KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2015/1505

(2015. gada 8. septembris),

kurā saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 22. panta 5. punktu izklāstītas tehniskās specifikācijas un formāti, kas attiecas uz uzticamības sarakstiem

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulu (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), un jo īpaši tās 22. panta 5. punktu,

tā kā:

(1) Uzticamības sarakstiem ir būtiska nozīme uzticēšanās veidošanā tirgus operatoru starpā, jo tajos norādīts pakalpojumu sniedzēja statuss pārraudzības brīdī.

(2) Elektronisko parakstu pārrobežu izmantošanu veicināja Komisijas Lēmums 2009/767/EK ([2]), kas noteica pienākumu dalībvalstīm izveidot, uzturēt un publicēt uzticamības sarakstus, kuros ir informācija, kas attiecas uz sertifikācijas pakalpojumu sniedzējiem, kuri izdod kvalificētus sertifikātus sabiedrībai saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 1999/93/EK ([3]) un kurus pārrauga un akreditē dalībvalstis.

(3) Regulas (ES) Nr. 910/2014 22. pantā dalībvalstīm uzlikts par pienākumu izveidot, uzturēt un publicēt uzticamības sarakstus aizsargātā veidā, elektroniski parakstītus vai apzīmogotus, automatizētai apstrādei piemērotā formā un paziņot Komisijai, kuras struktūras atbild par valsts uzticamības sarakstu izveidi.

(4) Uzticamības pakalpojumu sniedzējs un tā sniegtie uzticamības pakalpojumi būtu jāuzskata par kvalificētiem, ja kvalifikācijas statuss tiek saistīts ar pakalpojumu sniedzēju uzticamības sarakstā. Lai nodrošinātu, ka citus Regulas (ES) Nr. 910/2014 uzliktos pienākumus, it īpaši 27. un 37. pantā noteiktos, pakalpojumu sniedzēji var viegli izpildīt no attāluma ar elektroniskiem līdzekļiem, un nekaitētu to citu sertifikācijas pakalpojumu sniedzēju tiesiskajai paļāvībai, kuri neizdod kvalificētus sertifikātus, bet sniedz ar elektroniskajiem parakstiem saistītus pakalpojumus saskaņā ar Direktīvu 1999/93/EK un ir uzskaitē līdz 2016. gada 30. jūnijam, būtu jāparedz iespēja dalībvalstīm brīvprātīgi valsts līmenī pievienot sarakstam uzticamības pakalpojumus, kas nav kvalificēti uzticamības pakalpojumi, ar noteikumu, ka tiek skaidri norādīts, ka tie nav kvalificēti saskaņā ar Regulu (ES) Nr. 910/2014.

(5) Saskaņā ar Regulas (ES) Nr. 910/2014 25. apsvērumu dalībvalstis var pievienot sarakstam arī tādus valsts noteiktus uzticamības pakalpojumu veidus, kas nav definēti Regulas (ES) Nr. 910/2014 3. panta 16. punktā, ar noteikumu, ka tiek skaidri norādīts, ka tie nav kvalificēti saskaņā ar Regulu (ES) Nr. 910/2014.

(6) Šajā lēmumā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi komiteja, kura izveidota ar Regulas (ES) Nr. 910/2014 48. pantu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Dalībvalstis izveido, publicē un uztur uzticamības sarakstus, kuros ir informācija par kvalificētu uzticamības pakalpojumu sniedzējiem, ko tās pārrauga, kā arī informācija par to sniegtajiem kvalificētajiem uzticamības pakalpojumiem. Minētie saraksti atbilst I pielikumā izklāstītajām tehniskajām specifikācijām.

([1]) OV L 257, 28.8.2014., 73. lpp.
([2]) Komisijas 2009. gada 16. oktobra Lēmums 2009/767/EK par pasākumiem, lai veicinātu procedūru veikšanu elektroniski, izmantojot vienotos kontaktpunktus atbilstoši Eiropas Parlamenta un Padomes Direktīvai 2006/123/EK par pakalpojumiem iekšējā tirgū (OV L 274, 20.10.2009., 36. lpp.).
([3]) Eiropas Parlamenta un Padomes 1999. gada 13. decembra Direktīva 1999/93/EK par Kopienas elektronisko parakstu sistēmu (OV L 13, 19.1.2000., 12. lpp.).

