Amtsblatt
der Europäischen Union

DE
Reihe L

2025/1944

30.9.2025

DURCHFÜHRUNGSVERORDNUNG (EU) 2025/1944 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 Referenzstandards für Prozesse des Absendens und Empfangens von Daten in qualifizierten Diensten für die Zustellung elektronischer Einschreiben und in Bezug auf die Interoperabilität dieser Dienste

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 44 Absatz 2 und Artikel 44 Absatz 2b,

in Erwägung nachstehender Gründe:

(1) Qualifizierte Dienste für die Zustellung elektronischer Einschreiben bieten einen sicheren Kanal für die Übermittlung von Dokumenten mit dem Nachweis der Absendung und des Empfangs der Daten. Sie sollen für Gewissheit bei der Identifizierung des Empfängers sorgen und ein hohes Maß an Vertrauenswürdigkeit bei der Identifizierung des Absenders gewährleisten.

(2) Die Konformitätsvermutung gemäß Artikel 44 Absatz 1a der Verordnung (EU) Nr. 910/2014 sollte nur gelten, wenn qualifizierte Vertrauensdienste, die Dienste für die Zustellung elektronischer Einschreiben erbringen, 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 des qualifizierten Vertrauensdienstes zu gewährleisten.

(3) Erfüllt ein Vertrauensdiensteanbieter die in Anhang I 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) Nach Artikel 44 Absatz 2a der Verordnung (EU) Nr. 910/2014 ist es wichtig, dass qualifizierte Vertrauensdiensteanbieter, die zustimmen, ihre Dienste interoperabel zu machen, die in Anhang II der vorliegenden Durchführungsverordnung festgelegten geeigneten Normen bzw. Standards und Spezifikationen einhalten, um Daten leicht als elektronische Einschreiben zwischen zwei oder mehr qualifizierten Vertrauensdiensteanbietern zu übertragen und faire Verfahren im Binnenmarkt zu fördern.

(5) 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).

(6) 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 jede Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung.

(7) 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.

(8) 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 für qualifizierte Dienste für die Zustellung elektronischer Einschreiben

Die in Artikel 44 Absatz 2 der Verordnung (EU) Nr. 910/2014 genannten Referenzstandards und Spezifikationen sind in Anhang I der vorliegenden Verordnung festgelegt.

Artikel 2

Referenzstandards und Spezifikationen für die Interoperabilität zwischen qualifizierten Diensten für die Zustellung elektronischer Einschreiben

Die in Artikel 44 Absatz 2b der Verordnung (EU) Nr. 910/2014 genannten Referenzstandards und Spezifikationen sind in Anhang II der vorliegenden Verordnung festgelegt.

Artikel 3

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 I

Liste der Referenzstandards und Spezifikationen gemäß Artikel 1

Die Norm ETSI EN 319 521 V1.1.1 (2019-02) („ETSI EN 319 521“) gilt mit den folgenden Anpassungen:

1. Für ETSI EN 319 521

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 EN 319 411-1 V1.5.1 (2025-04) — Elektronische Signaturen und Infrastrukturen (ESI) — Regelungs- und Sicherheitsanforderungen an Vertrauensdiensteanbieter, die Zertifikate ausgeben — Teil 1: Allgemeine Anforderungen.

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) — Elektronische Signaturen und Infrastrukturen (ESI) — Dienste für die Zustellung elektronischer Einschreiben — Teil 1: Struktur und Aufbau.

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) — Elektronische Signaturen und Infrastrukturen (ESI) — Dienste für die Zustellung elektronischer Einschreiben — Teil 2: Semantische Inhalte.

— [5] Europäische Gruppe für die Cybersicherheitszertifizierung, Untergruppe für Kryptografie: „Agreed Cryptographic Mechanisms“ (Vereinbarte kryptografische Mechanismen), veröffentlicht von der Agentur der Europäischen Union für Cybersicherheit („ENISA“) ([1]).

— [6] ISO/IEC 15408-1:2022 — Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit.

— [7] Durchführungsverordnung (EU) 2024/482 der Kommission ([2]) 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] Durchführungsverordnung (EU) 2024/3144 der Kommission ([3]) zur Änderung der Durchführungsverordnung (EU) 2024/482 in Bezug auf geltende internationale Normen und zur Berichtigung der Durchführungsverordnung.

— [9] FIPS PUB 140-3 (2019) — Sicherheitsanforderungen an kryptografische Module.

