

KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2015/1505**2015 m. rugsėjo 8 d.****kuriu pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 22 straipsnio 5 dalį nustatomos patikimų sąrašų techninės specifikacijos ir formatai****(Tekstas svarbus EEE)**

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB ⁽¹⁾, ypač į jo 22 straipsnio 5 dalį,

kadangi:

- (1) patikimi sąrašai yra labai svarbūs tam, kad rinkos dalyviai įgytų tarpusavio pasitikėjimą, nes juose, atliekant priežiūrą, nurodomas paslaugos teikėjo statusas;
- (2) tarpvalstybinis elektroninių parašų naudojimas buvo palengvintas Komisijos sprendimu 2009/767/EB ⁽²⁾, kuriuo nustatyta valstybių narių pareiga sudaryti, tvarkyti ir skelbti patikimus sąrašus, kuriuose pateikta informacija apie valstybių narių priežiūrimus ir (arba) akredituotus sertifikavimo paslaugų teikėjus, pagal Europos Parlamento ir Tarybos direktyvą 1999/93/EB ⁽³⁾ visuomenei išduodančius kvalifikuotus sertifikatus;
- (3) Reglamento (ES) Nr. 910/2014/ES 22 straipsnyje nustatyta valstybių narių pareiga sudaryti, tvarkyti ir saugiai skelbti elektroniniu būdu pasirašytus arba užantspauduotus patikimus sąrašus tokia forma, kad juos būtų galima tvarkyti automatizuotomis priemonėmis, ir pranešti Komisijai apie įstaigas, atsakingas už nacionalinių patikimų sąrašų sudarymą;
- (4) patikimumo užtikrinimo paslaugų teikėjas ir jo teikiamos patikimumo užtikrinimo paslaugos turėtų būti laikomi kvalifikuotais, jei kvalifikacijos statusas yra susijęs su į patikimą sąrašą įrašytu paslaugų teikėju. Siekiant užtikrinti, kad paslaugų teikėjai galėtų lengvai nuotoliniu būdu ir elektroninėmis priemonėmis įvykdyti kitus įsipareigojimus, nustatytus Reglamente (ES) Nr. 910/2014, visų pirma jo 27 ir 37 straipsniuose, ir siekiant patenkinti teisėtus sertifikavimo paslaugų teikėjų, kurie neišduoda kvalifikuotų sertifikatų, bet teikia paslaugas, susijusias su elektroniniais parašais, pagal Direktyvą 1999/93/EB ir yra įtraukti į sąrašą iki 2016 m. birželio 30 d., lūkesčius, valstybėms narėms turėtų būti suteikta galimybė savanoriškai nacionaliniu lygiu į patikimus sąrašus įtraukti kitas nei kvalifikuotas patikimumo užtikrinimo paslaugas, su sąlyga, kad aiškiai nurodoma, jog jos yra nekvalifikuotos pagal Reglamentą (ES) Nr. 910/2014;
- (5) pagal Reglamento (ES) Nr. 910/2014 25 konstatuojamąją dalį valstybės narės gali įtraukti kitų rūšių nacionaliniu lygiu nustatytas patikimumo užtikrinimo paslaugas, nei nustatytas Reglamento (ES) Nr. 910/2014 3 straipsnio 16 dalyje, su sąlyga, kad aiškiai nurodoma, jog jos yra nekvalifikuotos pagal Reglamentą (ES) Nr. 910/2014;
- (6) šiame sprendime nustatytos priemonės atitinka pagal Reglamento (ES) Nr. 910/2014 48 straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Valstybės narės sudaro, skelbia ir tvarko patikimus sąrašus, į kuriuos įtraukta informacija apie kvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, kuriuos jos priežiūri, ir informacija apie jų teikiamas kvalifikuotas patikimumo užtikrinimo paslaugas. Tie sąrašai turi atitikti I priede nustatytas technines specifikacijas.

⁽¹⁾ O L L 257, 2014 8 28, p. 73.

⁽²⁾ 2009 m. spalio 16 d. Komisijos sprendimas 2009/767/EB, kuriu pagal Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje nustatomos priemonės procedūroms, atliekamoms naudojantis elektroninėmis priemonėmis ir kontaktinių centrų paslaugomis, palengvinti (O L L 274, 2009 10 20, p. 36).