2. pants

Uzticamības sarakstos dalībvalstis drīkst iekļaut informāciju par nekvalificētu uzticamības pakalpojumu sniedzējiem kopā ar informāciju par nekvalificētajiem uzticamības pakalpojumiem, ko tie sniedz. Sarakstā skaidri norāda, kuri uzticamības pakalpojumu sniedzēji un to sniegtie uzticamības pakalpojumi nav kvalificēti.

3. pants

1. Saskaņā ar Regulas (ES) Nr. 910/2014 22. panta 2. punktu dalībvalstis elektroniski paraksta vai apzīmogo sava uzticamības saraksta automatizētai apstrādei piemēroto formu saskaņā ar I pielikumā izklāstītajām tehniskajām specifikācijām.

2. Ja dalībvalsts elektroniski publicē cilvēklasāmu uzticamības saraksta formu, tā nodrošina, ka šajā uzticamības saraksta formā ir tie paši dati, kas automatizēti apstrādājamā formā, un to paraksta vai apzīmogo elektroniski saskaņā ar I pielikumā izklāstītajām tehniskajām specifikācijām.

4. pants

1. Regulas (ES) Nr. 910/2014 22. panta 3. punktā minēto informāciju dalībvalstis dara zināmu Komisijai, izmantojot II pielikuma veidni.

2. 1. punktā minētajā informācijā ietilpst divi vai vairāki shēmas operatora publiskās atslēgas sertifikāti ar vismaz trīs mēnešu derīguma termiņa nobīdi, kuri atbilst privātajām atslēgām, ko var izmantot, lai elektroniski parakstītu vai apzīmogotu automatizētai apstrādei piemēroto uzticamā saraksta formu un cilvēklasāmo formu, kad tā publicēta.

3. Saskaņā ar Regulas (ES) Nr. 910/2014 22. panta 4. punktu Komisija pa aizsargātu kanālu autentificētā tīmekļa serverī publisko dalībvalstu piegādāto 1. un 2. punktā minēto informāciju parakstītā vai apzīmogotā automatizētai apstrādei piemērotā formā.

4. Komisija var dalībvalstu piegādāto 1. un 2. punktā minēto informāciju parakstītā vai apzīmogotā cilvēklasāmā formā pa aizsargātu kanālu publiskot autentificētā tīmekļa serverī.

5. pants

Šis lēmums stājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šis lēmums uzliek saistības kopumā un ir tieši piemērojams visās dalībvalstīs.

Briselē, 2015. gada 8. septembrī

Komisijas vārdā –

priekšsēdētājs

Jean-Claude JUNCKER

I PIELIKUMS

VIENOTĀS UZTICAMĪBAS SARAKSTU VEIDNES TEHNISKĀS SPECIFIKĀCIJAS

I NODAĻA

VISPĀRĪGAS PRASĪBAS

Uzticamības sarakstā iekļauj gan kārtējo, gan visu senāko informāciju par sarakstā minēto uzticamības pakalpojumu statusu no brīža, kad uzticamības pakalpojuma sniedzējs iekļauts uzticamības sarakstos.

Jēdzieni "apstiprināt", "akreditēt" un/vai "pārraudzīt" šajās specifikācijās aptver arī valsts apstiprināšanas shēmas, taču papildinformāciju par tādu valsts shēmu īpatnībām dalībvalstis sniegs savos uzticamības sarakstos līdz ar skaidrojumu par iespējamām atšķirībām no pārraudzības shēmām, ko piemēro uzticamības pakalpojuma sniedzējiem un kvalificētajiem uzticamības pakalpojumiem, kurus tie sniedz.

Uzticamības sarakstā sniegtās informācijas galvenais mērķis ir atbalstīt kvalificētu uzticamības pakalpojumu marķieru validēšanu; marķieri ir kvalificētu uzticamības pakalpojumu rezultātā ģenerēti vai izdoti fiziski vai bināri (loģiskie) objekti, kā kvalificēti elektroniskie paraksti/zīmogi, uzlaboti elektroniskie paraksti/zīmogi, kurus balsta kvalificēts sertifikāts, kvalificēti laika zīmogi, kvalificēti elektroniskie piegādes pierādījumi utt.

