Amtsblatt der Europäischen Union

L 235

Ausgabe in deutscher Sprache

Rechtsvorschriften

58. Jahrgang

9. September 2015

Inhalt

II *Rechtsakte ohne Gesetzescharakter*

VERORDNUNGEN

★ **Durchführungsverordnung (EU) 2015/1501 der Kommission vom 8. September 2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt** [1] 1

★ **Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt** [1] 7

Durchführungsverordnung (EU) 2015/1503 der Kommission vom 8. September 2015 zur Festlegung pauschaler Einfuhrwerte für die Bestimmung der für bestimmtes Obst und Gemüse geltenden Einfuhrpreise 21

BESCHLÜSSE

★ **Durchführungsbeschluss (EU) 2015/1504 der Kommission vom 7. September 2015 zur Gewährung von Ausnahmen für bestimmte Mitgliedstaaten bezüglich der Bereitstellung von Statistiken gemäß der Verordnung (EG) Nr. 1099/2008 des Europäischen Parlaments und des Rates über die Energiestatistik** *(Bekanntgegeben unter Aktenzeichen C(2015) 6105)* [1] 24

★ **Durchführungsbeschluss (EU) 2015/1505 der Kommission vom 8. September 2015 über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten gemäß Artikel 22 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt** [1] 26

[1] Text von Bedeutung für den EWR

DE

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.

Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.

★ **Durchführungsbeschluss (EU) 2015/1506 der Kommission vom 8. September 2015 zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt anerkannt werden** [1] 37

[1] Text von Bedeutung für den EWR

II

(Rechtsakte ohne Gesetzescharakter)

VERORDNUNGEN

DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1501 DER KOMMISSION

vom 8. September 2015

über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

(Text von Bedeutung für den EWR)

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 12 Absatz 8,

in Erwägung nachstehender Gründe:

(1) Nach Artikel 12 Absatz 2 der Verordnung (EU) Nr. 910/2014 soll ein Interoperabilitätsrahmen geschaffen werden, um die Interoperabilität der nach Artikel 9 Absatz 1 der Verordnung notifizierten elektronischen Identifizierungssysteme herzustellen.

(2) Bei der Zusammenschaltung der elektronischen Identifizierungssysteme der Mitgliedstaaten kommt Knoten eine zentrale Rolle zu. Ihr Beitrag wird in der Dokumentation zu der durch die Verordnung (EU) Nr. 1316/2013 des Europäischen Parlaments und des Rates ([2]) geschaffenen Fazilität „Connecting Europe" erläutert, in der auch auf die Funktionen und Bestandteile des „eIDAS-Knotens" eingegangen wird.

(3) Stellt ein Mitgliedstaat oder die Kommission Software bereit, welche die Authentifizierung bei einem in einem anderen Mitgliedstaat betriebenen Knoten ermöglicht, kann derjenige, der die zur Authentifizierung eingesetzte Software liefert und aktualisiert, mit demjenigen, der das Hosting der Software übernimmt, eine Vereinbarung darüber schließen, wie der Betrieb des Authentifizierungsvorgangs verwaltet werden soll. Eine derartige Vereinbarung sollte dem Hosting-Betreiber keine überzogenen technischen Anforderungen auferlegen bzw. übermäßige Kosten verursachen (einschließlich Unterstützungs-, Haftungs-, Hosting- und sonstige Kosten).

(4) Soweit die Umsetzung des Interoperabilitätsrahmens es rechtfertigt, könnte die Kommission in Zusammenarbeit mit den Mitgliedstaaten weitere technische Spezifikationen mit Einzelheiten zu in dieser Verordnung festgelegten technischen Anforderungen ausarbeiten, insbesondere unter Berücksichtigung von Stellungnahmen des in Artikel 14 Buchstabe d des Durchführungsbeschlusses (EU) 2015/296 der Kommission ([3]) genannten Kooperationsnetzes. Solche Spezifikationen sollten entwickelt werden als Teil der digitalen Diensteinfrastrukturen entsprechend der Verordnung (EU) Nr. 1316/2013, in der die Mittel für die praktische Umsetzung eines Moduls für die elektronische Identifizierung vorgegeben werden.

([1]) ABl. L 257 vom 28.8.2014, S. 73.

([2]) Verordnung (EU) Nr. 1316/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 zur Schaffung der Fazilität „Connecting Europe", zur Änderung der Verordnung (EU) Nr. 913/2010 und zur Aufhebung der Verordnungen (EG) Nr. 680/2007 und (EG) Nr. 67/2010 (ABl. L 348 vom 20.12.2013, S. 129).

([3]) Durchführungsbeschluss (EU) 2015/296 der Kommission vom 24. Februar 2015 zur Festlegung von Verfahrensmodalitäten für die Zusammenarbeit zwischen den Mitgliedstaaten auf dem Gebiet der elektronischen Identifizierung gemäß Artikel 12 Absatz 7 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (ABl. L 53 vom 25.2.2015, S. 14).

(5) Die in dieser Verordnung festgelegten technischen Anforderungen sollten ungeachtet etwaiger Änderungen der technischen Spezifikationen gelten, die gemäß Artikel 12 dieser Verordnung entwickelt werden können.

(6) Das Großpilotprojekt STORK und die dort entwickelten Spezifikationen wie auch die Grundsätze und Begriffe des Europäischen Interoperabilitätsrahmens für öffentliche Dienste haben bei der Aufstellung der Regelungen für den durch diese Verordnung geschaffenen Interoperabilitätsrahmen die größtmögliche Berücksichtigung gefunden.

(7) Die Ergebnisse der Zusammenarbeit zwischen den Mitgliedstaaten wurden weitestgehend berücksichtigt.

(8) 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

Gegenstand

Diese Verordnung enthält technische und betriebliche Anforderungen für den Interoperabilitätsrahmen, durch die die Interoperabilität der elektronischen Identifizierungssysteme, die der Kommission von den Mitgliedstaaten notifiziert werden, gewährleistet werden soll.

Diese Anforderungen betreffen insbesondere

a) die technischen Mindestanforderungen an die Sicherheitsniveaus und die Entsprechung zwischen nationalen Sicherheitsniveaus notifizierter elektronischer Identifizierungsmittel, die nach einem notifizierten elektronischen Identifizierungssystem nach Artikel 8 der Verordnung (EU) Nr. 910/2014 ausgestellt wurden, gemäß den Artikeln 3 und 4;

b) die technischen Mindestanforderungen für die Interoperabilität gemäß den Artikeln 5 bis 8;

c) den Mindestsatz der Personenidentifizierungsdaten, die eine natürliche oder juristische Person eindeutig repräsentieren, gemäß Artikel 11 und dem Anhang;

d) gemeinsame Sicherheitsnormen für den Betrieb gemäß den Artikeln 6, 7, 9 und 10;

e) Regelungen zur Streitbeilegung gemäß Artikel 13.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten die folgenden Begriffsbestimmungen:

1. „Knoten“ ist ein Anschlusspunkt, der als Teil der Interoperabilitätsarchitektur für die elektronische Identifizierung an der grenzüberschreitenden Authentifizierung von Personen mitwirkt und der Datenübertragungen erkennen und verarbeiten oder an andere Knoten weiterleiten kann; er ermöglicht damit über eine Schnittstelle die Verbindung zwischen der nationalen elektronischen Identifizierungsinfrastruktur eines Mitgliedstaats und der nationalen elektronischen Identifizierungsinfrastruktur eines anderen Mitgliedstaats;

2. „Knotenbetreiber“ ist die Stelle, die dafür verantwortlich ist, dass der Knoten seine Funktion als Anschlusspunkt ordnungsgemäß und zuverlässig erfüllt.

Artikel 3

Technische Mindestanforderungen an die Sicherheitsniveaus

Die technischen Mindestanforderungen an die Sicherheitsniveaus werden in der Durchführungsverordnung (EU) 2015/1502 der Kommission ([1]) festgelegt.

Artikel 4

Entsprechung zwischen nationalen Sicherheitsniveaus

Die Entsprechung zwischen nationalen Sicherheitsniveaus der notifizierten Identifizierungssysteme richtet sich nach den Anforderungen der Durchführungsverordnung (EU) 2015/1502. Die Entsprechungsergebnisse werden der Kommission anhand des im Durchführungsbeschluss (EU) 2015/1505 der Kommission ([2]) festgelegten Notifizierungsmusters mitgeteilt.

Artikel 5

Knoten

(1) Ein Knoten in einem Mitgliedstaat muss in der Lage sein, sich mit Knoten in anderen Mitgliedstaaten zu verbinden.

(2) Die Knoten müssen in der Lage sein, anhand technischer Mittel zwischen öffentlichen Stellen und anderen vertrauenden Beteiligten zu unterscheiden.

(3) Durch die Umsetzung der in dieser Verordnung festgelegten technischen Anforderungen in einem Mitgliedstaat dürfen anderen Mitgliedstaaten, um mit dem in jenem Mitgliedstaat umgesetzten System zusammenwirken zu können, keine überzogenen technischen Anforderungen bzw. übermäßigen Kosten auferlegt bzw. verursacht werden.

Artikel 6

Datenschutz und Vertraulichkeit

(1) Der Schutz der Privatsphäre und der Vertraulichkeit der ausgetauschten Daten sowie die Erhaltung der Unversehrtheit der Daten zwischen den Knoten werden durch den Einsatz der besten verfügbaren technischen Lösungen und Schutzverfahren sichergestellt.

(2) Außer zu dem in Artikel 9 Absatz 3 genannten Zweck dürfen die Knoten keine personenbezogenen Daten speichern.

Artikel 7

Unversehrtheit und Echtheit der Daten bei der Übermittlung

Bei der Datenübermittlung wird die Unversehrtheit und Echtheit der Daten gewährleistet, um sicherzustellen, dass alle Abfragen und Antworten echt sind und nicht verfälscht worden sind. Zu diesem Zweck setzen die Knoten Lösungen ein, die sich im grenzüberschreitenden Betrieb bereits bewährt haben.

([1]) Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (siehe Seite 7 dieses Amtsblatts).

([2]) Durchführungsbeschluss (EU) 2015/1505 der Kommission vom 8. September 2015 über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten gemäß Artikel 22 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (siehe Seite 26 dieses Amtsblatts).

Artikel 8

Meldungsformat für die Übermittlung

Die Knoten verwenden als Syntax gemeinsame Meldungsformate, die auf Normen beruhen, welche bereits mehrfach zwischen Mitgliedstaaten eingesetzt worden sind und sich im Betriebsumfeld bewährt haben. Die Syntax muss Folgendes ermöglichen:

a) ordnungsgemäße Verarbeitung des Mindestsatzes von Personenidentifizierungsdaten, die eine natürliche oder juristische Person eindeutig repräsentieren;

b) ordnungsgemäße Verarbeitung der Sicherheitsniveaus der elektronischen Identifizierungsmittel;

c) Unterscheidung zwischen öffentlichen Stellen und anderen vertrauenden Beteiligten;

d) Flexibilität im Falle eines Bedarfs an zusätzlichen Merkmalen für die Identifizierung.

Artikel 9

Verwaltung von Sicherheitsinformationen und Metadaten

(1) Der Knotenbetreiber übermittelt die Metadaten der Knotenverwaltung in genormter maschinenlesbarer Form auf sichere und vertrauenswürdige Weise.

(2) Zumindest die sicherheitsbezogenen Parameter werden automatisch abgerufen.

(3) Der Knotenbetreiber speichert Daten, mit denen im Falle eines Vorfalls die Abfolge des Meldungsaustauschs rekonstruiert werden kann, damit Ort und Art des Vorfalls festgestellt werden können. Die Daten werden für einen Zeitraum gespeichert, der im Einklang mit nationalen Vorgaben steht, und müssen zumindest folgende Elemente umfassen:

a) Kennung des Knotens;

b) Kennung der Meldung;

c) Datum und Uhrzeit der Meldung.

Artikel 10

Informationssicherheit und Sicherheitsnormen

(1) Knotenbetreiber von Knoten, die eine Authentifizierung vornehmen, müssen durch Zertifizierung oder ein gleichwertiges Bewertungsverfahren oder durch Einhaltung nationaler Rechtsvorschriften nachweisen, dass ihr Knoten im Hinblick auf die am Interoperabilitätsrahmen beteiligten Knoten die Anforderungen der Norm ISO/IEC 27001 erfüllt.

(2) Knotenbetreiber führen sicherheitskritische Aktualisierungen unverzüglich durch.

Artikel 11

Personenidentifizierungsdaten

(1) Wird ein Mindestsatz von Personenidentifizierungsdaten, die eine natürliche oder juristische Person eindeutig repräsentieren, in einem grenzüberschreitenden Umfeld verwendet, so muss er den Anforderungen des Anhangs entsprechen.

(2) Wird ein Mindestdatensatz einer natürlichen Person, die eine juristische Person repräsentiert, in einem grenzüberschreitenden Umfeld verwendet, so muss er die Kombination der Merkmale enthalten, die im Anhang für natürliche und juristische Personen aufgeführt sind.

(3) Die Datenübertragung erfolgt in den Original-Schriftzeichen sowie gegebenenfalls transliteriert in lateinischen Schriftzeichen.

Artikel 12

Technische Spezifikationen

(1) Soweit der Prozess der Umsetzung des Interoperabilitätsrahmens es rechtfertigt, kann das durch den Durchführungsbeschluss (EU) 2015/296 der Kommission geschaffene Kooperationsnetz Stellungnahmen gemäß Artikel 14 Buchstabe d des genannten Beschlusses bezüglich des Bedarfs der Ausarbeitung technischer Spezifikationen abgeben. In solchen technischen Spezifikationen werden weitere Einzelheiten zu den technischen Anforderungen dieser Verordnung festgelegt.

(2) Aufgrund der in Absatz 1 genannten Stellungnahme arbeitet die Kommission in Zusammenarbeit mit den Mitgliedstaaten die technischen Spezifikationen als Teil der digitalen Diensteinfrastrukturen der Verordnung (EU) Nr. 1316/2013 aus.

