



**DURCHFÜHRUNGSVERORDNUNG (EU) 2025/1942 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 qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen und qualifizierte Validierungsdienste für qualifizierte 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 33 Absatz 2 und Artikel 40,

in Erwägung nachstehender Gründe:

- (1) Qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen und für qualifizierte elektronische Siegel gewährleisten die Integrität, Authentizität und Korrektheit des Prozesses und der Ergebnisse der Validierung qualifizierter elektronischer Signaturen und qualifizierter elektronischer Siegel. Diese qualifizierten Vertrauensdienste haben im digitalen Geschäftsumfeld eine große Bedeutung, weil sie den Übergang von herkömmlichen papiergestützten Verfahren zu entsprechenden elektronischen Verfahren fördern.
- (2) Die Konformitätsvermutung gemäß Artikel 33 Absatz 2 und Artikel 40 der Verordnung (EU) Nr. 910/2014 sollte nur gelten, wenn qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen und für qualifizierte elektronische Siegel den in der vorliegenden Verordnung festgelegten technischen 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 ihre Fähigkeit zu gewährleisten, den Qualifikationsstatus und die technische Gültigkeit qualifizierter elektronischer Signaturen und qualifizierter elektronischer Siegel zu überprüfen.
- (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.

<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>).

- (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.
- (6) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates <sup>(5)</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

Die in Artikel 33 Absatz 2 und Artikel 40 der Verordnung (EU) Nr. 910/2014 genannten Referenzstandards und Spezifikationen sind im Anhang 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>(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>).

<sup>(5)</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

**Liste der Referenzstandards und Spezifikationen für qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen und für qualifizierte Validierungsdienste für qualifizierte elektronische Siegel**

Die Normen ETSI TS 119 441 V1.2.1 (2023-10) <sup>(1)</sup> („ETSI TS 119 441“) und ETSI TS 119 172-4 V1.1.1 (2021-05) <sup>(2)</sup> („ETSI TS 119 172-4“) gelten mit den folgenden Anpassungen:

1. Für ETSI EN 119 441

1) 2.1 Normative Verweise

- [1] ETSI TS 119 101 V1.1.1 (2016-03) — Elektronische Signaturen und Infrastrukturen (ESI) — Regelungs- und Sicherheitsanforderungen an Anwendungen für die Erstellung und Validierung von Signaturen.
- [2] ETSI EN 319 401 V3.1.1 (2024-06) — Elektronische Signaturen und Infrastrukturen (ESI) — Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter.
- [3] ETSI EN 319 102-1 V1.4.1 (2024-06) — Elektronische Signaturen und Infrastrukturen (ESI) — Verfahren für die Erzeugung und Gültigkeitsprüfung digitaler AdES-Signaturen — Teil 1: Erzeugung und Gültigkeitsprüfung.
- [4] ISO/IEC 15408-1:2022 — Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit.
- [5] ungültig.
- [6] FIPS PUB 140-3 (2019) — Sicherheitsanforderungen an kryptografische Module.
- [7] Durchführungsverordnung (EU) 2024/482 der Kommission <sup>(3)</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).
- [8] ETSI TS 119 172-4 V1.1.1 (2021-05) — Elektronische Signaturen und Infrastrukturen (ESI) — Signaturregelungen — Teil 4: Regeln für die Anwendbarkeit von Signaturen (Validierungsregelung) für europäische qualifizierte elektronische Signaturen/Siegel unter Verwendung von Vertrauenslisten.
- [9] ETSI TS 119 102-2 V1.4.1 (2023-06) — Elektronische Signaturen und Infrastrukturen (ESI) — Verfahren für die Erzeugung und Gültigkeitsprüfung digitaler AdES-Signaturen — Teil 2: Signaturvalidierungsbericht.
- [10] 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>(4)</sup>.
- [11] Durchführungsverordnung (EU) 2024/3144 der Kommission <sup>(5)</sup> zur Änderung der Durchführungsverordnung (EU) 2024/4822 in Bezug auf geltende internationale Normen und zur Berichtigung der Durchführungsverordnung.
- [12] ETSI EN 319 411-1 — Elektronische Signaturen und Infrastrukturen (ESI) — Regelungs- und Sicherheitsanforderungen an Vertrauensdiensteanbieter, die Zertifikate ausgeben — Teil 1: Allgemeine Anforderungen.