II NODAĻA

VIENOTĀS UZTICAMĪBAS SARAKSTU VEIDNES DETALIZĒTAS SPECIFIKĀCIJAS

Šīs specifikācijas ir balstītas uz specifikācijām un prasībām, kas noteiktas ETSI TS 119 612 v2.1.1 (turpmāk "ETSI TS 119 612").

Ja šajās specifikācijās nav izvirzītas īpašas prasības, pilnībā piemēro ETSI TS 119 612 5. un 6. punkta prasības. Ja šajās specifikācijās ir izvirzītas īpašas prasības, tās ir pārākas par attiecīgajām ETSI TS 119 612 prasībām. Ja ir neatbilstības starp šīm specifikācijām un ETSI TS 119 612 specifikācijām, pārākas ir šīs specifikācijas.

Scheme name (5.3.6. punkts)

Šis lauks ir obligāts un atbilst specifikācijām TS 119 612 5.3.6. punktā, un shēmai izmanto šādu nosaukumu:

"*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 (5.3.7. punkts)

Šis lauks ir obligāts un atbilst specifikācijām TS 119 612 5.3.7. punktā, un "pienācīgajā informācijā par shēmu" tiek iekļauti vismaz šādi dati:

a) visām dalībvalstīm kopīga ievada informācija par uzticamības saraksta darbības jomu un kontekstu, pamatā esošo pārraudzības shēmu un – attiecīgā gadījumā – valsts apstiprināšanas (piem., akreditācijas) shēmām. Izmantojamais kopīgais teksts ir tālākais teksts, kurā rakstzīmju virkni "[*attiecīgās dalībvalsts nosaukums*]" aizstāj ar attiecīgās dalībvalsts nosaukumu:

> "Šis saraksts ir uzticamības saraksts, kurā iekļauta informācija par kvalificēta uzticamības pakalpojuma sniedzējiem, kurus pārrauga [*attiecīgās dalībvalsts nosaukums*], kā arī informācija par kvalificētajiem uzticamības pakalpojumiem, ko tie sniedz, saskaņā ar attiecīgajiem noteikumiem Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulā (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK.

Elektronisko parakstu pārrobežu izmantošanu veicinājis Komisijas 2009. gada 16. oktobra Lēmums 2009/767/EK, kas uzliek dalībvalstīm par pienākumu izveidot, uzturēt un publicēt uzticamības sarakstus ar informāciju par sertifikācijas pakalpojumu sniedzējiem, kuri izsniedz kvalificētus sertifikātus sabiedrībai saskaņā ar Eiropas Parlamenta un Padomes 1999. gada 13. decembra Direktīvu 1999/93/EK par Kopienas elektronisko parakstu sistēmu un kuru pārraudzību/akreditāciju veic dalībvalstis. Šis uzticamības saraksts ir ar Lēmumu 2009/767/EK izveidotā uzticamības saraksta turpinājums."

Uzticamības sarakstiem ir būtiska nozīme, veidojot uzticēšanos starp elektronisko sakaru tirgus operatoriem, jo tie ļauj lietotājiem noskaidrot uzticamības pakalpojumu sniedzēju un to pakalpojumu kvalifikācijas statusu un tā vēsturi.

Dalībvalstu uzticamības sarakstos tiek iekļauta vismaz Komisijas Īstenošanas lēmuma (ES) 2015/1505 1. un 2. pantā noteiktā informācija.

Dalībvalstis var uzticamības sarakstos iekļaut informāciju par nekvalificētiem uzticamības pakalpojumu sniedzējiem un informāciju par nekvalificētajiem uzticamības pakalpojumiem, ko tie sniedz. Ir skaidri jānorāda, ka tie nav kvalificēti saskaņā ar Regulu (ES) Nr. 910/2014.

