KOMISJONI RAKENDUSOTSUS (EL) 2015/1505,

8. september 2015,

millega kehtestatakse usaldusnimekirjade tehnilised kirjeldused ja vormingud vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 22 lõikele 5

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ), ([1]) eriti selle artikli 22 lõiget 5,

ning arvestades järgmist:

(1) Usaldusnimekirjad on turuosaliste vahelise usalduse loomisel väga olulised, sest need näitavad teenuseosutaja staatust järelevalve ajal.

(2) E-allkirjade piiriülesele kasutamisele aidati kaasa komisjoni otsusega 2009/767/EÜ, ([2]) milles sätestati liikmesriikide kohustus koostada, hallata ja avaldada usaldusnimekirju, mis sisaldavad teavet sertifitseerimisteenuse osutajate kohta, kes väljastavad üldsusele kvalifitseeritud sertifikaate vastavalt Euroopa Parlamendi ja nõukogu direktiivile 1999/93/EÜ ([3]) ning kelle üle teostavad järelevalvet ja kelle akrediteerimisega tegelevad liikmesriigid.

(3) Määruse (EL) nr 910/2014 artiklis 22 on sätestatud, et liikmesriigid on kohustatud koostama, haldama ja avaldama usaldusnimekirju turvalisel viisil, e-allkirja või e-templiga varustatult ja automaatseks töötlemiseks sobivas vormingus ning teatavad komisjonile nende asutuste nimed, kes vastutavad riigisiseste usaldusnimekirjade koostamise eest.

(4) Usaldusteenuse osutaja ja tema osutatavad usaldusteenused tuleks lugeda kvalifitseerituks, kui kvalifitseeritud staatus on seotud usaldusnimekirjas oleva osutajaga. Tagamaks, et teenuseosutajad saavad määrusest (EL) nr 910/2014 tulenevaid muid kohustusi, eeskätt artiklites 27 ja 37 sätestatud kohustusi hõlpsasti täita eemalt ja elektrooniliste vahendite abil, ning et täita selliste teiste sertifitseerimisteenuse osutajate õigustatud ootusi, kes ei väljasta kvalifitseeritud sertifikaate, kuid osutavad e-allkirjadega seotud teenuseid vastavalt direktiivile 1999/93/EÜ ja kes on nimekirja kantud 30. juuniks 2016, peaks liikmesriikidel olema võimalik lisada usaldusnimekirjadesse vabatahtlikkuse alusel muid usaldusteenuseid peale kvalifitseeritud usaldusteenuste, tingimusel et on selgelt märgitud, et need ei ole kvalifitseeritud teenused vastavalt määrusele (EL) nr 910/2014.

(5) Kooskõlas määruse (EL) nr 910/2014 põhjendusega 25 võivad liikmesriigid lisada nimekirja muud liiki riigisiseselt kindlaksmääratud usaldusteenuseid kui need, mis on määratletud määruse (EL) nr 910/2014 artikli 3 lõikes 16, kui on selgelt märgitud, et need ei ole kvalifitseeritud teenused vastavalt määrusele (EL) nr 910/2014.

(6) Käesoleva otsusega ettenähtud meetmed on kooskõlas määruse (EL) nr 910/2014 artikliga 48 loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Liikmesriigid koostavad, avaldavad ja haldavad usaldusnimekirju, mis sisaldavad teavet nende järelevalve all olevate kvalifitseeritud usaldusteenuse osutajate ja nende osutatavate kvalifitseeritud usaldusteenuste kohta. Need nimekirjad vastavad I lisas sätestatud tehnilistele kirjeldustele.

([1]) ELT L 257, 28.8.2014, lk 73.
([2]) Komisjoni otsus 2009/767/EÜ, 16. oktoober 2009, millega kehtestatakse meetmed elektrooniliste haldustoimingute kasutamise lihtsustamiseks ühtsete kontaktpunktide kaudu, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis 2006/123/EÜ teenuste kohta siseturul (ELT L 274, 20.10.2009, lk 36).
([3]) Euroopa Parlamendi ja nõukogu direktiiv 1999/93/EÜ, 13. detsember 1999, elektroonilisi allkirju käsitleva ühenduse raamistiku kohta (EÜT L 13, 19.1.2000, lk 12).

