



2025/1929

30.9.2025

**DURCHFÜHRUNGSVERORDNUNG (EU) 2025/1929 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 die Verknüpfung von Datums- und Zeitangaben mit Daten und zur Bestimmung der Richtigkeit der Zeitquellen für die Bereitstellung qualifizierter elektronischer Zeitstempel**

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 42 Absatz 2,

in Erwägung nachstehender Gründe:

- (1) Qualifizierte elektronische Zeitstempel haben im digitalen Umfeld eine große Bedeutung, weil sie den Übergang von herkömmlichen papiergestützten Verfahren zu entsprechenden elektronischen Verfahren fördern. Durch die Verknüpfung von Datums- und Zeitangaben mit elektronischen Daten tragen qualifizierte elektronische Zeitstempel dazu bei, dass die Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie die Unversehrtheit der mit dem Datum und der Zeit verbundenen digitalen Dokumente gewährleistet ist.
- (2) Die Konformitätsvermutung gemäß Artikel 42 Absatz 1a der Verordnung (EU) Nr. 910/2014 sollte nur gelten, wenn qualifizierte Vertrauensdienste für die Ausstellung qualifizierter Zeitstempel 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. Diese Standards bzw. Normen sollten so angepasst werden, dass sie zusätzliche Kontrollen umfassen, um die Sicherheit und Vertrauenswürdigkeit des qualifizierten Vertrauensdienstes und der Verknüpfung der Datums- und Zeitangaben sowie die Richtigkeit der Zeitquellen 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 Durchführungsverordnung 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*

Die in Artikel 42 Absatz 2 der Verordnung (EU) Nr. 910/2014 genannten Referenzstandards und Spezifikationen sind im Anhang der vorliegenden Verordnung festgelegt.

*Artikel 2*

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

**Liste der Referenzstandards und Spezifikationen für qualifizierte Zeitstempeldienste**

Die Normen ETSI EN 319 421 V1.3.1 <sup>(1)</sup> („ETSI EN 319 421“) und ETSI EN 319 422 V1.1.1 <sup>(2)</sup> („ETSI EN 319 422“) gelten mit den folgenden Anpassungen:

1. Für ETSI EN 319 421

1. 2.1 Normative Verweise:

- [3] ISO/IEC 15408-2022 (Teile 1 bis 5) — Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit.
- [4] ETSI EN 319 401 V3.1.1 (2024-06) — Elektronische Signaturen und Infrastrukturen (ESI) — Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter.
- [5] ETSI EN 319 422 V1.1.1 (2016-03) — Elektronische Signaturen und Infrastrukturen (ESI) — Zeitstempel-Protokoll und Zeitstempel-Token-Profile.
- [6] ungültig.
- [9] 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>(3)</sup>.
- [10] Durchführungsverordnung (EU) 2024/482 der Kommission vom 31. Januar 2024 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) <sup>(4)</sup>.
- [11] Durchführungsverordnung (EU) 2024/3144 der Kommission vom 18. Dezember 2024 zur Änderung der Durchführungsverordnung (EU) 2024/482 in Bezug auf geltende internationale Normen und zur Berichtigung der Durchführungsverordnung <sup>(5)</sup>.

2. 3.1 Begriffe

- Gültigkeitsdauer der Zertifikate: Zeitintervall von „notBefore“ bis „notAfter“ (inklusive), für das die Zertifizierungsstelle („CA“) die Aufbewahrung der Informationen über den Status des Zertifikats garantiert

3. 3.3 Abkürzungen

- EUCC — auf den Gemeinsamen Kriterien beruhendes europäisches System für die Cybersicherheitszertifizierung

4. 6.2 Praxiserklärung zum Vertrauensdienst

- OVR-6.2-03 Die TSA (Zeitstempelstelle) nimmt in ihre TSA-Offenlegungserklärung Erklärungen zur Verfügbarkeit ihres Zeitstempeldienstes auf.