Dalībvalstis var uzticamajā sarakstā iekļaut informāciju par valsts līmenī definētiem tādu veidu uzticamības pakalpojumiem, kas nav definēti Regulas (ES) Nr. 910/2014 3. panta 16. punktā. Ir skaidri jānorāda, ka tie nav kvalificēti saskaņā ar Regulu (ES) Nr. 910/2014;

b) īpaša informācija par pamatā esošo pārraudzības shēmu un – vajadzības gadījumā – valsts apstiprināšanas (piemēram, akreditācijas) shēmām, it īpaši ([1]):

1) informācija par valsts pārraudzības shēmu, kas piemērojama kvalificētiem un nekvalificētiem uzticamības pakalpojumu sniedzējiem un kvalificētajiem un nekvalificētajiem uzticamības pakalpojumiem, ko reglamentē Regula (ES) Nr. 910/2014;

2) attiecīgā gadījumā – informācija par valsts brīvprātīgās akreditācijas shēmām, ko piemēro sertifikācijas pakalpojumu sniedzējiem, kuri izdevuši kvalificētus sertifikātus saskaņā ar Direktīvu 1999/93/EK.

Šajā īpašajā informācijā par katru iepriekš uzskaitīto pamatā esošo shēmu iekļauj vismaz šādus datus:

1) vispārīgu aprakstu;

2) informāciju par procesu, kas jāievēro valstu uzraudzības sistēmā un – vajadzības gadījumā – apstiprināšanā saskaņā ar valsts apstiprināšanas shēmu;

3) informāciju par kritērijiem, pēc kuriem uzticamības pakalpojumu sniedzējus pārrauga vai attiecīgā gadījumā apstiprina;

4) informāciju par kritērijiem un noteikumiem, ko izmanto, lai izraudzītu pārraugus/revidentus, un par to, kā tie novērtē uzticamības pakalpojumu sniedzējus un to sniegtos uzticamības pakalpojumus;

5) attiecīgā gadījumā – citu kontaktinformāciju un vispārīgu informāciju, kas attiecas uz shēmas darbību.

Scheme type/community/rules (5.3.9. punkts)

Šis lauks ir obligāts un atbilst specifikācijām TS 119 612 5.3.9. punktā.

Tas ietver *URI* tikai AK angļu valodā.

([1]) Šiem informācijas kopumiem ir izšķiroša nozīme, lai atkarīgās puses varētu novērtēt šādu sistēmu kvalitātes un drošības līmeni. Šos informācijas kopumus nodrošina uzticamības saraksta līmenī, izmantojot pašreizējos laukus "Scheme information URI" (5.3.7. punkts – dalībvalsts sniegtā informācija), "Scheme type/community/rules" (5.3.9. punkts – izmantojot visām dalībvalstīm kopīgu tekstu) un "TSL policy/legal notice" (5.3.11. punkts – visām dalībvalstīm kopīgs teksts, kā arī iespēja katrai dalībvalstij pievienot specifisku tekstu/atsauces). Attiecīgā gadījumā un pēc vajadzības pakalpojuma līmenī var sniegt papildinformāciju par šādām sistēmām, kas attiecas uz nekvalificētiem uzticamības pakalpojumiem un valsts līmenī definētiem (kvalificētiem) uzticamības pakalpojumiem (piemēram, lai nošķirtu vairākus kvalitātes/drošības līmeņus), izmantojot lauku "Scheme service definition URI" (5.5.6. punkts).

Tas ietver vismaz divus *URI*:

1) vienu šādu *URI*, kas kopīgs visu dalībvalstu uzticamības sarakstiem un norāda uz aprakstošu tekstu, kurš piemērojams visiem uzticamības sarakstiem:

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

Aprakstošais teksts:

"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) vienu *URI*, kas specifisks katras dalībvalsts uzticamības sarakstam un norāda uz aprakstošo tekstu, kurš piemērojams šās dalībvalsts uzticamības sarakstam:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, kur CC ir ISO 3166-1 ([1]) valsts divburtu kods, kas lietots laukā "Scheme territory" (5.3.10. punkts),

— kur lietotāji var iegūt ziņas par attiecīgās dalībvalsts īpašo politiku/noteikumiem, pēc kuriem tiek novērtēti sarakstā iekļautie uzticamības pakalpojumi atbilstoši dalībvalsts attiecīgajai pārraudzības sistēmai un – attiecīgos gadījumos – apstiprināšanas shēmai,

