eli/dir/2002/58/oj>).

- (6) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates <sup>(7)</sup> angehört und gab am 6. Juni 2025 seine Stellungnahme ab.
- (7) Die in der vorliegenden Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 48 der Verordnung (EU) Nr. 910/2014 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

*Artikel 1*

**Referenzstandards und Spezifikationen für qualifizierte Zertifikate für elektronische Signaturen und qualifizierte Zertifikate für elektronische Siegel**

- (1) Die in Artikel 28 Absatz 6 der Verordnung (EU) Nr. 910/2014 genannten Referenzstandards und Spezifikationen sind in Anhang I der vorliegenden Verordnung festgelegt.
- (2) Die in Artikel 38 Absatz 6 der Verordnung (EU) Nr. 910/2014 genannten Referenzstandards und Spezifikationen sind in Anhang II der vorliegenden Verordnung festgelegt.

*Artikel 2*

**Inkrafttreten**

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 29. September 2025

*Für die Kommission*  
*Die Präsidentin*  
Ursula VON DER LEYEN

---

<sup>(7)</sup> Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

## ANHANG I

**Liste der Referenzstandards und Spezifikationen für qualifizierte Zertifikate für elektronische Signaturen**

Die Normen 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“) und ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5“) gelten mit den folgenden Anpassungen:

## 1. Für ETSI EN 319 411-2:

## 1) 2.1 Normative Verweise

- [1] ETSI EN 319 401 V3.1.1 (2024-06) – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter.
- [2] ETSI EN 319 411-1 V1.5.1 (2025-04) – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Regelungs- und Sicherheitsanforderungen an Vertrauensdiensteanbieter, die Zertifikate ausgeben – Teil 1: Allgemeine Anforderungen – mit den folgenden Anpassungen:

Abschnitt „2.1 Normative Verweise“ der Norm ETSI EN 319 411-1 V1.5.1 wird wie folgt geändert:

- [9] ETSI EN 319 401 V3.1.1 (2024-06) – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter.
- [10] ETSI EN 319 412-2 V2.4.1 – Elektronische Signaturen und Infrastrukturen (ESI) – Zertifikatsprofile – Teil 2: Zertifikatsprofil für natürlichen Personen ausgestellte Zertifikate.
- [14] ETSI EN 319 412-1 V1.6.1 – Elektronische Signaturen und Infrastrukturen (ESI) – Zertifikatsprofile – Teil 1: Übersicht und gemeinsame Datenstrukturen.
- [3] ETSI EN 319 412-5 V2.5.1 – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Zertifikatsprofile – Teil 5: QCStatements.
- [5] ETSI EN 319 412-1 V1.6.1 – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Zertifikatsprofile – Teil 1: Übersicht und gemeinsame Datenstrukturen.
- [6] CEN/TS 419261:2015 – Sicherheitsanforderungen für vertrauenswürdige Systeme zur Verwaltung von Zertifikaten für elektronische Signaturen und Zeitstempel.
- [7] Europäische Gruppe für die Cybersicherheitszertifizierung, Untergruppe für Kryptografie: „Agreed Cryptographic Mechanisms“ (Vereinbarte kryptografische Mechanismen), veröffentlicht von der Agentur der Europäischen Union für Cybersicherheit („ENISA“) <sup>(1)</sup>.
- [8] Durchführungsverordnung (EU) 2024/482 der Kommission <sup>(2)</sup> mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC).
- [9] Durchführungsverordnung (EU) 2024/3144 der Kommission <sup>(3)</sup> zur Änderung der Durchführungsverordnung (EU) 2024/482 in Bezug auf geltende internationale Normen und zur Berichtigung der Durchführungsverordnung.
- [10] ISO/IEC 15408:2022 (Teile 1 bis 5): Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Evaluationskriterien für IT-Sicherheit.
- [11] FIPS PUB 140-3 (2019) – Sicherheitsanforderungen an kryptografische Module.

<sup>(1)</sup> [https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography\\_en](https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en).

