Publicatieblad van de Europese Unie

L 235

Uitgave in de Nederlandse taal

Wetgeving

58e jaargang

9 september 2015

Inhoud

[1] Voor de EER relevante tekst

NL

Besluiten waarvan de titels mager zijn gedrukt, zijn besluiten van dagelijks beheer die in het kader van het landbouwbeleid zijn genomen en die in het algemeen een beperkte geldigheidsduur hebben.

Besluiten waarvan de titels vet zijn gedrukt en die worden voorafgegaan door een sterretje, zijn alle andere besluiten.

[1] Voor de EER relevante tekst

II

(Niet-wetgevingshandelingen)

VERORDENINGEN

UITVOERINGSVERORDENING (EU) 2015/1501 VAN DE COMMISSIE

van 8 september 2015

betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG ([1]), en met name artikel 12, lid 8,

Overwegende hetgeen volgt:

(1) In artikel 12, lid 2, van Verordening (EU) nr. 910/2014 wordt bepaald dat met het oog op de interoperabiliteit van de krachtens artikel 9, lid 1, van die verordening aangemelde nationale stelsels voor elektronische identificatie een interoperabiliteitskader moet worden opgezet.

(2) Knooppunten spelen een centrale rol met betrekking tot de interconnectie van de stelsels van de lidstaten voor elektronische identificatie. Hun bijdrage wordt uitgelegd in de documentatie over de financieringsfaciliteit voor Europese verbindingen die is vastgesteld bij Verordening (EU) nr. 1316/2013 van het Europees Parlement en de Raad ([2]), onder meer wat de werking en de onderdelen van het „eIDAS-knooppunt" betreft.

(3) Wanneer een lidstaat of de Commissie software ter beschikking stelt om authenticatie bij een knooppunt in een andere lidstaat mogelijk te maken, kan de partij die de voor het authenticatiemechanisme gebruikte software levert en bijhoudt, overeenkomen met de partij die de software host op welke wijze de werking ten aanzien van het authenticatiemechanisme zal worden beheerd. Een dergelijke overeenkomst mag niet leiden tot onevenredige technische vereisten of kosten (waaronder die voor ondersteuning, verantwoording, hosting en andere kosten) voor de partij die de software host.

(4) Voor zover de implementatie van het interoperabiliteitskader dat rechtvaardigt, zou de Commissie in samenwerking met de lidstaten nadere technische specificaties kunnen ontwikkelen met details over de technische vereisten zoals bij deze verordening vastgesteld, met name wat betreft de adviezen van het samenwerkingsnetwerk bedoeld in artikel 14, onder d), van Uitvoeringsbesluit (EU) 2015/296 van de Commissie ([3]). Die specificaties zouden moeten worden ontwikkeld als onderdeel van de digitale diensteninfrastructuren bedoeld in Verordening (EU) nr. 1316/2013, die de middelen biedt voor de praktische tenuitvoerlegging van een basis voor elektronische identificatie.

([1]) PB L 257 van 28.8.2014, blz. 73.

([2]) Verordening (EU) nr. 1316/2013 van het Europees Parlement en de Raad van 11 december 2013 tot vaststelling van de financieringsfaciliteit voor Europese verbindingen, tot wijziging van Verordening (EU) nr. 913/2010 en tot intrekking van Verordeningen (EG) nr. 680/2007 en (EG) nr. 67/2010 (PB L 348 van 20.12.2013, blz. 129).

([3]) Uitvoeringsbesluit (EU) 2015/296 van de Commissie van 24 februari 2015 tot vaststelling van procedurele voorschriften betreffende de samenwerking tussen de lidstaten op het gebied van elektronische identificatie overeenkomstig artikel 12, lid 7, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (PB L 53 van 25.2.2015, blz. 14).

(5) De bij deze verordening vastgestelde technische vereisten dienen van toepassing te zijn ongeacht eventuele wijzigingen van de technische specificaties die mogelijk uit hoofde van artikel 12 van deze verordening worden ontwikkeld.

(6) Bij het vaststellen van de in deze verordening vervatte regelingen voor het interoperabiliteitsnetwerk is terdege rekening gehouden met het grootschalige proefproject STORK, inclusief de in dat verband ontwikkelde specificaties, alsmede de beginselen en begrippen van het Europees interoperabiliteitskader voor Europese overheidsdiensten.

(7) Er is terdege rekening gehouden met de resultaten van de samenwerking tussen de lidstaten.

(8) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 48 van Verordening (EU) nr. 910/2014 ingestelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Onderwerp

Bij deze verordening worden de technische en operationele vereisten voor het interoperabiliteitskader vastgesteld teneinde de interoperabiliteit te waarborgen van de stelsels voor elektrische identificatie die de lidstaten bij de Commissie aanmelden.

Deze vereisten omvatten in het bijzonder:

a) minimale technische vereisten met betrekking tot de betrouwbaarheidsniveaus en het daaraan relateren van de nationale betrouwbaarheidsniveaus van aangemelde elektronische identificatiemiddelen die zijn uitgegeven in het kader van aangemelde stelsels voor elektronische identificatie overeenkomstig artikel 8 van Verordening (EU) nr. 910/2014, zoals opgenomen in de artikelen 3 en 4;

b) minimale technische vereisten voor interoperabiliteit, zoals opgenomen in de artikelen 5 en 8;

c) het minimale pakket persoonsidentificatiegegevens dat een natuurlijke persoon of rechtspersoon op unieke wijze vertegenwoordigt, zoals opgenomen in artikel 11 en de bijlage;

d) gemeenschappelijke operationele veiligheidsnormen, zoals opgenomen in de artikelen 6, 7, 9 en 10;

e) regelingen voor geschillenbeslechting, zoals opgenomen in artikel 13.

Artikel 2

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

1. „knooppunt": een aansluitpunt dat onderdeel is van de interoperabiliteitsarchitectuur voor elektronische identificatie en betrokken is bij de grensoverschrijdende authenticatie van personen, en dat in staat is berichten te herkennen en te verwerken of door te sturen naar andere knooppunten door mogelijk te maken dat de nationale elektronische identificatie-infrastructuur van een lidstaat gekoppeld wordt aan de nationale elektronische identificatie-infrastructuren van andere lidstaten;

2. „exploitant van een knooppunt": de entiteit die tot taak heeft ervoor te zorgen dat het knooppunt correct en betrouwbaar als aansluitpunt functioneert.

Artikel 3

Minimale technische vereisten met betrekking tot betrouwbaarheidsniveaus

De minimale technische vereisten met betrekking tot betrouwbaarheidsniveaus zijn opgenomen in Uitvoeringsverordening (EU) 2015/1502 van de Commissie ([1]).

Artikel 4

Gerelateerde nationale betrouwbaarheidsniveaus

Voor het relateren van nationale betrouwbaarheidsniveaus van aangemelde stelsels voor elektronische identificatie gelden de vereisten van Uitvoeringsverordening (EU) 2015/1502. De resultaten van het relateren worden aangemeld bij de Commissie met behulp van het aanmeldingsmodel dat is opgenomen in Uitvoeringsbesluit (EU) 2015/1505 van de Commissie ([2]).

Artikel 5

Knooppunten

1. Een knooppunt in een lidstaat is in staat een verbinding te maken met de knooppunten van andere lidstaten.

2. De knooppunten zijn in staat om met technische hulpmiddelen onderscheid te maken tussen organen van de publieke sector en andere partijen die van het knooppunt gebruikmaken.

3. De implementatie van de in deze verordening vervatte technische vereisten door een lidstaat legt geen onevenredige technische vereisten of kosten op aan andere lidstaten die naar interoperabiliteit streven met de implementatie die door de eerstgenoemde lidstaat is gekozen.

Artikel 6

Privacy en vertrouwelijkheid van gegevens

1. De bescherming van de privacy en vertrouwelijkheid van de door de knooppunten uitgewisselde gegevens en de handhaving van de integriteit van die gegevens wordt gewaarborgd door middel van de beste beschikbare technische oplossingen en beschermingsmethoden.

2. De knooppunten slaan geen persoonsgegevens op, behalve voor het in artikel 9, lid 3, genoemde doel.

Artikel 7

Integriteit en authenticiteit van de gecommuniceerde gegevens

Bij de communicatie tussen de knooppunten worden de integriteit en de authenticiteit van de gegevens verzekerd, teneinde te waarborgen dat alle verzoeken en responsen authentiek zijn en niet zijn gemanipuleerd. De knooppunten passen daartoe oplossingen toe die bij grensoverschrijdend operationeel gebruik deugdelijk zijn gebleken.

([1]) Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (zie bladzijde 7 van dit Publicatieblad).

([2]) Uitvoeringsbesluit (EU) 2015/1505 van de Commissie van 8 september 2015 tot vaststelling van de technische specificaties en formaten van vertrouwenslijsten overeenkomstig artikel 22, lid 5, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (zie bladzijde 26 van dit Publicatieblad).

Artikel 8

Voor de communicatie te gebruiken berichtformaat

De knooppunten maken voor de syntaxis van de berichten gebruik van gemeenschappelijke berichtformaten die reeds meermalen zijn toegepast door lidstaten en waarvan de deugdelijkheid in een operationele omgeving is aangetoond. De syntaxis maakt het volgende mogelijk:

a) de correcte verwerking van het minimale pakket persoonsidentificatiegegevens dat een natuurlijke persoon of rechtspersoon op unieke wijze vertegenwoordigt;

b) de correcte verwerking van het betrouwbaarheidsniveau van het elektronische identificatiemiddel;

c) het onderscheid tussen organen van de publieke sector en andere partijen die van het knooppunt gebruikmaken;

d) de nodige flexibiliteit om te kunnen voldoen aan de behoefte aan aanvullende attributen met betrekking tot identificatie.

Artikel 9

Beheer van beveiligingsinformatie en metagegevens

1. De exploitant van het knooppunt deelt de metagegevens betreffende het beheer van het knooppunt op veilige en betrouwbare wijze mee, met gebruikmaking van een gestandaardiseerde, machinaal verwerkbare methode.

2. In ieder geval worden de parameters die voor de beveiliging relevant zijn, automatisch opgehaald.

3. De exploitant van het knooppunt slaat gegevens op aan de hand waarvan, in geval van een incident, de uitwisseling van berichten in de juiste volgorde kan worden gereconstrueerd teneinde de plaats en de aard van het incident vast te stellen. De gegevens worden zolang bewaard als volgens de nationale voorschriften vereist is en bevatten ten minste de volgende elementen:

a) de identificatie van het knooppunt;

b) de identificatie van het bericht;

c) de datum en de tijd van het bericht.

Artikel 10

Informatiezekerheid en beveiligingsnormen

1. Ten aanzien van knooppunten die aan het interoperabiliteitskader deelnemen, tonen de exploitanten van knooppunten die authenticatie bieden aan dat het betrokken knooppunt aan de eisen van de norm ISO/IEC 27001 voldoet, door middel van certificering of gelijkwaardige beoordelingsmethoden, dan wel door te voldoen aan de nationale wetgeving.

2. De exploitanten van knooppunten installeren kritieke beveiligingsupdates zonder onnodig uitstel.

Artikel 11

Persoonsidentificatiegegevens

1. Het minimale pakket persoonsidentificatiegegevens dat een natuurlijke persoon of een rechtspersoon op unieke wijze vertegenwoordigt, voldoet bij gebruik in een grensoverschrijdende context aan de vereisten die in de bijlage zijn opgenomen.

2. Het minimale pakket persoonsidentificatiegegevens voor een natuurlijke persoon die een rechtspersoon vertegenwoordigt, bevat bij gebruik in een grensoverschrijdende context een combinatie van de attributen die in de bijlage voor natuurlijke personen en rechtspersonen zijn vermeld.

3. De gegevens worden doorgegeven in het oorspronkelijke schrift, voor zover nodig met een transliteratie in Latijns schrift.