— kur lietotāji var iegūt attiecīgās dalībvalsts norādīto īpašo aprakstu par to, kā izmantot un interpretēt uzticamības saraksta saturu, kas attiecas uz sarakstā iekļautajiem nekvalificētajiem uzticamības pakalpojumiem un/vai valsts līmenī definētajiem uzticamības pakalpojumiem. To var izmantot, lai norādītu potenciālo granularitāti valsts apstiprināšanas sistēmās, kas saistītas ar *CSP*, kuri neizsniedz *QC*, un to, kā šim nolūkam izmanto laukus "Scheme service definition URI" (5.5.6. punkts) un "Service information extension" (5.5.9. punkts).

Dalībvalstis var definēt un izmantot papildu *URI*, kas paplašina iepriekš norādīto dalībvalstij specifisko *URI* (t. i., *URI*, kas definēti no šā hierarhiskā specifiskā *URI*).

TSL policy/legal notice (5.3.11. punkts)

Šis lauks ir obligāts un atbilst specifikācijām TS 119 612 5.3.11. punktā, un tajā politikas/juridiskais paziņojums par shēmas juridisko statusu vai juridiskajām prasībām, kuras shēma ievēro saskaņā ar jurisdikciju, kurā tā ir reģistrēta,

([1]) ISO 3166-1:2006: "Valstu un to administratīvi teritoriālā iedalījuma vienību nosaukumu kodi. 1. daļa: Valstu kodi"

un/vai jebkuri ierobežojumi un nosacījumi, ar kuriem uzticamības saraksts tiek uzturēts un publicēts, ir daudzvalodu rakstzīmju virkne (sk. 5.1.4. punktu), kas obligāti AK angļu valodā un fakultatīvi vienā vai vairākās valstu valodās sniedz faktisko politikas/juridiskā paziņojuma tekstu ar šādu uzbūvi:

1. Pirmā, obligātā, visu dalībvalstu uzticamajiem sarakstiem kopīgā daļa, kas norāda uz piemērojamo tiesisko regulējumu un kuras teksts angļu valodā ir šāds:

   "*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.*"

   Teksts dalībvalsts valodā:

   "Šim uzticamības sarakstam piemērojamais tiesiskais regulējums ir Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regula (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK."

2. Otra, fakultatīva, katram uzticamības sarakstam specifiska daļa, ar atsaucēm uz īpašu piemērojamo valsts tiesisko regulējumu.

Service current status (5.5.4. punkts)

Šis lauks ir obligāts un atbilst specifikācijām TS 119 612 5.5.4. punktā.

ES dalībvalstu uzticamības sarakstā uzskaitīto pakalpojumu "Service current status" vērtības dienā pirms Regulas (ES) Nr. 910/2014 piemērošanas sākuma (t. i., 2016. gada 30. jūnija) migrēšanu veic regulas piemērošanas sākuma dienā (t. i., 2016. gada 1. jūlijā), kā norādīts ETSI TS 119 612 J pielikumā.

III NODAĻA

UZTICAMĪBAS SARAKSTU NEPĀRTRAUKTĪBA

Sertifikāti, par kuriem jāpaziņo Komisijai saskaņā ar šā lēmuma 4. panta 2. punktu, atbilst 5.7.1. punkta prasībām no ETSI TS 119 612, un tos izdod tādā veidā, ka:

— to derīguma termiņš atšķiras vismaz par trim mēnešiem ("Not After")

— un tos rada ar jauniem atslēgu pāriem. Agrāk izmantotus atslēgu pārus nedrīkst pārsertificēt.