(3) Das Kooperationsnetz gibt eine Stellungnahme gemäß Artikel 14 Buchstabe d des Durchführungsbeschlusses (EU) 2015/296 ab, in der es beurteilt, ob und in welchem Maße die gemäß Absatz 2 ausgearbeiteten technischen Spezifikationen dem in der Stellungnahme nach Absatz 1 festgestellten Bedarf oder den Anforderungen dieser Verordnung entsprechen. Es kann den Mitgliedstaaten empfehlen, die technischen Spezifikationen bei der Umsetzung des Interoperabilitätsrahmens zu berücksichtigen.

(4) Die Kommission stellt eine Referenzimplementierung als Beispiel für die Auslegung der technischen Spezifikationen bereit. Die Mitgliedstaaten können diese Referenzimplementierung anwenden oder sie als Muster zur Erprobung anderer Implementierungen der technischen Spezifikationen verwenden.

Artikel 13

Streitbeilegung

(1) Soweit möglich, werden Streitigkeiten in Bezug auf den Interoperabilitätsrahmen von den betroffenen Mitgliedstaaten auf dem Verhandlungsweg beigelegt.

(2) Wird keine Lösung gemäß Absatz 1 gefunden, ist das durch Artikel 12 des Durchführungsbeschlusses (EU) 2015/296 geschaffene Kooperationsnetz im Einklang mit seiner Geschäftsordnung für die Beilegung des Streits zuständig.

Artikel 14

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 8. September 2015

Für die Kommission

Der Präsident

Jean-Claude JUNCKER

ANHANG

Anforderungen an den Mindestsatz von Personenidentifizierungsdaten, die eine natürliche oder juristische Person eindeutig repräsentieren, gemäß Artikel 11

1. **Mindestdatensatz einer natürlichen Person**

Der Mindestdatensatz einer natürlichen Person muss alle folgenden obligatorischen Merkmale enthalten:

a) derzeitige(r) Familienname(n),

b) derzeitige(r) Vorname(n),

c) Geburtsdatum,

d) eine eindeutige Kennung, die vom übermittelnden Mitgliedstaat entsprechend den technischen Spezifikationen für die Zwecke der grenzüberschreitenden Identifizierung erstellt wurde und möglichst dauerhaft fortbesteht.

Der Mindestdatensatz einer natürlichen Person kann eines oder mehrere der folgenden zusätzlichen Merkmale enthalten:

a) Vorname(n) und Familienname(n) bei der Geburt,

b) Geburtsort,

c) derzeitige Anschrift,

d) Geschlecht.

2. **Mindestdatensatz einer juristischen Person**

Der Mindestdatensatz einer juristischen Person muss alle folgenden obligatorischen Merkmale enthalten:

a) derzeitige amtliche Bezeichnung,

b) eine eindeutige Kennung, die vom übermittelnden Mitgliedstaat entsprechend den technischen Spezifikationen für die Zwecke der grenzüberschreitenden Identifizierung erstellt wurde und möglichst dauerhaft fortbesteht.

Der Mindestdatensatz einer juristischen Person kann eines oder mehrere der folgenden zusätzlichen Merkmale enthalten:

a) derzeitige Anschrift,

b) Umsatzsteuer-Identifikationsnummer,

c) Steuerregisternummer,

d) Kennnummer in Bezug auf Artikel 3 Absatz 1 der Richtlinie 2009/101/EG des Europäischen Parlaments und des Rates ([1]),

e) Kennziffer der juristischen Person (LEI) gemäß der Durchführungsverordnung (EU) Nr. 1247/2012 der Kommission ([2]);

f) Registrierungs- und Identifizierungsnummer des Wirtschaftsbeteiligten (EORI-Nr.) gemäß der Durchführungsverordnung (EU) Nr. 1352/2013 der Kommission ([3]);

g) Verbrauchsteuernummer gemäß Artikel 2 Absatz 12 der Verordnung (EU) Nr. 389/2012 des Rates ([4]).

([1]) Richtlinie 2009/101/EG des Europäischen Parlaments und des Rates vom 16. September 2009 zur Koordinierung der Schutzbestimmungen, die in den Mitgliedstaaten den Gesellschaften im Sinne des Artikels 48 Absatz 2 des Vertrags im Interesse der Gesellschafter sowie Dritter vorgeschrieben sind, um diese Bestimmungen gleichwertig zu gestalten (ABl. L 258 vom 1.10.2009, S. 11).

([2]) Durchführungsverordnung (EU) Nr. 1247/2012 der Kommission vom 19. Dezember 2012 zur Festlegung technischer Durchführungsstandards im Hinblick auf das Format und die Häufigkeit von Transaktionsmeldungen an Transaktionsregister gemäß der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 352 vom 21.12.2012, S. 20).

([3]) Durchführungsverordnung (EU) Nr. 1352/2013 der Kommission vom 4. Dezember 2013 zur Festlegung der in der Verordnung (EU) Nr. 608/2013 des Europäischen Parlaments und des Rates zur Durchsetzung der Rechte geistigen Eigentums durch die Zollbehörden vorgesehenen Formblätter (ABl. L 341 vom 18.12.2013, S. 10).

([4]) Verordnung (EU) Nr. 389/2012 des Rates vom 2. Mai 2012 über die Zusammenarbeit der Verwaltungsbehörden auf dem Gebiet der Verbrauchsteuern und zur Aufhebung von Verordnung (EG) Nr. 2073/2004 (ABl. L 121 vom 8.5.2012, S. 1).

DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION

vom 8. September 2015

zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

(Text von Bedeutung für den EWR)

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 8 Absatz 3,

in Erwägung nachstehender Gründe:

(1) Laut Artikel 8 der Verordnung (EU) Nr. 910/2014 muss ein gemäß Artikel 9 Absatz 1 notifiziertes elektronisches Identifizierungssystem die Sicherheitsniveaus „niedrig", „substanziell" und/oder „hoch" angeben, die den nach diesem System ausgestellten elektronischen Identifizierungsmitteln zuerkannt wurden.

(2) Die Festlegung von Mindestanforderungen an die technischen Spezifikationen, Normen und Verfahren ist entscheidend, wenn es darum geht, ein gemeinsames Verständnis der Einzelheiten der Sicherheitsniveaus herzustellen und, wie in Artikel 12 Absatz 4 Buchstabe b der Verordnung (EU) Nr. 910/2014 vorgesehen, die Interoperabilität bei der Zuordnung der Entsprechungen zwischen nationalen Sicherheitsniveaus notifizierter elektronischer Identifizierungsmittel und den Sicherheitsniveaus des Artikels 8 zu gewährleisten.

(3) Bei der Ausarbeitung der in dieser Durchführungsverordnung festgelegten Spezifikationen und Verfahren wurde die internationale Norm ISO/IEC 29115 als die wichtigste internationale Norm auf dem Gebiet der Sicherheitsniveaus für elektronische Identifizierungsmittel berücksichtigt. Die Verordnung (EU) Nr. 910/2014 weist jedoch inhaltliche Unterschiede zu dieser internationalen Norm auf, insbesondere im Hinblick auf Anforderungen an Identitätsnachweis und -überprüfung, aber auch in Bezug darauf, wie die Unterschiede zwischen Identitätsvorschriften der Mitgliedstaaten und die diesbezüglich bestehenden EU-Instrumente berücksichtigt werden. Deshalb sollte der Anhang zwar auf dieser internationalen Norm beruhen, aber keine Verweise auf bestimmte Inhalte der Norm ISO/IEC 29115 enthalten.

(4) Diese Verordnung wurde nach einem ergebnisorientierten Ansatz ausgearbeitet, da dieser sich am besten eignete; dies spiegelt sich auch in den in den Begriffsbestimmungen verwendeten Bezeichnungen und Begriffen wider. Diese tragen dem Ziel der Verordnung (EU) Nr. 910/2014 in Bezug auf die Sicherheitsniveaus elektronischer Identifizierungsmittel Rechnung. Daher sollten das Großpilotprojekt STORK und die dort entwickelten Spezifikationen wie auch die Begriffsbestimmungen und Konzepte der Norm ISO/IEC 29115 bei der Festlegung der in dieser Durchführungsverordnung vorgesehenen Spezifikationen und Verfahren weitestgehend berücksichtigt werden.

(5) Je nach dem Zusammenhang, in dem ein bestimmter Aspekt eines Beweismittels für die Identität überprüft werden muss, können verlässliche Quellen viele verschiedene Formen haben, z. B. Register, Urkunden, Stellen usw. Selbst in einem ähnlichen Zusammenhang können solche verlässlichen Quellen in den verschiedenen Mitgliedstaaten sehr unterschiedlich sein.

(6) Anforderungen an Identitätsnachweis und -überprüfung sollten unterschiedliche Systeme und Verfahrensweisen berücksichtigen, gleichzeitig aber eine hinreichend hohe Sicherheit bieten, um das erforderliche Vertrauen zu schaffen. Daher sollte die Anerkennung von Verfahren, die zuvor für andere Zwecke als die Ausstellung elektronischer Identifizierungsmittel verwendet wurden, vom Nachweis abhängig gemacht werden, dass diese Verfahren die für das betreffende Sicherheitsniveau vorgesehenen Anforderungen erfüllen.

([1]) ABl. L 257 vom 28.8.2014, S. 73.

(7) Üblicherweise werden gewisse Authentifizierungsfaktoren wie Geheimnisse, die allen Beteiligten bekannt sind, physische Mittel oder körperliche Merkmale verwendet. Um die Sicherheit des Authentifizierungsprozesses zu erhöhen, sollte jedoch die Verwendung einer größeren Zahl von Authentifizierungsfaktoren, insbesondere auch aus verschiedenen Kategorien, gefördert werden.

(8) Diese Verordnung sollte Vertretungsbefugnisse juristischer Personen unberührt lassen. Der Anhang sollte aber Anforderungen an die Verknüpfung von elektronischen Identifizierungsmitteln natürlicher und juristischer Personen enthalten.

(9) Die Bedeutung von Informationssicherheits- und Dienstemanagementsystemen sollte genauso anerkannt werden wie die Bedeutung der Verwendung bewährter Methoden und der Anwendung der in Normenreihen wie ISO/IEC 27000 und ISO/IEC 20000 verankerten Grundsätze.

(10) In den Mitgliedstaaten angewandte bewährte Verfahren in Bezug auf Sicherheitsniveaus sollten ebenfalls berücksichtigt werden.

(11) Die IT-Sicherheitszertifizierung auf der Grundlage internationaler Normen ist ein wichtiges Instrument, mit dem überprüft werden kann, ob die Sicherheitsmerkmale der Produkte den Anforderungen dieser Durchführungsverordnung entsprechen.

(12) Der in Artikel 48 der Verordnung (EU) Nr. 910/2014 genannte Ausschuss hat innerhalb der von seinem Vorsitz festgelegten Frist keine Stellungnahme abgegeben —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

(1) Die Sicherheitsniveaus „niedrig", „substanziell" und „hoch" für elektronische Identifizierungsmittel, die nach einem notifizierten elektronischen Identifizierungssystem ausgestellt werden, werden unter Bezugnahme auf die Spezifikationen und Verfahren im Anhang bestimmt.

(2) Die im Anhang festgelegten Spezifikationen und Verfahren werden angewandt, um das Sicherheitsniveau der nach einem notifizierten elektronischen Identifizierungssystem ausgestellten elektronischen Identifizierungsmittel anhand der Zuverlässigkeit und Qualität folgender Elemente zu bestimmen:

a) Anmeldung nach Abschnitt 2.1 des Anhangs dieser Verordnung gemäß Artikel 8 Absatz 3 Buchstabe a der Verordnung (EU) Nr. 910/2014;

b) Verwaltung der elektronischen Identifizierungsmittel nach Abschnitt 2.2 des Anhangs dieser Verordnung gemäß Artikel 8 Absatz 3 Buchstaben b und f der Verordnung (EU) Nr. 910/2014;

c) Authentifizierung nach Abschnitt 2.3 des Anhangs dieser Verordnung gemäß Artikel 8 Absatz 3 Buchstabe c der Verordnung (EU) Nr. 910/2014;

d) Management und Organisation nach Abschnitt 2.4 des Anhangs dieser Verordnung gemäß Artikel 8 Absatz 3 Buchstaben d und e der Verordnung (EU) Nr. 910/2014.

(3) Erfüllt ein elektronisches Identifizierungsmittel, das nach einem notifizierten elektronischen Identifizierungssystem ausgestellt wird, eine Anforderung eines höheren Sicherheitsniveaus, so wird davon ausgegangen, dass es die entsprechende Anforderung eines niedrigeren Sicherheitsniveaus ebenfalls erfüllt.

(4) Soweit im betreffenden Teil des Anhangs nichts anderes festgelegt ist, müssen alle Elemente, die im Anhang zu einem bestimmten Sicherheitsniveau der nach einem notifizierten elektronischen Identifizierungssystem ausgestellten elektronischen Identifizierungsmittel aufgeführt sind, erfüllt sein, damit sie dem beanspruchten Sicherheitsniveau entsprechen.

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 8. September 2015

Für die Kommission

Der Präsident

Jean-Claude JUNCKER

ANHANG

Technische Spezifikationen und Verfahren für die Sicherheitsniveaus „niedrig", „substanziell" und „hoch" für elektronische Identifizierungsmittel, die nach einem notifizierten elektronischen Identifizierungssystem ausgestellt werden

1. **Begriffsbestimmungen**

Für die Zwecke dieses Anhangs gelten folgende Begriffsbestimmungen:

1. „Verlässliche Quelle" ist eine beliebige Informationsquelle, die auf verlässliche Weise präzise Daten, Informationen und/oder Beweismittel bereitstellt, die zum Identitätsnachweis verwendet werden können;

2. „Authentifizierungsfaktor" ist ein Element, das nachweislich mit einer Person verknüpft ist und (mindestens) einer der folgenden Kategorien angehört:

   a) „besitzabhängiger Authentifizierungsfaktor" ist ein Authentifizierungsfaktor, dessen Besitz der Nutzer bzw. das Subjekt nachweisen muss;

   b) „kenntnisabhängiger Authentifizierungsfaktor" ist ein Authentifizierungsfaktor, dessen Kenntnis der Nutzer bzw. das Subjekt nachweisen muss;

   c) „inhärenter Authentifizierungsfaktor" ist ein Authentifizierungsfaktor, der auf ein körperliches Merkmal einer natürlichen Person abstellt und bei dem der Nutzer nachweisen muss, dass er dieses körperliche Merkmal hat;

3. „dynamische Authentifizierung" ist ein elektronischer Prozess, der unter Einsatz kryptografischer oder anderer Methoden auf Abruf einen elektronischen Nachweis dafür erzeugt, dass der Benutzer bzw. das Subjekt die Identifizierungsdaten unter seiner Kontrolle hat oder besitzt; der Nachweis ändert sich dabei mit jedem Authentifizierungsvorgang zwischen dem Benutzer/Subjekt und dem System, das die Identität des Subjekts überprüft;

4. „Informationssicherheitsmanagementsystem" ist eine Reihe von Prozessen und Verfahren für das Management annehmbarer Risikostufen in Bezug auf die Informationssicherheit.