Artikel 12

Technische specificaties

1. Het bij Uitvoeringsbesluit (EU) 2015/296 opgerichte samenwerkingsnetwerk kan overeenkomstig artikel 14, onder d), van dat uitvoeringsbesluit adviezen vaststellen ten aanzien van de noodzaak om technische specificaties vast te stellen, indien dat in verband met de implementatie van het interoperabiliteitskader gerechtvaardigd is. In die technische specificaties worden nadere details geboden inzake de technische vereisten zoals bij deze verordening vastgesteld.

2. Naar aanleiding van het in lid 1 bedoelde advies ontwikkelt de Commissie de technische specificaties in samenwerking met de lidstaten, in het kader van de digitale diensteninfrastructuren van Verordening (EU) nr. 1316/2013.

3. Het samenwerkingsnetwerk stelt overeenkomstig artikel 14, onder d), van Uitvoeringsbesluit (EU) 2015/296 een advies vast waarin het evalueert of en in hoeverre de overeenkomstig lid 2 ontwikkelde technische specificaties overeenstemmen met de behoefte die in het in lid 1 bedoelde advies is vastgesteld of met de in deze verordening vastgestelde vereisten. Het samenwerkingsnetwerk kan aanbevelen dat de lidstaten bij de implementatie van het interoperabiliteitskader rekening houden met de technische specificaties.

4. Als voorbeeld voor de interpretatie van de technische specificaties stelt de Commissie een referentie-implementatie ter beschikking. De lidstaten kunnen deze referentie-implementatie toepassen of als testmateriaal gebruiken bij het testen van andere implementaties van de technische specificaties.

Artikel 13

Geschillenbeslechting

1. Indien mogelijk worden geschillen in verband met het interoperabiliteitskader door de betrokken lidstaten beslecht door middel van onderhandelingen.

2. Als geen oplossing wordt gevonden overeenkomstig lid 1, is het bij artikel 12 van Uitvoeringsbesluit (EU) 2015/296 opgerichte samenwerkingsnetwerk bevoegd om het geschil in overeenstemming met zijn reglement van orde te beslechten.

Artikel 14

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 8 september 2015.

Voor de Commissie

De voorzitter

Jean-Claude JUNCKER

BIJLAGE

Vereisten betreffende het minimale pakket persoonsidentificatiegegevens dat een natuurlijke persoon of rechtspersoon op unieke wijze vertegenwoordigt, als bedoeld in artikel 11

1. **Minimaal gegevenspakket voor een natuurlijke persoon**

Het minimale gegevenspakket voor een natuurlijke persoon bevat al de volgende verplichte attributen:

a) huidige familienaam of familienamen;

b) huidige voornaam of voornamen;

c) geboortedatum;

d) unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat deze zo lang mogelijk stabiel blijft.

Het minimale gegevenspakket voor een natuurlijke persoon kan één of meer van de volgende aanvullende attributen bevatten:

a) voornaam of voornamen en familienaam of familienamen bij geboorte;

b) geboorteplaats;

c) huidig adres;

d) geslacht.

2. **Minimaal gegevenspakket voor een rechtspersoon**

Het minimale gegevenspakket voor een rechtspersoon bevat al de volgende verplichte attributen:

a) huidige wettelijke naam;

b) unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat deze zo lang mogelijk stabiel blijft.

Het minimale gegevenspakket voor een rechtspersoon kan één of meer van de volgende aanvullende attributen bevatten:

a) huidig adres;

b) btw-nummer;

c) fiscaal referentienummer;

d) de identificatiecode bedoeld in artikel 3, lid 1, van Richtlijn 2009/101/EG van het Europees Parlement en de Raad ([1]);

e) de identificatiecode voor juridische entiteiten bedoeld in Uitvoeringsverordening (EU) nr. 1247/2012 van de Commissie ([2]);

f) het registratie- en identificatienummer van marktdeelnemer (EORI-nr.) bedoeld in Uitvoeringsverordening (EU) nr. 1352/2013 van de Commissie ([3]);

g) het accijnsnummer bedoeld in artikel 2, punt 12, van Verordening (EU) nr. 389/2012 van de Raad ([4]).

([1]) Richtlijn 2009/101/EG van het Europees Parlement en de Raad van 16 september 2009 strekkende tot het coördineren van de waarborgen, welke in de lidstaten worden verlangd van de vennootschappen in de zin van de tweede alinea van artikel 48 van het Verdrag, om de belangen te beschermen zowel van de deelnemers in deze vennootschappen als van derden, zulks teneinde die waarborgen gelijkwaardig te maken (PB L 258 van 1.10.2009, blz. 11).

([2]) Uitvoeringsverordening (EU) nr. 1247/2012 van de Commissie van 19 december 2012 tot vaststelling van technische uitvoeringsnormen met betrekking tot de formattering en de frequentie van de transactierapportage aan transactieregisters overeenkomstig Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad betreffende otc-derivaten, centrale tegenpartijen en transactieregisters (PB L 352 van 21.12.2012, blz. 20).

([3]) Uitvoeringsverordening (EU) nr. 1352/2013 van de Commissie van 4 december 2013 tot vaststelling van de formulieren waarin is voorzien in Verordening (EU) nr. 608/2013 van het Europees Parlement en de Raad inzake de handhaving van intellectuele-eigendomsrechten door de douane (PB L 341 van 18.12.2013, blz. 10).

([4]) Verordening (EU) nr. 389/2012 van de Raad van 2 mei 2012 betreffende administratieve samenwerking op het gebied van de accijnzen en houdende intrekking van Verordening (EG) nr. 2073/2004 (PB L 121 van 8.5.2012, blz. 1).

UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE

van 8 september 2015

tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG ([1]), en met name artikel 8, lid 3,

Overwegende hetgeen volgt:

(1) In artikel 8 van Verordening (EU) nr. 910/2014 wordt bepaald dat een stelsel voor elektronische identificatie dat is aangemeld krachtens artikel 9, lid 1, de betrouwbaarheidsniveaus laag, substantieel en hoog omschrijft voor op grond van dat stelsel uitgegeven elektronische identificatiemiddelen.

(2) De minimale technische specificaties, normen en procedures dienen te worden vastgesteld om een uniforme interpretatie te waarborgen van de details van de betrouwbaarheidsniveaus en de interoperabiliteit te verzekeren wanneer de nationale betrouwbaarheidsniveaus van aangemelde stelsels voor elektronische identificatie worden gerelateerd aan de betrouwbaarheidsniveaus volgens artikel 8, zoals bepaald in artikel 12, lid 4, onder b), van Verordening (EU) nr. 910/2014.

(3) Voor het vaststellen van de specificaties en procedures die in deze uitvoeringshandeling zijn opgenomen, is rekening gehouden met de internationale norm ISO/IEC 29115, de belangrijkste internationale norm op het gebied van betrouwbaarheidsniveaus voor elektronische identificatiemiddelen. Verordening (EU) nr. 910/2014 verschilt echter inhoudelijk van die internationale norm, met name wat betreft de vereisten voor het bewijs en de verificatie van de identiteit, alsmede wat betreft de wijze waarop de verschillen tussen de identiteitsregelingen van de lidstaten en de bestaande EU-instrumenten op dat gebied in aanmerking worden genomen. In de bijlage, die weliswaar op deze internationale norm is gestoeld, dient derhalve niet te worden verwezen naar enige specifieke inhoud van ISO/IEC 29115.

(4) Deze verordening is tot stand gekomen volgens een resultaatgestuurde aanpak, omdat die het meest geschikt is; hetzelfde geldt voor de definities van termen en begrippen. Daarbij is rekening gehouden met de doelstelling van Verordening (EU) nr. 910/2014 met betrekking tot de betrouwbaarheidsniveaus voor elektronische identificatiemiddelen. Bij het vaststellen van de specificaties en procedures in deze uitvoeringshandeling moet daarom terdege rekening worden gehouden met het grootschalige proefproject STORK, inclusief de in dat verband ontwikkelde specificaties, alsmede de definities en begrippen in ISO/IEC 29115.

(5) Afhankelijk van de context waarin verificatie van een aspect van het bewijs van de identiteit moet plaatsvinden, kunnen gezaghebbende bronnen in allerlei vormen voorkomen, zoals registers, documenten, instanties en dergelijke. In de verschillende lidstaten kunnen, zelfs in vergelijkbare contexten, verschillende gezaghebbende bronnen bestaan.

(6) De vereisten voor het bewijs en de verificatie van de identiteit dienen verschillende systemen en praktijken in aanmerking te nemen, waarbij een voldoende hoog betrouwbaarheidsniveau moet worden gewaarborgd om het noodzakelijke vertrouwen tot stand te brengen. Procedures die eerder werden gebruikt voor andere doeleinden dan de afgifte van elektronische identificatiemiddelen, mogen dan ook slechts worden aanvaard indien is bevestigd dat die procedures voldoen aan de eisen die voor het overeenkomstige betrouwbaarheidsniveau zijn vastgesteld.

([1]) PB L 257 van 28.8.2014, blz. 73.

(7) Er wordt doorgaans gebruikgemaakt van authenticatiefactoren zoals gedeelde geheime sleutels, fysieke hulpmiddelen en fysieke attributen. Om het authenticatieproces beter te beveiligen, is het echter aan te bevelen om een groter aantal authenticatiefactoren te gebruiken, en dan met name authenticatiefactoren die tot verschillende categorieën behoren.

(8) Deze verordening mag geen afbreuk doen aan de vertegenwoordigingsrechten van rechtspersonen. In de bijlage dienen echter vereisten te worden opgenomen inzake de koppeling tussen de elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen.

(9) Het belang van informatiebeveiliging en servicemanagementsystemen dient te worden erkend, evenals het belang van het gebruik van erkende methoden en toepassing van de beginselen die in normen zoals ISO/IEC 27000 en de normenreeks ISO/IEC 20000 zijn vervat.

(10) Tevens moet rekening worden gehouden met goede praktijken van de lidstaten inzake betrouwbaarheidsniveaus.

(11) Certificatie van de IT-beveiliging op basis van internationale normen is een belangrijk instrument voor de controle of producten voldoen aan de beveiligingseisen van deze uitvoeringshandeling.

(12) Het in artikel 48 van Verordening (EU) nr. 910/2014 bedoelde comité heeft binnen de door zijn voorzitter vastgestelde termijn geen advies uitgebracht,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

1. Voor elektronische identificatiemiddelen die op grond van een aangemeld stelsel voor elektronische identificatie zijn uitgegeven, worden de betrouwbaarheidsniveaus laag, substantieel en hoog bepaald onder verwijzing naar de specificaties en procedures in de bijlage.

2. De specificaties en procedures in de bijlage worden gebruikt voor het bepalen van het betrouwbaarheidsniveau voor elektronische identificatiemiddelen die op grond van een aangemeld stelsel voor elektronische identificatie zijn uitgegeven, door de betrouwbaarheid en de kwaliteit te bepalen van de volgende elementen:

a) inschrijving, zoals bedoeld in punt 2.1 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder a), van Verordening (EU) nr. 910/2014;

b) beheer van elektronische identificatiemiddelen, zoals bedoeld in punt 2.2 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder b) en f), van Verordening (EU) nr. 910/2014;

c) authenticatie, zoals bedoeld in punt 2.3 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder c), van Verordening (EU) nr. 910/2014;

d) beheer en organisatie, zoals bedoeld in punt 2.4 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder d) en e), van Verordening (EU) nr. 910/2014.

3. Indien het elektronische identificatiemiddel dat op grond van een aangemeld stelsel voor elektronische identificatie is uitgegeven, voldoet aan een vereiste dat voor een hoger betrouwbaarheidsniveau is vermeld, wordt het geacht ook te voldoen aan het overeenkomstige vereiste voor een lager betrouwbaarheidsniveau.