Artikkel 2

Liikmesriigid võivad lisada usaldusnimekirja teavet kvalifitseerimata usaldusteenuse osutajate ja nende osutatavate kvalifitseerimata usaldusteenuste kohta. Nimekirjas peab olema selgelt märgitud, millised usaldusteenuste osutajad ja nende osutatavad usaldusteenused ei ole kvalifitseeritud.

Artikkel 3

1. Vastavalt määruse (EL) nr 910/2014 artikli 22 lõikele 2 annavad liikmesriigid oma usaldusnimekirjale automaatseks töötlemiseks sobivas vormingus e-allkirja või e-templi vastavalt I lisas sätestatud tehnilistele kirjeldustele.

2. Kui liikmesriik avaldab usaldusnimekirja inimestele loetavas vormingus elektrooniliselt, tagab ta, et selles vormingus usaldusnimekiri sisaldab sama teavet kui automaatseks töötlemiseks sobiv nimekiri, ning annab sellele e-allkirja või e-templi vastavalt I lisas sätestatud tehnilistele kirjeldustele.

Artikkel 4

1. Liikmesriigid teatavad komisjonile määruse (EL) nr 910/2014 artikli 22 lõikes 3 osutatud teabe, kasutades selleks II lisas esitatud vormi.

2. Lõikes 1 osutatud teave sisaldab süsteemi käitaja vähemalt kahe avaliku võtme sertifikaate, mille kehtivusnihe on vähemalt kolm kuud ja mis vastavad privaatvõtmetele, mida saab kasutada e-allkirja või e-templi andmiseks usaldusnimekirjale automaatseks töötlemiseks sobivas vormingus ja inimestele loetavas vormingus, kui see avaldatakse.

3. Vastavalt määruse (EL) nr 910/2014 artikli 22 lõikele 4 teeb komisjon liikmesriikidelt saadud lõigetes 1 ja 2 osutatud teabe turvalise kanali kaudu autenditud veebiserveris avalikkusele kättesaadavaks e-allkirja või e-templiga varustatud vormingus, mis sobib automaatseks töötlemiseks.

4. Komisjon võib teha liikmesriikidelt saadud lõigetes 1 ja 2 osutatud teabe turvalise kanali kaudu autenditud veebiserveris avalikkusele kättesaadavaks e-allkirja või e-templiga varustatult ja inimestele loetavas vormingus.

Artikkel 5

Käesolev otsus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev otsus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 8. september 2015

Komisjoni nimel

president

Jean-Claude JUNCKER

I LISA

USALDUSNIMEKIRJADE ÜHTSE VORMI TEHNILISED NÕUDED

I PEATÜKK

ÜLDNÕUDED

Usaldusnimekirjad peavad sisaldama nimekirjas olevate usaldusteenuste staatuse kohta nii praegust kui ka kogu varasemat teavet alates usaldusteenuse osutaja usaldusnimekirja kandmisest.

Käesolevas kirjelduses hõlmavad terminid „heakskiidetud", „akrediteeritud" ja/või „järelevalvealune" ka riikide heakskiitmissüsteeme, kuid lisateabe selliste võimalike riiklike süsteemide kohta esitavad liikmesriigid oma usaldusnimekirjades, lisades selgitused võimalike erinevuste kohta, võrreldes kvalifitseeritud usaldusteenuste osutajate ja nende osutatavate usaldusteenuste suhtes kohaldatavate järelevalvesüsteemidega.

Usaldusnimekirjas esitatud teabe peamine eesmärk on toetada kvalifitseeritud usaldusteenuste märkide valideerimist. Nende märkide hulka kuuluvad füüsilised või binaarsed (loogilised) objektid, mis on loodud või väljastatud kvalifitseeritud usaldusteenuse kasutamise tulemusena, nt kvalifitseeritud e-allkirjad/e-templid, täiustatud e-allkirjad/e-templid, mida toetab kvalifitseeritud sertifikaat, kvalifitseeritud ajatemplid, kvalifitseeritud elektroonilise edastamise tõendid jms.