<sup>(2)</sup> ABl. L, 2024/482, 7.2.2024, ELI: [http://data.europa.eu/eli/reg\\_impl/2024/482/oj](http://data.europa.eu/eli/reg_impl/2024/482/oj).

<sup>(3)</sup> ABl. L, 2024/3144, 19.12.2024, ELI: [http://data.europa.eu/eli/reg\\_impl/2024/3144/oj](http://data.europa.eu/eli/reg_impl/2024/3144/oj).

- 2) 5.2 Anforderungen an Zertifizierungspraxiserklärungen
  - OVR-5.2-02 Die in den Unterlagen des Vertrauensdiensteanbieter (TSP) genannten Zertifikatsprofile (CPs) müssen die Anforderungen an die zu verwendenden Zertifikatsprofile enthalten.
- 3) 5.3 Name und Kennung der Zertifizierungsregelung
  - OVR-5.3-01 Werden an einem Zertifikatsprofil (CP), wie in Abschnitt 4.2.2 beschrieben, Änderungen vorgenommen, die sich auf die Anwendbarkeit auswirken, so ist die Regelungskennung zu ändern.
- 4) 6.1 Verantwortlichkeiten für Veröffentlichung und Datenablage (Repository)
  - OVR-6.1-02 Die in DIS-6.1-04 der Norm ETSI EN 319 411-1 [2] genannten Informationen müssen öffentlich und international verfügbar sein.
- 5) 6.2.2 Anfängliche Identitätsvalidierung
  - REG-6.2.2-01A Die Erfassung von Attributen und Nachweisen der Identität des Inhabers sowie deren Validierung erfolgt im Einklang mit den gemäß Artikel 24 Absatz 1c der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten.
  - REG-6.2.2-02 [QCP-n] und [QCP-n-qscd] Die Identität der natürlichen Person und gegebenenfalls spezifische Attribute der Person werden im Einklang mit den gemäß Artikel 24 Absatz 1c der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten überprüft.
  - ANMERKUNG 1 ungültig.
- 6) 6.3.3 Zertifikatsausstellung
  - GEN-6.3.3-01 Es gelten die Anforderungen GEN-6.3.3-01 bis GEN-6.3.3-10 der Norm ETSI EN 319 411-1 [2] Abschnitt 6.3.3.
  - GEN-6.3.3-02 [BEDINGT] Wird einer natürlichen Person, die in Verbindung mit der juristischen Person identifiziert wurde, ein Zertifikat ausgestellt, so müssen die Inhaberattribute zur Identifizierung der Organisation in dem Zertifikat die juristische Person oder Unterorganisation dieser juristischen Person repräsentieren, und der Inhaber-Identifikator in dem Zertifikat muss der natürlichen Person entsprechen.
  - GEN-6.3.3-03 Die CP-Kennung ist [AUSWAHL]:
    - a) [QCP-n]
      - gemäß Abschnitt 5.3 Buchstabe a und/oder
      - ein vom TSP oder einem anderen Beteiligten zugewiesener Objektbezeichner (OID) oder eine weitere Standardisierung der Regelung, um die in diesem Dokument festgelegten Regelungsanforderungen zu verbessern.
    - b) [QCP-n-qscd]
      - gemäß Abschnitt 5.3 Buchstabe c und/oder
      - ein vom TSP oder einem anderen Beteiligten zugewiesener Objektbezeichner (OID) oder eine weitere Standardisierung der Regelung, um die in diesem Dokument festgelegten Regelungsanforderungen zu verbessern.
- 7) 6.3.5 Verwendung von Schlüsselpaaren und Zertifikaten
  - SDP-6.3.5-02A [BEDINGT] Verwaltet der TSP die qualifizierte elektronische Signatur-/Siegelstellungseinheit (QSCD) für den Inhaber, so muss der TSP ein qualifizierter Vertrauensdiensteanbieter sein, der einen qualifizierten Vertrauensdienst zur Verwaltung einer qualifizierten elektronischen Fernsignaturerstellungseinheit gemäß der Verordnung (EU) Nr. 910/2014 [i.1] erbringt.