2. **Technische Spezifikationen und Verfahren**

Die Elemente technischer Spezifikationen und Verfahren in diesem Anhang werden verwendet um festzulegen, wie die Anforderungen und Kriterien des Artikels 8 der Verordnung (EU) Nr. 910/2014 auf elektronische Identifizierungsmittel, die nach einem notifizierten elektronischen Identifizierungssystem ausgestellt werden, anzuwenden sind.

2.1. *Anmeldung*

2.1.1. Beantragung und Eintragung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es ist gewährleistet, dass der Antragsteller die Geschäftsbedingungen für die Benutzung des elektronischen Identifizierungsmittels kennt. 2. Es ist gewährleistet, dass der Antragsteller die empfohlenen Sicherheitsvorkehrungen im Zusammenhang mit dem elektronischen Identifizierungsmittel kennt. 3. Die einschlägigen Identitätsdaten für den Nachweis und die Überprüfung der Identität werden erfasst.
Substanziell	Wie für das Niveau „Niedrig".
Hoch	Wie für das Niveau „Niedrig".

2.1.2. Identitätsnachweis und -überprüfung (natürliche Person)

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es kann davon ausgegangen werden, dass die Person im Besitz eines Beweismittels ist, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird und die beanspruchte Identität repräsentiert. 2. Es kann davon ausgegangen werden, dass das Beweismittel echt ist oder laut einer verlässlichen Quelle existiert und dass das Beweismittel dem Anschein nach gültig ist. 3. Eine verlässliche Quelle hat Kenntnis davon, dass die beanspruchte Identität existiert und es kann davon ausgegangen werden, dass die Person, die diese Identität beansprucht, damit identisch ist.
Substanziell	Zusätzlich zum Niveau „Niedrig“ muss eine der Alternativen der Nummern 1 bis 4 erfüllt sein: 1. Es ist überprüft worden, dass die Person im Besitz eines Beweismittels ist, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird und die beanspruchte Identität repräsentiert, und das Beweismittel ist geprüft worden, um seine Echtheit festzustellen, oder einer verlässlichen Quelle ist bekannt, dass es existiert und sich auf eine reale Person bezieht, und es wurden Vorkehrungen getroffen, um das Risiko zu mindern, dass die Identität der Person nicht mit der beanspruchten Identität übereinstimmt, z. B. im Hinblick auf verlorene, gestohlene, ausgesetzte, widerrufene oder abgelaufene Beweismittel. ODER 2. Ein Identitätsdokument wird im Rahmen eines Registrierungsverfahrens in dem Mitgliedstaat, in dem es ausgestellt wurde, vorgelegt und bezieht sich dem Anschein nach auf die Person, die es vorlegt, und es wurden Vorkehrungen getroffen, um das Risiko zu mindern, dass die Identität der Person nicht mit der beanspruchten Identität übereinstimmt, z. B. im Hinblick auf verlorene, gestohlene, ausgesetzte, widerrufene oder abgelaufene Dokumente. ODER 3. Bieten Verfahren, die zuvor von einer öffentlichen oder privaten Stelle in demselben Mitgliedstaat für andere Zwecke als die Ausstellung elektronischer Identifizierungsmittel verwendet wurden, eine gleichwertige Sicherheit, die der des Niveaus „Substanziell“ in Abschnitt 2.1.2 entspricht, so braucht die für die Registrierung zuständige Stelle solche früheren Verfahren nicht zu wiederholen, sofern die gleichwertige Sicherheit von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates ([1]) oder von einer gleichwertigen Stelle bestätigt wird. ODER 4. Werden elektronische Identifizierungsmittel aufgrund eines gültigen notifizierten elektronischen Identifizierungsmittels des Sicherheitsniveaus „Substanziell“ oder „Hoch“ und unter Berücksichtigung des Risikos einer Änderung der Personenidentifizierungsdaten ausgestellt, so brauchen die Prozesse für den Nachweis und die Überprüfung der Identität nicht wiederholt zu werden. Wurde das zugrunde gelegte elektronische Identifizierungsmittel nicht notifiziert, so muss das Sicherheitsniveau „Substanziell“ oder „Hoch“ von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt werden.

Sicherheitsniveau	Erforderliche Elemente
Hoch	Es müssen entweder die Anforderungen der Nummer 1 oder der Nummer 2 erfüllt sein: 1. Zusätzlich zum Niveau „Substanziell“ muss eine der Alternativen der Buchstaben a bis c erfüllt sein: a) Ist überprüft worden, dass die Person im Besitz eines mit Foto oder biometrischen Merkmalen versehenen Identitätsnachweises ist, der von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird, und dass der Identitätsnachweis die beanspruchte Identität repräsentiert, so wird das Beweismittel geprüft, um festzustellen, ob es laut einer verlässlichen Quelle gültig ist, und anhand des Vergleichs eines oder mehrerer körperlicher Merkmale der Person mit Angaben aus einer verlässlichen Quelle wird festgestellt, dass der Antragsteller mit der beanspruchten Identität übereinstimmt. ODER b) Bieten Verfahren, die zuvor von einer öffentlichen oder privaten Stelle in demselben Mitgliedstaat für andere Zwecke als die Ausstellung elektronischer Identifizierungsmittel verwendet wurden, eine gleichwertige Sicherheit, die der des Niveaus „Hoch“ in Abschnitt 2.1.2 entspricht, so braucht die für die Registrierung zuständige Stelle solche früheren Verfahren nicht zu wiederholen, sofern die gleichwertige Sicherheit von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt wird, und es werden Schritte unternommen, um zu belegen, dass die Ergebnisse der früheren Verfahren noch gültig sind. ODER c) Werden elektronische Identifizierungsmittel aufgrund eines gültigen notifizierten elektronischen Identifizierungsmittels des Sicherheitsniveaus „Hoch“ und unter Berücksichtigung des Risikos einer Änderung der Personenidentifizierungsdaten ausgestellt, so brauchen die Prozesse für den Nachweis und die Überprüfung der Identität nicht wiederholt zu werden. Wurde das zugrunde gelegte elektronische Identifizierungsmittel nicht notifiziert, so muss das Sicherheitsniveau „Hoch“ von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt werden, und es werden Schritte unternommen, um zu belegen, dass die Ergebnisse des früheren Verfahrens zur Ausstellung eines notifizierten elektronischen Identifizierungsmittels noch gültig sind. ODER 2. Legt der Antragsteller keinen anerkannten, mit Foto oder biometrischen Merkmalen versehenen Identitätsnachweis vor, so werden exakt dieselben Verfahren angewandt, die auf nationaler Ebene in dem Mitgliedstaat, zu dem die für die Registrierung zuständige Stelle gehört, erforderlich sind, um einen solchen anerkannten, mit Foto oder biometrischen Merkmalen versehenen Identitätsnachweis zu erlangen.

(1) Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).

2.1.3. Identitätsnachweis und -überprüfung (juristische Person)

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Die beanspruchte Identität der juristischen Person wird anhand eines Beweismittels nachgewiesen, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird.

Sicherheitsniveau	Erforderliche Elemente
	2. Das Beweismittel ist dem Anschein nach gültig und es kann davon ausgegangen werden, dass es echt ist oder laut einer verlässlichen Quelle existiert, sofern die Aufnahme einer juristischen Person in die verlässliche Quelle freiwillig und durch eine Vereinbarung zwischen der juristischen Person und der verlässlichen Quelle geregelt ist. 3. Die verlässliche Quelle hat keine Kenntnis davon, dass sich die juristische Person in einer Lage befindet, in der sie daran gehindert wäre, als diese juristische Person zu handeln.
Substanziell	Zusätzlich zum Niveau „Niedrig" muss eine der Alternativen der Nummern 1 bis 3 erfüllt sein: 1. Die beanspruchte Identität der juristischen Person wird anhand eines Beweismittels nachgewiesen, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird und aus dem der Name, die Rechtsform und gegebenenfalls die Registriernummer der juristischen Person hervorgehen, und das Beweismittel ist geprüft worden, um festzustellen, ob es echt ist oder laut einer verlässlichen Quelle existiert, sofern die Aufnahme der juristischen Person in die verlässliche Quelle für die Tätigkeit in ihrem Sektor erforderlich ist, und es wurden Vorkehrungen getroffen, um das Risiko zu mindern, dass die Identität der juristischen Person nicht mit der beanspruchten Identität übereinstimmt, z. B. im Hinblick auf verlorene, gestohlene, ausgesetzte, widerrufene oder abgelaufene Dokumente. ODER 2. Bieten die Verfahren, die zuvor von einer öffentlichen oder privaten Stelle in demselben Mitgliedstaat für andere Zwecke als die Ausstellung elektronischer Identifizierungsmittel verwendet wurden, eine gleichwertige Sicherheit, die der des Niveaus „Substanziell" in Abschnitt 2.1.3 entspricht, so braucht die für die Registrierung zuständige Stelle solche früheren Verfahren nicht zu wiederholen, sofern die gleichwertige Sicherheit von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt wird. ODER 3. Werden elektronische Identifizierungsmittel aufgrund eines gültigen notifizierten elektronischen Identifizierungsmittels des Sicherheitsniveaus „Substanziell" oder „Hoch" ausgestellt, so brauchen die Prozesse für den Nachweis und die Überprüfung der Identität nicht wiederholt zu werden. Wurde das zugrunde gelegte elektronische Identifizierungsmittel nicht notifiziert, so muss das Sicherheitsniveau „Substanziell" oder „Hoch" von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt werden.
Hoch	Zusätzlich zum Niveau „Substanziell" muss eine der Alternativen in den Nummern 1 bis 3 erfüllt sein: 1. Die beanspruchte Identität der juristischen Person wird anhand eines Beweismittels nachgewiesen, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird und aus dem der Name und die Rechtsform der juristischen Person sowie zumindest eine eindeutige Kennung, die die juristische im nationalen Umfeld repräsentiert, hervorgeht, und das Beweismittel ist geprüft worden, um festzustellen, ob es laut einer verlässlichen Quelle gültig ist. ODER

Sicherheitsniveau	Erforderliche Elemente
	2. Bieten die Verfahren, die zuvor von einer öffentlichen oder privaten Stelle in demselben Mitgliedstaat für andere Zwecke als die Ausstellung elektronischer Identifizierungsmittel verwendet wurden, eine gleichwertige Sicherheit, die der des Niveaus „Hoch" in Abschnitt 2.1.3 entspricht, so braucht die für die Registrierung zuständige Stelle solche früheren Verfahren nicht zu wiederholen, sofern die gleichwertige Sicherheit von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt wird, und es werden Schritte unternommen, um zu belegen, dass die Ergebnisse dieses früheren Verfahrens noch gültig sind. ODER 3. Werden elektronische Identifizierungsmittel aufgrund eines gültigen notifizierten elektronischen Identifizierungsmittels des Sicherheitsniveaus „Hoch" ausgestellt, so brauchen die Prozesse für den Nachweis und die Überprüfung der Identität nicht wiederholt zu werden. Wurde das zugrunde gelegte elektronische Identifizierungsmittel nicht notifiziert, so muss das Sicherheitsniveau „Hoch" von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt werden, und es werden Schritte unternommen, um zu belegen, dass die Ergebnisse des früheren Verfahrens zur Ausstellung eines notifizierten elektronischen Identifizierungsmittels noch gültig sind.

2.1.4. Verknüpfung von elektronischen Identifizierungsmitteln natürlicher und juristischer Personen

Für die Verknüpfung von elektronischen Identifizierungsmitteln natürlicher Personen und elektronischen Identifizierungsmitteln juristischer Personen („Verknüpfung") gelten, soweit zutreffend, folgende Bedingungen:

1. Es ist möglich, eine Verknüpfung auszusetzen und/oder zu widerrufen. Der Lebenszyklus einer Verknüpfung (z. B. Aktivierung, Aussetzung, Erneuerung, Widerruf) wird nach auf nationaler Ebene anerkannten Verfahren verwaltet.

2. Die natürliche Person, deren elektronisches Identifizierungsmittel mit dem elektronischen Identifizierungsmittel der juristischen Person verknüpft ist, kann die Ausübung der Verknüpfung nach auf nationaler Ebene anerkannten Verfahren an eine andere natürliche Person delegieren. Die delegierende natürliche Person bleibt jedoch verantwortlich.

3. Die Verknüpfung erfolgt auf folgende Weise:

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Der Identitätsnachweis der natürlichen Person, die im Namen der juristischen Person handelt, wird so überprüft, als erfolge er auf dem Niveau „Niedrig" oder höher. 2. Die Verknüpfung ist nach auf nationaler Ebene anerkannten Verfahren hergestellt worden. 3. Die verlässliche Quelle hat keine Kenntnis davon, dass sich die natürliche Person in einer Lage befindet, in der sie daran gehindert wäre, im Namen der juristischen Person zu handeln.
Substanziell	Zusätzlich zu Nummer 3 des Niveaus „Niedrig": 1. Der Identitätsnachweis der natürlichen Person, die im Namen der juristischen Person handelt, wird so überprüft, als erfolge er auf dem Niveau „Substanziell" oder „Hoch".