5. 7.3 Personalbezogene Sicherheit

- OVR-7.3-02 Das Personal der TSA, 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-7.3-03 Die Einhaltung von OVR-7.3-02 umfasst regelmäßige Aktualisierungen (mindestens alle 12 Monate) im Hinblick auf neue Bedrohungen und aktuelle Sicherheitspraktiken.

<sup>(1)</sup> EN 319 421 — Elektronische Signaturen und Infrastrukturen (ESI) — Policy- und Sicherheitsanforderungen an Vertrauensdiensteanbieter, die Zeitstempel ausgeben, V1.3.1.

<sup>(2)</sup> EN 319 422 — Elektronische Signaturen und Infrastrukturen (ESI) — Zeitstempel-Protokoll und Zeitstempel-Token-Profile, V1.1.1 (2016-03), [https://www.etsi.org/deliver/etsi\\_en/319400\\_319499/319422/01.01.01\\_60/en\\_319422v010101p.pdf](https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf).

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

<sup>(4)</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>(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).

## 6. 7.6.2 Schlüsselerzeugung mit der Zeitstempereinheit (TSU)

- TIS-7.6.2-03 Die Erzeugung des/der TSU-Schlüssel(s) erfolgt innerhalb eines sicheren Kryptomoduls, 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 [3] 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 [10][11], und mit EAL 4 oder höher zertifiziert, oder
  - c) bis 31.12.2030, FIPS PUB 140-3 [7] 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[10][11]-Zertifizierung, so ist dieses Modul entsprechend dieser Zertifizierung zu konfigurieren und zu verwenden.

- TIS-7.6.2-04 ungültig.
- ANMERKUNG 3 ungültig.
- TIS-7.6.2-05A Der TSU-Schlüsselerzeugungsalgorithmus, die erzeugte Signierschlüssellänge und der Signaturalgorithmus, die für die Unterzeichnung von Zeitstempeln bzw. für die Unterzeichnung von TSU-Public-Key-Zertifikaten verwendet werden, müssen den von der Europäischen Gruppe für die Cybersicherheitszertifizierung [9] gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen.
- ANMERKUNG 4 ungültig.
- TIS-7.6.2-06 Ein TSU-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. 7.6.3 Schutz privater TSU-Schlüssel

- TIS-7.6.3-02 Der private TSU-Schlüssel wird 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 [3] 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
  - b) dem auf den Gemeinsamen Kriterien beruhenden europäischen System für die Cybersicherheitszertifizierung (EUCC) [10][11], und mit EAL 4 oder höher zertifiziert, oder
  - c) bis 31.12.2030, FIPS PUB 140-3 [7] 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[10][11]-Zertifizierung, so ist dieses Modul entsprechend dieser Zertifizierung zu konfigurieren und zu verwenden.

- TIS-7.6.3-03 ungültig.
- ANMERKUNG 2 ungültig.

8. 7.6.7 Ende des Lebenszyklus des TSU-Schlüssels
    - TIS-7.6.7-03A Das Ablaufdatum für private TSU-Schlüssel muss den Vereinbarten kryptografischen Mechanismen [9] entsprechen.
    - ANMERKUNG 1 ungültig.
  9. 7.10 Netzsicherheit
    - OVR-7.10-05 Der in REQ-7.8-13 der Norm ETSI EN 319 401 [1] geforderte Schwachstellen-Scan ist mindestens einmal pro Quartal durchzuführen.
    - OVR-7.10-06 Der in REQ-7.8-17X der Norm ETSI EN 319 401 [1] geforderte Penetrationstest ist mindestens einmal pro Jahr durchzuführen.
    - OVR-7.10-07 Firewalls sind so zu konfigurieren, dass alle Protokolle und Zugänge, die nicht für den Betrieb der TSA erforderlich sind, verhindert werden.
  10. 7.14 TSA-Beendigung und -Beendigungspläne
    - OVR-7.14-01A Der Beendigungsplan des TSP muss den Anforderungen entsprechen, die in den gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 [i.4] erlassenen Durchführungsrechtsakten festgelegt sind.
2. Für ETSI EN 319 422
    1. 2.1 Normative Verweise
      - [5] ungültig.
      - [6] ungültig.
      - [8] Europäische Gruppe für die Cybersicherheitszertifizierung, Untergruppe für Kryptografie: „Agreed Cryptographic Mechanisms“ (Vereinbarte kryptografische Mechanismen).
      - [9] RFC 9110 HTTP-Semantik.
    2. 4.1.3 Zu verwendende Hash-Algorithmen
      - Dabei gilt die folgende Klausel:

