



2025/1946

30.9.2025

DURCHFÜHRUNGSVERORDNUNG (EU) 2025/1946 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 Bewahrungsdienste für qualifizierte elektronische Signaturen und 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 ⁽¹⁾, insbesondere auf Artikel 34 Absatz 2 und Artikel 40,

in Erwägung nachstehender Gründe:

- (1) Qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen und qualifizierte elektronische Siegel sorgen für eine langfristige Integrität, Authentizität, Existenzbeweisbarkeit und Zugänglichkeit des Bewahrungsnachweises solcher elektronischer Signaturen und elektronischer Siegel, um deren rechtliche Gültigkeit über lange Zeiträume zu gewährleisten und um sicherzustellen, dass diese ungeachtet künftiger technologischer Veränderungen noch validiert werden können. Diese Dienste werden unabhängig oder als Teil anderer qualifizierter Vertrauensdienste wie qualifizierter elektronischer Archivierungsdienste erbracht.
- (2) Die Konformitätsvermutung gemäß Artikel 34 Absatz 1a und Artikel 40 der Verordnung (EU) Nr. 910/2014 sollte nur gelten, wenn qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen und für qualifizierte elektronische 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 ihre Fähigkeit zu gewährleisten, den Qualifikationsstatus und die technische Gültigkeit der Signaturen und Siegel über lange Zeiträume 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 ⁽²⁾ 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.

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

⁽²⁾ 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 ⁽³⁾ und, sofern anwendbar, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ⁽⁴⁾ 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 ⁽⁵⁾ 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 34 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

⁽³⁾ 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>).

⁽⁴⁾ 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>).

⁽⁵⁾ 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 gemäß Artikel 2

Die Normen ETSI TS 119 511 V1.1.1 (2019-06) („ETSI TS 119 511“) und ETSI TS 119 172-4 V1.1.1 (2021-05) („ETSI TS 119 172-4“) gelten mit den folgenden Anpassungen:

1. Für ETSI EN 119 511:

(1) 2.1 Normative Verweise:

- [1] ETSI EN 319 401 V3.1.1 (2024-06) — Elektronische Signaturen und Infrastrukturen (ESI) — Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter.
- [2] ETSI TS 119 612 V2.3.1 — Elektronische Signaturen und Infrastrukturen (ESI) — Vertrauenslisten.
- [5] FIPS PUB 140-3 (2019) — Sicherheitsanforderungen an kryptografische Module.
- [6] Durchführungsverordnung (EU) 2024/482 der Kommission ⁽¹⁾ 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).
- [7] Durchführungsverordnung (EU) 2024/3144 der Kommission ⁽²⁾ zur Änderung der Durchführungsverordnung (EU) 2024/482 in Bezug auf geltende internationale Normen und zur Berichtigung der Durchführungsverordnung.
- [8] Europäische Gruppe für die Cybersicherheitszertifizierung, Untergruppe für Kryptografie: „Agreed Cryptographic Mechanisms“ (Vereinbarte kryptografische Mechanismen), veröffentlicht von der Agentur der Europäischen Union für Cybersicherheit („ENISA“) ⁽³⁾.
- [9] 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.
- [10] ISO/IEC 15408-2022 (Teile 1 bis 5) — Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit.

(2) 3.1 Begriffe

- sicheres Kryptomodul: Modul, in dem der private Schlüssel des Nutzers gespeichert ist, es schützt diesen Schlüssel vor Beeinträchtigungen und führt im Namen des Nutzers Signier- oder Entschlüsselungsfunktionen aus.

(3) 6.4 Bewahrungsprofile

- OVR-6.4-08A [WTS][WOS] Die voraussichtliche Nachweisdauer muss den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [8].
- ANMERKUNG 3 ungültig.

(4) 6.5 Bewahrungsnachweisregelung

- OVR-6.5-04A Die verwendeten kryptografischen Algorithmen müssen den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [8].
- ANMERKUNG 1 ungültig.

⁽¹⁾ ABl. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

⁽²⁾ ABl. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

⁽³⁾ https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

(5) 7.2 Personal

- OVR-7.2-02 Das Personal des Bewahrungsdiensteanbieters (PSP), 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.

(6) 7.5 Kryptografische Kontrollen

- OVR-7.5-05 [BEDINGT] Signiert ein PSP einen Bewahrungsnachweis (oder einen Teil davon), wird der private PSP-Signierschlüssel in einem sicheren Kryptomodul aufbewahrt und verwendet, bei dem es sich um ein vertrauenswürdigen System handelt, das zertifiziert ist gemäß
 - (a) 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: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 [6][7], und mit EAL 4 oder höher zertifiziert, oder
 - (c) bis 31.12.2030, FIPS PUB 140-3 [5] 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[6][7]-Zertifizierung, so ist dieses Modul entsprechend dieser Zertifizierung zu konfigurieren und zu verwenden.