⁽³⁾ 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos (O L L 13, 2000 1 19, p. 12).

2 straipsnis

Valstybės narės į patikimus sąrašus gali įtraukti informaciją apie nekvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, taip pat informaciją apie jų teikiamas nekvalifikuotas patikimumo užtikrinimo paslaugas. Sąraše turi būti aiškiai nurodyta, kurie patikimumo užtikrinimo paslaugų teikėjai yra nekvalifikuoti ir kurios jų teikiamos patikimumo užtikrinimo paslaugos yra nekvalifikuotos.

3 straipsnis

1. Pagal Reglamento (ES) Nr. 910/2014 22 straipsnio 2 dalį valstybės narės elektroniniu būdu pasirašo arba užantspauduoja patikimus sąrašus tokia forma, kad juos būtų galima tvarkyti automatizuotomis priemonėmis, remiantis I priede nustatytais techniniais specifikacijomis.
2. Jei valstybė narė elektroniniu būdu skelbia žmonėms suprantamos formos patikimą sąrašą, ji užtikrina, kad šios formos patikimame sąraše būtų pateikti tie patys duomenys kaip ir formos, kurią galima tvarkyti automatizuotomis priemonėmis, ir pasirašo arba užantspauduoja ją elektroniniu būdu, remdamasi I priede nustatytais techniniais specifikacijomis.

4 straipsnis

1. Valstybės narės pateikia Komisijai Reglamento (ES) Nr. 910/2014 22 straipsnio 3 dalyje nurodytą informaciją, naudodamos II priede pateiktą formą.
2. 1 dalyje nurodyta informacija apima du ar daugiau schemos operatoriaus viešojo rakto sertifikatų, kurių perkeltas galiojimo laikotarpis ne trumpesnis nei trys mėnesiai, atitinkančių privačius raktus, kurie gali būti naudojami siekiant elektroniniu būdu pasirašyti arba užantspauduoti patikimo sąrašo formą, kurią galima tvarkyti automatizuotomis priemonėmis, o kai jis paskelbtas – žmonėms suprantamą formą.
3. Pagal Reglamento (ES) Nr. 910/2014 22 straipsnio 4 dalį Komisija saugiu priegos prie patvirtinto žiniatinklio serverio kanalu visuomenei pateikia 1 ir 2 dalyse numatytą, kaip pranešta valstybių narių, pasirašytą arba užantspaudotą informaciją tokia forma, kad ją būtų galima tvarkyti automatizuotomis priemonėmis.
4. Komisija saugiu priegos prie patvirtinto žiniatinklio serverio kanalu visuomenei gali pateikti 1 ir 2 dalyse numatytą, kaip pranešta valstybių narių, pasirašytą arba užantspaudotą informaciją žmonėms suprantama forma.

5 straipsnis

Šis sprendimas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis sprendimas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2015 m. rugsėjo 8 d.

Komisijos vardu
Pirmininkas
Jean-Claude JUNCKER

I PRIEDAS

PATIKIMŲ SĄRAŠŲ BENDROSIOS FORMOS TECHNINĖS SPECIFIKACIJOS

I SKYRIUS

BENDRIEJI REIKALAVIMAI

Patikimuose sąrašuose pateikiama tiek dabartinė, tiek visa ankstesnė informacija apie į sąrašą įtrauktų patikimumo užtikrinimo paslaugų statusą nuo patikimumo užtikrinimo paslaugų teikėjo įtraukimo į patikimus sąrašus.

Sąvokos „patvirtinti“, „akredituoti“ ir (arba) „prižiūrėti“ šiose specifikacijose taip pat apima nacionalines patvirtinimo schemas, tačiau valstybės narės savo patikimame sąraše teiks papildomą informaciją apie bet kokių tokių nacionalinių schemų pobūdį, įskaitant galimų skirtumų nuo priežiūros schemų, taikomų kvalifikuotiems patikimumo užtikrinimo paslaugų teikėjams ir jų teikiamoms kvalifikuotoms patikimumo užtikrinimo paslaugoms, paaiškinimą.