Hash-Algorithmen, die verwendet werden, um aus den mit einem Zeitstempel zu versendenden Informationen einen Hashwert zu erzeugen, die erwartete Dauer des Zeitstempels und der ausgewählten Hash-Funktionen im Laufe der Zeit, müssen den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [8].
      - ANMERKUNG ungültig.
    3. 4.2.3 Zu unterstützende Algorithmen
      - Dabei gilt die folgende Klausel:

Die zu unterstützenden Zeitstempel-Token-Signaturalgorithmen müssen den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [8].
      - ANMERKUNG ungültig.
    4. 4.2.4 Zu unterstützende Schlüssellängen
      - Dabei gilt die folgende Klausel:

Die Schlüssellängen des Signaturalgorithmus müssen für den ausgewählten Signaturalgorithmus den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen.
      - ANMERKUNG ungültig.

5. 5.1.3 Zu unterstützende Algorithmen
  - Dabei gilt die folgende Klausel:

Hash-Algorithmen für die zu unterstützenden Zeitstempeldaten, die erwartete Dauer des Zeitstempels und der ausgewählten Hash-Funktionen im Laufe der Zeit müssen den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [8].
  - ANMERKUNG ungültig.
6. 5.2.3 Zu verwendende Algorithmen
  - Dabei gilt die folgende Klausel:

Hash-Algorithmen, die verwendet werden, um aus den mit einem Zeitstempel zu versendenden Informationen einen Hashwert zu erzeugen, und Zeitstempel-Token-Signaturalgorithmen müssen den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [8].
  - ANMERKUNG ungültig.
7. 6.3 Anforderungen an die Schlüssellängen
  - Dabei gilt die folgende Klausel:

Die Schlüssellänge des Signaturalgorithmus des TSU-Zertifikats muss den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [8].
  - ANMERKUNG ungültig.
8. 6.5 Anforderungen an die Algorithmen
  - Dabei gilt die folgende Klausel:

Der TSU-Public-Key und die TSU-Zertifikatsignatur müssen Algorithmen verwenden, die den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [8].
  - ANMERKUNG ungültig.
9. 7. Zu unterstützende Profile für die Transportprotokolle
  - Der Zeitstempel-Client und der Zeitstempel-Server müssen das Zeitstempelprotokoll über HTTPS [9] gemäß der Definition in Abschnitt 3.4 von IETF RFC 3161 [1] unterstützen.
10. 8. Objektbezeichner der kryptografischen Algorithmen
  - Dabei gilt die folgende Klausel:

Der TSU-Public-Key und die TSU-Zertifikatsignatur müssen Algorithmen verwenden, die den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [8].
11. 9.1 Erklärung der Einhaltung der Verordnung
  - Wird ein Zeitstempel-Token von der TSA als qualifizierter elektronischer Zeitstempel gemäß der Verordnung (EU) Nr. 910/2014 [i.2] angegeben, so muss er eine qcStatements-Erweiterung im Erweiterungsfeld des Zeitstempel-Tokens mit der Syntax gemäß IETF RFC 3739 [i.3] Abschnitt 3.2.6 enthalten.
  - Die qcStatements-Erweiterung muss eine Angabe „esi4-qtstStatement-1“ gemäß Anhang B enthalten.
  - Die qcStatements-Erweiterung darf nicht als kritisch gekennzeichnet sein.