- SDP-6.3.5-11A Erzeugt der Nutzer oder Inhaber die Schlüssel des Inhabers, hat der Nutzer (siehe Abschnitt 6.3.4) folgende Verpflichtungen:
  - a) eine Verpflichtung zur Erzeugung von Inhaberschlüsseln für die Verwendungen des zertifizierten Schlüssels gemäß dem CP mit einem Algorithmus, der den von der Europäischen Gruppe für die Cybersicherheitszertifizierung [7] gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entspricht;
  - b) eine Verpflichtung zur Verwendung einer Schlüssellänge und eines Algorithmus, die den von der Europäischen Gruppe für die Cybersicherheitszertifizierung [7] gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen, für die Verwendungen des zertifizierten Schlüssels gemäß dem CP während der Gültigkeitsdauer des Zertifikats.
- 8) 6.3.10 Zertifikatsstatusdienste
  - CSS-6.3.10-08 [BEDINGT] Werden Listen widerrufener Zertifikate (CRLs) bereitgestellt, muss der TSP die Integrität und Verfügbarkeit der letzten CRL mindestens für den in der Zertifizierungspraxiserklärung (CPS) angegebenen Zeitraum wahren, wie in CSS-6.3.10-12 gefordert.
- 9) 6.4.4 Personalkontrollen
  - OVR-6.4.4-02 Das Personal des Vertrauensdiensteanbieters, das Vertrauensaufgaben wahrnimmt, und gegebenenfalls deren Unterauftragnehmer, die Vertrauensaufgaben wahrnehmen, müssen die Anforderung an „Fachkenntnisse, Erfahrung und Qualifikationen“ durch formale Schulungen und Befähigungsnachweise oder tatsächliche Erfahrung oder eine Kombination aus beiden erfüllen können.
  - OVR-6.4.4-03 Die Einhaltung von OVR-6.4.4-02 umfasst regelmäßige Aktualisierungen (mindestens alle 12 Monate) im Hinblick auf neue Bedrohungen und aktuelle Sicherheitspraktiken.
  - OVR-6.4.4-04 Zusätzlich zu den in der Norm ETSI EN 319 401 [1] (Abschnitt 7.2-15) festgelegten Vertrauensaufgaben sind die Vertrauensaufgaben der Registrierungs- und Widerrufsbeauftragten mit Zuständigkeiten gemäß der Norm TS 419261 [6] zu unterstützen. Wird ein qualifizierter Vertrauensdiensteanbieter (QTSP) direkt von einem Mitgliedstaat oder einer öffentlichen Stelle bzw. in dessen/deren Namen verwaltet oder betrieben, können diese zusätzlichen Vertrauensaufgaben von einem oder mehreren offiziellen Vertretern wahrgenommen werden, die für die und im Namen der Registrierungs- und Widerrufsbeauftragten in lokalen oder regionalen Verwaltungen handeln.
- 10) 6.4.9 Beendigung durch die Zertifizierungsbehörde (CA) oder Registrierungsbehörde (RA)
  - OVR-6.4.9-02 Der Beendigungsplan des Vertrauensdiensteanbieters muss den Anforderungen entsprechen, die in den gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten festgelegt sind.
- 11) 6.5.1 Erzeugung und Installation von Schlüsselpaaren
  - OVR-6.5.1-01A Die Erzeugung von CA-Schlüsselpaaren für die Signierzwecke der CA erfolgt mit einem Algorithmus, der den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA [7] veröffentlichten Vereinbarten kryptografischen Mechanismen entspricht.
  - OVR-6.5.1-01B Die gewählte Schlüssellänge und der Algorithmus für den CA-Signierschlüssel für die Signierzwecke der CA stehen im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA [7] veröffentlichten Vereinbarten kryptografischen Mechanismen.
  - OVR-6.5.1-01C [BEDINGT] Erzeugt die CA die Schlüssel des Inhabers, so stehen die von der CA erzeugten Inhaberschlüssel im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA [7] veröffentlichten Vereinbarten kryptografischen Mechanismen für die im CP festgelegten Zwecke während der Gültigkeitsdauer des Zertifikats.