Sicherheitsniveau	Erforderliche Elemente
	2. Die Verknüpfung ist nach auf nationaler Ebene anerkannten Verfahren hergestellt worden, was zu einer Eintragung der Verknüpfung in einer verlässlichen Quelle geführt hat. 3. Die Verknüpfung ist aufgrund von Informationen einer verlässlichen Quelle überprüft worden.
Hoch	Zusätzlich zu Nummer 3 des Niveaus „Niedrig“ und zu Nummer 2 des Niveaus „Substanziell“: 1. Der Identitätsnachweis der natürlichen Person, die im Namen der juristischen Person handelt, wird so überprüft, als erfolge er auf dem Niveau „Hoch“. 2. Die Verknüpfung ist anhand einer im nationalen Umfeld verwendeten eindeutigen Kennung, die die juristische Person repräsentiert, sowie anhand von Informationen einer verlässlichen Quelle, die die natürliche Person eindeutig repräsentieren, überprüft worden.

2.2. *Verwaltung elektronischer Identifizierungsmittel*

2.2.1. Merkmale und Gestaltung elektronischer Identifizierungsmittel

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Das elektronische Identifizierungsmittel benutzt mindestens einen Authentifizierungsfaktor. 2. Das elektronische Identifizierungsmittel ist so gestaltet, dass der Aussteller zumutbare Vorkehrungen trifft, um zu prüfen, dass es nur unter der Kontrolle oder im Besitz der Person, der es gehört, verwendet wird.
Substanziell	1. Das elektronische Identifizierungsmittel benutzt mindestens zwei Authentifizierungsfaktoren unterschiedlicher Kategorien. 2. Das elektronische Identifizierungsmittel ist so gestaltet, dass davon ausgegangen werden kann, dass es nur unter der Kontrolle oder im Besitz der Person, der es gehört, verwendet wird.
Hoch	Zusätzlich zum Niveau „Substanziell“: 1. Das elektronische Identifizierungsmittel bietet Schutz vor Duplizierung und Fälschung wie auch vor Angreifern mit hohem Angriffspotential. 2. Das elektronische Identifizierungsmittel ist so gestaltet, dass es von der Person, der es gehört, zuverlässig vor einer Benutzung durch andere geschützt werden kann.

2.2.2. Ausstellung, Auslieferung und Aktivierung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	Nach der Ausstellung wird das elektronische Identifizierungsmittel auf eine Weise ausgeliefert, bei der davon ausgegangen werden kann, dass es nur die beabsichtigte Person erreicht.
Substanziell	Nach der Ausstellung wird das elektronische Identifizierungsmittel auf eine Weise ausgeliefert, bei der davon ausgegangen werden kann, dass es nur in den Besitz der Person gelangt, der es gehört.
Hoch	Im Aktivierungsprozess wird geprüft, dass das elektronische Identifizierungsmittel nur in den Besitz der Person gelangt ist, der es gehört.

2.2.3. Aussetzung, Widerruf und Reaktivierung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es ist möglich, ein elektronisches Identifizierungsmittel rasch und wirksam auszusetzen und/oder zu widerrufen. 2. Es bestehen Vorkehrungen, um eine unbefugte Aussetzung, einen unbefugten Widerruf oder eine unbefugte Reaktivierung zu verhindern. 3. Eine Reaktivierung darf nur erfolgen, wenn dieselben Sicherheitsanforderungen wie vor der Aussetzung oder vor dem Widerruf weiterhin erfüllt sind.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.2.4. Verlängerung und Ersetzung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	Unter Berücksichtigung des Risikos einer Änderung der Personenidentifizierungsdaten müssen für die Verlängerung oder Ersetzung dieselben Sicherheitsanforderungen wie beim ursprünglichen Identitätsnachweis- und -überprüfungsprozess erfüllt sein bzw. muss ein gültiges elektronisches Identifizierungsmittel desselben oder eines höheren Sicherheitsniveaus zugrunde gelegt werden.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Zusätzlich zum Niveau „Niedrig“: Erfolgt die Verlängerung oder Ersetzung aufgrund eines gültigen elektronischen Identifizierungsmittels, so werden die Identitätsdaten anhand einer verlässlichen Quelle überprüft.

2.3. *Authentifizierung*

Dieser Abschnitt betrifft die Bedrohungen im Zusammenhang mit der Verwendung der Authentifizierungsmechanismen und enthält Anforderungen an jedes Sicherheitsniveau. In diesem Abschnitt wird davon ausgegangen, dass die Kontrollmaßnahmen den Risiken des jeweiligen Sicherheitsniveaus angemessen sein müssen.

2.3.1. Authentifizierungsmechanismus

Die folgende Tabelle enthält für jedes Sicherheitsniveau die jeweiligen Anforderungen an den Authentifizierungsmechanismus, mit dem die natürliche oder juristische Person das elektronische Identifizierungsmittel verwendet, um einem vertrauenden Beteiligten ihre Identität zu bestätigen.

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Vor einer Herausgabe von Personenidentifizierungsdaten erfolgt eine zuverlässige Überprüfung des elektronischen Identifizierungsmittels und seiner Gültigkeit. 2. Werden Personenidentifizierungsdaten als Teil des Authentifizierungsmechanismus gespeichert, müssen sie gesichert sein, um sie vor Verlust und vor Beeinträchtigung, einschließlich Offline-Analyse, zu schützen. 3. Im Authentifizierungsmechanismus sind Sicherheitskontrollen zur Überprüfung des elektronischen Identifizierungsmittels implementiert, so dass es höchst unwahrscheinlich ist, dass ein Angreifer mit erhöhtem grundlegenden Angriffspotenzial durch Handlungen wie Erraten, Abhören, Replay oder Manipulation der Kommunikation den Authentifizierungsmechanismus aushebeln kann.

Sicherheitsniveau	Erforderliche Elemente
Substanziell	Zusätzlich zum Niveau „Niedrig“: 1. Vor einer Herausgabe von Personenidentifizierungsdaten erfolgt eine zuverlässige Überprüfung des elektronischen Identifizierungsmittels und seiner Gültigkeit durch dynamische Authentifizierung. 2. Im Authentifizierungsmechanismus sind Sicherheitskontrollen zur Überprüfung des elektronischen Identifizierungsmittels implementiert, so dass es höchst unwahrscheinlich ist, dass ein Angreifer mit mäßigem Angriffspotenzial durch Handlungen wie Erraten, Abhören, Replay oder Manipulation der Kommunikation den Authentifizierungsmechanismus aushebeln kann.
Hoch	Zusätzlich zum Niveau „Substanziell“: Im Authentifizierungsmechanismus sind Sicherheitskontrollen zur Überprüfung des elektronischen Identifizierungsmittels implementiert, so dass es höchst unwahrscheinlich ist, dass ein Angreifer mit hohem Angriffspotenzial durch Handlungen wie Erraten, Abhören, Replay oder Manipulation der Kommunikation den Authentifizierungsmechanismus aushebeln kann.

2.4. *Management und Organisation*

Alle Beteiligten, die im Zusammenhang mit der elektronischen Identifizierung im grenzüberschreitenden Umfeld einen Dienst betreiben („Betreiber“) müssen dokumentierte Verfahrensweisen und Vorgaben für das Informationssicherheitsmanagement, Risikomanagementkonzepte und andere anerkannte Kontrollmaßnahmen haben, damit sich die geeigneten Leitungsgremien der elektronischen Identifizierungssysteme in den jeweiligen Mitgliedstaaten vergewissern können, dass wirksame Verfahren bestehen. Im gesamten Abschnitt 2.4 wird davon ausgegangen, dass alle Anforderungen bzw. Elemente den Risiken des jeweiligen Sicherheitsniveaus angemessen sein müssen.

2.4.1. Allgemeine Bestimmungen

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Betreiber, die eine unter diese Verordnung fallende betriebliche Dienstleistung erbringen, sind eine Behörde oder eine juristische Person, die als solche nach den nationalen Rechtsvorschriften eines Mitgliedstaats anerkannt ist, verfügen über eine eingerichtete Organisationsstruktur und sind in allen Teilen, die für die Bereitstellung der Dienste von Bedeutung sind, voll betriebsfähig. 2. Die Betreiber erfüllen alle rechtlichen Anforderungen, die ihnen im Zusammenhang mit dem Betrieb und der Bereitstellung des Dienstes obliegen, unter anderem auch in Bezug darauf, welche Arten von Informationen abgefragt werden können, wie der Identitätsnachweis durchgeführt wird und welche Informationen wie lange aufbewahrt werden dürfen. 3. Die Betreiber können ihre Fähigkeit zur Übernahme des Haftungsrisikos für Schäden nachweisen und verfügen über ausreichende finanzielle Mittel für einen fortlaufenden Betrieb und eine fortlaufende Bereitstellung der Dienste. 4. Die Betreiber sind sowohl für die Erfüllung aller Verpflichtungen, die sie an andere Stellen untervergeben, als auch für die Einhaltung der Systemvorgaben verantwortlich, als würden sie alle Aufgaben selbst wahrnehmen. 5. Elektronische Identifizierungssysteme, die nicht durch nationale Rechtsvorschriften eingerichtet werden, müssen über einen wirksamen Beendigungsplan verfügen. In einem solchen Plan müssen auch eine geordnete Einstellung des Dienstes bzw. die Fortsetzung durch einen anderen Betreiber, die Art und Weise, wie einschlägige Behörden und Endnutzer informiert werden, sowie Einzelheiten dazu geregelt sein, wie Daten in Übereinstimmung mit den Systemvorgaben zu schützen, aufzubewahren bzw. zu zerstören sind.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.2. Veröffentlichte Bekanntmachungen und Benutzerinformationen

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es gibt eine veröffentlichte Definition des Dienstes mit allen geltenden Geschäftsbedingungen und Entgelten sowie möglichen Nutzungsbeschränkungen. Die Definition des Dienstes enthält auch eine Datenschutzerklärung. 2. Es sind geeignete Vorgaben und Verfahren zu schaffen, damit die Benutzer des Dienstes in rascher und verlässlicher Weise informiert werden, wenn sich die Definition des Dienstes selbst, die geltenden Geschäftsbedingungen oder die Datenschutzerklärung in Bezug auf den betreffenden Dienst ändern. 3. Es sind geeignete Vorgaben und Verfahren zu schaffen, damit Auskunftsersuchen vollständig und richtig beantwortet werden.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.3. Informationssicherheitsmanagement

Sicherheitsniveau	Erforderliche Elemente
Niedrig	Es besteht ein wirksames Informationssicherheitsmanagementsystem für das Management und die Beherrschung von Informationssicherheitsrisiken.
Substanziell	Zusätzlich zum Niveau „Niedrig“: Das Informationssicherheitsmanagementsystem folgt bewährten Normen oder Grundsätzen für das Management und die Beherrschung von Informationssicherheitsrisiken.
Hoch	Wie für das Niveau „Substanziell“.

2.4.4. Aufbewahrungspflichten

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Die Aufzeichnung und Aufbewahrung einschlägiger Informationen erfolgt mit einem effektiven Aufzeichnungsverwaltungssystem unter Beachtung geltender Vorschriften und bewährter Verfahren auf dem Gebiet des Datenschutzes und der Datenspeicherung. 2. Aufzeichnungen werden, soweit nach nationalem Recht oder anderen nationalen Verwaltungsregelungen zulässig, aufbewahrt und geschützt, solange dies für Prüfungszwecke und für die Untersuchung von Sicherheitsverletzungen sowie für die Zwecke der Datenspeicherung erforderlich ist; danach werden die Aufzeichnungen auf sichere Weise vernichtet.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.5. Einrichtungen und Personal

Die folgende Tabelle enthält die Anforderungen an Einrichtungen und Personal sowie an etwaige Unterauftragnehmer, die Aufgaben wahrnehmen, die unter diese Verordnung fallen. Die Einhaltung jeder dieser Anforderungen soll im Hinblick auf die Risiken des jeweiligen Sicherheitsniveaus verhältnismäßig sein.

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es gibt Verfahren, die sicherstellen, dass alle Mitarbeiter und Unterauftragnehmer eine ausreichende Ausbildung, Qualifikation und Erfahrung bezüglich der ihnen übertragenen Aufgaben haben. 2. Es gibt eine ausreichende Anzahl von Mitarbeitern und Unterauftragnehmern für einen angemessenen Betrieb und eine angemessene Ausstattung des Dienstes entsprechend den Vorgaben und Verfahren. 3. Die zur Bereitstellung des Dienstes genutzten Einrichtungen werden ständig überwacht und vor Schäden durch Umgebungseinflüsse, unbefugten Zugriff oder andere Faktoren geschützt, die die Sicherheit des Dienstes beeinträchtigen können. 4. Die zur Bereitstellung des Dienstes genutzten Einrichtungen gewährleisten, dass nur befugte Mitarbeiter und Unterauftragnehmer Zugang zu Bereichen haben, in denen personenbezogene Daten, kryptografische oder andere sensible Informationen verarbeitet werden.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.6. Technische Kontrollen

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es gibt angemessene technische Kontrollen für das Risikomanagement in Bezug auf die Sicherheit der Dienste sowie zum Schutz der Vertraulichkeit, Unversehrtheit und Verfügbarkeit der verarbeiteten Informationen. 2. Elektronische Kommunikationswege, die zur Übermittlung personenbezogener oder sensibler Informationen verwendet werden, müssen gegen Abhören, Manipulation und Replay geschützt sein. 3. Der Zugang zu sensiblem kryptografischen Material, das für die Ausstellung elektronischer Identifizierungsmittel und für die Authentifizierung verwendet wird, ist streng auf die Rollen und Anwendungen beschränkt, die diesen Zugang unbedingt benötigen. Es ist sichergestellt, dass solches Material niemals dauerhaft im Klartext gespeichert wird. 4. Es gibt Verfahren, die gewährleisten, dass die Sicherheit dauerhaft aufrechterhalten wird und dass auf geänderte Risikostufen, Vorfälle und Sicherheitsverletzungen reagiert werden kann. 5. Alle Speichermedien, die personenbezogene, kryptografische oder andere sensible Informationen enthalten, werden in sicherer und geschützter Weise aufbewahrt, transportiert und entsorgt.
Substanziell	Zusätzlich zum Niveau „Niedrig“: Sensibles kryptografisches Material, das für die Ausstellung elektronischer Identifizierungsmittel und für die Authentifizierung verwendet wird, ist vor Fälschung geschützt.
Hoch	Wie für das Niveau „Substanziell“.