<sup>(1)</sup> ETSI TS 119 441 — Elektronische Signaturen und Infrastrukturen (ESI) — Regelungsanforderungen an Vertrauensdiensteanbieter, die Signaturvalidierungsdienste erbringen, V1.2.1 (2023-10).

<sup>(2)</sup> ETSI TS 119 172-4 — Elektronische Signaturen und Infrastrukturen (ESI) — Signaturregelungen — Teil 4: Regeln für die Anwendbarkeit von Signaturen (Validierungsregelung) für europäische qualifizierte elektronische Signaturen/Siegel unter Verwendung von Vertrauenslisten, V1.1.1 (2021-05).

<sup>(3)</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>(4)</sup> [https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography\\_en](https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en).

<sup>(5)</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) 2.2 Normative Verweise
  - [i.11] ungültig.
- 3) 3.3 Abkürzungen
  - EUCC — auf den Gemeinsamen Kriterien beruhendes europäisches System für die Cybersicherheitszertifizierung
- 4) 4.3.3 Verfahren
  - ANMERKUNG 10 Zur Verwendung qualifizierter Signaturen oder Siegel in der EU siehe die Hinweise in ETSI EN 319 102-1 [3] und die zusätzlichen Hinweise in ETSI TS 119 172-4 [8].
- 5) 6.1 Praxiserklärung zum Signaturvalidierungsdienst
  - OVR-6.1-02 Die SVS-Praxiserklärung muss gemäß Anhang A strukturiert sein.
  - OVR-6.1-03 Die SVS-Praxiserklärung muss die unterstützten SVS-Regelungen auflisten oder darauf verweisen (z. B. durch OIDs) und diese kurz beschreiben.
- 6) 6.3 Informationssicherheitsregelung
  - OVR-6.3-02 Die Sicherheitsregelung muss die Sicherheits- und Datenschutzkontrollen dokumentieren, die zum Schutz personenbezogener Daten bestehen.
- 7) 7.2 Personal
  - OVR-7.2-02 Das Personal des Signaturvalidierungsdiensteanbieters (SVSP), 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-7.2-03 Die Einhaltung von OVR-7.2-02 umfasst regelmäßige Aktualisierungen (mindestens alle 12 Monate) im Hinblick auf neue Bedrohungen und aktuelle Sicherheitspraktiken.
- 8) 7.5 Kryptografische Kontrollen
  - OVR-7.5-02 [BEDINGT] Werden Validierungsberichte signiert, so wird das dem privaten SVSP-Signierschlüssel entsprechende öffentliche SVSP-Signierzertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) im Einklang mit der NCP+-Zertifizierungsregelung gemäß ETSI EN 319 411-1 [12] ausgestellt. Die Ausstellung sollte im Einklang mit einer geeigneten Zertifizierungsregelung gemäß ETSI EN 319 411-2 [i.17] erfolgen.
  - OVR-7.5-03 [BEDINGT] Werden Validierungsberichte signiert, wird der private SVPS-Signierschlüssel in einem sicheren Kryptomodul aufbewahrt und verwendet, bei dem es sich um ein vertrauenswürdiges System handelt, das zertifiziert ist gemäß
    - a) den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit gemäß der Norm ISO/IEC 15408 [4] oder den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit, Version CC:2022, 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
    - b) EUCC [7][11], und mit EAL 4 oder höher zertifiziert, oder
    - c) bis 31.12.2030, FIPS PUB 140-3 [6] 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[7][11]-Zertifizierung, so ist dieses Modul entsprechend dieser Zertifizierung zu konfigurieren und zu verwenden.