2) 3.1 Begriffe

— fortgeschrittenes elektronisches Siegel: im Sinne der Verordnung (EU) Nr. 910/2014 [i.1];

— fortgeschrittene elektronische Signatur: im Sinne der Verordnung (EU) Nr. 910/2014 [i.1];

— qualifiziertes elektronisches Siegel: im Sinne der Verordnung (EU) Nr. 910/2014 [i.1];

— qualifizierte elektronische Signatur: im Sinne der Verordnung (EU) Nr. 910/2014 [i.1];

— 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.

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) ABl. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) ABl. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

3) 5.1.1 Gemeinsame Bestimmungen

— REQ-ERDS-5.1.1-01 Der Dienst für die Zustellung elektronischer Einschreiben (ERDS) muss die Verfügbarkeit, Integrität und Vertraulichkeit der Nutzerinhalte während der Bearbeitung durch den ERDS angemessen gewährleisten, wozu geeignete kryptografische Techniken für die Wahrung der Integrität und Vertraulichkeit zu wählen sind, die den von der Europäischen Gruppe für Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen [5] entsprechen.

4) 5.2.1.1 Allgemeines

— REQ-QERDS-5.2.1.1-01 Der Anbieter des qualifizierten Dienstes für die Zustellung elektronischer Einschreiben (QERDSP) muss mit einem sehr hohen Maß an Vertrauen die Identität des Empfängers entweder unmittelbar oder unter Rückgriff auf einen Dritten und gegebenenfalls unter Verwendung eines der folgenden Mittel oder einer Kombination daraus überprüfen:

a) durch die physische Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person nach geeigneten Nachweisen und Verfahren im Einklang mit dem nationalen Recht;

b) aus der Ferne mit einem elektronischen Identifizierungsmittel, das die Anforderungen des Artikels 8 der Verordnung (EU) Nr. 910/2014 [i.1] in Bezug auf das Sicherheitsniveau „hoch“ erfüllt, oder mit der europäischen Brieftasche für die digitale Identität;

c) mit einem Zertifikat einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels;

d) mit anderen Identifizierungsmethoden, die gewährleisten, dass die natürliche Person oder der bevollmächtigte Vertreter der juristischen Person mit einem sehr hohen Maß an Vertrauen identifiziert werden kann. Die Sicherheit, dass diese Identifizierung mit einem sehr hohen Maß an Vertrauen erfolgt, wird von einer Konformitätsbewertungsstelle bestätigt.

— REQ-QERDS-5.2.1.1-01A Der Anbieter des qualifizierten Dienstes für die Zustellung elektronischer Einschreiben (QERDSP) muss die Identität des Absenders mit geeigneten Mitteln entweder unmittelbar oder unter Rückgriff auf einen Dritten mit einer der folgenden Methoden oder einer Kombination davon überprüfen:

a) durch die physische Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person nach geeigneten Nachweisen und Verfahren im Einklang mit dem nationalen Recht;

b) aus der Ferne mit der europäischen Brieftasche für die digitale Identität oder einem notifizierten elektronischen Identifizierungsmittel, das die Anforderungen des Artikels 8 der Verordnung (EU) Nr. 910/2014 [i.1] in Bezug auf das Sicherheitsniveau „substanziell“ erfüllt, sofern es auf der Grundlage der vorherigen physischen Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person ausgestellt wurde;

c) mit einem Zertifikat einer fortgeschrittenen elektronischen Signatur oder eines fortgeschrittenen elektronischen Siegels, sofern das Zertifikat der natürlichen Person oder einem bevollmächtigten Vertreter der juristischen Person im Rahmen einer normierten Zertifizierungsregelung (NCP) gemäß der Norm ETSI EN 319 411-1 [2] ausgestellt wurde, oder

d) mit anderen Identifizierungsmethoden, die gewährleisten, dass die natürliche Person oder der bevollmächtigte Vertreter der juristischen Person mit einem sehr hohen Maß an Vertrauen identifiziert werden kann. Die Sicherheit, dass diese Identifizierung mit einem hohen Maß an Vertrauen erfolgt, wird von einer Konformitätsbewertungsstelle bestätigt.

— ANMERKUNG Der Dritte, der die Identität des Absenders und des Empfängers überprüft, kann ein anderer QERDSP sein, wenn Absender und Empfänger verschiedene QERDSP in Anspruch nehmen.