2.4.7. Einhaltung und Prüfung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	Es gibt regelmäßige interne Prüfungen (Audits) aller Bestandteile, die für die Bereitstellung der Dienste von Bedeutung sind, um die Einhaltung der betreffenden Vorgaben zu gewährleisten.

Sicherheitsniveau	Erforderliche Elemente
Substanziell	Es gibt regelmäßige unabhängige interne oder externe Prüfungen (Audits) aller Bestandteile, die für die Bereitstellung der Dienste von Bedeutung sind, um die Einhaltung der betreffenden Vorgaben zu gewährleisten.
Hoch	1. Es gibt regelmäßige unabhängige externe Prüfungen (Audits) aller Bestandteile, die für die Bereitstellung der Dienste von Bedeutung sind, um die Einhaltung der betreffenden Vorgaben zu gewährleisten. 2. Wird das System direkt von einer staatlichen Stelle verwaltet, so erfolgen die Prüfungen nach den nationalen Rechtsvorschriften.

DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1503 DER KOMMISSION

vom 8. September 2015

zur Festlegung pauschaler Einfuhrwerte für die Bestimmung der für bestimmtes Obst und Gemüse geltenden Einfuhrpreise

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 1308/2013 des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über eine gemeinsame Marktorganisation für landwirtschaftliche Erzeugnisse und zur Aufhebung der Verordnungen (EWG) Nr. 922/72, (EWG) Nr. 234/79, (EG) Nr. 1037/2001 und (EG) Nr. 1234/2007 ([1]),

gestützt auf die Durchführungsverordnung (EU) Nr. 543/2011 der Kommission vom 7. Juni 2011 mit Durchführungsbestimmungen zur Verordnung (EG) Nr. 1234/2007 des Rates für die Sektoren Obst und Gemüse und Verarbeitungserzeugnisse aus Obst und Gemüse ([2]), insbesondere auf Artikel 136 Absatz 1,

in Erwägung nachstehender Gründe:

(1) Die in Anwendung der Ergebnisse der multilateralen Handelsverhandlungen der Uruguay-Runde von der Kommission festzulegenden, zur Bestimmung der pauschalen Einfuhrwerte zu berücksichtigenden Kriterien sind in der Durchführungsverordnung (EU) Nr. 543/2011 für die in ihrem Anhang XVI Teil A aufgeführten Erzeugnisse und Zeiträume festgelegt.

(2) Gemäß Artikel 136 Absatz 1 der Durchführungsverordnung (EU) Nr. 543/2011 wird der pauschale Einfuhrwert an jedem Arbeitstag unter Berücksichtigung variabler Tageswerte berechnet. Die vorliegende Verordnung sollte daher am Tag ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft treten —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Die in Artikel 136 der Durchführungsverordnung (EU) Nr. 543/2011 genannten pauschalen Einfuhrwerte sind im Anhang der vorliegenden Verordnung festgesetzt.

Artikel 2

Diese Verordnung tritt am Tag 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 8. September 2015

Für die Kommission,
im Namen des Präsidenten,
Jerzy PLEWA
Generaldirektor für Landwirtschaft und ländliche Entwicklung

([1]) ABl. L 347 vom 20.12.2013, S. 671.
([2]) ABl. L 157 vom 15.6.2011, S. 1.

ANHANG

Pauschale Einfuhrwerte für die Bestimmung der für bestimmtes Obst und Gemüse geltenden Einfuhrpreise

(EUR/100 kg)

KN-Code	Drittland-Code ([1])	Pauschaler Einfuhrwert
0702 00 00	MA	173,3
	MK	48,7
	XS	41,5
	ZZ	87,8
0707 00 05	MK	76,3
	TR	116,3
	XS	42,0
	ZZ	78,2
0709 93 10	TR	133,1
	ZZ	133,1
0805 50 10	AR	135,9
	BO	135,7
	CL	125,5
	UY	142,2
	ZA	136,9
	ZZ	135,2
0806 10 10	EG	239,8
	MK	63,9
	TR	129,5
	ZZ	144,4
0808 10 80	AR	188,7
	BR	93,9
	CL	134,4
	NZ	143,4
	US	112,5
	UY	110,5
	ZA	117,6
	ZZ	128,7
0808 30 90	AR	131,9
	CL	100,0
	TR	122,9
	ZA	113,5
	ZZ	117,1
0809 30 10, 0809 30 90	MK	80,1
	TR	141,7
	ZZ	110,9

(EUR/100 kg)

KN-Code	Drittland-Code (1)	Pauschaler Einfuhrwert
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Nomenklatur der Länder gemäß der Verordnung (EU) Nr. 1106/2012 der Kommission vom 27. November 2012 zur Durchführung der Verordnung (EG) Nr. 471/2009 des Europäischen Parlaments und des Rates über Gemeinschaftsstatistiken des Außenhandels mit Drittländern hinsichtlich der Aktualisierung des Verzeichnisses der Länder und Gebiete (ABl. L 328 vom 28.11.2012, S. 7). Der Code „ZZ“ steht für „Andere Ursprünge“.

BESCHLÜSSE

DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1504 DER KOMMISSION

vom 7. September 2015

zur Gewährung von Ausnahmen für bestimmte Mitgliedstaaten bezüglich der Bereitstellung von Statistiken gemäß der Verordnung (EG) Nr. 1099/2008 des Europäischen Parlaments und des Rates über die Energiestatistik

(Bekanntgegeben unter Aktenzeichen C(2015) 6105)

(Nur der estnische, französische, griechische, niederländische und slowakische Text sind verbindlich)

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EG) Nr. 1099/2008 des Europäischen Parlaments und des Rates vom 22. Oktober 2008 über die Energiestatistik ([1]), insbesondere auf Artikel 5 Absatz 4 und Artikel 10 Absatz 2,

in Erwägung nachstehender Gründe:

(1) Im Einklang mit Artikel 5 Absatz 4 der Verordnung (EG) Nr. 1099/2008 können auf gebührend begründeten Antrag eines Mitgliedstaats für solche Teile der nationalen Statistiken, deren Erhebung zu einem übermäßigen Beantwortungsaufwand führen würde, Ausnahmen gewährt werden.

(2) Belgien, Estland, Zypern und die Slowakei übermittelten Anträge auf die Gewährung von Ausnahmen bezüglich der Bereitstellung von Statistiken über den genauen Energieverbrauch in Haushalten, aufgeschlüsselt nach Art des Endverbrauchs für bestimmte Referenzjahre.

(3) Die von diesen Mitgliedstaaten übermittelten Informationen rechtfertigen die Gewährung von Ausnahmen.

(4) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des Ausschusses für das Europäische Statistische System —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Die folgenden Ausnahmen von den Bestimmungen der Verordnung (EG) Nr. 1099/2008 werden gewährt:

1. Belgien wird eine Ausnahme von der Vorlage von Daten für das Referenzjahr 2015 bezüglich folgender Punkte gewährt: 1.2.3 (4.2.1 bis 4.2.5), 2.2.3 (4.2.1 bis 4.2.5), 3.2.3 (3.1 bis 3.6), 4.2.3 (7.2.1 bis 7.2.5) und 5.2.4 (4.2.1 bis 4.2.5) von Anhang B betreffend Statistiken über den genauen Energieverbrauch in Haushalten nach Art des Endverbrauchs (gemäß der Definition unter Punkt 2.3 (26 „Sonstige Sektoren — Haushalte“ in Anhang A)).

([1]) ABl. L 304 vom 14.11.2008, S. 1.

2. Estland wird eine Ausnahme von der Vorlage von Daten für die Referenzjahre 2015, 2016 und 2017 bezüglich folgender Punkte gewährt: 1.2.3 (4.2.1 bis 4.2.5), 2.2.3 (4.2.1 bis 4.2.5), 3.2.3 (3.1 bis 3.6), 4.2.3 (7.2.1 bis 7.2.5) und 5.2.4 (4.2.1 bis 4.2.5) von Anhang B betreffend Statistiken über den genauen Energieverbrauch in Haushalten nach Art des Endverbrauchs (gemäß der Definition unter Punkt 2.3 (26 „Sonstige Sektoren — Haushalte“ in Anhang A)).

3. Zypern wird eine Ausnahme von der Vorlage von Daten für die Referenzjahre 2015, 2016 und 2017 bezüglich folgender Punkte gewährt: 1.2.3 (4.2.1 bis 4.2.5), 2.2.3 (4.2.1 bis 4.2.5), 3.2.3 (3.1 bis 3.6) und 5.2.4 (4.2.1 bis 4.2.5) von Anhang B betreffend Statistiken über den genauen Energieverbrauch in Haushalten nach Art des Endverbrauchs (gemäß der Definition unter Punkt 2.3 (26 „Sonstige Sektoren — Haushalte“ in Anhang A)).

4. Der Slowakei wird eine Ausnahme von der Vorlage von Daten für die Referenzjahre 2015 und 2016 bezüglich folgender Punkte gewährt: 1.2.3 (4.2.1 bis 4.2.5), 2.2.3 (4.2.1 bis 4.2.5), 3.2.3 (3.1 bis 3.6), 4.2.3 (7.2.1 bis 7.2.5) und 5.2.4 (4.2.1 bis 4.2.5) von Anhang B betreffend Statistiken über den genauen Energieverbrauch in Haushalten nach Art des Endverbrauchs (gemäß der Definition unter Punkt 2.3 (26 „Sonstige Sektoren — Haushalte“ in Anhang A)).

Artikel 2

Dieser Beschluss ist an das Königreich Belgien, die Republik Estland, die Republik Zypern und die Slowakische Republik gerichtet.

Brüssel, den 7. September 2015

Für die Kommission

Marianne THYSSEN

Mitglied der Kommission

DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1505 DER KOMMISSION

vom 8. September 2015

über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten gemäß Artikel 22 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

(Text von Bedeutung für den EWR)

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 22 Absatz 5,

in Erwägung nachstehender Gründe:

(1) Vertrauenslisten sind wesentlich für die Schaffung von Vertrauen unter den Marktteilnehmern, denn sie geben Auskunft über den Status des Diensteanbieters zum Zeitpunkt der Beaufsichtigung.

(2) Die grenzüberschreitende Verwendung elektronischer Signaturen wurde durch die Entscheidung 2009/767/EG der Kommission ([2]) erleichtert, mit der die Mitgliedstaaten erstmals zur Aufstellung, Führung und Veröffentlichung von Vertrauenslisten mit Angaben zu Zertifizierungsdiensteanbietern verpflichtet wurden, die gemäß der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates ([3]) öffentlich qualifizierte Zertifikate ausstellen und von den Mitgliedstaaten beaufsichtigt und akkreditiert werden.

(3) Artikel 22 der Verordnung (EU) Nr. 910/2014 verpflichtet die Mitgliedstaaten, auf gesicherte Weise elektronisch unterzeichnete oder besiegelte Vertrauenslisten in einer für die automatisierte Verarbeitung geeigneten Form zu erstellen, zu führen und zu veröffentlichen und der Kommission unverzüglich die für die Erstellung der nationalen Vertrauenslisten verantwortlichen Stellen zu melden.

(4) Vertrauensdiensteanbieter und die von ihnen erbrachten Leistungen sollten als qualifiziert angesehen werden, wenn dem Diensteanbieter auf der Vertrauensliste der qualifizierte Status zugeordnet ist. Damit gewährleistet ist, dass anderweitige Verpflichtungen aus der Verordnung (EU) Nr. 910/2014, insbesondere den Artikeln 27 und 37 von den Diensteanbietern leicht problemlos aus der Ferne und auf elektronischem Wege erfüllt werden können, und um den Vertrauensschutz anderer Zertifizierungsdiensteanbieter zu wahren, die keine qualifizierten Zertifikate ausstellen, aber Dienste im Zusammenhang mit elektronischen Signaturen gemäß der Richtlinie 1999/93/EG erbringen und bis zum 30. Juni 2016 in die Liste aufgenommen werden, sollte es den Mitgliedstaaten möglich sein, auf nationaler Ebene auf freiwilliger Basis andere Dienste als die qualifizierten Vertrauensdienste in die Vertrauenslisten aufzunehmen, sofern deutlich gekennzeichnet wird, dass diese Dienste nicht gemäß der Verordnung (EU) Nr. 910/2014 qualifiziert sind.

(5) Im Einklang mit Erwägungsgrund 25 der Verordnung (EU) Nr. 910/2014 können die Mitgliedstaaten auch andere, auf nationaler Ebene festgelegte Arten von Vertrauensdiensten zusätzlich zu jenen festlegen, die in Artikel 3 Absatz 16 der Verordnung (EU) Nr. 910/2014 definiert sind, sofern deutlich gekennzeichnet wird, dass diese Dienste nicht gemäß der Verordnung (EU) Nr. 910/2014 qualifiziert sind.

(6) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 48 der Verordnung (EU) Nr. 910/2014 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Jeder Mitgliedstaat sorgt für die Aufstellung, Veröffentlichung und Führung von Vertrauenslisten, die Angaben zu den qualifizierten Vertrauensdiensteanbietern, für deren Beaufsichtigung sie zuständig sind, und zu den von ihnen erbrachten qualifizierten Vertrauensdiensten enthalten. Diese Listen erfüllen die technischen Spezifikationen des Anhangs I.

([1]) ABl. L 257 vom 28.8.2014, S. 73.
([2]) Entscheidung 2009/767/EG der Kommission vom 16. Oktober 2009 über Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über „einheitliche Ansprechpartner“ gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt (ABl. L 274 vom 20.10.2009, S. 36).
([3]) Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. L 13 vom 19.1.2000, S. 12).

Artikel 2

Die Mitgliedstaaten können in die Vertrauenslisten Angaben über nicht qualifizierte Vertrauensdiensteanbieter samt den von diesen erbrachten nicht qualifizierten Vertrauensdiensten aufnehmen. In der Liste muss deutlich gekennzeichnet sein, welche Vertrauensdiensteanbieter samt den von ihnen erbrachten Vertrauensdiensten nicht qualifiziert sind.

Artikel 3

(1) Nach Artikel 22 Absatz 2 der Verordnung (EU) Nr. 910/2014 müssen die Mitgliedstaaten die für die automatisierte Verarbeitung geeignete Fassung ihrer Vertrauensliste im Einklang mit den technischen Spezifikationen des Anhangs I elektronisch unterzeichnen oder besiegeln.

