



DURCHFÜHRUNGSVERORDNUNG (EU) 2025/1566 DER KOMMISSION

vom 29. Juli 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 die Überprüfung der Identität und der Attribute der Person, der das qualifizierte Zertifikat oder die qualifizierte elektronische Attributsbescheinigung ausgestellt werden soll

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 24 Absatz 1c,

in Erwägung nachstehender Gründe:

- (1) Nach Artikel 24 der Verordnung (EU) Nr. 910/2014 müssen qualifizierte Vertrauensdiensteanbieter die Identität und gegebenenfalls spezifische Attribute einer natürlichen oder juristischen Person überprüfen, bevor sie ihr qualifizierte Zertifikate oder qualifizierte elektronische Attributsbescheinigungen ausstellen.
- (2) Um die Gleichbehandlung und die Vertrauenswürdigkeit des Ergebnisses des Überprüfungsprozesses zu gewährleisten, sollten die Überprüfungen bei der Ausstellung eines qualifizierten Zertifikats oder einer qualifizierten elektronischen Attributsbescheinigung von allen qualifizierten Vertrauensdiensteanbietern in gleicher Weise durchgeführt werden. Im Einklang mit den Zielen der Verordnung (EU) Nr. 910/2014 wurde eine Reihe von Standards bzw. Normen ausgewählt, um diese spezifischen Anforderungen zu erfüllen. 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 zu gewährleisten und gleichzeitig die grenzüberschreitende Interoperabilität und das wirksame Funktionieren des Binnenmarkts zu erleichtern.
- (3) Es sollte ein angemessener Übergangszeitraum für qualifizierte Vertrauensdiensteanbieter vorgesehen werden, damit sie die Anforderungen der Verordnung (EU) Nr. 910/2014 erfüllen können. Um einen ausreichenden Zeitrahmen einzuräumen, damit bei den Vertrauensdiensteanbietern die Einhaltung der Anforderungen dieser Verordnung geprüft werden kann, sollte die Anwendung dieser Verordnung 24 Monate nach ihrem Inkrafttreten beginnen.
- (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.
- (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.

⁽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>).

⁽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>).

- (6) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ⁽⁷⁾ angehört und gab am 6. Juni 2025 seine Stellungnahme ab.
- (7) Die in dieser 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 24 Absatz 1c 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 gilt ab dem 19. August 2027.

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

Brüssel, den 29. Juli 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

⁽⁷⁾ 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

Referenzstandard für die Überprüfung der Identität und der Attribute von Personen, denen ein qualifiziertes Zertifikat oder eine qualifizierte elektronische Attributsbescheinigung ausgestellt werden soll

Für die Konformität mit Anhang C Abschnitt C.3 gilt die Norm ETSI TS 119461 V2.1.1 (2025-02) mit den folgenden Anpassungen:

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. C.3 Anwendungsfälle für die Ausstellung qualifizierter Zertifikate oder qualifizierter elektronischer Attributsbescheinigungen gemäß Artikel 24 Absätze 1, 1a und 1b der Verordnung (EU) Nr. 910/2014
 - [BEDINGT] QTS-C3-01: Falls eine Identitätsüberprüfung für ein qualifiziertes Zertifikat oder eine qualifizierte elektronische Bescheinigung in Verbindung mit einer Identitätsüberprüfung zur Ausstellung eines verbindlichen Nachweises erfolgt, so muss dieser Identitätsüberprüfungsprozess
 - von einer akkreditierten Konformitätsbewertungsstelle einer gegenseitigen Begutachtung unterzogen oder zertifiziert worden sein, um die Anforderungen der Sicherheitsstufe „hoch“ gemäß der Verordnung (EU) Nr. 910/2014 zu erfüllen, oder
 - die Anforderungen der Abschnitte C3.1 bis C3.6 erfüllen.
3. C.3.4 Anwendungsfall für den Identitätsnachweis mit anderen Identifizierungsmitteln
 - QTS-C.3.4-06A: Die in Abschnitt [BEDINGT] QTS-C.3.4-06 Buchstabe c genannte unabhängige Konformitätsbewertungsstelle muss gemäß Artikel 3 Nummer 18 der Verordnung (EU) Nr. 910/2014 akkreditiert sein, und die Bewertung sollte — wenn alle geltenden Anforderungen erfüllt sind — zu einer Konformitätsbescheinigung auf der Grundlage einer Zertifizierungsprüfung führen. Dieser förmliche Zertifizierungsprozess muss auf einem Sicherheitsbewertungsprozess beruhen, der sich auf die Sicherheitsstufen bezieht, die für notifizierte elektronische Identifizierungsmittel oder zertifizierte europäische Brieffaschen für die digitale Identität gemäß der Verordnung (EU) Nr. 910/2014 festgelegt wurden, und strenge Tests zur Bewertung der Widerstandsfähigkeit gegen potenzielle Sicherheitsbedrohungen vorsehen. Bei diesen Bewertungen werden einschlägige technische Standards angewandt, um die Robustheit gegenüber solchen Angriffen nachzuweisen.
4. 9.2.3.4 Anwendungsfall für den automatisierten Betrieb
 - USE-9.2.3.4-04: Der Identitätsnachweisdiensteanbieter (IPSP) legt Zielwerte für die Falschakzeptanzrate (FAR) und die Falschrückweisungsrate (FRR) auf der Grundlage einer Risikoanalyse und seines Bedrohungsanalyseverfahrens fest und befolgt dabei in vollständig automatisierten Identitätsnachweisprozessen die im ENISA-Bericht „Methodology for sectoral cybersecurity assessments“ (Methodik für sektorale Cybersicherheitsbewertungen) [i.28] festgelegte Methodik oder eine gleichwertige Methodik. Diese Zielwerte dürfen die für Hybrid-Anwendungsfälle festgelegten Werte, sofern vorhanden, nicht übersteigen. Der IPSP hält diese Zielwerte für die FAR und die FRR konsequent aufrecht und stützt sich dabei auf eine Risikoanalyse und sein Bedrohungsanalyseverfahren.
5. 8.3.3 Validierung eines physischen Identitätsdokuments
 - VAL-8.3.3-21: Die Wirksamkeit der Maßnahmen zur Erfüllung der Anforderungen VAL-8.3.3-05X, VAL-8.3.3-05A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07A und VAL-8.3.3-07X wird von einem akkreditierten Laboratorium oder einer zuständigen nationalen Behörde, sofern eine solche benannt worden ist, spätestens bis zum 19. August 2027 und danach alle zwei Jahre getestet.
6. 7.12 Beendigung und Beendigungspläne
 - OVR-7.12-02: Der Beendigungsplan muss den Anforderungen entsprechen, die in den gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten festgelegt sind.