5) 5.2.1.2 Identifizierung des Empfängers und Übergabe der Nutzerinhalte

— REQ-QERDS-5.2.1.2-03 Wenn die Identifizierung des Empfängers auf einem internen Verfahren des QERDS beruht, muss der QERDSP den gesamten Prozess in einer gesicherten und kontrollierten Umgebung durchführen.

6) 5.2.2 Bestimmungen für die EU-QERDS-Authentifizierung

— REQ-QERDS-5.2.2-03 [BEDINGT] Wenn der QERDSP Authentifizierungsmittel mit einer gemäß Abschnitt 5.2.1 überprüften Absenderidentität verknüpft, muss es sich dabei um eines der Folgenden handeln:

a) Zwei-Faktor-Authentifizierungsmechanismen;

b) europäische Brieftasche für die digitale Identität oder notifiziertes elektronisches Identifizierungsmittel, das die Anforderungen des Artikels 8 der Verordnung (EU) Nr. 910/2014 [i.1] hinsichtlich der Sicherheitsniveaus „hoch“ oder „substanziell“ erfüllt;

c) gegenseitige TLS-Authentifizierung, einschließlich des Zertifikats, das dem Absender im Rahmen einer NCP gemäß ETSI EN 319 411-1 [2] ausgestellt wurde;

d) digitale Signatur gestützt auf ein Zertifikat, das im Rahmen einer NCP gemäß ETSI EN 319 411-1 [2] ausgestellt wurde;

e) andere Mittel, die die Authentifizierung des identifizierten Absenders gewährleisten. Die Konformität der Verknüpfung wird von einer Konformitätsbewertungsstelle bestätigt. Beispiel: Ein in den Buchstaben a, b und d genanntes Mittel wird verwendet, um ein TLS-Client-Zertifikat für eine automatisierte Übermittlung mit gegenseitiger TLS-Authentifizierung zu registrieren oder um ein zur Besiegelung von Nachweisen beim ERDS verwendetes digitales Siegelzertifikat zu registrieren. Andere Mechanismen, bei denen die identifizierten Absender auf Dienste zurückgreifen, die an Dritte delegiert wurden, können ebenfalls verwendet werden.

— REQ-QERDS-5.2.2-03A [BEDINGT] Wenn der QERDSP Authentifizierungsmittel mit einer gemäß Abschnitt 5.2.1 überprüften Empfängeridentität verknüpft, muss es sich dabei um eines der Folgenden handeln, sofern die Mittel oder eine Kombination davon ein sehr hohes Maß an Vertrauen in die Identität des authentifizierten Empfängers gewährleisten:

a) Multifaktor-Authentifizierungsmechanismus;

b) europäische Brieftasche für die digitale Identität oder notifiziertes elektronisches Identifizierungsmittel, das die Anforderungen des Artikels 8 der Verordnung (EU) Nr. 910/2014 [i.1] hinsichtlich der Sicherheitsniveaus „hoch“ oder „substanziell“ erfüllt;

c) Zertifikat einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels;

d) andere Mittel, die die Authentifizierung des identifizierten Empfängers gewährleisten. Die Konformität der Verknüpfung wird von einer Konformitätsbewertungsstelle bestätigt. Beispiel: Ein in den Buchstaben a bis c genanntes Mittel wird verwendet, um ein TLS-Client-Zertifikat für eine automatisierte Übermittlung mit gegenseitiger TLS-Authentifizierung zu registrieren oder um ein zur Besiegelung von Nachweisen beim ERDS verwendetes digitales Siegelzertifikat zu registrieren. Andere Mechanismen, bei denen die identifizierten Absender auf Dienste zurückgreifen, die an Dritte delegiert wurden, können ebenfalls verwendet werden.

— REQ-QERDS-5.2.2-04 [BEDINGT] Wenn der Absender eine Verbindung zum QERDS über eine gesicherte Verbindung herstellt, die eine gegenseitige Maschine-Maschine-Authentifizierung zwischen dem Gerät des Absenders und dem Server des QERDS mit Zertifikaten erfordert, die im Rahmen einer NCP gemäß ETSI EN 319 411-1 [2] ausgestellt wurden, können nach der Herstellung dieser gesicherten Verbindung in einer zweiten Phase der Absenderauthentifizierung Einfaktor-Authentifizierungsmechanismen verwendet werden, sofern die eingerichteten organisatorischen Verfahren und Sicherheitsmaßnahmen das Vertrauen in die Authentifizierung des Absenders gewährleisten.