Ja ir notecējis viens no publiskās atslēgas sertifikātiem, ko var izmantot uzticamības saraksta paraksta vai zīmoga validēšanai, par kuru ir paziņots Komisijai un kas ir publicēts Komisijas centrālajā norāžu sarakstā, dalībvalstis:

— gadījumā, ja publicētais uzticamības saraksts bijis parakstīts vai apzīmogots ar privāto atslēgu, kuras publiskās atslēgas sertifikāts ir notecējis, nekavējoties izdod jaunu uzticamības sarakstu, kas parakstīts vai apzīmogots ar privāto atslēgu, kuras izziņotais publiskās atslēgas sertifikāts nav notecējis,

— pēc vajadzības ģenerē jaunus atslēgu pārus, ko var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai, un to atbilstošos publiskās atslēgas sertifikātus,

— tūlīt dara zināmu Komisijai publiskās atslēgas sertifikātu jauno sarakstu, kas atbilst privātajām atslēgām, kuras var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai.

Ja ir kompromitēta vai norakstīta viena no privātajām atslēgām, kas atbilst publiskās atslēgas sertifikātam, kuru var izmantot uzticamības saraksta paraksta validēšanai un kurš ir paziņots Komisijai un publicēts Komisijas centrālajā norāžu sarakstā, dalībvalstis:

— nekavējoties izdod jaunu uzticamības sarakstu, kas parakstīts vai apzīmogots ar nekompromitētu privāto atslēgu, gadījumā, ja publicētais uzticamības saraksts ticis parakstīts ar kompromitētu vai norakstītu privātu atslēgu,

— pēc vajadzības ģenerē jaunus atslēgu pārus, ko var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai, un to atbilstošos publiskās atslēgas sertifikātus,

— tūlīt dara zināmu Komisijai publiskās atslēgas sertifikātu jauno sarakstu, kas atbilst privātajām atslēgām, kuras var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai.

Ja ir kompromitētas vai norakstītas visas privātās atslēgas, kas atbilst publiskās atslēgas sertifikātiem, kurus var izmantot uzticamības saraksta paraksta validēšanai un kuri ir paziņoti Komisijai un publicēti Komisijas centrālajā norāžu sarakstā, dalībvalstis:

— ģenerē jaunus atslēgu pārus, ko var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai, un to atbilstošos publiskās atslēgas sertifikātus,

— nekavējoties izdod jaunu uzticamības sarakstu, kas parakstīts vai apzīmogots ar vienu no šīm jaunajām privātajām atslēgām un par kura atbilstošo publiskās atslēgas sertifikātu ir jāpaziņo,

— tūlīt dara zināmu Komisijai publiskās atslēgas sertifikātu jauno sarakstu, kas atbilst privātajām atslēgām, kuras var izmantot uzticamības saraksta parakstīšanai vai apzīmogošanai.

IV NODAĻA

UZTICAMĪBAS SARAKSTA CILVĒKLASĀMĀS FORMAS SPECIFIKĀCIJAS

Ja izveido un publicē uzticamības saraksta cilvēklasāmo formu, tā sniedzama ISO 32000 ([1]) atbilstoša pārnesama dokumentu formāta (*PDF*) veidā, kas formatēts saskaņā ar profilu *PDF/A* (ISO 19005 ([2])).

Uz *PDF/A* balstītās uzticamības saraksta cilvēklasāmās formas saturam jāatbilst šādām prasībām:

— cilvēklasāmās formas struktūrai jāatspoguļo loģiskais modelis, kas aprakstīts TS 119 612,

— jāattēlo katrs ietvertais lauks, un tajā jānorāda:

  — lauka nosaukums (piemēram, *Service type identifier*),

  — lauka vērtība (piemēram, "http://uri.etsi.org/TrstSvc/Svctype/CA/QC"),

  — attiecīgā gadījumā – lauka vērtības nozīme (apraksts) (piemēram, "*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*");

  — attiecīgā gadījumā – vairākas versijas dabiskajās valodās, kas paredzētas uzticamības sarakstā;

— cilvēklasāmajā formā norāda vismaz šādus laukus un atbilstošās laukā "Service digital identity" norādīto digitālo sertifikātu vērtības ([3]):

  — versija,

  — sertifikāta sērijas numurs,

  — paraksta algoritms,

  — izdevējs – visi attiecīgie atšķiramu nosaukumu lauki,

  — derīguma termiņš,

  — subjekts – visi attiecīgie atšķiramu nosaukumu lauki,

([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]) Ieteikums *ITU-T X.509 | ISO/IEC 9594-8: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks* (sk. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— publiskā atslēga,