- OVR-7.5-04 ungültig.
  - OVR-7.5-06 Ein privater SVSP-Signierschlüssel darf nur dann exportiert und in ein anderes sicheres Kryptomodul importiert werden, wenn dieser Export und Import sicher und im Einklang mit der Zertifizierung dieser Module durchgeführt werden.
- 9) 7.7 Betriebssicherheit
- OVR-7.7-02 Um sicherzustellen, dass in den Systemen, in denen die Anwendung entwickelt wird, geeignete Sicherheitsmaßnahmen bestehen und die Systeme an besondere Anwendungsumgebungen angepasst werden, muss die Signaturvalidierungsanwendung (SVA) eine Anwendungsumgebung verwenden, die mit aktuellen Sicherheitspatches gepflegt wird.
  - OVR-7.7-03 Für die SVA gelten die folgenden Anforderungen der Norm ETSI TS 119 101 [1] Abschnitt 5.2: GSM 1.3.
- 10) 7.8 Netzsicherheit
- OVR-7.8-02 Wird der Fernzugriff auf Systeme, in denen vertrauliche Daten gespeichert oder verarbeitet werden, erlaubt, muss dafür eine förmliche Regelung festgelegt und als Teil der nach OVR-6.3-02 erforderlichen Elemente beschrieben werden.
  - OVR-7.8-04 Der in REQ-7.8-13 der Norm ETSI EN 319 401 [1] geforderte Schwachstellen-Scan ist mindestens einmal pro Quartal durchzuführen.
  - OVR-7.8-05 Der in REQ-7.8-17X der Norm ETSI EN 319 401 [1] geforderte Penetrationstest ist mindestens einmal pro Jahr durchzuführen.
  - OVR-7.8-06 Firewalls sind so zu konfigurieren, dass alle Protokolle und Zugänge, die nicht für den Betrieb des Signaturvalidierungsdiensteanbieters (SVSP) erforderlich sind, verhindert werden.
- 11) 7.12 Beendigung und Beendigungspläne in Bezug auf die Erbringung des Signaturvalidierungsdienstes
- OVR-7.12-02 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.
- 12) 7.14 Lieferkette
- OVR-7.14-01 Es gelten die Anforderungen der Norm ETSI EN 319 401 [2] Abschnitt 7.14.
- 13) 8.1 Signaturvalidierungsprozess
- VPR-8.1-07 Die Signaturvalidierungsanwendung (SVA) muss den Anforderungen der Norm ETSI TS 119 101 [1] Abschnitt 7.4 SIA 1 bis SIA 4 entsprechen.
  - VPR-8.1-11 [BEDINGT] Wenn der Signaturvalidierungsdienst (SVS) qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel gemäß Artikel 32 Absatz 1 (bzw. Artikel 40) der Verordnung (EU) Nr. 910/2014 [i.1] validieren soll, muss der Validierungsprozess den Anforderungen der Norm ETSI TS 119 172-4 [8] entsprechen.
- 14) 8.2 Signaturvalidierungsprotokoll
- SVP-8.2-03 Die Signaturvalidierungsantwort muss die OID der SVS-Regelung enthalten.
- 15) 8.4 Signaturvalidierungsbericht
- SVR-8.4-02 Der Validierungsbericht muss der Norm ETSI TS 119 102-2 [9] entsprechen.
  - SVR-8.4-07 [BEDINGT] Wird eine Signaturvalidierungsregelung vom Signaturvalidierungsdienst (SVS) nicht vollständig verarbeitet, so sind in dem Bericht neben validierten Beschränkungen auch ignorierte oder übergangene Beschränkungen anzugeben.