- 12) 6.5.2 Schutz privater Schlüssel und technische Kontrollen des kryptografischen Moduls
- GEN-6.5.2-01 Es gelten alle Anforderungen der Norm ETSI EN 319 411-1 [2] Abschnitt 6.5.2 mit Ausnahme der Anforderungen OVR-6.5.2-01, OVR-6.5.2-03 und OVR-6.5.2-04.
  - GEN-6.5.2-02 Die Erzeugung von Schlüsselpaaren durch den TSP, einschließlich der von Widerrufs- und Registrierungsdiensten verwendeten Schlüssel, erfolgt in einem sicheren Kryptomodul, bei dem es sich um ein vertrauenswürdigen System handelt, das zertifiziert ist gemäß
  - den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit gemäß der Norm ISO/IEC 15408 [10] oder den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit, Version CC:2002, Teile 1 bis 5, veröffentlicht von den Beteiligten der Anerkennungsvereinbarung für die nach den Gemeinsamen Kriterien ausgestellten Zertifikate auf dem Gebiet der IT-Sicherheit (CCRA) und mit Vertrauenswürdigkeitsstufe der Evaluierung (*Evaluation Assurance Levels*, EAL) 4 oder höher zertifiziert, oder
  - dem auf den Gemeinsamen Kriterien beruhenden europäischen System für die Cybersicherheitszertifizierung (EUCC) [8][9], und mit EAL 4 oder höher zertifiziert, oder
  - bis 31.12.2030, FIPS PUB 140-3 [11] Stufe 3.
- Diese Zertifizierung erfolgt auf der Grundlage einer Risikoanalyse und unter Berücksichtigung physischer und anderer nicht technischer Sicherheitsmaßnahmen für ein Sicherheitsziel, ein Schutzprofil oder eine Modulentwurfs- und Sicherheitsdokumentation, die den Anforderungen des vorliegenden Dokuments entspricht.
- Verfügt das sichere Kryptomodul über eine EUCC [8][9]-Zertifizierung, so ist dieses Modul entsprechend dieser Zertifizierung zu konfigurieren und zu verwenden.
- GEN-6.5.2-03 Der private CA-Signierschlüssel wird in einem sicheren Kryptomodul aufbewahrt und verwendet, das die Anforderungen GEN-6.5.2-01 und GEN-6.5.2-02 erfüllt.
- 13) 6.5.7 Kontrollen der Netzsicherheit
- OVR-6.5.7-02 Der in REQ-7.8-13 der Norm ETSI EN 319 401 [1] geforderte Schwachstellen-Scan ist mindestens einmal pro Quartal durchzuführen.
  - OVR-6.5.7-03 Der in REQ-7.8-17X der Norm ETSI EN 319 401 [1] geforderte Penetrationstest ist mindestens einmal pro Jahr durchzuführen.
  - OVR-6.5.7-04 Firewalls sind so zu konfigurieren, dass alle Protokolle und Zugänge, die nicht für den Betrieb des Vertrauensdiensteanbieters (TSP) erforderlich sind, verhindert werden.
- 14) 6.6.1 Zertifikatsprofil
- GEN-6.6.1-05 Das Zertifikat muss eine der in GEN-6.3.3-03 [AUSWAHL] festgelegten Regelungskennungen enthalten. Das Zertifikat kann andere vom TSP zugewiesene OIDs enthalten.
2. Für ETSI EN 319 412-2:
- 1) 2.1 Normative Verweise
- [2] ETSI EN 319 412-5 V2.5.1 – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Zertifikatsprofile – Teil 5: QCStatements.
  - [9] Europäische Gruppe für die Cybersicherheitszertifizierung, Untergruppe für Kryptografie, „vereinbarte kryptografische Mechanismen“, veröffentlicht von ENISA.
- 2) 4.2.2 Signatur
- GEN-4.2.2-2 Der Signaturalgorithmus wird im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen ausgewählt [9].
  - ANMERKUNG ungültig.