Informacija, pateikta patikimame sąraše, visų pirma skirta padėti tvirtinti kvalifikuotų patikimumo užtikrinimo paslaugų ženklus, t. y. fizinius arba dvejotinius (loginius) objektus, sukurtus arba išduotus teikiant kvalifikuotą patikimumo užtikrinimo paslaugą, pvz., kvalifikuotus elektroninius parašus/spaudus; pažangiuosius elektroninius parašus/spaudus, patvirtintus kvalifikuotu sertifikatu; kvalifikuotas laiko žymas; kvalifikuotus elektroninio pristatymo įrodymus ir kt.

II SKYRIUS

PATIKIMŲ SĄRAŠŲ BENDROSIOS FORMOS IŠSAMIOS SPECIFIKACIJOS

Šios specifikacijos pagrįstos specifikacijomis ir reikalavimais, nustatytais ETSI TS 119 612 v2.1.1 (toliau – ETSI TS 119 612).

Jeigu šiose specifikacijose konkretus reikalavimas nenurodytas, taikomi visi ETSI TS 119 612 5 ir 6 punktuose nustatyti reikalavimai. Jeigu šiose specifikacijose pateikti konkretūs reikalavimai, jiems teikiama pirmenybė prieš atitinkamus ETSI TS 119 612 nustatytus reikalavimus. Jei šios specifikacijos prieštarauja ETSI TS 119 612 specifikacijoms, pirmenybė teikiama šioms specifikacijoms.

Schemos pavadinimas (5.3.6 punktas)

Šis laukas turi būti įtrauktas ir turi atitikti TS 119 612 5.3.6 punkte nustatytas specifikacijas, pagal kurias schemai pavadinti turi būti naudojamas toks pavadinimas:

„EN_name_value“ = „Patikimas sąrašas, į kurį įtraukta informacija apie kvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, kuriuos prižiūri išduodančioji valstybė narė, taip pat informacija apie jų teikiamas kvalifikuotas patikimumo užtikrinimo paslaugas, laikantis atitinkamų nuostatų, nustatytų 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB“.

Schemos informacijos UII (5.3.7 punktas)

Šis laukas turi būti įtrauktas ir turi atitikti TS 119 612 5.3.7 punkte nustatytas specifikacijas, pagal kurias į tinkamą schemos informaciją turi būti įtraukta bent ši informacija:

- visoms valstybėms narėms vienoda įvadinė informacija apie patikimo sąrašo taikymo sritį ir aplinkybes, pamatinę priežiūros schemą ir, kai taikytina, nacionalinę (-es) patvirtinimo (pvz., akreditacijos) schemą (-as). Bendras naudotinas tekstas – jame rašmenų eilutė „[atitinkamos valstybės narės pavadinimas]“ turi būti pakeista atitinkamos valstybės narės pavadinimu – yra toks:

„Šis sąrašas – tai patikimas sąrašas, į kurį įtraukta informacija apie kvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, kuriuos prižiūri [atitinkamos valstybės narės pavadinimas], taip pat informacija apie jų teikiamas kvalifikuotas patikimumo užtikrinimo paslaugas, laikantis atitinkamų nuostatų, nustatytų 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.“

Tarpvalstybinis elektroninių parašų naudojimas palengvintas 2009 m. spalio 16 d. Komisijos sprendimu 2009/767/EB, kuriuo nustatyta valstybių narių pareiga sudaryti, tvarkyti ir skelbti patikimus sąrašus, kuriuose būtų pateikta informacija apie valstybių narių prižiūrimus ir (arba) akredituotus sertifikavimo paslaugų teikėjus, išduodančius kvalifikuotus sertifikatus pagal 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvą 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos visuomenei. Šis patikimas sąrašas – tai Sprendimu 2009/767/EB nustatyto patikimo sąrašo tęsinys.“

Patikimi sąrašai yra labai svarbūs didinant pasitikėjimą tarp elektroninės rinkos operatorių, nes leidžia vartotojams nustatyti patikimumo užtikrinimo paslaugų teikėjų ir jų teikiamų paslaugų kvalifikacijos statusą ir statuso istoriją.