— iestādes atslēgas identifikators,

— subjekta atslēgas identifikators,

— atslēgas lietošana,

— atslēgas lietošanas paplašinājums,

— sertifikātu politika – visi politikas identifikatori un politikas kvalifikatori,

— politikas attiecinājumi,

— subjekta alternatīvais nosaukums,

— subjekta direktorija atribūti,

— pamatierobežojumi,

— politikas ierobežojumi,

— *CRL* izplatīšanas vietas ([1]),

— piekļuve iestādes informācijai,

— piekļuve subjekta informācijai,

— kvalificēta sertifikāta definējums ([2]),

— jaucējalgoritms,

— sertifikāta jaucējvērtība.

— Cilvēklasāmajai formai jābūt viegli drukājamai.

— Cilvēklasāmo formu shēmas operators paraksta un apzīmogo saskaņā ar Komisijas Īstenošanas lēmuma (ES) 2015/1505 1. un 3. punktā noteikto *PDF* uzlaboto parakstu.

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

II PIELIKUMS

VEIDNE DALĪBVALSTU PAZIŅOJUMIEM

Informācijā, ko dalībvalstis sniedz saskaņā ar šā lēmuma 4. panta 1. punktu, iekļaujami šādi dati un to izmaiņas:

1. Dalībvalsts, izmantojot ISO 3166-1 ([1]) divburtu kodus, ar šādiem izņēmumiem:

   a) Apvienotās Karalistes valsts kods ir "UK";

   b) Grieķijas valsts kods ir "EL".

2. Struktūra/struktūras, kas atbild par uzticamības sarakstu izveidi, uzturēšanu un publicēšanu automatizētai apstrādei piemērotā formā un cilvēklasāmā formā:

   a) shēmas operatora nosaukums: sniegtajai informācijai ir jābūt identiskai – reģistrjutīgi – ar vērtību "Shēmas operatora nosaukums", kas ir uzticamības sarakstā, tik valodās, cik izmantotas uzticamības sarakstā;

   b) fakultatīva informācija Komisijas iekšējai lietošanai tikai tādos gadījumos, ja ir vajadzīgs sazināties ar attiecīgo struktūru (informācija netiks publicēta EK uzticamības sarakstu apkopotajā sarakstā):

      — shēmas operatora adrese,

      — atbildīgo personu kontaktinformācija (vārds, uzvārds, tālruņa numurs, e-pasta adrese).

3. Vieta, kur tiek publicēta uzticamības saraksta automatizētai apstrādei piemērotā forma *(vieta, kur ir publicēts pašreizējais uzticamības saraksts)*.

4. Attiecīgā gadījumā – vieta, kur tiek publicēts cilvēklasāmais uzticamības saraksts *(vieta, kur ir publicēts pašreizējais uzticamības saraksts)*. Ja cilvēklasāmais uzticamības saraksts vairs netiek publicēts, uz šo faktu jānorāda.

5. Publiskās atslēgas sertifikāti, kuri atbilst privātajām atslēgām, ko var izmantot, lai elektroniski parakstītu vai apzīmogotu automatizētai apstrādei piemēroto uzticamības saraksta formu un uzticamības sarakstu cilvēklasāmo formu: šos sertifikātus nodrošina paaugstināta privātuma pasta *Base64* šifrētu *DER* sertifikātu veidā. Paziņošanai par izmaiņu – papildu informācija gadījumā, kad jaunam sertifikātam ir jāaizstāj konkrēts sertifikāts Komisijas sarakstā, un gadījumā, kad paziņotais sertifikāts ir jāpievieno esošajiem bez aizstāšanas.

6. 1.–5. punktā paziņoto datu iesniegšanas datums.

Datus, ko paziņo saskaņā ar 1. punktu, 2. punkta a) apakšpunktu, 3., 4. un 5. punktu, iekļauj EK uzticamības sarakstu apkopotajā sarakstā, nomainot agrāk paziņoto informāciju, kas iekļauta minētajā apkopotajā sarakstā.

([1]) ISO 3166-1: "Valstu un to administratīvi teritoriālā iedalījuma vienību nosaukumu kodi. 1. daļa. Valstu kodi".