- 3) 4.2.3.1 Aussteller, die juristische Personen sind
    - GEN-4.2.3.1-3 Ist eine geeignete Registriernummer bekannt, so enthält die Identität des Ausstellers einen „organizationIdentifier“ mit dem Wert dieser Registriernummer aus der entsprechenden amtlichen Eintragung, mit der diese Registriernummer festgelegt wurde.
  - 4) 4.2.5 Informationen über den öffentlichen Schlüssel des Inhabers
    - GEN-4.2.5-2 Der öffentliche Schlüssel des Inhabers wird im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen ausgewählt [9].
    - ANMERKUNG ungültig.
  - 5) 4.2.6 Seriennummer
    - GEN-4.2.6-01 Die „serialNumber“ des Zertifikats (gemäß IETF RFC 5280 [1] Abschnitt 4.1.2.2) muss für jedes vom TSP ausgestellte Zertifikat eindeutig sein.
-

## ANHANG II

**Liste der Referenzstandards und Spezifikationen für qualifizierte Zertifikate für elektronische Siegel**

Die Normen 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“) und ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5“) gelten mit den folgenden Anpassungen:

## 1. Für ETSI EN 319 411-2:

## 1) 2.1 Normative Verweise

- [1] ETSI EN 319 401 V3.1.1 (2024-06) – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter.
- [2] ETSI EN 319 411-1 V1.5.1 (2025-04) – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Regelungs- und Sicherheitsanforderungen an Vertrauensdiensteanbieter, die Zertifikate ausgeben – Teil 1: Allgemeine Anforderungen – mit den folgenden Anpassungen:

Abschnitt „2.1 Normative Verweise“ der Norm ETSI EN 319 411-1 V1.5.1 wird wie folgt geändert:

- [9] ETSI EN 319 401 V3.1.1 (2024-06) – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter.
- [10] ETSI EN 319 412-2 V2.4.1 – Elektronische Signaturen und Infrastrukturen (ESI) – Zertifikatsprofile – Teil 2: Zertifikatsprofil für natürlichen Personen ausgestellte Zertifikate.
- [14] ETSI EN 319 412-1 V1.6.1 – Elektronische Signaturen und Infrastrukturen (ESI) – Zertifikatsprofile – Teil 1: Übersicht und gemeinsame Datenstrukturen.
- [3] ETSI EN 319 412-5 V2.5.1 – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Zertifikatsprofile – Teil 5: QCStatements.
- [5] ETSI EN 319 412-1 V1.6.1 – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Zertifikatsprofile – Teil 1: Übersicht und gemeinsame Datenstrukturen.
- [6] CEN/TS 419261:2015 – Sicherheitsanforderungen für vertrauenswürdige Systeme zur Verwaltung von Zertifikaten für elektronische Signaturen und Zeitstempel (vom CEN erstellt).
- [7] Europäische Gruppe für die Cybersicherheitszertifizierung, Untergruppe für Kryptografie: Vereinbarte kryptografische Mechanismen, veröffentlicht von ENISA.
- [8] Durchführungsverordnung (EU) 2024/482 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC).
- [9] Durchführungsverordnung (EU) 2024/3144 zur Änderung der Durchführungsverordnung (EU) 2024/482 in Bezug auf geltende internationale Normen und zur Berichtigung der Durchführungsverordnung.
- [10] ISO/IEC 15408:2022 (Teile 1 bis 5) – Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Evaluationskriterien für IT-Sicherheit.
- [11] FIPS PUB 140-3 (2019) – Sicherheitsanforderungen an kryptografische Module.

## 2) 5.2 Anforderungen an Zertifizierungspraxiserklärungen

- OVR-5.2-02 Die in den Unterlagen des Vertrauensdiensteanbieter (TSP) genannten Zertifikatsprofile (CPs) müssen die Anforderungen an die zu verwendenden Zertifikatsprofile enthalten.