Valstybių narių patikimuose sąrašuose pateikiama bent jau informacija, nurodyta Komisijos įgyvendinimo sprendimo (ES) 2015/1505 1 ir 2 straipsniuose.

Valstybės narės į patikimus sąrašus gali įtraukti informaciją apie nekvalifikuotus patikimumo užtikrinimo paslaugų teikėjus, taip pat informaciją apie jų teikiamas nekvalifikuotas patikimumo užtikrinimo paslaugas. Turi būti aiškiai nurodyta, kad teikėjai ir paslaugos yra nekvalifikuoti pagal Reglamentą (ES) Nr. 910/2014.

Valstybės narės į patikimus sąrašus gali įtraukti informaciją apie nacionaliniu lygiu apibrėžtas kitų rūšių, nei nustatytos Reglamente (ES) Nr. 910/2014 3 straipsnio 16 dalyje, patikimumo užtikrinimo paslaugas. Turi būti aiškiai nurodyta, kad jos yra nekvalifikuotos pagal Reglamentą (ES) Nr. 910/2014;

b) specifinė informacija apie pamatinę priežiūros schemą ir, kai taikoma, nacionalinę (-es) patvirtinimo (pvz., akreditacijos) schemą (-as), visų pirma ⁽¹⁾:

- 1) informacija apie nacionalinę priežiūros sistemą, taikomą kvalifikuotų ir nekvalifikuotų patikimumo užtikrinimo paslaugų teikėjams ir kvalifikuotoms ir nekvalifikuotoms patikimumo užtikrinimo paslaugoms, kaip numatyta Reglamente (ES) Nr. 910/2014;
- 2) atitinkamais atvejais informacija apie nacionalines savanoriškos akreditacijos schemas, taikomas sertifikavimo paslaugų teikėjams, kurie išdavė kvalifikuotus sertifikatus pagal Direktyvą 1999/93/EB.

Teikiant šią specifinę informaciją apie kiekvieną nurodytą pamatinę schemą turi būti pateikta bent tokia informacija:

- 1) bendras aprašas;
- 2) informacija apie nacionalinės priežiūros sistemos procesą ir atitinkamais atvejais patvirtinimo pagal nacionalinę patvirtinimo schemą procesą;
- 3) informacija apie kriterijus, pagal kuriuos vykdoma patikimumo užtikrinimo paslaugų teikėjų priežiūra arba atitinkamais atvejais jie yra patvirtinami;
- 4) informacija apie kriterijus ir taisykles, taikomus prižiūrėtojams ir (arba) auditoriams atrinkti ir nustatyti, kaip jie turi vertinti patikimumo užtikrinimo paslaugų teikėjus ir jų teikiamas patikimumo užtikrinimo paslaugas;
- 5) atitinkamais atvejais kita informacija ryšiams ir bendra informacija apie schemos veikimą.

Schemos tipas, naudotojai ir (arba) taisyklės (5.3.9 punktas)

Šis laukas turi būti įtrauktas ir turi atitikti TS 119 612 5.3.9 punkte nustatytas specifikacijas.

Jame turi būti pateikti tik UII Jungtinės Karalystės anglų kalba.

⁽¹⁾ Šie informacijos rinkiniai yra ypač svarbūs, kad susijusios šalys galėtų įvertinti tokių sistemų kokybę ir saugumą. Tie informacijos rinkiniai teikiami patikimo sąrašo lygmeniu naudojant šį lauką „Schemos informacijos UII“ (5.3.7 punktas – informaciją teikia valstybės narės), „Schemos tipas, naudotojai ir (arba) taisyklės“ (5.3.9 punktas – naudojamas visoms valstybėms narėms bendras tekstas) ir „PUPSS politika ir (arba) teisinė informacija“ (5.3.11 punktas – visoms valstybėms narėms bendras tekstas; be to, kiekviena valstybė narė gali pateikti papildomą jai svarbų tekstą ir (arba) nuorodų). Kai reikia ir reikalaujama, paslaugos lygmeniu naudojant lauką „Pagal schemą teikiamos paslaugos apibrėžties UII“ (5.5.6 punktas) gali būti teikiama papildoma informacija apie tokias nekvalifikuotų patikimumo užtikrinimo paslaugų ir nacionaliniu mastu nustatytų (kvalifikuotų) patikimumo užtikrinimo paslaugų sistemas (pvz., norint išskirti keletą kokybės ir (arba) saugumo lygmenų).