II PEATÜKK

USALDUSNIMEKIRJADE ÜHTSE VORMI ÜKSIKASJALIKUD NÕUDED

Käesolevad kirjeldused tuginevad standardis ETSI TS 119 612 v2.1.1 (edaspidi „ETSI TS 119 612") sätestatud kirjeldustele ja nõuetele.

Kui käesolevates nõuetes ei ole sätestatud erinõudeid, siis peab täielikult kohaldama ETSI TS 119 612 punktide 5 ja 6 nõudeid. Kui käesolevates nõuetes on sätestatud erinõuded, peab neid käsitama vastavate ETSI TS 119 612 nõuete suhtes ülimuslikena. Käesolevates nõuetes ja ETSI TS 119 612 nõuetes esinevate lahknevuste korral peab ülimuslikuks pidama käesolevaid nõudeid.

Scheme name (punkt 5.3.6)

See väli on kohustuslik ja peab vastama TS 119 612 punkti 5.3.6 nõuetele, kusjuures süsteemi puhul peab kasutama järgmist nime:

„EN_name_value" = „Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, 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."

Scheme information URI (punkt 5.3.7)

See väli on kohustuslik ja peab vastama TS 119 612 punkti 5.3.7 nõuetele, kus „asjakohane teave süsteemi kohta" peab sisaldama vähemalt järgmist.

a) Kõigi liikmesriikide jaoks ühine tutvustav teave usaldusnimekirja ulatuse ja tausta, kasutatava järelevalvesüsteemi ja vajaduse korral riiklike heakskiitmissüsteemide (nt akrediteerimisüsteemide) kohta. Ühine tekst, mida tuleb kasutada, on järgmine, kusjuures märgistringi „[*asjaomase liikmesriigi nimi*]" peab asendama asjaomase liikmesriigi nimega:

> „Käesolev nimekiri on usaldusnimekiri, mis sisaldab teavet [*asjaomase liikmesriigi nimi*] järelevalve all olevate usaldusteenuse osutajate kohta ja usaldusteenuste kohta, mida nad osutavad, kooskõlas Euroopa Parlamendi ja nõukogu 23. juuli 2014 aasta määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ) asjaomaste sätetega.

E-allkirjade piiriülesele kasutamisele aidatakse kaasa komisjoni 16. oktoobri 2009. aasta otsusega 2009/767/EÜ, milles on sätestatud liikmesriikide kohustus koostada, hallata ja avaldada usaldusnimekirju, mis sisaldavad teavet sertifitseerimisteenuse osutajate kohta, kes väljastavad üldsusele kvalifitseeritud sertifikaate vastavalt Euroopa Parlamendi ja nõukogu 13. detsembri 1999. aasta direktiivile 1999/93/EÜ elektroonilisi allkirju käsitleva ühenduse raamistiku kohta ning kelle üle teostavad järelevalvet ja kelle akrediteerimisega tegelevad liikmesriigid. Käesolev usaldusnimekiri on jätkuks otsusega 2009/767/EÜ kehtestatud usaldusnimekirjale."

Usaldusnimekirjad on olulised komponendid, mis aitavad luua usaldust e-turul tegutsejate seas, võimaldades kasutajatel kindlaks teha, milline on usaldusteenuse osutajate ja nende teenuste kvalifitseeritud staatus praegu ja milline on see olnud varem.

Liikmesriikide usaldusnimekirjad peavad sisaldama vähemalt komisjoni rakendusotsuse (EL) 2015/1505 artiklites 1 ja 2 osutatud teavet.

Liikmesriigid võivad lisada usaldusnimekirja teavet kvalifitseerimata usaldusteenuse osutajate ja nende osutatavate kvalifitseerimata usaldusteenuste kohta. Sellisel juhul tuleb selgelt märkida, et need ei ole kvalifitseeritud vastavalt määrusele (EL) nr 910/2014.