- 3) 5.3 Name und Kennung der Zertifizierungsregelung
  - OVR-5.3-01 Werden an einem CP, wie in Abschnitt 4.2.2 beschrieben, Änderungen vorgenommen, die sich auf die Anwendbarkeit auswirken, so ist die Regelungskennung zu ändern.
- 4) 6.1 Verantwortlichkeiten für Veröffentlichung und Datenablage (Repository)
  - OVR-6.1-02 Die in DIS-6.1-04 der Norm ETSI EN 319 411-1 [2] genannten Informationen müssen öffentlich und international verfügbar sein.
- 5) 6.2.2 Anfängliche Identitätsvalidierung
  - REG-6.2.2-01A Die Erfassung von Attributen und Nachweisen der Identität des Inhabers sowie deren Validierung erfolgt im Einklang mit den gemäß Artikel 24 Absatz 1c der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten.
  - REG-6.2.2-03 [QCP-l] und [QCP-l-qscd] Die Identität der juristischen Person und gegebenenfalls spezifische Attribute der Person werden im Einklang mit den gemäß Artikel 24 Absatz 1c der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten überprüft.
  - ANMERKUNG 3 Siehe Anmerkung 2.
- 6) 6.3.3 Zertifikatsausstellung
  - GEN-6.3.3-01 Es gelten die Anforderungen GEN-6.3.3-01 bis GEN-6.3.3-10 der Norm ETSI EN 319 411-1 [2] Abschnitt 6.3.3.
  - GEN-6.3.3-02 Die CP-Kennung ist [AUSWAHL]:
    - a) [QCP-l]
      - gemäß Abschnitt 5.3 Buchstabe b und/oder
      - ein vom TSP oder einem anderen Beteiligten zugewiesener Objektbezeichner (OID) oder eine weitere Standardisierung der Regelung, um die in diesem Dokument festgelegten Regelungsanforderungen zu verbessern.
    - b) [QCP-l-qscd]
      - gemäß Abschnitt 5.3 Buchstabe d und/oder
      - ein vom TSP oder einem anderen Beteiligten zugewiesener Objektbezeichner (OID) oder eine weitere Standardisierung der Regelung, um die in diesem Dokument festgelegten Regelungsanforderungen zu verbessern.
- 7) 6.3.5 Verwendung von Schlüsselpaaren und Zertifikaten
  - SDP-6.3.5-02A [BEDINGT] Verwaltet der TSP die qualifizierte elektronische Signatur-/Siegelerstellungseinheit (QSCD) für den Inhaber, so muss der TSP ein qualifizierter Vertrauensdiensteanbieter sein, der einen qualifizierten Vertrauensdienst zur Verwaltung einer qualifizierten elektronischen Fernsiegelerstellungseinheit gemäß der Verordnung (EU) Nr. 910/2014 [i.1] erbringt.
  - SDP-6.3.5-11A Erzeugt der Nutzer oder Inhaber die Schlüssel des Inhabers, hat der Nutzer (siehe Abschnitt 6.3.4) folgende Verpflichtungen:
    - a) eine Verpflichtung zur Erzeugung von Inhaberschlüsseln für die Verwendungen des zertifizierten Schlüssels gemäß dem CP mit einem Algorithmus, der den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA [7] veröffentlichten Vereinbarten kryptografischen Mechanismen entspricht, und
    - b) eine Verpflichtung zur Verwendung einer Schlüssellänge und eines Algorithmus für die Verwendungen des zertifizierten Schlüssels gemäß dem CP während der Gültigkeitsdauer des Zertifikats, die den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA [7] veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen.