(2) Veröffentlicht ein Mitgliedstaat eine menschenlesbare Fassung der Vertrauensliste in elektronischer Form, so stellt er sicher, dass diese Fassung der Liste dieselben Angaben enthält wie die für die automatisierte Verarbeitung geeignete Fassung, und unterzeichnet oder besiegelt sie elektronisch im Einklang mit den technischen Spezifikationen des Anhangs I.

Artikel 4

(1) Die Mitgliedstaaten melden der Kommission die in Artikel 22 Absatz 3 der Verordnung (EU) Nr. 910/2014 genannten Angaben unter Verwendung des Musters in Anhang II.

(2) Zu den in Absatz 1 genannten Angaben gehören auch zwei oder mehr Public-Key-Zertifikate eines Systembetreibers mit einer um mindestens drei Monate zeitversetzten Gültigkeitsdauer, die den privaten Schlüsseln entsprechen, die verwendet werden können, um die für die automatisierte Verarbeitung geeignete Fassung sowie die menschenlesbare Fassung der Vertrauensliste elektronisch zu unterzeichnen oder zu besiegeln, wenn diese veröffentlicht werden.

(3) Nach Artikel 22 Absatz 4 der Verordnung (EU) Nr. 910/2014 macht die Kommission die in den Absätzen 1 und 2 genannten Angaben in der von den Mitgliedstaaten gemeldeten Fassung in signierter oder besiegelter und für die automatisierte Verarbeitung geeigneter Form über einen sicheren Kanal auf einem authentifizierten Web-Server öffentlich zugänglich.

(4) Die Kommission macht die in den Absätzen 1 und 2 genannten Angaben in der von den Mitgliedstaaten gemeldeten Fassung in signierter oder besiegelter menschenlesbarer Form über einen sicheren Kanal auf einem authentifizierten Web-Server öffentlich zugänglich.

Artikel 5

Dieser Beschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Dieser Beschluss ist in allen seinen Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 8. September 2015

Für die Kommission

Der Präsident

Jean-Claude JUNCKER

ANHANG I

TECHNISCHE SPEZIFIKATIONEN FÜR EINE GEMEINSAME VORLAGE FÜR VERTRAUENSLISTEN

KAPITEL I

ALLGEMEINE ANFORDERUNGEN

Vertrauenslisten müssen sowohl die aktuellen als auch alle historischen Daten über den Status der gelisteten Vertrauensdienste ab dem Zeitpunkt der Aufnahme eines Vertrauensdiensteanbieters in die Vertrauenslisten enthalten.

Die in diesen Spezifikationen verwendeten Begriffe „genehmigt", „akkreditiert" und/oder „beaufsichtigt" gelten auch für die einzelstaatlichen Genehmigungssysteme, doch müssen die Mitgliedstaaten in ihrer Vertrauensliste Zusatzinformationen zu diesen einzelstaatlichen Regelungen geben, einschließlich präziser Angaben zu den etwaigen Unterschieden gegenüber den Aufsichtssystemen, denen qualifizierte Vertrauensdiensteanbieter und die von ihnen angebotenen qualifizierten Vertrauensdienste unterliegen.

Die in der Vertrauensliste zur Verfügung gestellten Informationen sollen der besseren Validierung qualifizierter Vertrauensdienst-Tokens, d. h. physischer oder binärer (logischer) Objekte, dienen, die von qualifizierten Vertrauensdiensten erzeugt oder ausgestellt werden (z. B. qualifizierte elektronische Signaturen/Siegel, fortgeschrittene elektronische Signaturen/Siegel, die auf einem qualifizierten Zertifikat beruhen, qualifizierte Zeitstempel oder qualifizierte Zustellbelege).

KAPITEL II

DETAILLIERTE SPEZIFIKATIONEN FÜR EINE GEMEINSAME VORLAGE FÜR VERTRAUENSLISTEN

Die vorliegenden Spezifikationen beruhen auf den in ETSI TS 119 612 Version 2.1.1 (im Folgenden „ETSI TS 119 612") festgelegten Spezifikationen und Anforderungen.

Soweit in den vorliegenden Spezifikationen keine besonderen Anforderungen festgelegt sind, müssen die Anforderungen aus ETSI TS 119 612 Abschnitte 5 und 6 in ihrer Gesamtheit erfüllt werden. Soweit in den vorliegenden Spezifikationen besondere Anforderungen festgelegt sind, haben diese Vorrang vor den entsprechenden Anforderungen aus ETSI TS 119 612. Bei Unterschieden zwischen den vorliegenden Spezifikationen und den Spezifikationen laut ETSI TS 119 612 haben die vorliegenden Spezifikationen Vorrang.

Name des Systembetreibers (Abschnitt 5.3.6)

Dieses Feld muss vorhanden sein und den Spezifikationen laut TS 119 612 Abschnitt 5.3.6 entsprechen. Dabei muss der Systemname wie folgt lauten:

„EN_name_value" = „Vertrauensliste mit Angaben zu den qualifizierten Vertrauensdiensteanbietern, die vom ausstellenden Mitgliedstaat beaufsichtigt werden, sowie Angaben zu den von ihnen angebotenen qualifizierten Vertrauensdiensten gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG."

URI zu den Systeminformationen (Abschnitt 5.3.7)

Dieses Feld muss vorhanden sein und den Spezifikationen gemäß TS 119 612 Abschnitt 5.3.7 entsprechen. Dabei müssen die „angemessenen Informationen" über das System mindestens Folgendes enthalten:

a) Für alle Mitgliedstaaten identische einleitende Informationen über den Umfang und Hintergrund der Vertrauensliste, das zugrunde liegende Aufsichtssystem und gegebenenfalls die nationale Genehmigungssysteme (z. B. Akkreditierungssysteme). Zu verwenden ist der nachstehende gemeinsame Text, in dem die Zeichenkette „*[Name des betreffenden Mitgliedstaats]*" durch den Namen des betreffenden Mitgliedstaats ersetzt werden muss:

> „Bei der vorliegenden Liste handelt es sich um die Vertrauensliste mit Angaben zu den qualifizierten Vertrauensdiensteanbietern, die von *[Name des jeweiligen Mitgliedstaats]* beaufsichtigt werden, sowie mit Angaben zu den von ihnen angebotenen qualifizierten Vertrauensdiensten gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

Die grenzüberschreitende Verwendung elektronischer Signaturen wurde durch die Entscheidung 2009/767/EG der Kommission vom 16. Oktober 2009 erleichtert, mit der die Mitgliedstaaten erstmals zur Aufstellung, Führung und Veröffentlichung von Vertrauenslisten mit Angaben zu Zertifizierungsdiensteanbietern verpflichtet wurden, die gemäß der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen öffentlich qualifizierte Zertifikate ausstellen und von den Mitgliedstaaten beaufsichtigt/akkreditiert werden. Mit dieser Vertrauensliste wird die im Wege der Entscheidung 2009/767/EG aufgestellte Vertrauensliste fortgeschrieben."

Vertrauenslisten sind für die Vertrauensbildung unter den Betreibern der elektronischen Kommunikation von großer Bedeutung, da sie es den Nutzern ermöglichen, den qualifizierten Status sowie die Chronik des Status eines Vertrauensdiensteanbieters und seiner Dienste abzufragen.

Die Vertrauenslisten der Mitgliedstaaten enthalten mindestens die in den Artikeln 1 und 2 des Durchführungsbeschlusses (EU) 2015/1505 der Kommission genannten Angaben.

Die Mitgliedstaaten können in die Vertrauenslisten auch Angaben über nichtqualifizierte Vertrauensdiensteanbieter samt den von diesen bereitgestellten nichtqualifizierten Vertrauensdiensten aufnehmen. Dabei ist jedoch deutlich anzugeben, dass diese nicht gemäß der Verordnung (EU) Nr. 910/2014 qualifiziert sind.

Die Mitgliedstaaten können in die Vertrauenslisten auch Informationen über auf nationaler Ebene festgelegte Vertrauensdienste aufnehmen, die sich von den Vertrauensdiensten nach Artikel 3 Absatz 16 der Verordnung (EU) Nr. 910/2014 unterscheiden. Dabei ist jedoch deutlich anzugeben, dass diese nicht gemäß der Verordnung (EU) Nr. 910/2014 qualifiziert sind.

b) Besondere Informationen über das zugrunde liegende Aufsichtssystem und gegebenenfalls nationale Genehmigungssysteme (z. B. Akkreditierungssysteme), insbesondere ([1]):

(1) Angaben zum nationalen Aufsichtssystem, das für qualifizierte und nicht qualifizierte Vertrauensdiensteanbieter und die von ihnen angebotenen qualifizierten und nicht qualifizierten Vertrauensdienste gemäß der Verordnung (EU) Nr. 910/2014 gilt;

(2) gegebenenfalls Angaben zu den nationalen freiwilligen Akkreditierungssystemen für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate gemäß der Richtlinie 1999/93/EG ausstellen.

Diese besonderen Angaben müssen für jedes der obengenannten zugrunde liegenden Systeme zumindest Folgendes enthalten:

(1) allgemeine Beschreibung;

(2) Angaben zu dem im Rahmen des nationalen Aufsichtssystems angewandten Verfahren und gegebenenfalls dem Vorgehen im Rahmen eines nationalen Genehmigungsverfahrens;

(3) Angaben zu den Kriterien, nach denen Vertrauensdiensteanbieter beaufsichtigt werden oder gegebenenfalls eine Genehmigung erhalten;

(4) Angaben zu den Kriterien und Vorschriften für die Auswahl von Aufsichts- und Auditpersonal und zu den Methoden, die dieses zur Prüfung von Vertrauensdiensteanbietern und den von ihnen angebotenen Vertrauensdiensten anwendet;

(5) gegebenenfalls weitere Kontaktdaten und allgemeine Informationen über den Betrieb des Systems.

Systemart/Gemeinschaft/Regeln (Abschnitt 5.3.9)

Dieses Feld muss vorhanden sein und den Spezifikationen laut TS 119 612 Abschnitt 5.3.9 entsprechen.

Es enthält ausschließlich URIs in britischem Englisch.

([1]) Diese Informationen sind für die vertrauenden Beteiligten von entscheidender Bedeutung für die Beurteilung des Qualitäts- und Sicherheitsgrads solcher Systeme. Diese Informationen werden auf der Ebene der Vertrauensliste bereitgestellt, und zwar durch die Verwendung der vorhandenen Felder „URI zur Systeminformation" (Abschnitt 5.3.7 — von den Mitgliedstaaten bereitgestellte Informationen), „Systemart/Gemeinschaft/Regeln" (Abschnitt 5.3.9 — Verwendung eines allen Mitgliedstaaten gemeinsamen Texts) und „Vertrauenslistenrichtlinien/rechtlicher Hinweis" (Abschnitt 5.3.11 — ein allen Mitgliedstaaten einheitlicher Text, der die Möglichkeit bietet, einen länderspezifischen Text bzw. Verweise hinzuzufügen). Zusatzinformationen über solche Systeme für nicht qualifizierte Vertrauensdienste und auf nationaler Ebene festgelegte (qualifizierte) Vertrauensdienste können gegebenenfalls auf der Dienstebene und soweit erforderlich (z. B. zur Unterscheidung zwischen verschiedenen Qualitäts-/Sicherheitsstufen) durch die Verwendung der „URI zur Definition des Systemdienstes" (Abschnitt 5.5.6) zur Verfügung gestellt werden.

Es enthält mindestens zwei URIs:

(1) Einen allen Vertrauenslisten der Mitgliedstaaten gemeinsamen URI, der zu einem deskriptiven Text führt, der für alle Vertrauenslisten gilt:

URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

Deskriptiver Text:

„Participation in a scheme

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

Policy/rules for the assessment of the listed services

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision 2015/1505.

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

Interpretation of the Trusted List

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

The ‚qualified' status of a trust service is indicated by the combination of the ‚Service type identifier' (‚Sti') value in a service entry and the status according to the ‚Service current status' field value as from the date indicated in the ‚Current status starting date and time'. Historical information about such a qualified status is similarly provided when applicable.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

A ‚CA/QC' ‚Service type identifier' (‚Sti') entry (possibly further qualified as being a ‚RootCA-QC' through the use of the appropriate ‚Service information extension' (‚Sie') additionalServiceInformation Extension)

— indicates that any end-entity certificate issued by or under the CA represented by the ‚Service digital identifier' (‚Sdi') CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

  — the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),

  — the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. ‚undersupervision', ‚supervisionincessation', ‚accredited' or ‚granted') for that entry.

— **and IF** ‚Sie' ‚Qualifications Extension' information is present, then in addition to the above default rule, those certificates that are identified through the use of ‚Sie' ‚Qualifications Extension' information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the ‚SSCD support' and/or ‚Legal person as subject' (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific ‚Key usage' pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension usw.). These qualifiers are part of the following set of ‚Qualifiers' used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

  — to indicate the qualified certificate nature:

    — ‚QCStatement' meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC;

    — ‚QCForESig' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014;

    — ‚QCForESeal' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014;

    — ‚QCForWSA' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014.

  — to indicate that the certificate is not to be considered as qualified:

    — ‚NotQualified' meaning the identified certificate(s) is(are) not to be considered as qualified; and/or

  — to indicate the nature of the SSCD support:

    — ‚QCWithSSCD' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

    — ‚QCNoSSCD' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

    — ‚QCSSCDStatusAsInCert' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

  — to indicate the nature of the QSCD support:

    — ‚QCWithQSCD' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

    — ‚QCNoQSCD' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

    — ‚QCQSCDStatusAsInCert' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

    — ‚QCQSCDManagedOnBehalf' indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; and/or

— to indicate issuance to Legal Person:

— ‚QCForLegalPerson' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

— if none of the id-etsi-qcs 1 statement, QCP OID or QCP+ OID information is included in an end-entity certificate, and

— if no ‚Sie' ‚Qualifications Extension' information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a ‚QCStatement' qualifier, or

— an ‚Sie' ‚Qualifications Extension' information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a ‚NotQualified' qualifier,

then the certificate is not to be considered as qualified.

‚Service digital identifiers' are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other ‚Sti' type entry is that, for that ‚Sti' identified service type, the listed service named according to the ‚Service name' field value and uniquely identified by the ‚Service digital identity' field value has the current qualified or approval status according to the ‚Service current status' field value as from the date indicated in the ‚Current status starting date and time'.