Liikmesriigid võivad lisada usaldusnimekirja teavet muud liiki riigisiseselt kindlaksmääratud usaldusteenuste kohta kui need, mis on määratletud määruse (EL) nr 910/2014 artikli 3 lõike 16 alusel. Sellisel juhul tuleb selgelt märkida, et need ei ole kvalifitseeritud vastavalt määrusele (EL) nr 910/2014.

b) Konkreetne teave kasutatava järelevalvesüsteemi kohta ja vajaduse korral riiklike heakskiitmissüsteemide (st akrediteerimisüsteemide) kohta, eeskätt ([1]):

1) teave riigisisese järelevalve süsteemi kohta, mida kohaldatakse kvalifitseeritud ja kvalifitseerimata usaldusteenuste osutajate ning nende osutatavate kvalifitseeritud ja kvalifitseerimata usaldusteenuste suhtes vastavalt määrusele (EL) nr 910/2014;

2) vajaduse korral teave riigisiseste vabatahtlike akrediteerimissüsteemide koha, mida kohaldatakse sertifitseerimisteenuse osutajate suhtes, kes on väljastanud kvalifitseeritud sertifikaate vastavalt direktiivile 1999/93/EÜ.

See konkreetne teave peab sisaldama iga eespool loetletud süsteemi kohta vähemalt järgmist:

1) üldine kirjeldus;

2) teave protsessi kohta, mida järgitakse riigisisese järelevalve süsteemi ja vajaduse korral riigisisese heakskiitmissüsteemi alusel heakskiitmise jaoks;

3) teave kriteeriumide kohta, mille alusel toimub usaldusteenuse osutajate järelevalve või vajaduse korral heakskiitmine;

4) teave kriteeriumide ja õigusnormide kohta, mida kasutatakse järelevalve teostajate/audiitorite valikul ja selle kindlaksmääramisel, kuidas nad usaldusteenuse osutajaid ja nende osutatavaid usaldusteenuseid hindavad;

5) vajaduse korral muud kontaktandmed ja üldteave süsteemi toimimise kohta.

Scheme type/community/rules (punkt 5.3.9)

See väli on kohustuslik ja peab vastama TS 119 612 punkti 5.3.9 nõuetele.

Väljal esitatakse URId ainul Briti inglise keeles.

([1]) Need teaberühmad on eriti olulised, et tuginevad isikud saaksid hinnata selliste süsteemide kvaliteedi ja turvalisuse taset. Need teaberühmad tuleb esitada usaldusnimekirja tasandil, kasutades käesolevat välja „Scheme information URI" (punkt 5.3.7 – liikmesriikide esitatav teave), välja „Scheme type/community/rules" (punkt 5.3.9 – kasutades kõigi liikmesriikide jaoks ühist teksti) ja välja „TSL policy/legal notice" (punkt 5.3.11 – kõigi liikmesriikide jaoks ühine tekst koos võimalusega, et iga liikmesriik võib lisada teksti/viiteid oma liikmesriigi kohta). Vajaduse korral ja kui see on nõutav (nt et eristada mitut kvaliteedi/turvalisuse taset), võib teenuse tasandil esitada lisateavet kvalifitseerimata usaldusteenuste ja riigisiseselt kindlaksmääratud (kvalifitseeritud) usaldusteenuste selliste süsteemide kohta, kasutades välja „Scheme service definition URI" (punkt 5.5.6).

Esitatakse vähemalt kaks URI:

1) kõigi liikmesriikide usaldusnimekirjade jaoks ühine URI, mis viitab kirjeldavale tekstile, mida peab kasutama kõigi usaldusnimekirjade puhul järgmiselt:

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

Kirjeldav 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) iga liikmesriigi usaldusnimekirja URI, mis viitab kirjeldavale tekstile, mida peab kohaldama selle liikmesriigi usaldusnimekirja suhtes:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, kus CC = standardile ISO 3166-1 ([1]) vastav kahetäheline riigikood, mida kasutatakse väljal „Scheme territory" (punkt 5.3.10)

— kus kasutajad pääsevad ligi asjaomase liikmesriigi põhimõtetele/õigusnormidele, mille põhjal nimekirja kantud usaldusteenuseid hinnatakse vastavalt liikmesriigi järelevalvesüsteemile ja vajaduse korral heakskiitmissüsteemile;

— kus kasutajad võivad leida asjaomase liikmesriigi konkreetse kirjelduse selle kohta, kuidas kasutada ja tõlgendada usaldusnimekirja sisu nimekirjas olevate kvalifitseerimata usaldusteenuste ja/või riigisiseselt kindlaksmääratud usaldusteenuste puhul. Seda võib kasutada selleks, et viidata QCsid mitteväljastavate CSPdega seotud riiklike heakskiitmissüsteemide võimalikule detailsusele ja sellele, kuidas kasutada välju „Scheme service definition URI" (punkt 5.5.6) ja „Service information extension" (punkt 5.5.9) sellel eesmärgil.