7) 5.4.1 Gemeinsame Bestimmungen

— REQ-ERDS-5.4.1-06 Der ERDS muss ERDS-Nachweise über ERD-Vorgänge gemäß der Definition in Abschnitt 6 der Norm ETSI EN 319 522-1 [3] erzeugen und den berechtigten interessierten Parteien zur Verfügung stellen.

— REQ-ERDS-5.4.1-07 Der ERDSP muss den Nachweis und/oder Nachweiszusammenfassungen für jeden von ihm ausgestellten Nachweis archivieren.

— REQ-ERDS-5.4.1-08 Die vom ERDS erzeugten ERDS-Nachweise müssen den in Abschnitt 8 der Norm ETSI EN 319 522-2 [4] definierten Nachweisen entsprechen.

8) 7.2.1 Gemeinsame Bestimmungen

— REQ-ERDS-7.2.1-02 Das Personal des ERDSP, das Vertrauensaufgaben wahrnimmt, muss die Anforderung an „Fachkenntnisse, Erfahrung und Qualifikationen" durch formale Schulungen und Befähigungsnachweise oder tatsächliche Erfahrung oder eine Kombination aus beiden erfüllen können.

— REQ-ERDS-7.2.1-03 Die Einhaltung von REQ-ERDS-7.2.1-02 umfasst regelmäßige Aktualisierungen (mindestens alle 12 Monate) im Hinblick auf neue Bedrohungen und aktuelle Sicherheitspraktiken.

9) 7.3.2 Umgang mit Medien

— REQ-ERDS-7.3.1-02 Es gelten alle Anforderungen der Norm ETSI EN 319 401 [1] Abschnitt 7.3.3.

10) 7.5 Kryptografische Kontrollen

— REQ-ERDS-7.5-01A Der ERDS muss geeignete Algorithmen auswählen und verwenden, die den von der Europäischen Gruppe für Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen entsprechen [5].

— REQ-ERDSP-7.5-03 Der private ERDS-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 [6] 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) [7][8], und mit EAL 4 oder höher zertifiziert, oder

c) bis 31.12.2030, FIPS PUB 140-3 [9] 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][8]-Zertifizierung, so ist dieses Modul entsprechend dieser Zertifizierung zu konfigurieren und zu verwenden.

11) 7.8 Netzsicherheit

— REQ-ERDSP-7.8-04 Der ERDSP verwendet modernste Protokolle und Algorithmen für die Verschlüsselung in der Transportschicht, die den von der Europäischen Gruppe für Cybersicherheitszertifizierung gebilligten und von der ENISA veröffentlichten Vereinbarten kryptografischen Mechanismen [5] entsprechen.

— REQ-ERDSP-7.8-06 Der in REQ-7.8-13 der Norm ETSI EN 319 401 [1] geforderte Schwachstellen-Scan ist mindestens einmal pro Quartal durchzuführen.

— REQ-ERDSP-7.8-07 Der in REQ-7.8-17X der Norm ETSI EN 319 401 [1] geforderte Penetrationstest ist mindestens einmal pro Jahr durchzuführen.

— REQ-ERDSP-7.8-08 Firewalls sind so zu konfigurieren, dass alle Protokolle und Zugänge, die nicht für den Betrieb des Vertrauensdiensteanbieters (TSP) erforderlich sind, verhindert werden.

12) 7.12 ERDSP-Beendigung und ERDS-Beendigungspläne

— REQ-ERDS-7.12-03 Der Beendigungsplan des ERDSP muss den Anforderungen entsprechen, die in den gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten festgelegt sind.

13) 7.14 Lieferkette

— REQ-ERDS-7.14-01 Es gelten die Anforderungen der Norm ETSI EN 319 401 [1] Abschnitt 7.14.

ANHANG II

Liste der Referenzstandards und Spezifikationen gemäß Artikel 2

Es gelten die Normen ETSI EN 319 522-1 V1.2.1 (2024-01) („ETSI EN 319 522-1“), ETSI EN 319 522-2 V1.2.1 (2024-01) („ETSI EN 319 522-2“), ETSI EN 319 522-3 V1.2.1 (2024-01) („ETSI EN 319 522-3“), ETSI EN 319 522-4-1 V1.2.1 (2019-01) („ETSI EN 319 522-4-1“), ETSI EN 319 522-4-2 V1.1.1 (2018-09) („ETSI EN 319 522-4-2“) und ETSI EN 319 522-4-3 V1.1.1 (2018-09) („ETSI EN 319 522-4-3“).