- OVR-7.5-06 [BEDINGT] ungültig.
- OVR-7.5-07 [BEDINGT] Signiert ein PSP einen Bewahrungsnachweis (oder einen Teil davon), sind Sicherungskopien der privaten PSP-Signierschlüssel mittels des sicheren Kryptomoduls zu schützen, um deren Integrität und Vertraulichkeit zu gewährleisten, bevor die Sicherungskopien außerhalb dieses Moduls gespeichert werden.
- OVR-7.5-08 Ein privater PSP-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.

(7) 7.8 Netzsicherheit

- OVR-7.8-03 Der in REQ-7.8-13 der Norm ETSI EN 319 401 [1] geforderte Schwachstellen-Scan ist mindestens einmal pro Quartal durchzuführen.
- OVR-7.8-04 Der in REQ-7.8-17X der Norm ETSI EN 319 401 [1] geforderte Penetrationstest ist mindestens einmal pro Jahr durchzuführen.
- OVR-7.8-05 Firewalls sind so zu konfigurieren, dass alle Protokolle und Zugänge, die nicht für den Betrieb des PSP erforderlich sind, verhindert werden.

(8) 7.14 Kryptografische Überwachung

- OVR-7.14-03A Die Bewertung des kryptografischen Algorithmus in OVR-7.14.01 und OVR-7.14.02 muss den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [8].
- ANMERKUNG ungültig.

- (9) 7.12 TSP-Beendigung und -Beendigungspläne
 - OVR-7.12-01A Der Beendigungsplan des Vertrauensdiensteanbieters muss den Anforderungen entsprechen, die in den gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 [i.2] erlassenen Durchführungsrechtsakten festgelegt sind.
- (10) 7.17 Lieferkette
 - OVR-7.17-01 Es gelten die Anforderungen der Norm ETSI EN 319 401 [1] Abschnitt 7.14.
- (11) Anhang A (normativ): Qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen (QES) gemäß Artikel 34 der Verordnung (EU) Nr. 910/2014
 - OVR-A-02 [PDS][PDS+PGD]
 - (a) Der Bewahrungsdienst bewahrt alle Informationen auf, die für die Überprüfung des Qualifikationsstatus der elektronischen Signatur oder des elektronischen Siegels erforderlich sind und die bis zum Ende des Bewahrungszeitraums nicht öffentlich zugänglich wären;
 - (b) der Bewahrungsdienst stellt sicher, dass die bewahrten Informationen zu jedem beliebigen Zeitpunkt während des Bewahrungszeitraums so beschaffen sind, dass, wenn sie als Eingaben für das in Abschnitt 4.4 der Norm ETSI TS 119 172-4 [9] beschriebene Verfahren bereitgestellt werden, das Ergebnis dieses Prozesses eindeutig bestätigt, ob die digitale Signatur oder das digitale Siegel zum Zeitpunkt ihrer/seiner Bewahrung technisch geeignet war, eine qualifizierte elektronische Signatur oder ein qualifiziertes elektronisches Siegel der EU umzusetzen.
 - OVR-A-03 [PDS] [PDS+PGD] Zeitstempel, die in den Bewahrungsnachweisen verwendet werden, müssen qualifizierte Zeitstempel gemäß der Verordnung (EU) Nr. 910/2014 [i.2] sein.

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 — 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 Erzeugung 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 0 für das Signierzertifikat zu verwenden, sodass die Widerrufsinformationen nur akzeptiert werden, wenn sie nach der besten Signaturzeit erstellt wurden. Für andere Zertifikate als die Signierzertifikate, auch Zertifikate mit Zeitstempel, darf für die „RevocationFreshnessConstraints“ kein Wert gesetzt werden.
- (3) 4.3 Anforderungen an die Verfahren der Signaturvalidierung und der Prüfung der Regeln für die Anwendbarkeit
- REQ-4.3-02 Signaturvalidierungsanwendungen müssen der Norm ETSI TS 119 101 [13] entsprechen.
- (4) 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:
 - der Prozess wird beendet,
 - die Signatur wird technisch als unbestimmt behandelt, d. h. weder als qualifizierte elektronische Signatur der EU noch als qualifiziertes elektronisches Siegel der EU,
 - das obige Ergebnis und die Prozessergebnisse aller Zwischenprozesse werden im Bericht über die Überprüfung der Regeln für die Anwendbarkeit der Signaturen aufgeführt.
-