Liikmesriigid VÕIVAD määratleda ja kasutada täiendavaid URIsid laiendades eespool nimetatud liikmesriigi URI (st URId, mis on määratletud selle hierarhilise URI põhjal).

TSL policy/legal notice (punkt 5.3.11)

See väli on kohustuslik ja peab vastama TS 119 612 punkti 5.3.11 nõuetele, kusjuures põhimõtted/õiguslik teade, mis käsitleb süsteemi juriidilist staatust või selles riigis süsteemi suhtes kohaldatavaid õigusnõudeid, kus süsteem on

([1]) ISO 3166-1:2006: „Maade ja nende jaotiste nimetuste tähised. Osa 1: Maatähised".

kehtestatud, ja/või mis tahes piiranguid ja tingimusi, mille alusel usaldusnimekirja hallatakse ja avaldatakse, peab olema mitmekeelsete märgistringide jada (vt punkt 5.1.4), milles esitatakse selliste põhimõtete või teate tekst järgmiselt (kohustuslik on need esitada Briti inglise keeles, võib esitada veel ühes või mitmes muus riigikeeles):

1) esimene osa on kohustuslik ja ühine kõigi liikmesriikide usaldusnimekirjade puhul; selles märgitakse kohaldatav õigusraamistik ning inglise keeles on tekst järgmine:

   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 liikmesriigi riigikeeles:

   Käesoleva usaldusnimekirja suhtes kohaldatav õigusraamistik on Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ.

2) Teine, vabatahtlik osa oleneb konkreetsest usaldusnimekirjast ja selles esitatakse viited konkreetsetele kohaldatavatele riiklikele õigusraamistikele.

Service current status (punkt 5.5.4)

See väli on kohustuslik ja peab vastama TS 119 612 punkti 5.5.4 nõuetele.

ELi liikmesriigi usaldusnimekirjas olevate teenuste välja „Service current status" väärtused määruse (EL) nr 910/2014 kohaldamise kuupäeva eelse päeva seisuga (s.o 30. juuni 2016) viiakse üle päeval, mil määrust hakatakse kohaldama (s.o 1. juulil 2016) vastavalt ETSI TS 119 612 J lisa sätetele.

III PEATÜKK

USALDUSNIMEKIRJADE JÄRJEPIDEVUS

Sertifikaadid, millest tuleb komisjonile teatada vastavalt käesoleva otsuse artikli 4 lõikele 2, peavad vastama ETSI TS 119 612 punkti 5.7.1 nõuetele ning need tuleb väljastada selliselt, et:

— nende kehtivuse lõppkuupäevad erinevad vähemalt kolme kuu võrra (väli „Not After");

— nad luuakse uute võtmepaaridega. Varem kasutatud võtmepaare ei tohi uuesti sertifitseerida.

Kui aegub üks avaliku võtme sertifikaat, mida saaks kasutada sellise usaldusnimekirja allkirja või templi valideerimiseks ning millest on komisjonile teatatud ja mis on avaldatud komisjoni viidete kesknimekirjas, peavad liikmesriigid:

— juhul kui parajasti avaldatud usaldusnimekirjale on antud allkiri või tempel privaatvõtmega, mille avaliku võtme sertifikaat on aegunud, andma viivitamata uuesti välja uue usaldusnimekirja, millele on antud allkiri või tempel privaatvõtmega, mille teatatud avaliku võtme sertifikaat ei ole aegunud;

— vajaduse korral tekitama uued võtmepaarid, mida saaks kasutada usaldusnimekirjale allkirja või templi andmiseks, ja hoolitsema neile vastavate avaliku võtme sertifikaatide loomise eest;

— kiiresti edastama komisjonile uue nimekirja avaliku võtme sertifikaatidest, mis vastavad privaatvõtmetele, mida saaks kasutada usaldusnimekirjale allkirja või templi andmiseks.