Jame turi būti pateikti bent du UII:

- 1) visų valstybių narių patikimiems sąrašams bendras UII kaip nuoroda į aprašomąjį tekstą, kuris turi būti taikomas visiems patikimiems sąrašams:

UII: <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>

Aprašomasis tekstas:

„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 (ES) 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 (ES) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

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

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

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

Interpretation of the Trusted List

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (ES) 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, ir t. t.). 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 (ES) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists.“

- 2) specifinis kiekvienos valstybės narės patikimo sąrašo UII kaip nuoroda į aprašomąjį tekstą, kuris turi būti taikomas šios valstybės narės patikimam sąrašui:

<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC>, CC – ISO 3166-1 ⁽¹⁾ dviejų raidžių šalies kodas, nurodytas lauke „Schemos teritorija“ (5.3.10 punktas).

- šiame tekste naudotojai gali rasti informacijos apie specifinę nurodytos valstybės narės politiką ir (arba) taisykles, pagal kurias, laikantis tos valstybės narės priežiūros režimo ir, kai taikytina, patvirtinimo schemos, vertinamos į sąrašą įtrauktos patikimos paslaugos,
- šiame tekste naudotojai gali rasti specifinį nurodytos valstybės narės aprašą, kaip naudoti ir aiškinti patikimo sąrašo turinį, susijusį su į sąrašą įtrauktomis nekvalifikuotomis patikimumo užtikrinimo paslaugomis ir (arba) nacionaliniu lygiu nustatytais patikimumo užtikrinimo paslaugomis. Šis tekstas gali būti naudojamas galimam nacionalinių patvirtinimo sistemų, susijusių su kvalifikuotų sertifikatų neišduodančiais sertifikavimo paslaugų teikėjais, hierarchijos lygiui nurodyti, taip pat nurodyti, kaip šiuo tikslu naudojami laukai „Pagal schemą teikiamos paslaugos apibrėžties UII“ (5.5.6 punktas) ir „Informacijos apie paslaugą plėtinys“ (5.5.9 punktas).

Valstybės narės, praplėsdamos minėtą specifinį valstybės narės UII, GALI nustatyti ir naudoti papildomus UII (t. y. UII, nustatomus remiantis šiuo specifiniu hierarchiniu UII).

Informacija apie PUPSS politiką ir (arba) teisinė informacija (5.3.11 punktas)

Šis laukas turi būti įtrauktas ir turi atitikti TS 119 612 5.3.11 punkte nustatytas specifikacijas, pagal kurias informacija apie politiką ir (arba) teisinė informacija apie teisinį schemos statusą arba teisinius reikalavimus, kuriuos schema turi atitikti atsižvelgiant į jurisdikciją, pagal kurią taikoma ši schema, ir (arba) visus apribojimus ir sąlygas, pagal kuriuos

⁽¹⁾ ISO 3166-1:2006: „Šalių ir jų regionų pavadinimų kodai. 1 dalis. Šalių kodai“

patikimas sąrašas yra tvarkomas ir skelbiamas, turi būti įvairiakalbių rašmenų eilučių seka (žr. 5.1.4 punktą), pateikiant (privaloma kalba – Jungtinės Karalystės anglų kalba ir pasirinktinai viena arba daugiau nacionalinių kalbų) bet kokios tokios informacijos apie politiką ar teisinės informacijos faktinį tekstą, sudarytą iš:

- 1) visų valstybių narių patikimiems sąrašams bendros pirmosios privalomosios dalies, kurioje nurodomas taikomas teisinis pagrindas ir kurios tekstas anglų kalba yra toks:

The applicable legal framework for the present trusted list is Regulation (ES) 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.

Tekstas valstybės narės nacionaline (-ėmis) kalba (-omis):

Taikomas esamo patikimo sąrašo teisinis pagrindas yra 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.

