Amtsblatt
der Europäischen Union

DE
Reihe L

2026/1735

22.7.2026

DURCHFÜHRUNGSVERORDNUNG (EU) 2026/1735 DER KOMMISSION

vom 15. Juli 2026

zur Änderung der Durchführungsverordnung (EU) 2025/1569 in Bezug auf geltende Standards bzw. Normen und Spezifikationen

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 45d Absatz 5, Artikel 45e Absatz 2, Artikel 45f Absätze 6 und 7,

in Erwägung nachstehender Gründe:

(1) Um ein Höchstmaß an Harmonisierung zwischen den Mitgliedstaaten bei der Entwicklung europäischer Brieftaschen für die digitale Identität zu gewährleisten, beruhen die technischen Spezifikationen für die Brieftaschen auf den Arbeiten, die auf Grundlage der Empfehlung (EU) 2021/946 der Kommission ([2]) durchgeführt wurden, insbesondere auf der Architektur und dem Referenzrahmen. Da sich die Architektur und der Referenzrahmen seit der Annahme der Durchführungsverordnung (EU) 2025/1569 ([3]) der Kommission erheblich weiterentwickelt haben, sollte die Durchführungsverordnung (EU) 2025/1569 nun geändert werden, um sie an die neuen Standards bzw. Normen und Spezifikationen anzupassen.

(2) Im Einklang mit den Zielen der Verordnung (EU) Nr. 910/2014 wurde eine Reihe von Standards bzw. Normen ausgewählt, um die für die Ausstellung, Verwaltung und Überprüfung elektronischer Attributsbescheinigungen geltenden Anforderungen zu erfüllen. Diese Standards bzw. Normen sollten bewährte Verfahren widerspiegeln und in den betreffenden Sektoren weithin anerkannt sein. Diese Standards bzw. Normen sollten erforderlichenfalls angepasst oder ergänzt werden, um ein hohes Maß an Sicherheit und Integrität elektronischer Attributsbescheinigungen zu gewährleisten und gleichzeitig die grenzübergreifende Interoperabilität und das wirksame Funktionieren des Binnenmarkts zu fördern. Im Einklang mit diesem Ziel werden mit dieser Verordnung die für die Ausstellung und den Widerruf qualifizierter elektronischer Attributsbescheinigungen sowie elektronischer Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, geltenden Anforderungen für die Unterzeichnung und Besiegelung von Überprüfungsergebnissen anhand authentischer Quellen aktualisiert.

(3) Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([4]) und, sofern anwendbar, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([5]) gelten für jede 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]) Empfehlung (EU) 2021/946 der Kommission vom 3. Juni 2021 für ein gemeinsames Instrumentarium der Union für ein koordiniertes Herangehen an einen Rahmen für die europäische digitale Identität (ABl. L 210 vom 14.6.2021, S. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Durchführungsverordnung (EU) 2025/1569 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 qualifizierte elektronische Attributsbescheinigungen und von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen bereitgestellte elektronische Attributsbescheinigungen (ABl. L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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).

([5]) 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).

(4) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([6]) angehört und gab am 17. April 2026 seine Stellungnahme ab ([7]).

(5) 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

Änderung der Durchführungsverordnung (EU) 2025/1569

Die Durchführungsverordnung (EU) 2025/1569 wird wie folgt geändert:

1. Artikel 3 Absatz 2 erhält folgende Fassung:

„(2) Stellen Anbieter qualifizierter elektronischer Attributsbescheinigungen und Anbieter elektronischer Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, elektronische Attributsbescheinigungen aus, die in Regelungen enthalten sind, die im Katalog der Attributsbescheinigungsregelungen registriert sind, so müssen sie die Anforderungen der entsprechenden Attributsbescheinigungsregelung einhalten. Konzepte und Verfahren, die von den Ausstellern von Bescheinigungen festgelegt werden, um die Anforderungen an Attributsbescheinigungsregelungen einzuhalten, sind Teil der Konformitätsbewertung gemäß der Verordnung (EU) Nr. 910/2014."

