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".