- 8) 6.3.10 Zertifikatsstatusdienste
- CSS-6.3.10-08 [BEDINGT] Werden Listen widerrufenen Zertifikate (CRLs) bereitgestellt, muss der TSP die Integrität und Verfügbarkeit der letzten CRL mindestens für den in der Zertifizierungspraxiserklärung (CPS) angegebenen Zeitraum wahren, wie in CSS-6.3.10-12 gefordert.
- 9) 6.4.4 Personalkontrollen
- OVR-6.4.4-02 Das Personal des Vertrauensdiensteanbieters, das Vertrauensaufgaben wahrnimmt, und gegebenenfalls deren Unterauftragnehmer, die Vertrauensaufgaben wahrnehmen, müssen die Anforderung an „Fachkenntnisse, Erfahrung und Qualifikationen“ durch formale Schulungen und Befähigungsnachweise oder tatsächliche Erfahrung oder eine Kombination aus beiden erfüllen können.
  - OVR-6.4.4-03 Die Einhaltung von OVR-6.4.4-02 umfasst regelmäßige Aktualisierungen (mindestens alle 12 Monate) im Hinblick auf neue Bedrohungen und aktuelle Sicherheitspraktiken.
  - OVR-6.4.4-04 Zusätzlich zu den in der Norm ETSI EN 319 401 [1] (Abschnitt 7.2-15) festgelegten Vertrauensaufgaben sind die Vertrauensaufgaben der Registrierungs- und Widerrufsbeauftragten mit Zuständigkeiten gemäß der Norm TS 419261 [6] zu unterstützen. Wird ein qualifizierter Vertrauensdiensteanbieter (QTSP) direkt von einem Mitgliedstaat oder einer öffentlichen Stelle bzw. in dessen/deren Namen verwaltet oder betrieben, können diese zusätzlichen Vertrauensaufgaben von einem oder mehreren offiziellen Vertretern wahrgenommen werden, die für die und im Namen der Registrierungs- und Widerrufsbeauftragten in lokalen oder regionalen Verwaltungen handeln.
- 10) 6.4.9 Beendigung durch die Zertifizierungsbehörde (CA) oder Registrierungsbehörde (RA)
- OVR-6.4.9-02 Der Beendigungsplan des Vertrauensdiensteanbieters muss den Anforderungen entsprechen, die in den gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten festgelegt sind.
- 11) 6.5.1 Erzeugung und Installation von Schlüsselpaaren
- OVR-6.5.1-01A Die Erzeugung von CA-Schlüsselpaaren für die Signierzwecke der CA erfolgt mit einem Algorithmus, der den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA [7] veröffentlichten Vereinbarten kryptografischen Mechanismen entspricht.
  - OVR-6.5.1-01B Die gewählte Schlüssellänge und der Algorithmus für den CA-Signierschlüssel für die Signierzwecke der CA stehen im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA [7] veröffentlichten Vereinbarten kryptografischen Mechanismen.
  - OVR-6.5.1-01C [BEDINGT] Erzeugt die CA die Schlüssel des Inhabers, so stehen die von der CA erzeugten Inhaberschlüssel im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA [7] veröffentlichten Vereinbarten kryptografischen Mechanismen für die im CP festgelegten Zwecke während der Gültigkeitsdauer des Zertifikats.
- 12) 6.5.2 Schutz privater Schlüssel und technische Kontrollen des kryptografischen Moduls
- GEN-6.5.2-01 Es gelten alle Anforderungen der Norm ETSI EN 319 411-1 [2] Abschnitt 6.5.2 mit Ausnahme der Anforderungen OVR-6.5.2-01, OVR-6.5.2-03 und OVR-6.5.2-04.
  - GEN-6.5.2-02 Die Erzeugung von Schlüsselpaaren durch den TSP, einschließlich der von Widerrufs- und Registrierungsdiensten verwendeten Schlüssel, erfolgt in einem sicheren Kryptomodul, bei dem es sich um ein vertrauenswürdigen System handelt, das zertifiziert ist gemäß
    - den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit gemäß der Norm ISO/IEC 15408 [10] oder den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit, Version CC:2002, Teile 1 bis 5, veröffentlicht von den Beteiligten der Anerkennungsvereinbarung für die nach den Gemeinsamen Kriterien ausgestellten Zertifikate auf dem Gebiet der IT-Sicherheit (CCRA) und mit Vertrauenswürdigkeitsstufe der Evaluierung (*Evaluation Assurance Levels, EAL*) 4 oder höher zertifiziert, oder
    - dem auf den Gemeinsamen Kriterien beruhenden europäischen System für die Cybersicherheitszertifizierung (EUCC) [8][9], und mit EAL 4 oder höher zertifiziert, oder
    - bis 31.12.2030, FIPS PUB 140-3 [11] Stufe 3.