2. Artikel 4 wird wie folgt geändert:

a) Absatz 1 wird gestrichen.

b) Absatz 3 erhält folgende Fassung:

„(3) Anbieter qualifizierter elektronischer Attributsbescheinigungen und Anbieter elektronischer Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, widerrufen solche Bescheinigungen – sofern diese mit einer Gültigkeitsdauer von über 24 Stunden ausgestellt werden – zumindest unter den folgenden Umständen:

a) auf Verlangen der Person, der die elektronische Attributsbescheinigung ausgestellt wurde, oder gegebenenfalls der Person, auf die sich die Bescheinigung bezieht;

b) wenn der Anbieter Kenntnis davon erlangt, dass die Sicherheit oder Vertrauenswürdigkeit der qualifizierten elektronischen Attributsbescheinigungen oder der elektronischen Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, beeinträchtigt ist;

c) in anderen Fällen, wenn dies nach Unionsrecht oder nationalem Recht erforderlich ist."

c) Absatz 4 erhält folgende Fassung:

„(4) Anbieter qualifizierter elektronischer Attributsbescheinigungen und Anbieter elektronischer Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, richten Techniken und Verwaltungsmethoden für Widerrufe ein, die die Privatsphäre gewährleisten und eine Verknüpfbarkeit und Rückverfolgbarkeit verhindern. Die Techniken für Widerrufe entsprechen den in Anhang II festgelegten Anforderungen."

([6]) 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).

([7]) EDPS Formal comments on the draft Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties | Europäischer Datenschutzbeauftragter.

3. Artikel 9 wird wie folgt geändert:

   a) Nach Absatz 2 wird folgender Absatz 2a eingefügt:

   „(2a) Der Überprüfungsmechanismus entspricht den in Anhang IV festgelegten Spezifikationen."

   b) Absatz 4 erhält folgende Fassung:

   „(4) Im Ergebnis der Überprüfung wird angegeben, ob das Attribut bestätigt wurde oder nicht, sowie die für die authentische Quelle zuständige öffentliche Stelle oder gegebenenfalls die öffentliche Stelle, die benannt wurde, um im Namen der authentischen Quelle zu handeln, anhand der das Attribut überprüft wurde.

   Die Überprüfungsergebnisse werden von der für eine authentische Quelle zuständigen öffentlichen Stelle oder vom auf nationaler Ebene anerkannten benannten Vermittler mit zumindest einer fortgeschrittenen elektronischen Signatur, die auf einem qualifizierten Zertifikat für elektronische Signaturen beruht, bzw. einem fortgeschrittenen elektronischen Siegel, das auf einem qualifizierten Zertifikat für elektronische Siegel beruht, unterzeichnet bzw. besiegelt."

4. Anhang I erhält die Fassung des Anhangs I der vorliegenden Verordnung.

5. Anhang II erhält die Fassung des Anhangs II der vorliegenden Verordnung.

6. Der Wortlaut von Anhang III der vorliegenden Verordnung wird als Anhang IV angefügt.

Artikel 2

Inkrafttreten

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

Artikel 1 Absatz 3 gilt ab dem 1. Januar 2027.

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

Brüssel, den 15. Juli 2026

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG I

„ANHANG I

Liste der Referenzstandards und Spezifikationen gemäß Artikel 3

ETSI TS 119 471 V1.1.1 (2025-05) mit den folgenden Anpassungen:

(1) 2.1 Normative references (Normative Verweise):

[1] ETSI EN 319 401 V3.2.1 (2026-01): Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers (Elektronische Signaturen und Infrastrukturen (ESI) – Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter);

[2] 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] FIPS PUB 140-3 (2019) – Security Requirements for Cryptographic Modules (Sicherheitsanforderungen an kryptografische Module);

[4] Durchführungsverordnung (EU) 2024/482 der Kommission ([1]);

[5] Durchführungsverordnung (EU) 2024/3144 der Kommission ([2]);

[6] ISO/IEC 15408:2022 (Teile 1 bis 5): Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Evaluationskriterien für IT-Sicherheit.

(2) 3.1 Terms (Begriffe):

Der folgende Begriff wird angefügt:

— 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) 4. EAA trust services (EAA-Vertrauensdienste)

— Abschnitt 4.2.2.2 „Verification of attributes against authentic sources" (Überprüfung von Attributen anhand authentischer Quellen) findet keine Anwendung.