Kui rikutud või kasutuselt kõrvaldatud on üks privaatvõti, mis vastab ühele avaliku võtme sertifikaadile, mida saaks kasutada usaldusnimekirja allkirja või templi valideerimiseks ning millest on komisjonile teatatud ja mis on avaldatud komisjoni viidete kesknimekirjas, peavad liikmesriigid:

— viivitamata väljastama uue usaldusnimekirja, millele on antud allkiri või tempel rikkumata privaatvõtmega, kui avaldatud usaldusnimekirjale oli allkiri või tempel antud rikutud või kasutuselt kõrvaldatud privaatvõtmega;

— vajaduse korral tekitama uued võtmepaarid, mida saaks kasutada usaldusnimekirjale allkirja või templi andmiseks, ja hoolitsema neile vastavate avaliku võtme sertifikaatide loomise eest;

— kiiresti edastama komisjonile uue nimekirja avaliku võtme sertifikaatidest, mis vastavad privaatvõtmetele, mida saaks kasutada usaldusnimekirjale allkirja või templi andmiseks.

Kui rikutud või kasutuselt kõrvaldatud on kõik privaatvõtmed, mis vastavad avaliku võtme sertifikaatidele, mida saaks kasutada usaldusnimekirja allkirja valideerimiseks ning millest on komisjonile teatatud ja mis on avaldatud komisjoni viidete kesknimekirjas, peavad liikmesriigid:

— tekitama uued võtmepaarid, mida võiks kasutada usaldusnimekirjale allkirja või templi andmiseks, ja hoolitsema neile vastavate avaliku võtme sertifikaatide loomise eest;

— viivitamata väljastama uue usaldusnimekirja, millele on antud allkiri või tempel ühega nendest uutest privaatvõtmetest ja millele vastava avaliku võtme sertifikaat tuleb edastada;

— kiiresti edastama komisjonile uue nimekirja avaliku võtme sertifikaatidest, mis vastavad privaatvõtmetele, mida saaks kasutada usaldusnimekirjale allkirja või templi andmiseks.

IV PEATÜKK

USALDUSNIMEKIRJA INIMLOETAVA VORMI NÕUDED

Inimloetava usaldusnimekirja koostamise ja avaldamise korral tuleb see esitada ISO 32000 ([1]) kohase PDF-dokumendina, mis tuleb vormindada PDF/A-profiili (ISO 19005) ([2]) kohaselt.

PDF/A-profiilil põhineva inimloetava usaldusnimekirja sisu peab vastama järgmistele nõuetele:

— inimloetava vormi struktuur peab kajastama tehnilistes nõuetes TS 119 612 kirjeldatud loogilist mudelit;

— igal olemasoleval väljal peab olema näidatud ja esitatud:

  — välja nimi (nt „*Service type identifier*”);

  — välja väärtus (nt „http://uri.etsi.org/TrstSvc/Svctype/CA/QC}”);

  — vajaduse korral välja väärtuse tähendus (kirjeldus) (nt „*Sertifikaadi loomise teenus, mille raames luuakse ja allkirjastatakse kvalifitseeritud sertifikaadid, tuginedes identiteedile ja muudele asjaomase registreerimisteenuse kontrollitud atribuutidele.*”);

  — vajaduse korral mitu keeleversiooni loomulikes keeltes vastavalt usaldusnimekirjas esitatule;

— inimloetavas vormis peavad olema esitatud vähemalt järgmised väljal „Service digital identity” olevad digitaalsete sertifikaatide väljad ja vastavad väärtused ([3]):

  — versioon;

  — sertifikaadi seerianumber;

  — allkirja algoritm;

  — väljastaja – kõik asjaomased eristavad nimeväljad;

  — kehtivusaeg;

  — subjekt – kõik asjaomased eristavad nimeväljad;