- 2) antrosios neprivalomos specifinės kiekvienam patikimam sąrašui dalies, kurioje pateikiamos nuorodos į konkretų taikomą nacionalinį teisinį pagrindą.

Dabartinis paslaugos statusas (5.5.4 punktas)

Šis laukas turi būti įtrauktas ir turi atitikti TS 119 612 5.5.4 punkte nustatytas specifikacijas.

Į ES valstybės narės patikimą sąrašą prieš įsigaliojant Reglamentui (ES) Nr. 910/2014 (t. y. 2016 m. birželio 30 d.) įtrauktų paslaugų „dabartinio paslaugos statuso“ vertė perkeliama reglamento taikymo pradžios dieną (t. y. 2016 m. liepos 1 d.), kaip nurodyta ETSI TS 119 612 J priede.

III SKYRIUS

PATIKIMŲ SĄRAŠŲ TĘSTINUMAS

Sertifikatai, apie kuriuos Komisijai turi būti pranešta pagal šio sprendimo 4 straipsnio 2 dalį, turi atitikti ETSI TS 119 612 5.7.1 punkto reikalavimus ir turi būti išduodami taip, kad:

- jų galiojimo pabaigos data („ne vėliau kaip“) skirtųsi bent trim mėnesiais,
- jie būtų sukurti naudojant naujas raktų poras. Anksčiau naudotos raktų poros neturi būti pakartotinai sertifikuotos.

Jeigu pasibaigia vieno iš viešųjų raktų sertifikatų, kuris galėtų būti naudojamas patikimo sąrašo parašui ar spaudui tvirtinti, apie kurį buvo pranešta Komisijai ir kuris yra paskelbtas pagrindiniame Komisijos nuorodų sąrašė, galiojimas, valstybės narės turi:

- jeigu šiuo metu paskelbtas patikimas sąrašas buvo pasirašytas arba užantspauduotas privačiuoju raktu, kurio viešojo rakto sertifikato galiojimas pasibaigęs, nedelsdamos pakartotinai sudaryti naują patikimą sąrašą, pasirašytą arba užantspauduotą privačiuoju raktu, kurio viešojo rakto sertifikatas, apie kurį pranešta, nepasibaigęs,
- prireikus parengti naujas raktų poras, kurios galėtų būti naudojamos patikimam sąrašui pasirašyti ar užantspauduoti, ir imtis parengti jų atitinkamus viešųjų raktų sertifikatus,
- skubiai perduoti Komisijai naują viešųjų raktų sertifikatų, atitinkančių privačiuosius raktus, kurie galėtų būti naudojami patikimam sąrašui pasirašyti ar užantspauduoti, sąrašą.

Jeigu vienas iš privačiųjų raktų, atitinkančių viešojo rakto sertifikatą, kuris galėtų būti naudojamas patikimo sąrašo parašui ar spaudui tvirtinti, apie kurį buvo pranešta Komisijai ir kuris yra paskelbtas pagrindiniame Komisijos nuorodų sąrašė, yra pažeidžiamas arba nutraukiamas jo naudojimas, valstybės narės turi:

- nedelsdamos pakartotinai sudaryti naują patikimą sąrašą, pasirašytą arba užantspauduotą nepažeistu privačiuoju raktu, jeigu paskelbtas patikimas sąrašas buvo pasirašytas arba užantspauduotas privačiuoju raktu, kuris buvo pažeistas ar kurio naudojimas buvo nutrauktas,

- prireikus parengti naujas raktų poras, kurios galėtų būti naudojamos patikimam sąrašui pasirašyti ar patvirtinti spaudu, ir imtis parengti jų atitinkamus viešųjų raktų sertifikatus,
- skubiai perduoti Komisijai naują viešųjų raktų sertifikatų, atitinkančių privačiuosius raktus, kurie galėtų būti naudojami patikimam sąrašui pasirašyti ar užantspauduoti, sąrašą.