— REQ-EAASP-4.2.2.3-02: Der EAASP authentifiziert sich gegenüber der EUDI-Brieftascheninstanz mithilfe der Mechanismen zur gegenseitigen Authentifizierung unter Verwendung eines gültigen Zugriffszertifikats.

— REQ-EAASP-4.2.2.3-03: Der EAASP validiert die EUDI-Einzelbrieftasche und prüft, ob die EUDI-Brieftascheninstanz widerrufen wurde.

— Abschnitt 4.3.2 „EUDIW Specific" (Speziell für EUDI-Brieftaschen) findet keine Anwendung.

(4) 6.1 EAAS practice statement (EAAS-Praxiserklärung):

— REQ-EAASP-6.1-02: Der EAASP dokumentiert den Widerrufsmechanismus in der EAAS-Praxiserklärung.

(5) 6.3 Information security policy (Informationssicherheitsregelung):

— REQ-EAASP-6.3-02: Der EAASP legt im Einklang mit den Geschäftsanforderungen und den einschlägigen Rechts- und Verwaltungsvorschriften, auch den Anforderungen der gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 erlassenen Durchführungsrechtsakte, Verfahren zur Unterrichtung der Aufsichtsstelle über Änderungen bei der Erbringung des Vertrauensdienstes für die elektronische Attributsbescheinigung und über die beabsichtigte Einstellung dieser Tätigkeiten fest. Der EAASP unterrichtet die zuständige Aufsichtsstelle davon zumindest

  — einen Monat vor der Durchführung einer Änderung,

  — drei Monate vor der geplanten Einstellung der Erbringung eines Vertrauensdienstes.

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

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

(6) 7.5 Cryptographic controls (Kryptografische Kontrollen):

— REQ-EAASP-7.5.2-05: ungültig

— REQ-EAASP-7.5.2-06: ungültig

— REQ-EAASP-7.5.3-01A: Es bestehen angemessene Sicherheitskontrollen in Bezug auf die Verwaltung kryptografischer Schlüssel, kryptografischer Algorithmen und kryptografischer Geräte während ihres gesamten Lebenszyklus, soweit angemessen nach einem Krypto-Agilitätsansatz.

— REQ-EAASP-7.5.3-01B: Der EAASP muss geeignete Algorithmen auswählen und verwenden, die den von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [2].

— REQ-EAASP-7.5.3-02: Der EAASP stellt sicher, dass das von ihm für digitale Signaturen oder Siegel eines EEA verwendete sichere Kryptomodul eine qualifizierte Signatur- oder Siegelerstellungseinheit ist und dass alle anderen digitalen Signaturen oder Siegel, die zur Erbringung des entsprechenden Vertrauensdienstes für die elektronische Attributsbescheinigung oder eines Teils davon verwendet werden, mithilfe eines sicheren Kryptomoduls erstellt werden, bei der es sich um ein vertrauenswürdiges System handelt, das zertifiziert ist gemäß

a) den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit, nämlich gemäß den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit Version 3.1 (CC3.1, bis zum 31.8.2027) oder 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), oder gemäß der Norm ISO/IEC 15408 [6], 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), [4][5], und mit EAL 4 oder höher zertifiziert, oder

c) FIPS-140-2 Stufe 3 (bis zum 31.8.2027 für bestehende zertifizierte Systeme) oder FIPS PUB 140-3 [3] Stufe 3 (bis zum 31.12.2030).

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[4][5]-Zertifizierung, so ist dieses Modul entsprechend dieser Zertifizierung zu konfigurieren und zu verwenden.

— REQ-EAASP-7.5.5-01: ungültig

— REQ-EAASP-7.5.5-02: ungültig

— REQ-EAASP-7.5.5-04: ungültig

(7) 7.9 Vulnerabilities and Incident management (Schwachstellen und Management von Vorfällen):

— REQ-EAASP-7.9-02: Überwachungstätigkeiten tragen der Sensibilität aller erfassten oder analysierten Informationen Rechnung.