Diese Zertifizierung erfolgt auf der Grundlage einer Risikoanalyse und unter Berücksichtigung physischer und anderer nicht technischer Sicherheitsmaßnahmen für ein Sicherheitsziel, ein Schutzprofil oder eine Modulentwurfs- und Sicherheitsdokumentation, die den Anforderungen des vorliegenden Dokuments entspricht.

Verfügt das sichere Kryptomodul über eine EUCC [8][9]-Zertifizierung, so ist dieses Modul entsprechend dieser Zertifizierung zu konfigurieren und zu verwenden.

- GEN-6.5.2-03 Der private CA-Signierschlüssel wird in einem sicheren Kryptomodul aufbewahrt und verwendet, das die Anforderungen GEN-6.5.2-01 und GEN-6.5.2-02 erfüllt.

13) 6.5.7 Kontrollen der Netzsicherheit

- OVR-6.5.7-02 Der in REQ-7.8-13 der Norm ETSI EN 319 401 [1] geforderte Schwachstellen-Scan ist mindestens einmal pro Quartal durchzuführen.
- OVR-6.5.7-03 Der in REQ-7.8-17X der Norm ETSI EN 319 401 [1] geforderte Penetrationstest ist mindestens einmal pro Jahr durchzuführen.
- OVR-6.5.7-04 Firewalls sind so zu konfigurieren, dass alle Protokolle und Zugänge, die nicht für den Betrieb des Vertrauensdiensteanbieters (TSP) erforderlich sind, verhindert werden.

14) 6.6.1 Zertifikatsprofil

- GEN-6.6.1-05 Das Zertifikat muss eine der in GEN-6.3.3-02 [AUSWAHL] festgelegten Regelungskennungen enthalten.

2. Für ETSI EN 319 412-3:

1) 2.1 Normative Verweise

- [2] ETSI EN 319 412-2 V2.4.1 – Elektronische Signaturen und Infrastrukturen (ESI) – Zertifikatsprofile – Teil 2: Zertifikatsprofil für natürlichen Personen ausgestellte Zertifikate.

2) 4.2.1 Inhaber

- LEG-4.2.1-6 Das Attribut „organizationIdentifier“ muss eine vom Namen der Organisation abweichende Kennung der Inhaberorganisation enthalten. Ist eine geeignete Registriernummer bekannt, so enthält das Attribut „organizationIdentifier“ den Wert dieser Registriernummer aus der entsprechenden amtlichen Eintragung, mit der diese Registriernummer festgelegt wurde.

3. Für ETSI EN 319 412-2:

1) 2.1 Normative Verweise

- [2] ETSI EN 319 412-5 V2.5.1 – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) – Zertifikatsprofile – Teil 5: QCStatements.
- [9] Europäische Gruppe für die Cybersicherheitszertifizierung, Untergruppe für Kryptografie: Vereinbarte kryptografische Mechanismen, veröffentlicht von ENISA.

2) 2.2 Informative Verweise

- [i.7] ungültig.

3) 4.2.2 Signatur

- GEN-4.2.2-2 Der Signaturalgorithmus wird im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen ausgewählt [9].
- ANMERKUNG ungültig.

- 4) 4.2.3.1 Aussteller, die juristische Personen sind
    - GEN-4.2.3.1-3 Ist eine geeignete Registriernummer bekannt, so enthält die Identität des Ausstellers einen „organizationIdentifier“ mit dem Wert dieser Registriernummer aus der entsprechenden amtlichen Eintragung, mit der diese Registriernummer festgelegt wurde.
  - 5) 4.2.5 Informationen über den öffentlichen Schlüssel des Inhabers
    - GEN-4.2.5-2 Der öffentliche Schlüssel des Inhabers wird im Einklang mit den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen ausgewählt [9].
    - ANMERKUNG ungültig.
  - 6) 4.2.6 Seriennummer
    - GEN-4.2.6-01 Die „serialNumber“ des Zertifikats (gemäß IETF RFC 5280 [1] Abschnitt 4.1.2.2) muss für jedes vom TSP ausgestellte Zertifikat eindeutig sein.
-