4. Tenzij in het desbetreffende deel van de bijlage anders is aangegeven, kan een elektronisch identificatiemiddel dat op grond van een aangemeld stelsel voor elektronische identificatie is uitgegeven, slechts aan het opgegeven betrouwbaarheidsniveau voldoen indien is voldaan aan alle elementen die in de bijlage voor dat betrouwbaarheidsniveau zijn vermeld.

Artikel 2

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 8 september 2015.

Voor de Commissie

De voorzitter

Jean-Claude JUNCKER

BIJLAGE

Technische specificaties en procedures voor de betrouwbaarheidsniveaus laag, substantieel en hoog betreffende op grond van een aangemeld stelsel voor elektronische identificatie uitgegeven elektronische identificatiemiddelen

1. Definities

Voor de toepassing van deze bijlage wordt verstaan onder:

1. „gezaghebbende bron": elke bron, ongeacht de vorm ervan, waarvan kan worden verwacht dat deze nauwkeurige gegevens, informatie of bewijsmateriaal biedt op basis waarvan een identiteit kan worden aangetoond;

2. „authenticatiefactor": een factor waarvan is bevestigd dat deze gebonden is aan een persoon en die onder een van de volgende categorieën valt:

   a) „op bezit gebaseerde authenticatiefactor": een authenticatiefactor waarvan de betrokkene moet aantonen dat deze in zijn bezit is;

   b) „op kennis gebaseerde authenticatiefactor": een authenticatiefactor waarvan de betrokkene moet aantonen dat hij ervan kennis draagt;

   c) „inherente authenticatiefactor": een authenticatiefactor die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit;

3. „dynamische authenticatie": een elektronisch proces, dat met gebruikmaking van cryptografie of een andere techniek de middelen biedt om op verzoek een elektronisch bewijs op te maken dat de betrokkene de controle heeft over of in het bezit is van de identificatiegegevens, en dat verandert telkens als authenticatie plaatsvindt tussen de betrokkene en het systeem dat diens identiteit verifieert;

4. „beheerssysteem voor informatiebeveiliging": een geheel van processen en procedures die zijn ontworpen om de informatieveiligheidsrisico's tot een aanvaardbaar niveau te beperken.

2. Technische specificaties en procedures

Aan de hand van de in deze bijlage beschreven elementen van de technische specificaties en procedures wordt bepaald op welke wijze de vereisten en criteria van artikel 8 van Verordening (EU) nr. 910/2014 worden toegepast op elektronische identificatiemiddelen die zijn uitgegeven op grond van een stelsel voor elektronische identificatie.

2.1. *Inschrijving*

2.1.1. Aanvraag en registratie

Betrouwbaarheids-niveau	Vereiste elementen
Laag	1. De aanvrager moet bekend zijn met de voorwaarden die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. 2. De aanvrager moet bekend zijn met de aanbevolen veiligheidsvoorzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. 3. De relevante identiteitsgegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, moeten zijn verzameld.
Substantieel	Hetzelfde als niveau laag.
Hoog	Hetzelfde als niveau laag.

2.1.2. Bewijs en verificatie van identiteit (natuurlijke persoon)

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. De persoon kan worden verondersteld in het bezit te zijn van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt. 2. Het bewijs kan worden verondersteld echt te zijn, dan wel volgens een gezaghebbende bron te bestaan, en het bewijs lijkt geldig te zijn. 3. Een gezaghebbende bron weet dat de opgegeven identiteit bestaat en er kan worden verondersteld dat de persoon die de identiteit opgeeft, dezelfde persoon is.
Substantieel	Niveau laag plus een van de onder de punten 1 tot en met 4 vermelde alternatieven. 1. Er is geverifieerd dat de persoon in het bezit is van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt; en het bewijs is gecontroleerd op de echtheid ervan; of het bestaan ervan is volgens een gezaghebbende bron bekend en het heeft betrekking op een werkelijk bestaande persoon; en er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat het bewijsstuk verloren, gestolen, geschorst, ingetrokken of verlopen is. of 2. Er is een identiteitsdocument overgelegd tijdens een registratieproces in de lidstaat waar het document is afgegeven, en het document lijkt betrekking te hebben op de persoon die het heeft overgelegd; en er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn. of 3. Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau substantieel, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad ([1]) of een daaraan gelijkwaardige instantie. of 4. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau substantieel of hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie.

Betrouwbaarheidsniveau	Vereiste elementen
Hoog	Er moet zijn voldaan aan de vereisten van punt 1 of punt 2. 1. Niveau substantieel plus een van de onder a) tot en met c) vermelde alternatieven. a) Indien is geverifieerd dat de persoon in het bezit is van een bewijs dat voorzien is van een foto of biometrische gegevens, dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt, wordt het bewijs gecontroleerd op geldigheid aan de hand van een gezaghebbende bron; en de door de aanvrager opgegeven identiteit wordt geverifieerd door vergelijking van één of meer fysieke kenmerken van de persoon met een gezaghebbende bron. of b) Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau hoog, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie; en er zijn maatregelen getroffen om aan te tonen dat de resultaten van de eerdere procedures nog steeds geldig zijn. of c) Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie. en er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere uitgifteprocedure van een aangemeld elektronisch identificatiemiddel nog steeds geldig zijn. OF 2. Indien de aanvrager geen erkend identiteitsdocument met een foto of biometrische kenmerken overlegt, worden dezelfde procedures toegepast die op nationaal niveau van toepassing zijn in de lidstaat van de verantwoordelijke instantie voor de verkrijging van een dergelijk bewijsstuk met foto of biometrische kenmerken.

([1]) Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PB L 218 van 13.8.2008, blz. 30).

2.1.3. Bewijs en verificatie van identiteit (rechtspersoon)

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. De opgegeven identiteit van de rechtspersoon wordt aangetoond aan de hand van een bewijsstuk dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan.

Betrouwbaarheidsniveau	Vereiste elementen
	2. Het bewijsstuk lijkt geldig en kan worden verondersteld echt te zijn dan wel volgens een gezaghebbende bron te bestaan, indien de rechtspersoon op vrijwillige basis in de gezaghebbende bron is opgenomen op basis van een regeling tussen de rechtspersoon en de gezaghebbende bron. 3. De rechtspersoon bevindt zich volgens een gezaghebbende bron niet in een toestand die verhindert dat zij als die rechtspersoon optreedt.
Substantieel	Niveau laag plus een van de onder de punten 1 tot en met 3 vermelde alternatieven. 1. De opgegeven identiteit van de rechtspersoon wordt aangetoond aan de hand van een bewijsstuk dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, inclusief de naam, de rechtsvorm en (indien van toepassing) het registratienummer van de rechtspersoon; en het bewijsstuk wordt gecontroleerd om te bepalen of het echt is dan wel volgens een gezaghebbende bron bestaat, indien de rechtspersoon in de gezaghebbende bron is opgenomen omdat dat voor de rechtspersoon verplicht is om in de betrokken sector actief te mogen zijn; en er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de rechtspersoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn. of 2. Indien de procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.3 voor het betrouwbaarheidsniveau substantieel, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie. of 3. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau substantieel of hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie.
Hoog	Niveau substantieel plus een van de onder de punten 1 tot en met 3 vermelde alternatieven. 1. De opgegeven identiteit van de rechtspersoon wordt aangetoond aan de hand van een bewijsstuk dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, inclusief de naam en de rechtsvorm van de rechtspersoon en ten minste één in een nationale context gebruikte unieke identificatiecode die de rechtspersoon vertegenwoordigt; en het bewijs is gecontroleerd om de geldigheid ervan volgens een gezaghebbende bron te bepalen. of

Betrouwbaarheidsniveau	Vereiste elementen
	2. Indien de procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.3 voor het betrouwbaarheidsniveau hoog, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie; en er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere procedure nog steeds geldig zijn. of 3. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau hoog, is het niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie; en er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere uitgifteprocedure van een aangemeld elektronisch identificatiemiddel nog steeds geldig zijn.

2.1.4. Koppeling tussen de elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen

Indien van toepassing gelden de volgende voorwaarden voor de koppeling tussen het elektronische identificatiemiddel van een natuurlijke persoon en het elektronische identificatiemiddel van een rechtspersoon:

1. Het moet mogelijk zijn een koppeling te schorsen en/of te herroepen. De verschillende koppelingsstadia (o.a. activering, schorsing, hernieuwing, herroeping) worden beheerd volgens op nationaal niveau erkende procedures.

2. De natuurlijke persoon wiens elektronische identificatiemiddel is gekoppeld aan het elektronische identificatiemiddel van de rechtspersoon kan volgens op nationaal niveau erkende procedures de uitoefening van de koppeling delegeren aan een andere natuurlijke persoon. De delegerende natuurlijke persoon blijft echter aansprakelijk.

3. De koppeling wordt op de volgende wijze uitgevoerd:

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er is geverifieerd dat het bewijs van de identiteit van de natuurlijke persoon die namens de rechtspersoon optreedt, heeft plaatsgevonden op het niveau laag of hoger. 2. De koppeling is tot stand gebracht volgens op nationaal niveau erkende procedures. 3. De natuurlijke persoon bevindt zich volgens een gezaghebbende bron niet in een toestand die verhindert dat hij namens die rechtspersoon optreedt.
Substantieel	Punt 3 van niveau laag, plus: 1. er is geverifieerd dat het bewijs van de identiteit van de natuurlijke persoon die namens de rechtspersoon optreedt, heeft plaatsgevonden op het niveau substantieel of hoog;

Betrouwbaarheidsniveau	Vereiste elementen
	2. de koppeling is tot stand gebracht volgens op nationaal niveau erkende procedures, wat ertoe heeft geleid dat de koppeling in een gezaghebbende bron is geregistreerd; 3. de koppeling is geverifieerd op basis van informatie uit een gezaghebbende bron.
Hoog	Punt 3 van niveau laag en punt 2 van niveau substantieel, plus: 1. er is geverifieerd dat het bewijs van de identiteit van de natuurlijke persoon die namens de rechtspersoon optreedt, heeft plaatsgevonden op het niveau hoog; 2. de koppeling is geverifieerd op basis van een in een nationale context gebruikte unieke identificatiecode die de rechtspersoon vertegenwoordigt, en op basis van uit een gezaghebbende bron afkomstige informatie die op unieke wijze een natuurlijke persoon vertegenwoordigt.

2.2. *Beheer van elektronische identificatiemiddelen*

2.2.1. Kenmerken en ontwerp van elektronische identificatiemiddelen

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Het elektronische identificatiemiddel maakt gebruik van ten minste één authenticatiefactor. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat de uitgever ervan redelijke stappen onderneemt om te verifiëren dat het slechts wordt gebruikt door of onder controle van de persoon aan wie het toebehoort.
Substantieel	1. Het elektronische identificatiemiddel maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon aan wie het toebehoort.
Hoog	Niveau substantieel, plus: 1. Het elektronische identificatiemiddel biedt bescherming tegen kopiëring en vervalsing en tegen aanvallers met een hoog aanvalspotentieel. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat het door de persoon aan wie het toebehoort op betrouwbare wijze kan worden beschermd tegen gebruik door anderen.

2.2.2. Uitgifte, uitreiking en activering

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee het kan worden verondersteld alleen de beoogde persoon te bereiken.
Substantieel	Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee kan worden verondersteld dat alleen de persoon aan wie het toebehoort in het bezit ervan wordt gesteld.
Hoog	Bij het activeringsproces wordt geverifieerd dat slechts de persoon aan wie het elektronische identificatiemiddel toebehoort ervan in het bezit wordt gesteld.