Specific interpretation rules for any additional information with regard to a listed service (e.g. ‚Service information extensions' field) may be found, when applicable, in the Member State specific URI as part of the present ‚Scheme type/community/rules' field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists."

(2) Ein der Vertrauensliste eines Mitgliedstaats jeweils eigener URI, der auf einen deskriptiven Text verweist, der für diese Vertrauensliste des Mitgliedstaats gilt:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC; dabei ist CC der im Feld „Systemgebiet" (Abschnitt 5.3.10) verwendete ISO 3166-1 [1]-Alpha-2-Ländercode.

— Angaben dazu, wo Nutzer länderspezifische Richtlinien/Vorschriften des betreffenden Mitgliedstaats finden können, anhand derer die in die Liste aufgenommenen Vertrauensdienste gemäß dem Aufsichtssystem und gegebenenfalls dem Genehmigungssystem des Mitgliedstaats bewertet werden.

— Angaben dazu, wo Nutzer eine länderspezifische Anleitung des betreffenden Mitgliedstaats zur Verwendung und Auslegung des Inhalts der Vertrauensliste im Hinblick auf die aufgeführten nichtqualifizierten Vertrauensdienste und/oder auf nationaler Ebene definierten Vertrauensdienste finden können. Darin kann in Bezug auf Zertifizierungsdiensteanbieter, die keine qualifizierten Zertifikate ausstellen, auf eine potenzielle Granularität im einzelstaatlichen Genehmigungssystem hingewiesen und erläutert werden, wie die Felder „URI zur Definition des Systemdienstes" (Abschnitt 5.5.6) und „Dienstinformations-Endung" (Abschnitt 5.5.9) zu diesem Zweck verwendet werden.

Die Mitgliedstaaten KÖNNEN den obigen länderspezifischen URI erweitern, indem sie zusätzliche URIs definieren und verwenden (d. h. URIs, die auf diesem hierarchischen spezifischen URI basieren).

Vertrauenslistenrichtlinien/Rechtlicher Hinweis (Abschnitt 5.3.11)

Dieses Feld muss vorhanden sein und den Spezifikationen laut TS 119 612 Abschnitt 5.3.11 entsprechen. Es muss die Richtlinien bzw. einen rechtlichen Hinweis zum Rechtsstatus des Systems bzw. die vom System in der Rechtsordnung, der es angehört, erfüllten rechtlichen Anforderungen und/oder alle Beschränkungen und Bedingungen enthalten, unter denen die Vertrauensliste veröffentlicht und gepflegt wird. Dabei muss es sich um eine Abfolge von mehrsprachigen

[1] ISO 3166-1:2006: Codes für die Namen von Ländern und deren Untereinheiten — Teil 1: Codes für Ländernamen.

Zeichenketten (siehe Abschnitt 5.1.4) handeln, die den tatsächlichen Text der Richtlinie oder des Hinweises nach der folgenden Struktur — obligatorisch in britischem Englisch und optional in einer oder mehreren weiteren Sprache der Mitgliedstaaten — enthält und sich zusammensetzt aus:

(1) einem obligatorischen, allen Vertrauenslisten der Mitgliedstaaten gemeinsamen Teil, in dem auf den geltenden Rechtsrahmen hingewiesen wird und dessen englische Fassung wie folgt lautet:

> The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

der Fassung des Texts in der/den Sprache(n) des Mitgliedstaats:

> Der für diese Vertrauenslisten geltende Rechtsrahmen ist 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;

(2) einem zweiten optionalen Teil für jede einzelne Vertrauensliste, in dem auf besondere nationale Rechtsvorschriften hingewiesen wird.

Aktueller Dienststatus (Abschnitt 5.5.4)

Dieses Feld muss vorhanden sein und den Spezifikationen laut TS 119 612 Abschnitt 5.5.4 entsprechen.

Die Migration des vor dem Inkrafttreten der Verordnung (EU) Nr. 910/2014 (d. h. dem 30. Juni 2016) im Feld „Aktueller Dienststatus“ enthaltenen Wertes für die in den Vertrauenslisten der EU-Mitgliedstaaten aufgeführten Dienste erfolgt gemäß dem Anhang J der Spezifikationen TS 119 612 des ETSI an dem Tag, an dem die Verordnung anwendbar wird (d. h. am 1. Juli 2016).

KAPITEL III

KONTINUITÄT DER VERTRAUENSLISTEN

Zertifikate, die der Kommission gemäß Artikel 4 Absatz 2 dieses Beschlusses zu notifizieren sind, müssen die Anforderungen aus ETSI TS 119 612 Abschnitt 5.7.1 erfüllen und in einer Weise ausgestellt werden, dass

— ihr letzter Gültigkeitstag („Not After“) um mindestens drei Monate auseinander liegt,

— sie anhand neuer Schlüsselpaare generiert werden. Bereits verwendete Schlüsselpaare dürfen nicht neu zertifiziert werden.

Bei Ablauf eines Public-Key-Zertifikats, das zur Validierung der Signatur oder des Siegels der Vertrauensliste verwendet werden kann, die der Kommission notifiziert und in deren zentralen Zeigerlisten veröffentlicht wurde, müssen die Mitgliedstaaten

— im Falle, dass eine aktuell veröffentlichte Vertrauensliste mit einem privaten Schlüssel signiert oder besiegelt wurde, dessen Public-Key-Zertifikat abgelaufen ist, unverzüglich eine neue, mit einem privaten Schlüssel, dessen Public-Key-Zertifikat nicht abgelaufen ist, signierte oder besiegelte Vertrauensliste erstellen;

— erforderlichenfalls neue Schlüsselpaare erstellen, die für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können, und die dazugehörigen Public-Key-Zertifikate erstellen;

— der Kommission unverzüglich die neue Liste der zu den privaten Schlüsseln gehörenden Public-Key-Zertifikate übermitteln, welche für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können.

Bei Kompromittierung oder Außerkraftsetzung eines privaten Schlüssels, der zu einem Public-Key-Zertifikat gehört, das zur Validierung der Signatur oder des Siegels der Vertrauensliste verwendet werden kann und der Kommission notifiziert und in ihrer zentralen Zeigerliste veröffentlicht wurde, müssen die Mitgliedstaaten

— unverzüglich eine neue, mit einem nicht kompromittierten privaten Schlüssel signierte oder besiegelte Vertrauensliste ausstellen, sofern die veröffentlichte Liste mit einem kompromittierten oder außer Kraft gesetzten privaten Schlüssel signiert oder besiegelt wurde;

— erforderlichenfalls neue Schlüsselpaare erstellen, die für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können, und die dazugehörigen Public-Key-Zertifikate erstellen;

— der Kommission unverzüglich die neue Liste der zu den privaten Schlüsseln gehörenden Public-Key-Zertifikate übermitteln, welche für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können.

Bei Kompromittierung oder Außerkraftsetzung aller privaten Schlüssel, die zu den Public-Key-Zertifikaten gehören, welche zur Validierung der Signatur der Vertrauensliste verwendet werden konnten und der Kommission notifiziert und in deren zentralen Zeigerlisten veröffentlicht wurden, müssen die Mitgliedstaaten

— neue Schlüsselpaare erstellen, die für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können, und die dazugehörigen Public-Key-Zertifikate generieren;

— unverzüglich eine neue, mit einem dieser neuen privaten Schlüssel signierte oder besiegelte Vertrauensliste erstellen und das das dazugehörige Public-Key-Zertifikat übermitteln;

— der Kommission unverzüglich die neue Liste der zu den privaten Schlüsseln gehörenden Public-Key-Zertifikate übermitteln, welche für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können.

KAPITEL IV

SPEZIFIKATIONEN FÜR DIE MENSCHENLESBARE FASSUNG DER VERTRAUENSLISTE

Wird eine menschenlesbare Fassung der Vertrauensliste erstellt und veröffentlicht, muss die Bereitstellung im PDF-Format gemäß ISO 32000 ([1]) erfolgen; die Formatierung muss dem Profil PDF/A (ISO 19005 ([2])) entsprechen.

Der Inhalt der auf PDF/A beruhenden menschenlesbaren Fassung der Vertrauensliste muss folgende Anforderungen erfüllen:

— Die Struktur der menschenlesbaren Fassung muss dem in TS 119 612 beschriebenen logischen Modell entsprechen.

— Jedes vorhandene Feld muss sichtbar sein und Folgendes enthalten:

  — die Bezeichnung des Felds (z. B. „*Dienstart-Identifikator*“);

  — den Wert des Felds (z. B. „http://uri.etsi.org/TrstSvc/Svctype/CA/QC“);

  — gegebenenfalls die Bedeutung (Beschreibung) des Feldwertes (z. B. „*Ein Zertifikatsgenerierungsdienst, mit dem qualifizierte Zertifikate anhand der Identität und anderer, von den zuständigen Registrierungsstellen geprüfter Merkmale erstellt und signiert werden.*“);

  — gegebenenfalls mehrere Fassungen in natürlichen Sprachen, wie in der Vertrauensliste vorgesehen.

— Die menschenlesbare Fassung muss mindestens die nachstehenden Felder und dazugehörigen Werte der digitalen Zertifikate ([3]) enthalten, sofern sie sich im Feld „Digitale Dienstidentität“ befinden:

  — Version,

  — Seriennummer des Zertifikats,

  — Signaturalgorithmus,

  — Aussteller — alle relevanten eindeutigen Namensfelder,

  — Gültigkeitszeitraum,

  — Inhaber — alle relevanten eindeutigen Namensfelder,

([1]) ISO 32000-1/2008: Dokumenten-Management — Portables Dokumenten Format — Teil 1: PDF 1.7
([2]) ISO 19005-2:2011: Dokumenten-Management. Elektronisches Dokumenten-Dateiformat für die Langzeitarchivierung — Teil 2: Anwendung der ISO 32000-1 (PDF/A-2)
([3]) Empfehlung ITU-T X.509 | ISO/IEC 9594-8: Informationstechnik — Kommunikation offener Systeme — Verzeichnisdienst: Rahmenrichtlinien für „Public Key“ und Attribut-Zertifikat (siehe http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509)

— öffentlicher Schlüssel,

— Ausstellerschlüssel-Identifikator,

— Inhaberschlüssel-Identifikator,

— Schlüsselverwendung,

— erweiterte Schlüsselverwendung,

— Zertifikatrichtlinien — alle Richtlinien-Identifikatoren und Richtlinien-Qualifikatoren,

— Richtlinienzuordnungen,

— alternativer Inhabername,

— Inhaberverzeichnisattribute,

— grundlegende Beschränkungen,

— Richtlinienbeschränkungen,

— CRL-Verteilungspunkte ([1]),

— Zugang zu Daten über zuständige Stellen,

— Zugang zu Daten über Inhaber,

— Erklärungen zu qualifizierten Zertifikaten ([2]),

— Hash-Algorithmus,

— Hashwert des Zertifikats.

— Die menschenlesbare Fassung muss leicht auszudrucken sein.

— Die menschenlesbare Fassung muss vom Systembetreiber mit der in den Artikeln 1 und 3 des Durchführungsbeschlusses (EU) 2015/1505 beschriebenen fortgeschrittenen PDF-Signatur unterzeichnet oder besiegelt werden.

([1]) RFC 5280: Internet X.509 PKI Certificate and CRL Profile.
([2]) RFC 3739: Internet X.509 PKI: Qualified Certificates Profile.

ANHANG II

MUSTER FÜR DIE MELDUNGEN DER MITGLIEDSTAATEN

Die von den Mitgliedstaaten nach Artikel 4 Absatz 1 dieses Beschlusses zu übermittelnden Angaben umfassen folgende Daten sowie deren etwaige Änderungen:

(1) Mitgliedstaat, unter Verwendung der ISO 3166-1 ([1])-Alpha-2-Ländercodes mit den folgenden Ausnahmen:

a) der Ländercode für das Vereinigte Königreich lautet „UK“,

b) der Ländercode für Griechenland lautet „EL“;

(2) die Stelle(n), die für die Aufstellung, Führung und Veröffentlichung der Vertrauenslisten in für die automatisierte Verarbeitung geeigneter sowie in menschenlesbarer Fassung zuständig ist (sind):

a) Name des Systembetreibers: Die Angaben müssen in allen in der Vertrauensliste verwendeten Sprachen mit dem Wert „Name des Systembetreibers“ *(Scheme operator name)* in der Vertrauensliste identisch sein (auch in Groß- und Kleinschreibung);

b) fakultative Angaben für den internen Gebrauch der Kommissionsdienststellen nur falls die zuständige Stelle kontaktiert werden muss (diese Angaben werden in der von der Europäischen Kommission geführten Liste der Vertrauenslisten nicht veröffentlicht):

— Anschrift des Systembetreibers;

— Kontaktdaten der zuständigen Person(en) (Name, Telefon, E-Mail-Adresse);

(3) der Ort, an dem die für die automatisierte Verarbeitung geeignete Fassung der Vertrauensliste veröffentlicht wird *(Ort, an dem die derzeitige Vertrauensliste veröffentlicht wird)*;

(4) gegebenenfalls der Ort, an dem die menschenlesbare Fassung der Vertrauensliste veröffentlicht wird *(Ort, an dem die derzeitige Vertrauensliste veröffentlicht wird)*. Wird eine menschenlesbare Form der Vertrauensliste nicht mehr veröffentlicht, ist ein entsprechender Hinweis anzubringen;

(5) die Public-Key-Zertifikate, die den privaten Schlüsseln entsprechen, die zur elektronischen Unterzeichnung oder Besiegelung der zur automatisierten Verarbeitung geeigneten Fassung und der menschenlesbaren Fassung der Vertrauenslisten verwendet werden können: Diese Zertifikate werden als DER-Zertifikate im Base64-kodierten PEM-Format bereitgestellt. Bei Änderungsmeldungen zusätzliche Informationen, wenn ein neues Zertifikat ein bestimmtes Zertifikat auf der Liste der Kommission ersetzen soll und wenn ein gemeldetes Zertifikat zu dem/den vorhandenen ohne Ersetzung hinzugefügt werden soll;

(6) Meldezeitpunkt der unter Punkt 1 bis 5 gemeldeten Daten.