(8) 7.12 EAASP and EAAS termination and termination plans (EAASP- und EAAS-Beendigung und -Beendigungspläne):

— REQ-EAASP-7.12-04: Der Beendigungsplan des EAASP muss den Anforderungen entsprechen, die in den gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten festgelegt sind.“

ANHANG II

„ANHANG II

Technische Spezifikationen gemäß Artikel 3 und Artikel 4

Die Anbieter qualifizierter elektronischer Attributsbescheinigungen und die Anbieter elektronischer Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, stellen ihre Bescheinigungen im Einklang mit zumindest einer der in Anhang II der Durchführungsverordnung (EU) 2024/2979 der Kommission ([1]) aufgeführten Normen aus und wenden die ebenfalls in Anhang II der Durchführungsverordnung (EU) 2024/2979 aufgeführten einschlägigen Techniken für Widerrufe an.“

([1]) Durchführungsverordnung (EU) 2024/2979 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Integrität und die Kernfunktionen europäischer Brieftaschen für die digitale Identität (ABl. L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

ANHANG III

„ANHANG IV

Liste der Standards bzw. Normen und technischen Spezifikationen gemäß Artikel 9

Die in Artikel 9 genannten Überprüfungsmechanismen entsprechen einer oder beiden der folgenden Spezifikationen mit den folgenden Anpassungen:

a) technische Spezifikationen in Abschnitt 6.1.1 der Norm ETSI TS 119 478 V1.1.1 (2026-01) – Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources (Elektronische Signaturen und Vertrauensinfrastrukturen (ESI); Spezifikation von Schnittstellen zu authentischen Quellen);

— REQ-ASIP-6.1.1.2-04-01 [BEDINGT]: Entspricht das attributeVerificationResult entweder http://uri.etsi.org/19478/VerificationResult/Match oder http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, so kann das attributeVerificationResult ein attributeValue-Element enthalten.

— REQ-ASIP-6.1.1.2-04-02 [BEDINGT]: Entspricht das zurückgesendete attributeVerificationResult http://uri.etsi.org/19478/VerificationResult/Match und enthält das attributeVerificationResult ein attributeValue-Element, so muss das attributeValue-Element den in der Abfrage angegebenen Wert enthalten.

— REQ-ASIP-6.1.1.2-04-03 [BEDINGT]: Entspricht das zurückgesendete attributeVerificationResult http://uri.etsi.org/19478/VerificationResult/MatchWithVariation und enthält das attributeVerificationResult ein attributeValue-Element, so muss das attributeValue-Element den in der authentischen Quelle gespeicherten Attributswert enthalten.

— REQ-ASIP-6.1.1.2-06-04-01 [BEDINGT]: Entspricht das fragmentVerificationResult entweder http://uri.etsi.org/19478/VerificationResult/Match oder http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, so kann das attributeVerificationResult ein fragmentValue-Element enthalten.

— REQ-ASIP-6.1.1.2-06-04-02 [BEDINGT]: Entspricht das zurückgesendete fragmentVerificationResult http://uri.etsi.org/19478/VerificationResult/Match und enthält das attributeVerificationResult ein fragmentValue-Element, so muss das fragmentValue-Element den in der Abfrage angegebenen Wert enthalten.

— REQ-ASIP-6.1.1.2-06-04-03 [BEDINGT]: Entspricht das zurückgesendete fragmentVerificationResult http://uri.etsi.org/19478/VerificationResult/MatchWithVariation und enthält das attributeVerificationResult ein fragmentValue-Element, so muss das fragmentValue-Element den in der authentischen Quelle gespeicherten Wert des Fragments des Attributs enthalten.

b) technische Spezifikationen in Abschnitt 6.2.3 der Norm ETSI TS 119 478 V1.1.1 (2026-01) – Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources (Elektronische Signaturen und Vertrauensinfrastrukturen (ESI); Spezifikation von Schnittstellen zu authentischen Quellen).

— REQ-ASIP-6.2.3.2.1-08-04: Das AttributeVerificationResponse-Element kann genau ein Kindelement des Typs TextValue, XMLValue oder AttributeProperties enthalten.“