2.2.3. Schorsing, herroeping en reactivering

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Het is mogelijk het elektronische identificatiemiddel snel en doeltreffend te schorsen en/of te herroepen. 2. Er bestaan maatregelen om ongeoorloofde schorsing, herroeping en reactivering te voorkomen. 3. Een elektronisch identificatiemiddel mag slechts worden gereactiveerd indien nog steeds wordt voldaan aan dezelfde betrouwbaarheidsvereisten als die welke voorafgaand aan de schorsing of herroeping van kracht waren.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

2.2.4. Verlenging en vervanging

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Rekening houdend met het risico dat de persoonsidentificatiegegevens zijn gewijzigd, moet voor verlenging of vervanging aan dezelfde betrouwbaarheidsvereisten zijn voldaan als voor het initiële proces van bewijs en verificatie van de identiteit, of moet worden uitgegaan van een geldig elektronisch identificatiemiddel met hetzelfde of een hoger betrouwbaarheidsniveau.
Substantieel	Zelfde als niveau laag.
Hoog	Niveau laag, plus: Als voor verlenging of vervanging wordt uitgegaan van een geldig elektronisch identificatiemiddel, worden de identiteitsgegevens geverifieerd aan de hand van een gezaghebbende bron.

2.3. *Authenticatie*

Dit onderdeel is met name gericht op dreigingen die gepaard gaan met het gebruik van het authenticatiemechanisme. Het vermeldt de vereisten voor elk van de betrouwbaarheidsniveaus. In dit onderdeel wordt ervan uitgegaan dat de controles in overeenstemming zijn met de risico's op het desbetreffende niveau.

2.3.1. Authenticatiemechanisme

In onderstaande tabel worden voor elk betrouwbaarheidsniveau de vereisten weergegeven voor het authenticatiemechanisme, door middel waarvan de natuurlijke persoon of rechtspersoon het elektronische identificatiemiddel gebruikt om zijn identiteit te bevestigen tegenover een vertrouwende partij.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd. 2. Indien als onderdeel van het authenticatiemechanisme persoonsidentificatiegegevens worden opgeslagen, wordt die informatie beveiligd ter bescherming tegen verlies en schending, met inbegrip van offlineanalyse. 3. Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een laag aanvalspotentieel.

Betrouwbaarheidsniveau	Vereiste elementen
Substantieel	Niveau laag, plus: 1. Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd door middel van dynamische authenticatie. 2. Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een gematigd aanvalspotentieel.
Hoog	Niveau substantieel, plus: Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een hoog aanvalspotentieel.

2.4. *Beheer en organisatie*

Alle deelnemers die een dienst verlenen op het gebied van elektronische identificatie in een grensoverschrijdende context (hierna „aanbieders" genoemd) beschikken over gedocumenteerde methoden en beleid voor het beheer van informatiebeveiliging, benaderingen voor risicobeheersing en andere erkende controlemethoden, zodat zij de bevoegde bestuursorganen van de lidstaten op het gebied van stelsels voor elektronische identificatie garanties kunnen bieden dat in doeltreffende praktijken is voorzien. In onderdeel 2.4 wordt ervan uitgegaan dat alle vereisten/elementen in overeenstemming zijn met de risico's op het desbetreffende niveau.

2.4.1. Algemene bepalingen

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Aanbieders die een operationele dienst aanbieden die onder deze verordening valt, zijn een overheidsinstantie of een rechtspersoon die door het nationale recht van een lidstaat als zodanig wordt erkend, over een gevestigde organisatie beschikt en volledig operationeel is op alle gebieden die voor de verlening van de diensten relevant zijn. 2. De aanbieders voldoen aan al hun wettelijke verplichtingen in verband met het verrichten en leveren van de dienst, onder meer wat betreft de soorten informatie die mogen worden gevraagd, de wijze waarop het bewijs van de identiteit wordt geleverd, welke informatie mag worden bewaard en hoe lang deze mag worden bewaard. 3. De aanbieders kunnen aantonen dat zij in staat zijn het risico van de aansprakelijkheid voor schade op zich te nemen en over voldoende financiële middelen beschikken om hun activiteiten en de dienstverlening voort te zetten. 4. De aanbieders zijn verantwoordelijk voor het naleven van alle verplichtingen die zij aan andere entiteiten hebben uitbesteed en voor het voldoen aan het beleid inzake het stelsel, op dezelfde wijze als wanneer zij deze taken zelf vervulden. 5. Stelsels voor elektronische identificatie die niet volgens nationaal recht zijn opgezet, moeten over een doeltreffend beëindigingsplan beschikken. Dat plan omvat voorzieningen voor de ordelijke stopzetting van de dienstverlening of de voortzetting daarvan door een andere aanbieder, voor de wijze waarop de betrokken autoriteiten en eindgebruikers worden ingelicht, alsook voor de wijze waarop de administratie wordt beschermd, bewaard en vernietigd overeenkomstig het voor het stelsel geldende beleid.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

2.4.2. Gepubliceerde mededelingen en informatie voor de gebruikers

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er bestaat een gepubliceerde beschrijving van de dienst met alle toepasselijke voorwaarden en vergoedingen, inclusief eventuele gebruiksbeperkingen. De beschrijving van de dienst omvat een privacyverklaring. 2. Er dient te worden voorzien in passend beleid en passende procedures om de gebruikers van de dienst tijdig en op betrouwbare wijze te informeren over elke wijziging van de beschrijving van de dienst, alle toepasselijke voorwaarden en de privacyverklaring. 3. Er dient te worden voorzien in passend beleid en passende procedures om verzoeken om informatie volledig en correct te beantwoorden.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

2.4.3. Beheer van informatiebeveiliging

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Er bestaat een doeltreffend beheerssysteem voor informatiebeveiliging dat zorg draagt voor het beheer en de beheersing van informatiebeveiligingsrisico's.
Substantieel	Niveau laag, plus: Het beheerssysteem voor informatiebeveiliging voldoet aan beproefde normen en beginselen voor het beheer en de beheersing van informatiebeveiligingsrisico's.
Hoog	Zelfde als niveau substantieel.

2.4.4. Bijhouden van de administratie

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Relevante informatie wordt vastgelegd en bewaard met behulp van een doeltreffend documentenbeheersysteem, met inachtneming van de toepasselijke wetgeving en goede praktijken op het gebied van gegevensbescherming en gegevensbewaring. 2. De gegevens moeten worden bewaard voor zover dat is toegestaan door het nationale recht of een andere nationale bestuurlijke regeling, en beschermd gedurende de termijn die noodzakelijk is met het oog op financiële controle en onderzoek van beveiligingsinbreuken; na afloop van de bewaringstermijn worden de gegevens veilig vernietigd.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

2.4.5. Faciliteiten en personeel

Onderstaande tabel bevat de vereisten inzake faciliteiten alsmede inzake personeelsleden en eventuele subcontractanten die taken uitvoeren die onder deze verordening vallen. Aan elk van de vereisten moet worden voldaan in verhouding tot het risiconiveau waarmee het desbetreffende betrouwbaarheidsniveau gepaard gaat.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er zijn procedures om te waarborgen dat personeelsleden en subcontractanten voldoende zijn opgeleid en gekwalificeerd en dat zij ervaren zijn in de vaardigheden die vereist zijn voor de taken die zij vervullen. 2. Er zijn voldoende personeelsleden en subcontractanten om de dienstverlening voldoende te waarborgen overeenkomstig het beleid en de procedures. 3. De voor de dienstverlening gebruikte faciliteiten staan onder permanente controle en worden permanent beschermd tegen schade door milieu-invloeden, ongeoorloofde toegang en andere factoren die de veiligheid van de dienst kunnen aantasten. 4. De voor de dienstverlening gebruikte faciliteiten zijn zodanig ingericht dat de toegang tot zones met persoonsgegevens, cryptografische gegevens en andere gevoelige informatie beperkt is tot bevoegde personeelsleden of subcontractanten.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

2.4.6. Technische controles

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er is voorzien in proportionele controles ter beheersing van de risico's voor de veiligheid van de diensten, waarbij de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkte informatie worden beschermd. 2. De elektronische communicatiekanalen die voor de uitwisseling van persoonsgegevens en gevoelige gegevens worden gebruikt, worden beschermd tegen afluisteren, manipuleren en herafspelen. 3. De toegang tot gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, is beperkt tot de uitoefening van taken en toepassingen waarvoor de toegang strikt noodzakelijk is. Er wordt op toegezien dat dergelijk materiaal niet permanent in onversleutelde staat wordt opgeslagen. 4. Er zijn procedures die waarborgen dat de veiligheid duurzaam wordt gehandhaafd en dat een respons mogelijk is op wijzigingen van het risiconiveau, incidenten en veiligheidsinbreuken. 5. Alle media die persoonsgegevens, cryptografische informatie of andere gevoelige informatie bevatten, worden veilig opgeslagen, vervoerd en verwijderd.
Substantieel	Zelfde als niveau laag, plus: Gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, wordt beschermd tegen ongeoorloofde manipulatie.
Hoog	Zelfde als niveau substantieel.

2.4.7. Compliance en audit

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Er vinden periodieke interne audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen.

Betrouwbaarheids-niveau	Vereiste elementen
Substantieel	Er vinden periodieke onafhankelijke interne of externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen.
Hoog	1. Er vinden periodieke onafhankelijke externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen. 2. Indien een stelsel wordt beheerd door een overheidsinstantie, vinden audits plaats overeenkomstig het nationaal recht.

UITVOERINGSVERORDENING (EU) 2015/1503 VAN DE COMMISSIE

van 8 september 2015

tot vaststelling van de forfaitaire invoerwaarden voor de bepaling van de invoerprijs van bepaalde groenten en fruit

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 1308/2013 van het Europees Parlement en de Raad van 17 december 2013 tot vaststelling van een gemeenschappelijke ordening van de markten voor landbouwproducten en tot intrekking van de Verordeningen (EEG) nr. 922/72, (EEG) nr. 234/79, (EG) nr. 1037/2001 en (EG) nr. 1234/2007 van de Raad ([1]),

Gezien Uitvoeringsverordening (EU) nr. 543/2011 van de Commissie van 7 juni 2011 tot vaststelling van nadere bepalingen voor de toepassing van Verordening (EG) nr. 1234/2007 van de Raad, wat de sectoren groenten en fruit en verwerkte groenten en fruit betreft ([2]), en met name artikel 136, lid 1,

Overwegende hetgeen volgt:

(1) Bij Uitvoeringsverordening (EU) nr. 543/2011 zijn, op grond van de resultaten van de multilaterale handelsbesprekingen van de Uruguayronde, de criteria vastgesteld aan de hand waarvan de Commissie voor de producten en de perioden die in bijlage XVI, deel A, bij die verordening zijn vermeld, de forfaitaire waarden bij invoer uit derde landen vaststelt.

(2) De forfaitaire invoerwaarde wordt elke dag berekend overeenkomstig artikel 136, lid 1, van Uitvoeringsverordening (EU) nr. 543/2011, met inachtneming van de variabele gegevens voor die dag. Bijgevolg moet deze verordening in werking treden op de dag van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

De in artikel 136 van Uitvoeringsverordening (EU) nr. 543/2011 bedoelde forfaitaire invoerwaarden worden vastgesteld in de bijlage bij de onderhavige verordening.

Artikel 2

Deze verordening treedt in werking op de dag van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 8 september 2015.

Voor de Commissie,
namens de voorzitter,
Jerzy PLEWA
Directeur-generaal Landbouw en Plattelandsontwikkeling

([1]) PB L 347 van 20.12.2013, blz. 671.
([2]) PB L 157 van 15.6.2011, blz. 1.