([1]) ISO 32000-1:2008: Document management – Portable document format – Part 1: PDF 1.7.
([2]) ISO 19005-2:2011: Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2).
([3]) ITU soovitus-T X.509 | ISO/IEC 9594-8: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks (vt http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— avalik võti;

— väljaandja võtme identifikaator;

— subjekti võtme identifikaator;

— võtmekasutus;

— võtme laiendatud kasutus;

— sertifikaadipoliitika – kõik poliitika identifikaatorid ja täpsustid;

— poliitika kaardistamine;

— subjekti alternatiivne nimi;

— subjekti kataloogi atribuudid;

— põhipiirangud;

— poliitikapiirangud;

— CRLi jaotuspunktid ([1]);

— juurdepääs väljastaja teabele;

— juurdepääs subjekti teabele;

— kvalifitseeritud sertifikaadi määrang ([2]);

— räsialgoritm;

— sertifikaadi räsi väärtus;

— inimloetav vorm peab olema kergesti prinditav;

— süsteemi käitaja peab inimloetava vormi varustama allkirja või tempiga vastavalt komisjoni rakendusotsuse (EL) 2015/1505 artiklites 1 ja 3 sätestatud täiustatud PDF-allkirjale.

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

II LISA

LIIKMESRIIKIDE ESITATAVATE TEADETE VORM

Teave, mille liikmesriigid peavad esitama vastavalt käesoleva otsuse artikli 4 lõikele 1, peab sisaldama järgmisi andmeid ja nende võimalikke muudatusi:

1) Liikmesriik, kasutades standardile ISO 3166-1 ([1]) vastavalt kahetähelist riigikoodi, järgmiste eranditega:

   a) Ühendkuningriigi riigikood on „UK".

   b) Kreeka riigikood on „EL".

2) Asutus/asutused, kes vastutab/vastutavad automaatseks töötlemiseks sobivas vormingus ja inimestele loetavas vormingus usaldusnimekirjade koostamise, haldamise ja avaldamise eest.

   a) Süsteemi käitaja nimi: esitatav teave peab olema identne (tõstutundlik) väärtusega usaldusnimekirja väljal „Scheme operator name" kõigis usaldusnimekirjas kasutatud keeltes.

   b) Vabatahtlikult esitatav teave komisjonisiseseks kasutamiseks ainult juhtudel, kui asjaomase asutusega on vaja ühendust võtta (teavet ei avaldata komisjoni koostatavas usaldusnimekirjade nimekirjas):

      — süsteemi käitaja aadress;

      — vastutava(te) isiku(te) kontaktandmed (nimi, telefon, e-posti aadress).

3) Koht, kus avaldatakse usaldusnimekiri automaatseks töötlemiseks sobivas vormingus *(koht, kus on avaldatud kehtiv usaldusnimekiri)*.

4) Vajaduse korral koht, kus avaldatakse usaldusnimekiri inimestele loetavas vormingus *(koht, kus on avaldatud kehtiv usaldusnimekiri)*. Kui usaldusnimekirja inimestele loetavas vormingus enam ei avaldata, siis märge selle kohta.

5) Avalike võtmete sertifikaadid, mis vastavad privaatvõtmetele, mida saab kasutada e-allkirja või e-templi andmiseks automaatseks töötlemiseks sobivas vormingus usaldusnimekirjale ja inimestele loetavas vormingus usaldusnimekirjadele: need sertifikaadid esitatakse Privacy Enhanced Mail Base64 meetodiga kodeeritud DER-vormingus sertifikaatidena. Muutusest teatamise korral lisateave juhul, kui uus sertifikaat asendab konkreetse sertifikaadi komisjoni nimekirjas ja kui sertifikaat, millest teatatakse, tuleb olemasolevatele lisada ilma, et midagi asendataks.

6) Punktides 1–5 esitatud andmete esitamise kuupäev.

Andmed, mis esitatakse vastavalt punktidele 1, 2a, 3, 4 ja 5, lisatakse Euroopa Komisjoni koostatud usaldusnimekirjade nimekirja, kus need asendavad selles nimekirjas oleva varem esitatud teabe.

([1]) ISO 3166-1: „Maade ja nende jaotiste nimetuste tähised. Osa 1: Maatähised".