Daten, die nach Nummer 1, Nummer 2 Buchstabe a oder den Nummern 3, 4 und 5 gemeldet werden, werden in die von der Europäischen Kommission geführte Liste der Vertrauenslisten anstelle der zuvor für diese Liste gemeldeten Angaben aufgenommen.

([1]) ISO 3166-1: „Codes für die Namen von Ländern und deren Untereinheiten — Teil 1: Ländercodes“.

DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 DER KOMMISSION

vom 8. September 2015

zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt anerkannt werden

(Text von Bedeutung für den EWR)

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 27 Absatz 5 und Artikel 37 Absatz 5,

in Erwägung nachstehender Gründe:

(1) Die Mitgliedstaaten müssen die notwendigen technischen Voraussetzungen schaffen, damit elektronisch signierte Dokumente verarbeiten werden können, die für Online-Dienste, die von oder im Namen von öffentlichen Stellen angeboten werden, erforderlich sind.

(2) Nach der Verordnung (EU) Nr. 910/2014 sind Mitgliedstaaten, die als Voraussetzung für die Nutzung von Online-Diensten, die von oder im Namen von öffentlichen Stellen angeboten werden, fortgeschrittene elektronische Signaturen oder Siegel verlangen, verpflichtet, fortgeschrittene elektronische Signaturen und Siegel sowie auf einem qualifizierten Zertifikat beruhende fortgeschrittene elektronische Signaturen und Siegel wie auch qualifizierte elektronische Signaturen und Siegel in bestimmten Formaten oder nach besonderen Referenzmethoden validierte alternative Formate anzuerkennen.

(3) Bei der Festlegung besonderer Formate und Referenzmethoden sollte der gängigen Praxis sowie bestehenden Normen und Unionsrechtsvorschriften Rechnung getragen werden.

(4) Im Durchführungsbeschluss 2014/148/EU [2] der Kommission sind einige der am weitesten verbreiteten Formate fortgeschrittener elektronische Signaturen definiert, die von den Mitgliedstaaten technisch unterstützt werden sollen, wenn solche bei Online-Verwaltungsverfahren verlangt werden. Die Festlegung von Referenzformaten soll die grenzüberschreitende Validierung elektronischer Signaturen erleichtern und die grenzübergreifende Interoperabilität elektronischer Verfahren verbessern.

(5) Die im Anhang dieses Beschlusses aufgeführten Normen sind die bestehenden Formate für fortgeschrittene elektronische Signaturen. Da die Formen für die langfristige Archivierung der Referenzformate derzeit von den Normungsgremien überarbeitet werden, werden Normen zur langfristigen Archivierung vom Geltungsbereich dieses Beschlusses ausgenommen. Sobald die neue Fassung der Referenznormen vorliegt, werden die Verweise auf die Normen und die Klauseln über die langfristige Archivierung überarbeitet werden.

(6) Fortgeschrittene elektronische Signaturen und fortgeschrittene elektronische Siegel ähneln sich in technischer Hinsicht. Deshalb sollten die Normen für die Formate fortgeschrittener elektronischer Signaturen sinngemäß auch für die Formate fortgeschrittener elektronischer Siegel gelten.

(7) Werden zum Signieren oder Besiegeln andere Formate elektronischer Signaturen oder Siegel als diejenigen verwendet, die im Allgemeinen technisch unterstützt werden, sollten Validierungsmöglichkeiten zur Verfügung stehen, die eine grenzüberschreitende Überprüfung elektronischer Signaturen und Siegel ermöglichen. Damit die empfangenden Mitgliedstaaten sich auf die Validierungswerkzeuge der anderen Mitgliedstaaten verlassen können, müssen leicht zugängliche Informationen über diese Validierungswerkzeuge bereitgestellt werden, und zwar in den elektronischen Dokumenten, den elektronischen Signaturen oder den elektronischen Dokument-Containern.

---

[1] ABl. L 257 vom 28.8.2014, S. 73.

[2] Durchführungsbeschluss 2014/148/EU der Kommission vom 17. März 2014 zur Änderung des Beschlusses 2011/130/EU der Kommission über Mindestanforderungen für die grenzüberschreitende Verarbeitung von Dokumenten, die gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt von zuständigen Behörden elektronisch signiert worden sind (ABl. L 80 vom 19.3.2014, S. 7).

(8) Stehen im Rahmen der öffentlichen Dienste eines Mitgliedstaats für die automatische Verarbeitung geeignete Validierungsmöglichkeiten zur Verfügung, sollten diese verfügbar gemacht und dem empfangenden Mitgliedstaat bereitgestellt werden. Dennoch sollte dieser Beschluss die Anwendung des Artikels 27 Absätze 1 und 2 und des Artikels 37 Absätze 1 und 2 der Verordnung (EU) Nr. 910/2014 nicht verhindern, wenn die automatische die Verarbeitung von Validierungsmöglichkeiten für alternative Methoden nicht möglich ist.

(9) Um vergleichbare Anforderungen für die Validierung zu bieten und das Vertrauen in die von den Mitgliedstaaten bereitgestellten Validierungsmöglichkeiten für andere als die gemeinsam unterstützten Formate elektronischer Signaturen und Siegel zu stärken, stützen sich die in diesem Beschluss festgelegten Anforderungen für die Validierungswerkzeuge auf die Anforderungen für die Validierung qualifizierter elektronischer Signaturen und Siegel der Artikel 32 und 40 der Verordnung (EU) Nr. 910/2014.

(10) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 48 der Verordnung (EU) Nr. 910/2014 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Mitgliedstaaten, die gemäß Artikel 27 Absätze 1 und 2 der Verordnung (EU) Nr. 910/2014 fortgeschrittene elektronische Signaturen oder auf einem qualifizierten Zertifikat beruhende fortgeschrittene elektronische Signaturen verlangen, erkennen fortgeschrittene elektronische XML-, CMS- und PDF-Signaturen der Konformitätsstufen B, T oder LT und Signaturen mit zugehörigen Containern an, wenn diese Signaturen die technischen Spezifikationen des Anhangs erfüllen.

Artikel 2

(1) Mitgliedstaaten, die gemäß Artikel 27 Absätze 1 und 2 der Verordnung (EU) Nr. 910/2014 fortgeschrittene elektronische Signaturen oder auf einem qualifizierten Zertifikat beruhende fortgeschrittene elektronische Signaturen verlangen, erkennen andere als die in Artikel 1 dieses Beschlusses genannten Formate elektronischer Signaturen an, sofern der Mitgliedstaat, in dem der vom Unterzeichner genutzte Vertrauensdiensteanbieter niedergelassenen ist, anderen Mitgliedstaaten Signaturvalidierungsmöglichkeiten bietet, die sich, soweit möglich, zur automatischen Verarbeitung eignen.

(2) Die Signaturvalidierungsmöglichkeiten müssen

a) es anderen Mitgliedstaaten gestatten, die empfangenen elektronischen Signaturen online, gebührenfrei und in einer für Nichtmuttersprachler verständlichen Weise zu validieren;

b) im unterzeichneten Dokument, in der elektronischen Signatur oder im elektronischen Dokument-Container angegeben sein und

c) die Gültigkeit einer fortgeschrittenen elektronischen Signatur bestätigen, sofern

(1) das der fortgeschrittenen elektronischen Signatur zugrunde liegende Zertifikat zum Zeitpunkt des Signierens gültig war, und, wenn die fortgeschrittene elektronische Signatur auf einem qualifizierten Zertifikat beruht, es sich bei dem der fortgeschrittenen elektronischen Signatur zugrunde liegenden qualifizierten Zertifikat zum Zeitpunkt des Signierens um ein qualifiziertes Zertifikat für elektronische Signaturen handelte, das mit Anhang I der Verordnung (EU) Nr. 910/2014 im Einklang stand und von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde;

(2) die Signaturvalidierungsdaten den Daten entsprechen, die dem vertrauenden Beteiligten bereitgestellt werden;

(3) der eindeutige Datensatz, der den Unterzeichner repräsentiert, dem vertrauenden Beteiligten korrekt bereitgestellt wird;

(4) die etwaige Benutzung eines Pseudonyms dem vertrauenden Beteiligten eindeutig angegeben wird, wenn zum Zeitpunkt des Signierens ein Pseudonym benutzt wurde;

(5) die etwaige Verwendung einer qualifizierten elektronischen Signaturerstellungseinheit, mit der die fortgeschrittene elektronische Signatur erstellt wird, dem vertrauenden Beteiligten eindeutig angezeigt wird;

(6) die Unversehrtheit der unterzeichneten Daten nicht beeinträchtigt ist;

(7) die Anforderungen des Artikels 26 der Verordnung (EU) Nr. 910/2014 zum Zeitpunkt des Signierens erfüllt waren;

(8) das zur Validierung der fortgeschrittenen elektronischen Signatur verwendete System dem vertrauenden Beteiligten das Ergebnis des Validierungsprozesses korrekt bereitstellt und es ihm ermöglicht, etwaige Sicherheitsprobleme zu erkennen.

Artikel 3

Mitgliedstaaten, die gemäß Artikel 37 Absätze 1 und 2 der Verordnung (EU) Nr. 910/2014 fortgeschrittene elektronische Siegel oder auf einem qualifizierten Zertifikat beruhende fortgeschrittene elektronische Siegel verlangen, erkennen fortgeschrittene elektronische XML-, CMS- und PDF-Siegel der Konformitätsstufen B, T oder LT und Siegel mit dazugehörigen Containern an, wenn diese Siegel die technischen Spezifikationen des Anhangs erfüllen.

Artikel 4

(1) Mitgliedstaaten, die gemäß Artikel 37 Absätze 1 und 2 der Verordnung (EU) Nr. 910/2014 fortgeschrittene elektronische Siegel oder auf einem qualifizierten Zertifikat beruhende fortgeschrittene elektronische Siegel verlangen, erkennen andere als die in Artikel 3 dieses Beschlusses genannten Formate elektronischer Siegel an, sofern der Mitgliedstaat, in dem der vom Siegelersteller genutzte Vertrauensdiensteanbieter niedergelassenen ist, anderen Mitgliedstaaten Siegelvalidierungsmöglichkeiten bietet, die sich, soweit möglich, zur automatischen Verarbeitung eignen.

(2) Die Siegelvalidierungsmöglichkeiten müssen

a) es anderen Mitgliedstaaten gestatten, die empfangenen elektronischen Siegel online, gebührenfrei und in einer für Nichtmuttersprachler verständlichen Weise zu validieren;

b) im unterzeichneten Dokument, im elektronischen Siegel oder im elektronischen Dokument-Container angegeben sein;

c) die Gültigkeit eines fortgeschrittenen elektronischen Siegels bestätigen, sofern

(1) das dem fortgeschrittenen elektronischen Siegel zugrunde liegende Zertifikat zum Zeitpunkt der Besiegelung gültig war, und, wenn die fortgeschrittene elektronische Signatur auf einem qualifizierten Zertifikat beruht, es sich bei dem dem fortgeschrittenen elektronischen Siegel zugrunde liegenden qualifizierten Zertifikat zum Zeitpunkt der Besiegelung um ein qualifiziertes Zertifikat für elektronische Siegel handelte, das mit Anhang III der Verordnung (EU) Nr. 910/2014 im Einklang stand und von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde;

(2) die Siegelvalidierungsdaten den Daten entsprechen, die dem vertrauenden Beteiligten bereitgestellt werden;

(3) der eindeutige Datensatz, der den Siegelersteller repräsentiert, dem vertrauenden Beteiligten korrekt bereitgestellt wird;

(4) die etwaige Benutzung eines Pseudonyms dem vertrauenden Beteiligten eindeutig angegeben wird, wenn zum Zeitpunkt der Besiegelung ein Pseudonym benutzt wurde;

(5) die etwaige Verwendung einer qualifizierten elektronischen Siegelerstellungseinheit, mit der das fortgeschrittene elektronische Siegel erstellt wird, dem vertrauenden Beteiligten eindeutig angezeigt wird;

(6) die Unversehrtheit der mit dem Siegel versehenen Daten nicht beeinträchtigt ist;

(7) die Anforderungen des Artikels 36 der Verordnung (EU) Nr. 910/2014 zum Zeitpunkt der Besiegelung erfüllt waren;

(8) das zur Validierung des fortgeschrittenen elektronischen Siegels verwendete System dem vertrauenden Beteiligten das Ergebnis des Validierungsprozesses korrekt bereitstellt und es ihm ermöglicht, etwaige Sicherheitsprobleme zu erkennen.

Artikel 5

Dieser Beschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Dieser Beschluss ist in allen seinen Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 8. September 2015

Für die Kommission

Der Präsident

Jean-Claude JUNCKER

ANHANG

Liste der technischen Spezifikationen für fortgeschrittene elektronische Signaturen im XML-, CMS- oder PDF-Format und zugehörige Containerdateien

Die in Artikel 1 des Beschlusses genannten fortgeschrittenen elektronischen Signaturen müssen mit Ausnahme der Klausel 9 einer der technischen Spezifikationen des ETSI genügen:

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1 ([1])
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1 ([2])
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2 ([3])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
([2]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
([3]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

Die in Artikel 1 des Beschlusses genannten Signatur-Containerdateien müssen den folgenden technischen Spezifikationen des ETSI genügen:

Associated Signature Container Baseline Profile	ETSI TS 103174 v.2.2.1 ([1])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

Liste der technischen Spezifikationen für fortgeschrittene elektronische Siegel im XML-, CMS- oder PDF-Format und zugehörige Containerdateien

Die in Artikel 3 des Beschlusses genannten fortgeschrittenen elektronischen Siegel müssen mit Ausnahme der Klausel 9 den technischen Spezifikationen des ETSI für eines der folgenden Profile genügen:

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2

Die in Artikel 3 des Beschlusses genannten Siegel-Containerdateien müssen den folgenden technischen Spezifikationen des ETSI genügen:

Associated Seal Container Baseline Profile	ETSI TS 103174 v.2.2.1

ISSN 1977-0642 (elektronische Ausgabe)
ISSN 1725-2539 (Papierausgabe)

Amt für Veröffentlichungen der Europäischen Union
2985 Luxemburg
LUXEMBURG

DE