BIJLAGE

Forfaitaire invoerwaarden voor de bepaling van de invoerprijs van bepaalde groenten en fruit

(EUR/100 kg)

GN-code	Code derde landen (1)	Forfaitaire invoerwaarde
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)

GN-code	Code derde landen (1)	Forfaitaire invoerwaarde
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Landennomenclatuur vastgesteld bij Verordening (EU) nr. 1106/2012 van de Commissie van 27 november 2012 tot uitvoering van Verordening (EG) nr. 471/2009 van het Europees Parlement en de Raad betreffende communautaire statistieken van de buitenlandse handel met derde landen, wat de bijwerking van de nomenclatuur van landen en gebieden betreft (PB L 328 van 28.11.2012, blz. 7). De code „ZZ" staat voor „overige oorsprong".

BESLUITEN

UITVOERINGSBESLUIT (EU) 2015/1504 VAN DE COMMISSIE

van 7 september 2015

waarbij aan bepaalde lidstaten afwijkingen worden toegestaan ten aanzien van de indiening van statistieken overeenkomstig Verordening (EG) nr. 1099/2008 van het Europees Parlement en de Raad betreffende energiestatistieken

(Kennisgeving geschied onder nummer C(2015) 6105)

(Slechts de teksten in de Nederlandse, Estse, Franse, Griekse en Slowaakse taal zijn authentiek)

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EG) nr. 1099/2008 van het Europees Parlement en de Raad van 22 oktober 2008 betreffende energiestatistieken ([1]), en met name artikel 5, lid 4, en artikel 10, lid 2,

Overwegende hetgeen volgt:

(1) Op naar behoren gemotiveerd verzoek van een lidstaat kunnen, ingevolge artikel 5, lid 4, van Verordening (EG) nr. 1099/2008 afwijkingen worden toestaan van die elementen van de nationale statistieken die voor de respondenten een buitensporige last zouden meebrengen.

(2) België, Estland, Cyprus en Slowakije hebben om afwijkingen verzocht ten aanzien van de indiening van statistieken betreffende het gedetailleerde energieverbruik in huishoudens per type eindgebruik voor bepaalde referentiejaren.

(3) De door deze lidstaten verstrekte informatie rechtvaardigt de toekenning van de afwijkingen.

(4) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het Comité voor het Europees statistisch systeem,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

De volgende afwijkingen van de bepalingen van Verordening (EG) nr. 1099/2008 worden toegestaan:

1) België wordt een afwijking verleend voor de productie van resultaten voor het referentiejaar 2015 voor punt 1.2.3, posten 4.2.1 tot en met 4.2.5, punt 2.2.3, posten 4.2.1 tot en met 4.2.5, punt 3.2.3, posten 3.1 tot en met 3.6, punt 4.2.3, posten 7.2.1 tot en met 7.2.5, en punt 5.2.4, posten 4.2.1 tot en met 4.2.5, van bijlage B betreffende het gedetailleerde energieverbruik in huishoudens per type eindgebruik (zoals omschreven in punt 2.3, post 26 „Overige sectoren — woningen" van bijlage A).

([1]) PB L 304 van 14.11.2008, blz. 1.

2) Estland wordt een afwijking verleend voor de productie van resultaten voor de referentiejaren 2015, 2016 en 2017 voor punt 1.2.3, posten 4.2.1 tot en met 4.2.5, punt 2.2.3, posten 4.2.1 tot en met 4.2.5, punt 3.2.3, posten 3.1 tot en met 3.6, punt 4.2.3, posten 7.2.1 tot en met 7.2.5, en punt 5.2.4, posten 4.2.1 tot en met 4.2.5, van bijlage B betreffende het gedetailleerde energieverbruik in huishoudens per type eindgebruik (zoals omschreven in punt 2.3, post 26 „Overige sectoren — woningen" van bijlage A).

3) Cyprus wordt een afwijking verleend voor de productie van resultaten voor de referentiejaren 2015, 2016 en 2017 voor punt 1.2.3, posten 4.2.1 tot en met 4.2.5, punt 2.2.3, posten 4.2.1 tot en met 4.2.5, punt 3.2.3, posten 3.1 tot en met 3.6, en punt 5.2.4, posten 4.2.1 tot en met 4.2.5, van bijlage B betreffende het gedetailleerde energieverbruik in huishoudens per type eindgebruik (zoals omschreven in punt 2.3, post 26 „Overige sectoren — woningen" van bijlage A).

4) Slowakije wordt een afwijking verleend voor de productie van resultaten voor de referentiejaren 2015 en 2016 voor punt 1.2.3, posten 4.2.1 tot en met 4.2.5, punt 2.2.3, posten 4.2.1 tot en met 4.2.5, punt 3.2.3, posten 3.1 tot en met 3.6, punt 4.2.3, posten 7.2.1 tot en met 7.2.5, en punt 5.2.4, posten 4.2.1 tot en met 4.2.5, van bijlage B betreffende het gedetailleerde energieverbruik in huishoudens per type eindgebruik (zoals omschreven in punt 2.3, post 26 „Overige sectoren — woningen" van bijlage A).

Artikel 2

Dit besluit is gericht tot het Koninkrijk België, de Republiek Estland, de Republiek Cyprus, en de Slowaakse Republiek.

Gedaan te Brussel, 7 september 2015.

Voor de Commissie
Marianne THYSSEN
Lid van de Commissie

UITVOERINGSBESLUIT (EU) 2015/1505 VAN DE COMMISSIE

van 8 september 2015

tot vaststelling van de technische specificaties en formaten van vertrouwenslijsten overeenkomstig artikel 22, lid 5, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG ([1]), en met name artikel 22, lid 5,

Overwegende hetgeen volgt:

(1) Vertrouwenslijsten zijn essentieel voor het opbouwen van vertrouwen tussen marktdeelnemers, omdat zij informatie bevatten over de status van de dienstverlener op het moment van toezicht.

(2) Elektronische handtekeningen kunnen gemakkelijker grensoverschrijdend worden gebruikt door Beschikking 2009/767/EG van de Commissie ([2]), volgens welke de lidstaten vertrouwenslijsten moeten opzetten, bijhouden en publiceren. Die lijsten bevatten onder meer informatie over certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven overeenkomstig Richtlijn 1999/93/EG van het Europees Parlement en de Raad ([3]), en die onder toezicht staan van en worden geaccrediteerd door de lidstaten.

(3) Volgens artikel 22 van Verordening (EU) nr. 910/2014 moeten de lidstaten op een veilige manier elektronisch ondertekende of verzegelde vertrouwenslijsten opstellen, bijhouden en publiceren in een formaat dat geschikt is voor automatische verwerking en moeten zij de Commissie in kennis stellen van de organen die verantwoordelijk zijn voor het opstellen van de nationale vertrouwenslijsten.

(4) Een verlener van vertrouwensdiensten en de door hem verleende vertrouwensdiensten moeten gekwalificeerd worden geacht als de gekwalificeerde status verbonden is aan de verlener in de vertrouwenslijst. Om ervoor te zorgen dat de overige verplichtingen van Verordening (EU) nr. 910/2014, in het bijzonder die van de artikelen 27 en 37, gemakkelijk vanop afstand en met elektronische middelen door de dienstverleners kunnen worden vervuld, en om tegemoet te komen aan het gewettigd vertrouwen van de overige certificatiedienstverleners die geen gekwalificeerde certificaten afgeven maar diensten verlenen die betrekking hebben op elektronische handtekeningen in de zin van Richtlijn 1999/93/EG en uiterlijk op 30 juni 2016 in een lijst zijn opgenomen, moeten de lidstaten andere dan de gekwalificeerde vertrouwensdiensten op vrijwillige basis en op nationaal niveau in de vertrouwenslijsten kunnen opnemen, op voorwaarde dat duidelijk wordt aangegeven dat die niet zijn gekwalificeerd volgens Verordening (EU) nr. 910/2014.

(5) In overeenstemming met overweging 25 van Verordening (EU) nr. 910/2014 kunnen de lidstaten andere soorten nationaal gedefinieerde vertrouwensdiensten opnemen dan die welke zijn vastgesteld in artikel 3, lid 16, van Verordening (EU) nr. 910/2014, op voorwaarde dat duidelijk wordt aangegeven dat die niet zijn gekwalificeerd volgens Verordening (EU) nr. 910/2014.

(6) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 48 van Verordening (EU) nr. 910/2014 ingestelde comité,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Door de lidstaten worden vertrouwenslijsten opgesteld, gepubliceerd en bijgehouden met informatie over de gekwalificeerde verleners van vertrouwensdiensten die zij controleren, alsmede informatie over de gekwalificeerde vertrouwensdiensten die door hen worden verleend. Die lijsten moeten voldoen aan de technische specificaties van bijlage I.

([1]) PB L 257 van 28.8.2014, blz. 73.
([2]) Beschikking 2009/767/EG van de Commissie van 16 oktober 2009 inzake maatregelen voor een gemakkelijker gebruik van elektronische procedures via het „één-loket" in het kader van Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt (PB L 274 van 20.10.2009, blz. 36).
([3]) Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PB L 13 van 19.1.2000, blz. 12).

Artikel 2

De lidstaten kunnen in de vertrouwenslijsten informatie over niet-gekwalificeerde verleners van vertrouwensdiensten opnemen, alsmede informatie over de niet-gekwalificeerde vertrouwensdiensten die door hen worden verleend. De lijst vermeldt duidelijk welke verleners van vertrouwensdiensten en welke door hen verleende vertrouwensdiensten niet gekwalificeerd zijn.

Artikel 3

1. Overeenkomstig artikel 22, lid 2, van Verordening (EU) nr. 910/2014 moeten de lidstaten de versie van hun vertrouwenslijst die geschikt is voor automatische verwerking, elektronisch ondertekenen of verzegelen volgens de technische specificaties van bijlage I.

2. Als een lidstaat een menselijk leesbare versie van de vertrouwenslijst publiceert, zorgt hij ervoor dat die versie van de vertrouwenslijst dezelfde gegevens bevat als de automatisch verwerkbare versie en ondertekent of verzegelt hij die elektronisch volgens de technische specificaties van bijlage I.

Artikel 4

1. De lidstaten stellen de Commissie in kennis van de gegevens als bedoeld in artikel 22, lid 3, van Verordening (EU) nr. 910/2014 volgens het model in bijlage II.

2. De in lid 1 bedoelde informatie omvat twee of meer publieke sleutelcertificaten van uitvoerders van de regeling, met niet-gelijklopende geldigheidstermijnen van ten minste drie maanden, die overeenkomen met de privésleutels die kunnen worden gebruikt voor het elektronisch ondertekenen of verzegelen van de voor automatische verwerking geschikte versie van de vertrouwenslijst en van de menselijk leesbare versie, als die is gepubliceerd.

3. Overeenkomstig artikel 22, lid 4, van Verordening (EU) nr. 910/2014 maakt de Commissie via een beveiligd kanaal naar een geauthenticeerde webserver de informatie bekend als bedoeld in de leden 1 en 2, zoals aangemeld door de lidstaten, in een ondertekende of verzegelde versie die geschikt is voor automatische verwerking.

4. De Commissie kan via een beveiligd kanaal naar een geauthenticeerde webserver de informatie als bedoeld in de leden 1 en 2 en zoals aangemeld door de lidstaten, bekendmaken in een ondertekende of verzegelde menselijk leesbare versie.

Artikel 5

Dit besluit treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Dit besluit is verbindend in al zijn onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 8 september 2015.

Voor de Commissie

De voorzitter

Jean-Claude JUNCKER

BIJLAGE I

TECHNISCHE SPECIFICATIES VOOR EEN GEMEENSCHAPPELIJK MODEL VOOR VERTROUWENSLIJSTEN

HOOFDSTUK I

ALGEMENE VOORSCHRIFTEN

De vertrouwenslijsten bevatten zowel de huidige als historische gegevens over de status van vertrouwensdiensten, te rekenen vanaf de opneming van een verlener van vertrouwensdiensten in de vertrouwenslijsten.