- SVR-8.4-15 Im Validierungsbericht ist die Herkunft der einzelnen PoE eindeutig anzugeben (aus der Signatur, vom Client, vom Server).
  - SVR-8.4-16 Der Validierungsbericht muss eine Validierungsberichtssignatur enthalten, bei der es sich um die digitale Signatur des SVSP handelt.
  - SVR-8.4-17 [BEDINGT] Werden Validierungsberichte unterzeichnet, so müssen Format und Ziel der Signatur der Norm ETSI TS 119 102-2 [9] entsprechen.
- 16) 9. Rahmen für die Aufstellung von Validierungsdienstregelungen auf der Grundlage einer im vorliegenden Dokument festgelegten Vertrauensdienstregelung:
- OVR-9-05 [BEDINGT] Bei der Aufstellung einer SVS-Regelung aufgrund einer im vorliegenden Dokument festgelegten Vertrauensdienstregelung wird eine Risikobewertung durchgeführt, um die Geschäftsanforderungen zu bewerten und die Sicherheitsanforderungen zu bestimmen, die in die Regelung für die angegebene Gemeinschaft und Anwendbarkeit aufzunehmen sind.
  - OVR-9-06 [BEDINGT] Bei der Aufstellung einer SVS-Regelung aufgrund einer im vorliegenden Dokument festgelegten Vertrauensdienstregelung erfolgt die Annahme und Änderung der Regelung nach einem festgelegten Überprüfungsprozess, der auch die Zuständigkeiten für die Aufrechterhaltung der Regelung umfasst.
  - OVR-9-07 [BEDINGT] Bei der Aufstellung einer SVS-Regelung aufgrund einer im vorliegenden Dokument festgelegten Vertrauensdienstregelung muss ein festgelegter Überprüfungsprozess bestehen, damit die Regelung durch die Praxiserklärungen untermauert wird.
  - OVR-9-08 [BEDINGT] Bei der Aufstellung einer SVS-Regelung aufgrund einer im vorliegenden Dokument festgelegten Vertrauensdienstregelung stellt der TSP seiner Nutzergemeinschaft die von ihm unterstützten Regelungen zur Verfügung.
  - OVR-9-09 [BEDINGT] Bei der Aufstellung einer SVS-Regelung aufgrund einer im vorliegenden Dokument festgelegten Vertrauensdienstregelung werden Überarbeitungen der vom TSP unterstützten Regelungen den Nutzern zur Verfügung gestellt.
- 17) Anhang B (normativ) Qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen (QES) gemäß Artikel 33 der Verordnung (EU) Nr. 910/2014:
- VPR-B-02 [BEDINGT] Wenn der Signaturvalidierungsdiensteanbieter (SVSP) ein qualifizierter Signaturvalidierungsdiensteanbieter (QSVSP) ist, muss die Umsetzung den Anforderungen der Norm ETSI TS 119 172-4 [8] entsprechen.
  - ANMERKUNG 2 ungültig.
  - OVR-B-04 [BEDINGT] Wenn der SVSP ein QSVSP ist, müssen bei den Prüfungen in OVR-B-03 unterschiedliche, positive und negative Anwendungsfälle geprüft werden.
  - VPR-B-11 [BEDINGT] Wenn der SVSP ein QSVSP ist, kontrolliert er die Hashberechnung (indem er entweder die Berechnung auf dem Server durchführt oder aber den Client kontrolliert, falls die Berechnung beim Client zulässig ist).
  - ANMERKUNG 5 ungültig.
  - ANMERKUNG 6 ungültig.
  - VPR-B-15 [BEDINGT] Wenn der SVSP ein QSVSP ist, muss der Validierungsbericht den Anforderungen der Norm ETSI TS 119 102-2 [9] entsprechen, um die Anforderungen in VPR-B-13 bis VPR-B-14 zu erfüllen.
  - VPR-B-16 [BEDINGT] Wenn der SVSP ein QSVSP ist, muss die Umsetzung für den Einsatz geeigneter kryptografischer Techniken bei der Erbringung qualifizierter Validierungsdienste für qualifizierte elektronische Signaturen den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen [10] entsprechen.