De woorden „goedgekeurd", „geaccrediteerd" en/of „onder toezicht" in deze specificaties hebben ook betrekking op de nationale goedkeuringsregelingen, maar de lidstaten verstrekken in hun vertrouwenslijsten bijkomende informatie over de aard van elke nationale regeling, met inbegrip van een toelichting op de mogelijke verschillen met de toezichtregelingen die worden toegepast op gekwalificeerde verleners van vertrouwensdiensten en de door hen geleverde gekwalificeerde vertrouwensdiensten.

De informatie in de vertrouwenslijst is in de eerste plaats bedoeld om de validering van tokens voor gekwalificeerde vertrouwensdiensten te ondersteunen: dit zijn fysieke of binaire (logische) objecten die worden verkregen of uitgegeven als gevolg van het gebruik van een gekwalificeerde vertrouwensdienst, bijvoorbeeld gekwalificeerde elektronische handtekeningen en zegels, geavanceerde elektronische handtekeningen en zegels die door een gekwalificeerd certificaat worden ondersteund, gekwalificeerde tijdstempels, gekwalificeerde elektronische bewijzen van afgifte enz.

HOOFDSTUK II

GEDETAILLEERDE SPECIFICATIES VOOR EEN GEMEENSCHAPPELIJK MODEL VOOR VERTROUWENSLIJSTEN

De onderhavige specificaties zijn gebaseerd op de specificaties en vereisten in ETSI TS 119 612 v2.1.1 (hierna „ETSI TS 119 612" genoemd).

Als in de onderhavige specificaties geen specifieke vereisten worden gesteld, zijn de vereisten van clausules 5 en 6 van ETSI TS 119 612 volledig van toepassing. Als in de onderhavige specificaties specifieke vereisten worden gesteld, hebben die voorrang op de overeenkomstige vereisten in ETSI TS 119 612. In geval van afwijkingen tussen de onderhavige specificaties en de specificaties in ETSI TS 119 612, hebben de onderhavige specificaties voorrang.

Benaming van de regeling (clausule 5.3.6)

Dit veld moet worden gebruikt en moet voldoen aan de specificaties van clausule 5.3.6 van ETSI TS 119 612, waar de volgende naam voor de regeling wordt gebruikt:

„EN_name_value" = „vertrouwenslijst met onder meer informatie over de gekwalificeerde verleners van vertrouwensdiensten die onder toezicht staan van de lidstaat van afgifte, alsmede informatie over de gekwalificeerde vertrouwensdiensten die door hen worden verleend, in overeenstemming met de relevante bepalingen van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.".

URI met informatie over de regeling (clausule 5.3.7)

Dit veld moet worden gebruikt en moet voldoen aan de specificaties van clausule 5.3.7 van ETSI TS 119 612, waar de „passende informatie over de regeling" minstens het volgende moet bevatten:

a) inleidende informatie die voor alle lidstaten gemeenschappelijk is, over het toepassingsgebied en de context van de vertrouwenslijst, de onderliggende toezichtregeling en, indien van toepassing, de nationale goedkeuringsregeling(en) (bv. accreditatie). De gemeenschappelijke tekst die moet worden gebruikt, is de onderstaande, waarin de tekenreeks „[*naam van de lidstaat*]" moet worden vervangen door de naam van de betrokken lidstaat:

> „De onderhavige lijst is de vertrouwenslijst met onder meer informatie over de gekwalificeerde verleners van vertrouwensdiensten die onder toezicht staan van [*naam van de lidstaat*], alsmede informatie over de gekwalificeerde vertrouwensdiensten die door hen worden verleend, in overeenstemming met de relevante bepalingen van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

Elektronische handtekeningen kunnen gemakkelijker grensoverschrijdend worden gebruikt dankzij Beschikking 2009/767/EG van de Commissie van 16 oktober 2009, volgens welke de lidstaten vertrouwenslijsten moeten opstellen, bijhouden en publiceren met informatie over certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven overeenkomstig Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, en die onder toezicht staan/geaccrediteerd zijn in de lidstaten. De onderhavige vertrouwenslijst is de voortzetting van de vertrouwenslijst die is opgezet bij Beschikking 2009/767/EG.".

Vertrouwenslijsten zijn essentieel voor het opbouwen van vertrouwen tussen elektronische marktdeelnemers, omdat zij gebruikers de mogelijkheid geven om de gekwalificeerde status en de statusgeschiedenis van verleners van vertrouwensdiensten en hun diensten vast te stellen.

De vertrouwenslijsten van de lidstaten omvatten minstens de informatie bedoeld in de artikelen 1 en 2 van Uitvoeringsbesluit (EU) 2015/1505 van de Commissie.

De lidstaten kunnen in de vertrouwenslijsten informatie opnemen over niet-gekwalificeerde verleners van vertrouwensdiensten, alsmede informatie over de niet-gekwalificeerde vertrouwensdiensten die zij verlenen. Er wordt duidelijk aangegeven dat zij niet zijn gekwalificeerd overeenkomstig Verordening (EU) nr. 910/2014.

De lidstaten kunnen in de vertrouwenslijsten informatie opnemen over andere nationaal gedefinieerde vertrouwensdiensten dan die welke zijn vastgesteld in artikel 3, lid 16, van Verordening (EU) nr. 910/2014. Er wordt duidelijk aangegeven dat zij niet zijn gekwalificeerd overeenkomstig Verordening (EU) nr. 910/2014;

b) specifieke informatie over de onderliggende toezichtregeling en, indien van toepassing, nationale goedkeuringsregeling(en) (bv. accreditatie), met name ([1]):

1) informatie over het nationaal toezichtsysteem dat van toepassing is op gekwalificeerde en niet-gekwalificeerde verleners van vertrouwensdiensten en de gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten die zij verlenen, zoals voorgeschreven door Verordening (EU) nr. 910/2014;

2) informatie, indien van toepassing, over de nationale vrijwillige accreditatieregelingen die van toepassing zijn op de certificatiedienstverleners die gekwalificeerde certificaten hebben uitgegeven volgens Richtlijn 1999/93/EG.

Deze specifieke informatie moet voor elke hierboven vermelde onderliggende regeling minstens de volgende informatie bevatten:

1) een algemene beschrijving;

2) informatie over de gevolgde procedure voor het nationale toezichtsysteem en, indien van toepassing, voor de goedkeuring in het kader van een nationale goedkeuringsregeling;

3) informatie over de criteria voor het toezicht op of, indien van toepassing, de goedkeuring van verleners van vertrouwensdiensten;

4) informatie over de criteria en regels om toezichthouders/auditoren te selecteren en over hoe de verleners van vertrouwensdiensten en de vertrouwensdiensten die zij verlenen worden beoordeeld;

5) andere contactgegevens en algemene informatie over de uitvoering van de regeling, indien van toepassing.

Type regeling/publiek/regelgeving (clausule 5.3.9)

Dit veld moet worden gebruikt en moet voldoen aan de specificaties van clausule 5.3.9 van ETSI TS 119 612.

Het mag alleen URI's in Brits Engels bevatten.

([1]) Deze informatie is van doorslaggevend belang voor derden om het kwaliteits- en veiligheidsniveau van dergelijke systemen te beoordelen. Deze informatie zal in de vertrouwenslijst worden opgenomen via „URI met informatie over de regeling" (clausule 5.3.7 — informatie die door lidstaten wordt verstrekt), „Type regeling/publiek/regelgeving" (clausule 5.3.9 — door het gebruik van een voor alle lidstaten gemeenschappelijke tekst) en „SLV-beleidslijnen/juridische informatie" (clausule 5.3.11 — een voor alle lidstaten gemeenschappelijke tekst, met de mogelijkheid voor elke lidstaat om lidstaatspecifieke tekst/referenties toe te voegen). Bijkomende informatie over dergelijke systemen voor niet-gekwalificeerde vertrouwensdiensten en nationaal gedefinieerde (gekwalificeerde) vertrouwensdiensten kan op dienstenniveau worden verstrekt als dat van toepassing is en wordt vereist (bv. om onderscheid te maken tussen verschillende kwaliteits-/veiligheidsniveaus) via „URI met definitie van de dienst onder de regeling" (clausule 5.5.6).

Het moet minstens twee URI's bevatten:

1) een URI die voor alle vertrouwenslijsten van de lidstaten gemeenschappelijk is en die leidt naar een beschrijvende tekst die van toepassing is op alle vertrouwenslijsten, als volgt:

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

Beschrijvende tekst:

„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 (EU) 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, etc.). 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) een specifieke URI voor de vertrouwenslijst van elke lidstaat, die leidt naar een beschrijvende tekst die van toepassing is op de vertrouwenslijst van deze lidstaat:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC waarbij CC = de ISO 3166-1 ([1]) alpha-2-landcode die is gebruikt in het veld „Grondgebied van de regeling" (clausule 5.3.10)

— gebruikers kunnen hier de lidstaatspecifieke beleidslijnen/regels vinden die worden gebruikt voor de beoordeling van de diensten op de lijst, overeenkomstig het toezichtsysteem en, indien van toepassing, de goedkeuringsregeling van de lidstaat;

— gebruikers kunnen hier een lidstaatspecifieke beschrijving vinden over hoe de inhoud van de vertrouwenslijst kan worden gebruikt en geïnterpreteerd met betrekking tot de in de lijst opgenomen niet-gekwalificeerde en/of nationaal gedefinieerde vertrouwensdiensten. Dit kan worden gebruikt om een mogelijke onderverdeling aan te duiden in het nationale goedkeuringssysteem voor CDV's die geen KC's afgeven, en om uit te leggen hoe de velden „URI met definitie van de dienst onder de regeling" (clausule 5.5.6) en „Uitbreiding dienstinformatie" (clausule 5.5.9) daartoe worden gebruikt.

Lidstaten KUNNEN bijkomende URI's definiëren en gebruiken, vertrekkende vanuit de bovenvermelde lidstaatspecifieke URI (d.w.z. URI's die worden gedefinieerd vanuit deze hiërarchische, specifieke URI).

SLV-beleidslijnen/juridische informatie (clausule 5.3.11)

Dit veld moet worden gebruikt en moet voldoen aan de specificaties van clausule 5.3.11 van ETSI TS 119 612, volgens welke de beleidslijnen/juridische informatie over de juridische status van de regeling of de wettelijke vereisten waaraan de regeling voldoet in het rechtsgebied waarin de regeling wordt ingevoerd en/of de beperkingen en voorwaarden die

([1]) ISO 3166-1:2006: „Codes voor namen van landen en hun onderverdelingen. Deel 1: Landcodes".

gelden voor het bijwerken en publiceren van de vertrouwenslijst, een meertalige tekenreeks (zie clausule 5.1.4) moet zijn die verplicht in het Brits Engels en eventueel in één of meer nationale talen is opgesteld en waarbij de tekst van die beleidslijnen of juridische informatie volgens deze structuur is opgesteld:

1) een verplicht deel, dat gemeenschappelijk is voor alle vertrouwenslijsten van de lidstaten en waarin het toepasselijke juridische kader wordt aangegeven, waarvan de Engelse versie als volgt luidt:

   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.

   Tekst in de nationale taal/talen van de lidstaat:

   Het toepasselijk juridisch kader voor onderhavige vertrouwenslijst wordt gevormd door Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

2) een facultatief deel, specifiek voor elke vertrouwenslijst, met verwijzingen naar specifieke toepasselijke nationale wettelijke kaders.

Huidige status van de dienst (clausule 5.5.4)

Dit veld moet worden gebruikt en moet voldoen aan de specificaties van clausule 5.5.4 van ETSI TS 119 612.

De migratie van de waarde „huidige status van de dienst" van de in de vertrouwenslijsten van de EU-lidstaten opgenomen diensten op de laatste dag vóór de datum waarop Verordening (EU) nr. 910/2014 van toepassing wordt (30 juni 2016), gebeurt op de dag waarop de verordening van toepassing wordt (1 juli 2016), zoals beschreven in bijlage J bij ETSI TS 119 612.