- 18) Anhang C (informativ) Zuordnung der Anforderungen der Verordnung (EU) Nr. 910/2014 in Bezug auf die Durchführung einer Validierung gemäß Artikel 32 Absatz 1:
- Um sicherzustellen, dass alle in Artikel 32 Absatz 1 und Artikel 40 der Verordnung (EU) Nr. 910/2014 [i.1] verlangten Bedingungen überprüft werden, ist ein korrekter Validierungsalgorithmus erforderlich. Er liefert das gleiche deterministische Ergebnis für eine Signatur oder ein Siegel, die/das zur Validierung vorgelegt wird. Dabei kommt es entscheidend auf die Signaturvalidierungsregelung an. Zu diesem Zweck ist die Norm ETSI TS 119 172-4 [8] auf der Grundlage des in der Norm ETSI EN 319 102-1 [3] spezifizierten Validierungsalgorithmus herausgegeben worden.
2. Für ETSI TS 119 172-4
- 1) 2.1 Normative Verweise:
- [1] ETSI EN 319 102-1 V1.4.1 (2024-06) — Elektronische Signaturen und Vertrauensinfrastrukturen (ESI) — Verfahren für die Erzeugung und Gültigkeitsprüfung digitaler AdES-Signaturen — Teil 1: Erzeugung und Gültigkeitsprüfung.
  - Alle Bezugnahmen auf „ETSI TS 119 102-1 [1]“ sind als Bezugnahmen auf „ETSI EN 319 102-1 [1]“ zu verstehen.
  - [2] ETSI TS 119 612 V2.3.1 (2024-11) — Elektronische Signaturen und Infrastrukturen (ESI) — Vertrauenslisten.
  - [13] ETSI TS 119 101 V1.1.1 (2016-03) — Elektronische Signaturen und Infrastrukturen (ESI) — Regelungs- und Sicherheitsanforderungen an Anwendungen für die Erstellung und Validierung von Signaturen.
- 2) 4.2 Validierungsbeschränkungen und Validierungsverfahren, Anforderung REQ-4.2-03 Abschnitt „X.509 Validierungsbeschränkungen“ Buchstabe c:
- i) Wenn das Zertifikat einer End-Entität einen Vertrauensanker darstellt, dürfen die „RevocationCheckingConstraints“ nicht verwendet werden.
  - ii) Wenn das Zertifikat einer End-Entität keinen Vertrauensanker darstellt, sind die „RevocationCheckingConstraints“ gemäß ETSI TS 119 172-1 [3] Abschnitt A.4.2.1 Tabelle A.2 Zeile (m)2.1 auf „eitherCheck“ zu setzen.
  - iii) Wenn das Zertifikat einer End-Entität einen Vertrauensanker darstellt, dürfen die „RevocationFreshnessConstraints“ gemäß ETSI TS 119 172-1 [3] Abschnitt A.4.2.1 Tabelle A.2 Zeile (m)2.2 nicht verwendet werden.
  - iv) Wenn das Zertifikat einer End-Entität keinen Vertrauensanker darstellt, sind die „RevocationFreshnessConstraints“ gemäß ETSI TS 119 172-1 [3] Abschnitt A.4.2.1 Tabelle A.2 Zeile (m)2.2 mit einem Höchstwert von 24 Stunden für das Signierzertifikat zu verwenden. Für andere Zertifikate als die Signierzertifikate, einschließlich Zertifikate mit Zeitstempel, darf für die „RevocationFreshnessConstraints“ kein Wert gesetzt werden.
- 3) 4.4 Prozess der Prüfung der technischen Anwendbarkeit (Regeln)
- REQ-4.4.2-03 Falls eine in REQ-4.4.2-01 angegebene Prüfung scheitert, so gilt Folgendes:
    - a) der Prozess wird beendet,
    - b) die Signatur wird technisch als unbestimmt behandelt, d. h. weder als qualifizierte elektronische Signatur der EU noch als qualifiziertes elektronisches Siegel der EU,
    - c) das obige Ergebnis und die Prozessergebnisse aller Zwischenprozesse werden im Bericht über die Prüfung der Regeln für die Anwendbarkeit der Signaturen aufgeführt.