HOOFDSTUK III

CONTINUÏTEIT VAN VERTROUWENSLIJSTEN

Certificaten die bij de Commissie moeten worden gemeld overeenkomstig artikel 4, lid 2, van dit besluit, voldoen aan de eisen van clausule 5.7.1 van ETSI TS 119 612 en worden uitgegeven zodat:

— de einddatum van de geldigheidstermijn („niet na") minstens drie maanden verschilt;

— zij gecreëerd worden op grond van nieuwe sleutelparen. Eerder gebruikte sleutelparen mogen niet opnieuw worden gecertificeerd.

Als een van de publieke sleutelcertificaten verloopt die gebruikt zou kunnen worden voor het valideren van de handtekening of het zegel op de vertrouwenslijst die aan de Commissie is meegedeeld en die is gepubliceerd in de centrale lijsten van verwijzingen van de Commissie, moeten de lidstaten:

— in geval dat de lopende gepubliceerde vertrouwenslijst was ondertekend of verzegeld met een privésleutel waarvan het publieke sleutelcertificaat is verlopen, onmiddellijk een nieuwe vertrouwenslijst publiceren die is ondertekend of verzegeld met een privésleutel waarvan het publieke sleutelcertificaat niet is verlopen;

— zo nodig nieuwe sleutelparen genereren die gebruikt kunnen worden voor de ondertekening of verzegeling van de vertrouwenslijst en de bijbehorende publieke sleutelcertificaten genereren;

— de Commissie onmiddellijk de nieuwe lijst meedelen van publieke sleutelcertificaten die overeenkomen met de privésleutels die voor de ondertekening of verzegeling van de vertrouwenslijst kunnen worden gebruikt.

In geval van compromittering of het buiten gebruik stellen van een van de privésleutels die overeenkomen met een van de publieke sleutelcertificaten die gebruikt zou kunnen worden voor het valideren van de handtekening of het zegel op de vertrouwenslijst die aan de Commissie is meegedeeld en die is gepubliceerd in de centrale lijsten van verwijzingen van de Commissie, moeten de lidstaten:

— onmiddellijk een nieuwe vertrouwenslijst publiceren die ondertekend of verzegeld is met een niet-gecompromitteerde privésleutel als de gepubliceerde vertrouwenslijst was ondertekend of verzegeld met een gecompromitteerde of buiten gebruik gestelde privésleutel;

— zo nodig nieuwe sleutelparen genereren die gebruikt kunnen worden voor de ondertekening of verzegeling van de vertrouwenslijst en de bijbehorende publieke sleutelcertificaten genereren;

— de Commissie onmiddellijk de nieuwe lijst meedelen van publieke sleutelcertificaten die overeenkomen met de privésleutels die voor de ondertekening of verzegeling van de vertrouwenslijst kunnen worden gebruikt.

In geval van compromittering of het buiten gebruik stellen van alle privésleutels die overeenkomen met de publieke sleutelcertificaten die gebruikt zouden kunnen worden voor het valideren van de handtekening op de vertrouwenslijst en die aan de Commissie zijn meegedeeld en zijn gepubliceerd in de centrale lijsten van verwijzingen van de Commissie, moeten de lidstaten:

— zo nodig nieuwe sleutelparen genereren die gebruikt kunnen worden voor de ondertekening of verzegeling van de vertrouwenslijst en de bijbehorende publieke sleutelcertificaten genereren;

— onmiddellijk een nieuwe vertrouwenslijst publiceren die ondertekend of verzegeld is met een van deze nieuwe privésleutels en waarvan het corresponderende publieke sleutelcertificaat moet worden meegedeeld;

— de Commissie onmiddellijk de nieuwe lijst meedelen van publieke sleutelcertificaten die overeenkomen met de privésleutels die voor de ondertekening of verzegeling van de vertrouwenslijst kunnen worden gebruikt.

HOOFDSTUK IV

SPECIFICATIES VOOR DE MENSELIJK LEESBARE VERSIE VAN DE VERTROUWENSLIJST

Als een menselijk leesbare versie van de vertrouwenslijst wordt opgesteld en gepubliceerd, moet die worden verstrekt als een pdf-document overeenkomstig ISO 32000 ([1]), dat is geformatteerd volgens het PDF/A-profiel (ISO 19005 ([2])).

De inhoud van de menselijk leesbare versie in PDF/A van de vertrouwenslijst moet voldoen aan de volgende vereisten:

— de structuur van de menselijke leesbare versie moet het logische model uit ETSI TS 119 612 weergeven;

— elk veld moet zichtbaar zijn en het volgende weergeven:

  — de titel van het veld (bv. „*Identificatiecode diensttype*”);

  — de waarde van het veld (bv. „http://uri.etsi.org/TrstSvc/Svctype/CA/QC}”);

  — de betekenis (omschrijving) van de waarde van het veld, indien van toepassing (bv. „*een dienst voor het verkrijgen van certificaten voor het creëren en ondertekenen van gekwalificeerde certificaten die zijn gebaseerd op de identiteit en andere kenmerken die zijn gecontroleerd door de desbetreffende inschrijvingsdiensten*”);

  — indien van toepassing, meerdere versies in natuurlijke talen zoals bepaald in de vertrouwenslijst;

— in de menselijk leesbare versie moeten minstens de volgende velden en overeenkomstige waarden van de digitale certificaten ([3]) in het veld „digitale dienstidentiteit” worden weergegeven:

  — versie;

  — serienummer van het certificaat;

  — algoritme van de handtekening;

  — uitgever — alle relevante kenmerkende naamvelden;

  — geldigheidsperiode;

  — onderwerp — alle relevante kenmerkende naamvelden;

([1]) ISO 32000-1:2008: Documentbeheer — Portable document format — Deel 1: PDF 1.7.
([2]) ISO 19005-2:2011: Documentbeheer — Bestandsformaat voor elektronische documenten voor langdurige bewaring — Deel 2: Gebruik van ISO 32000-1 (PDF/A-2).
([3]) Aanbeveling ITU-T X.509 | ISO/IEC 9594-8: Informatietechnologie — Open-systeemverbinding — De directory: Kaders voor publiek sleutelcertificaat en kenmerkencertificaat (zie http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— publieke sleutel;

— identificatiecode autoriteitsleutel;

— identificatiecode onderwerpsleutel;

— gebruik sleutel;

— uitgebreid gebruik sleutel;

— certificaatbeleid — alle beleidsidentificatoren en -kwalificatoren;

— beleidsmappings;

— alternatieve naam van het onderwerp;

— directorykenmerken van het onderwerp;

— basisbeperkingen;

— beleidsbeperkingen;

— LIC-verdeelpunten ([1]);

— toegang tot gegevens van de autoriteit;

— toegang tot gegevens van het onderwerp;

— verklaringen van het gekwalificeerd certificaat ([2]);

— hash-algoritme;

— hashwaarde van het certificaat;

— de menselijk leesbare versie moet gemakkelijk kunnen worden afgedrukt;

— de menselijk leesbare versie wordt ondertekend of verzegeld door de uitvoerder van de regeling volgens de geavanceerde pdf-handtekening als bedoeld in de artikelen 1 en 3 van Uitvoeringsbesluit (EU) 2015/1505 van de Commissie.

([1]) RFC 5280: Internet X.509 PKI-certificaat en LIC-profiel.
([2]) RFC 3739: Internet X.509 PKI: Profiel van het gekwalificeerd certificaat.

BIJLAGE II

MODEL VOOR MELDINGEN VAN DE LIDSTATEN

Overeenkomstig artikel 4, lid 1, van onderhavig besluit moeten de lidstaten de volgende gegevens en alle daarin aangebrachte wijzigingen melden:

1) lidstaat volgens de ISO 3166-1 ([1]) Alpha-2-codes, met de volgende uitzonderingen:

   a) de landcode voor het Verenigd Koninkrijk is „UK";

   b) de landcode voor Griekenland is „EL";

2) instantie(s) verantwoordelijk voor het opstellen, bijwerken en publiceren van de voor automatische verwerking geschikte versie en de menselijk leesbare versie van de vertrouwenslijsten:

   a) naam van de uitvoerder van de regeling: de verstrekte informatie moet volledig gelijk zijn (let op: hoofdlettergevoelig) aan de waarde „Naam van de uitvoerder van de regeling" in de vertrouwenslijst, in even veel talen als er worden gebruikt in de vertrouwenslijst;

   b) facultatieve informatie, uitsluitend voor intern gebruik door de Commissie als met de bevoegde instantie contact moet worden opgenomen (de gegevens worden niet gepubliceerd in de door de Commissie opgestelde overzichtslijst van vertrouwenslijsten):

      — adres van de uitvoerder van de regeling;

      — contactgegevens van de verantwoordelijke persoon/personen (naam, telefoonnummer, e-mailadres);

3) plaats waar de voor automatische verwerking geschikte versie van de vertrouwenslijst is gepubliceerd (*plaats waar de huidige vertrouwenslijst is gepubliceerd*);

4) indien van toepassing, plaats waar de menselijk leesbare versie van de vertrouwenslijst is gepubliceerd (*plaats waar de huidige vertrouwenslijst is gepubliceerd*). Als een menselijk leesbare vertrouwenslijst niet langer wordt gepubliceerd, moet dat worden vermeld;

5) de publieke sleutelcertificaten die overeenkomen met de privésleutels die kunnen worden gebruikt voor het elektronisch ondertekenen of verzegelen van de voor automatische verwerking geschikte versie van de vertrouwenslijst en de menselijk leesbare versie van de vertrouwenslijsten: deze certificaten worden verstrekt als Privacy Enhanced Mail Base 64 gecodeerde DER-certificaten. Als een wijziging wordt gemeld, moet aanvullende informatie worden verstrekt in geval een nieuw certificaat een specifiek certificaat in de lijst van de Commissie vervangt en in geval het aangemelde certificaat moet worden toegevoegd aan het/de bestaande certificaat/certificaten, zonder dat er een wordt vervangen;

6) datum van indiening van de gegevens van de punten 1 tot en met 5.

Gegevens die volgens de punten 1, 2, onder a), 3, 4 en 5 worden gemeld, worden opgenomen in de door de Commissie opgestelde overzichtslijst van vertrouwenslijsten ter vervanging van de eerder gemelde informatie die in die overzichtslijst is opgenomen.

([1]) ISO 3166-1: „Codes voor namen van landen en hun onderverdelingen — Deel 1: Landcodes".

UITVOERINGSBESLUIT (EU) 2015/1506 VAN DE COMMISSIE

van 8 september 2015

tot vaststelling van specificaties betreffende formaten van geavanceerde elektronische handtekeningen en geavanceerde zegels die door openbare instanties moeten worden erkend overeenkomstig respectievelijk artikel 27, lid 5, en artikel 37, lid 5, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG ([1]), en met name artikel 27, lid 5, en artikel 37, lid 5,

Overwegende hetgeen volgt:

(1) De lidstaten dienen te voorzien in de noodzakelijke technische voorzieningen met het oog op de verwerking van elektronisch ondertekende documenten die vereist zijn voor het gebruik van een onlinedienst die door of namens een openbare instantie wordt aangeboden.

(2) Een lidstaat die voor het gebruik van een door of namens een openbare instantie aangeboden onlinedienst een geavanceerde elektronische handtekening of een geavanceerd elektronisch zegel vereist, dient overeenkomstig Verordening (EU) nr. 910/2014 erkenning te verlenen aan geavanceerde elektronische handtekeningen en zegels, geavanceerde elektronische handtekeningen en zegels gebaseerd op een gekwalificeerd certificaat en gekwalificeerde elektronische handtekeningen en zegels in specifieke formaten, of volgens specifieke referentiemethoden gevalideerde alternatieve formaten.

(3) Bij het vaststellen van deze specifieke formaten en referentiemethoden dient rekening te worden gehouden met bestaande praktijken, normen en rechtshandelingen van de Unie.

(4) Bij Uitvoeringsbesluit 2014/148/EU van de Commissie ([2]) is een aantal van de meest voorkomende formaten van geavanceerde elektronische handtekeningen vastgesteld, waarvoor lidstaten die in het kader van een online administratieve procedure geavanceerde elektronische handtekeningen verplicht stellen, technische ondersteuning moeten bieden. De vaststelling van referentieformaten is bedoeld om de grensoverschrijdende validering van elektronische handtekeningen te vergemakkelijken en de grensoverschrijdende interoperabiliteit van elektronische procedures te verbeteren.

(5) In de bijlage bij dit besluit worden de thans geldende normen voor formaten van geavanceerde elektronische handtekeningen vermeld. In verband met de lopende herziening van de voor langdurige archivering bestemde vormen van de referentieformaten door de normalisatie-instanties vallen normen inzake langdurige archivering buiten het toepassingsgebied van dit besluit. Wanneer de nieuwe versie van de referentienormen beschikbaar is, zullen de verwijzingen naar de normen en de clausules inzake langdurige archivering worden herzien.

(6) Geavanceerde elektronische handtekeningen en geavanceerde elektronische zegels zijn uit technisch oogpunt vergelijkbaar. De normen voor formaten van geavanceerde elektronische handtekeningen dienen derhalve van overeenkomstige toepassing te zijn op geavanceerde elektronische zegels.

(7) Indien voor het ondertekenen of verzegelen andere formaten elektronische handtekeningen of zegels worden gebruikt dan de formaten die gewoonlijk technisch worden ondersteund, dient te worden voorzien in valideringsinstrumenten die het mogelijk maken dat de elektronische handtekeningen of zegels grensoverschrijdend worden geverifieerd. Om ervoor te zorgen dat de ontvangende lidstaten op die valideringsinstrumenten van een andere lidstaat kunnen vertrouwen, moet informatie over de valideringsinstrumenten op een gemakkelijk toegankelijke wijze beschikbaar worden gesteld door de informatie in de elektronische documenten, in de elektronische handtekeningen of in de elektronische documentdragers op te nemen.

([1]) PB L 257 van 28.8.2014, blz. 73.

([2]) Uitvoeringsbesluit 2014/148/EU van de Commissie van 17 maart 2014 tot wijziging van Besluit 2011/130/EU tot vaststelling van minimumvoorschriften voor de grensoverschrijdende verwerking van documenten die door de bevoegde autoriteiten elektronisch zijn ondertekend krachtens Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt (PB L 80 van 19.3.2014, blz. 7).

(8) Indien bij de openbare instanties van een lidstaat voor geautomatiseerde verwerking geschikte mogelijkheden voor de validering van elektronische handtekeningen of zegels beschikbaar zijn, dienen die valideringsmogelijkheden ter beschikking te worden gesteld van de ontvangende lidstaat en aan deze te worden aangeboden. Dit besluit mag echter de toepassing van artikel 27, leden 1 en 2, en artikel 37, leden 1 en 2, van Verordening (EU) nr. 910/2014 niet in de weg staan, indien geautomatiseerde verwerking van de valideringsmogelijkheden voor alternatieve methoden niet mogelijk is.

(9) Teneinde te voorzien in vergelijkbare valideringsvereisten en het vertrouwen te versterken in de valideringsmogelijkheden die lidstaten bieden voor andere dan de algemeen ondersteunde formaten elektronische handtekeningen of zegels, dienen de bij dit besluit vastgestelde vereisten voor de valideringsinstrumenten te worden gebaseerd op de vereisten voor de validering van gekwalificeerde elektronische handtekeningen en zegels bedoeld in de artikelen 32 en 40 van Verordening (EU) nr. 910/2014.

(10) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 48 van Verordening (EU) nr. 910/2014 ingestelde comité,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Lidstaten die een geavanceerde elektronische handtekening of een op een gekwalificeerd certificaat gebaseerde geavanceerde elektronische handtekening vereisen, zoals bedoeld in artikel 27, leden 1 en 2, van Verordening (EU) nr. 910/2014, erkennen geavanceerde elektronische XML-, CMS- of PDF-handtekeningen die voldoen aan conformiteitsniveau B, T of LT of die gebruikmaken van een drager van de bijbehorende handtekening, indien die handtekeningen voldoen aan de in de bijlage opgenomen technische specificaties.

Artikel 2

1. Lidstaten die een geavanceerde elektronische handtekening of een op een gekwalificeerd certificaat gebaseerde geavanceerde elektronische handtekening vereisen, zoals bedoeld in artikel 27, leden 1 en 2, van Verordening (EU) nr. 910/2014, erkennen andere formaten van elektronische handtekeningen dan die bedoeld in artikel 1 van dit besluit, indien de lidstaat waar de door de ondertekenaar gebruikte verlener van vertrouwensdiensten is gevestigd, aan andere lidstaten mogelijkheden voor de validering van handtekeningen aanbiedt, die zo mogelijk voor geautomatiseerde verwerking geschikt zijn.

2. De mogelijkheden voor de validering van handtekeningen:

a) laten toe dat andere lidstaten de ontvangen elektronische handtekeningen online, kosteloos en op een voor niet-moedertaalsprekers begrijpelijke wijze valideren;

b) worden aangegeven in het ondertekende document, in de elektronische handtekening of in de elektronische documentdrager; en

c) bevestigen de geldigheid van een geavanceerde elektronische handtekening, mits is voldaan aan de volgende voorwaarden:

   1. het certificaat dat de geavanceerde elektronische handtekening ondersteunt, was geldig op het tijdstip van ondertekening; indien de geavanceerde elektronische handtekening wordt ondersteund door een gekwalificeerd certificaat, was het gekwalificeerde certificaat dat de geavanceerde elektronische handtekening ondersteunt op het tijdstip van ondertekening een gekwalificeerd certificaat voor elektronische handtekeningen overeenkomstig bijlage I bij Verordening (EU) nr. 910/2014 dat was uitgegeven door een gekwalificeerde verlener van vertrouwensdiensten;

   2. de gegevens voor het valideren van de handtekening stemmen overeen met de gegevens die aan de vertrouwende partij zijn verstrekt;

   3. de unieke reeks gegevens die de ondertekenaar vertegenwoordigt, is correct doorgegeven aan de vertrouwende partij;

   4. de vertrouwende partij is duidelijk gewezen op het eventuele gebruik van een pseudoniem op het tijdstip van ondertekening;

5. indien de geavanceerde elektronische handtekening is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen, is het gebruik van een dergelijk middel duidelijk ter kennis gebracht van de vertrouwende partij;

6. de integriteit van de ondertekende gegevens is niet aangetast;

7. aan de eisen van artikel 26 van Verordening (EU) nr. 910/2014 werd op het tijdstip van ondertekening voldaan;

8. het systeem dat is gebruikt voor het valideren van de geavanceerde elektronische handtekening verstrekt het juiste resultaat van het valideringsproces aan de vertrouwende partij en stelt deze in de gelegenheid om veiligheidsproblemen te identificeren.

Artikel 3

Lidstaten die een geavanceerd elektronisch zegel of een op een gekwalificeerd certificaat gebaseerd geavanceerd elektronisch zegel vereisen, zoals bedoeld in artikel 37, leden 1 en 2, van Verordening (EU) nr. 910/2014, erkennen geavanceerde elektronische XML-, CMS- of PDF-zegels die voldoen aan conformiteitsniveau B, T of LT of die gebruikmaken van een drager van het bijbehorende zegel, indien die voldoet aan de in de bijlage opgenomen technische specificaties.

Artikel 4

1. Lidstaten die een geavanceerd elektronisch zegel of een op een gekwalificeerd certificaat gebaseerd geavanceerd elektronisch zegel vereisen, zoals bedoeld in artikel 37, leden 1 en 2, van Verordening (EU) nr. 910/2014, erkennen andere formaten van elektronische zegels dan die bedoeld in artikel 3 van dit besluit, indien de lidstaat waar de door de aanmaker van het zegel gebruikte verlener van vertrouwensdiensten is gevestigd, aan andere lidstaten mogelijkheden voor de validering van zegels aanbiedt, die zo mogelijk voor geautomatiseerde verwerking geschikt zijn.

2. De mogelijkheden voor de validering van zegels:

a) laten toe dat andere lidstaten de ontvangen elektronische zegels online, kosteloos en op een voor niet-moedertaalsprekers begrijpelijke wijze valideren;

b) worden aangegeven in het verzegelde document, in het elektronische zegel of in de elektronische documentdrager;

c) bevestigen de geldigheid van een geavanceerd elektronisch zegel, mits is voldaan aan de volgende voorwaarden:

1. het certificaat dat het geavanceerde elektronische zegel ondersteunt, was geldig op het tijdstip van verzegeling; indien het geavanceerde elektronische zegel wordt ondersteund door een gekwalificeerd certificaat, was het gekwalificeerde certificaat dat het geavanceerde elektronische zegel ondersteunt op het tijdstip van verzegeling een gekwalificeerd certificaat voor elektronische zegels overeenkomstig bijlage III bij Verordening (EU) nr. 910/2014 dat was uitgegeven door een gekwalificeerde verlener van vertrouwensdiensten;

2. de gegevens voor het valideren van het zegel stemmen overeen met de gegevens die aan de vertrouwende partij zijn verstrekt;

3. de unieke reeks gegevens die verwijst naar de aanmaker van het zegel, is correct doorgegeven aan de vertrouwende partij;

4. de vertrouwende partij is duidelijk gewezen op het eventuele gebruik van een pseudoniem op het tijdstip van verzegeling;

5. indien het geavanceerde elektronische zegel is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische zegels, is het gebruik van een dergelijk middel duidelijk ter kennis gebracht van de vertrouwende partij;

6. de integriteit van de verzegelde gegevens is niet aangetast;

7. aan de eisen van artikel 36 van Verordening (EU) nr. 910/2014 werd op het tijdstip van verzegeling voldaan;

8. het systeem dat is gebruikt voor het valideren van het geavanceerde elektronische zegel verstrekt het juiste resultaat van het valideringsproces aan de vertrouwende partij en stelt deze in de gelegenheid om veiligheidsproblemen te identificeren.

Artikel 5

Dit besluit treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Dit besluit is verbindend in al zijn onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 8 september 2015.

Voor de Commissie

De voorzitter

Jean-Claude JUNCKER

BIJLAGE

Lijst van technische specificaties voor geavanceerde elektronische XML-, CMS- of PDF-handtekeningen en de bijbehorende drager van de handtekening

De in artikel 1 van het besluit vermelde geavanceerde elektronische handtekeningen moeten voldoen aan een van de volgende technische specificaties van het ETSI, met uitzondering van clausule 9 daarvan:

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

De in artikel 1 van het besluit vermelde bijbehorende drager van de handtekening moet voldoen aan de volgende technische specificaties van het ETSI:

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

Lijst van technische specificaties voor geavanceerde elektronische XML-, CMS- of PDF-zegels en de bijbehorende drager van het zegel

De in artikel 3 van het besluit vermelde geavanceerde elektronische zegels moeten voldoen aan een van de volgende technische specificaties van het ETSI, met uitzondering van clausule 9 daarvan:

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

De in artikel 3 van het besluit vermelde bijbehorende drager van het zegel moet voldoen aan de volgende technische specificaties van het ETSI:

Associated Seal Container Baseline Profile	ETSI TS 103174 v.2.2.1

ISSN 1977-0758 (elektronische uitgave)
ISSN 1725-2598 (papieren uitgave)

Bureau voor publicaties van de Europese Unie
2985 Luxemburg
LUXEMBURG

NL