Jeigu visi privatieji raktai, atitinkantys viešųjų raktų sertifikatus, kurie galėtų būti naudojami patikimo sąrašo parašui tvirtinti, apie kuriuos buvo pranešta Komisijai ir kurie yra paskelbti pagrindiniame Komisijos nuorodų sąrašė, yra pažeidžiami arba nutraukiamas jų naudojimas, valstybės narės turi:

- parengti naujas raktų poras, kurios galėtų būti naudojamos patikimam sąrašui pasirašyti ar patvirtinti spaudu, ir imtis parengti jų atitinkamus viešųjų raktų sertifikatus,
- nedelsdamos pakartotinai sudaryti naują patikimą sąrašą, pasirašytą arba užantspauduotą vienu iš tų naujų privačiųjų raktų, apie kurių atitinkamą viešojo rakto sertifikatą turi būti pranešta,
- skubiai perduoti Komisijai naują viešųjų raktų sertifikatų, atitinkančių privačiuosius raktus, kurie galėtų būti naudojami patikimam sąrašui pasirašyti ar užantspauduoti, sąrašą.

IV SKYRIUS

ŽMONĖMS SUPRANTAMOS PATIKIMO SĄRAŠO FORMOS SPECIFIKACIJOS

Jeigu sudaromas ir skelbiamas žmonėms suprantamos formos patikimas sąrašas, jis teikiamas kaip portatyvaus formato (PDF) dokumentas, parengtas pagal ISO 32000 ⁽¹⁾, ir jo formatas atitinka PDF/A aprašą (ISO 19005 ⁽²⁾).

PDF/A aprašu pagrįsto žmonėms suprantamos formos patikimo sąrašo turinys turi atitikti šiuos reikalavimus:

- žmonėms suprantamos formos struktūra turi atitikti loginį modelį, aprašytą TS 119612,
- kiekvienas esamas laukas turi būti rodomas ir jame turi būti nurodyta:
 - lauko pavadinimas (pvz., „Paslaugos rūšies identifikatorius“),
 - lauko reikšmė (pvz., „<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>“),
 - kai taikoma, lauko vertės reikšmė (aprašymas) (pvz., „sertifikatų sudarymo tarnyba, rengianti ir pasirašanti kvalifikuotus sertifikatus remdamasi tapatybe ir kitais požymiais, patikrintais atitinkamų registracijos tarnybų“),
 - jeigu reikia, įvairios žmonių kalbų versijos, numatytos patikimame sąrašė,
- žmonėms suprantama forma turi būti pateikti bent toliau nurodyti laukai ir atitinkamos skaitmeninių sertifikatų ⁽³⁾, jeigu jos nurodytos lauke „Paslaugos skaitmeninis identifikatorius“, reikšmės:
 - versija,
 - sertifikato serijos numeris,
 - parašo algoritmas,
 - išdavėjas – visi atitinkami išskirtiniai pavadinimo laukai,
 - galiojimo laikotarpis,
 - subjektas – visi atitinkami išskirtiniai pavadinimo laukai,

⁽¹⁾ ISO 32000-1:2008: „Dokumentų tvarkyba. Portatyvus dokumento formatas. 1 dalis. PDF 1.7“.

⁽²⁾ ISO 19005-2:2011: „Dokumentų tvarkyba. Ilgalaikio saugojimo elektroninio dokumento rinkmenos formatas. 2 dalis. ISO 32000-1 (PDF/A-2) naudojimas“.

⁽³⁾ Rekomendacija ITU-T X.509 | ISO/IEC 9594-8: Informacinė technologija. Atvirųjų sistemų jungtis. Rodyklė: Viešojo rakto ir požymių sertifikato sistemos (žr. <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>).

- viešasis raktas,
- institucijos rakto identifikatorius,
- subjekto rakto identifikatorius,
- rakto naudojimas,
- pratęstas rakto naudojimas,
- sertifikavimo politika – visi politikos identifikatoriai ir kvalifikatoriai,
- politikos nustatymas,
- subjekto alternatyvus pavadinimas,
- subjekto rodyklės požymiai,
- pagrindiniai apribojimai,
- politikos apribojimai,
- CRL paskirstymo taškai ⁽¹⁾,
- institucijos informacijos prieiga,
- subjekto informacijos prieiga,
- kvalifikuoto sertifikato patvirtinimai ⁽²⁾,
- maišos algoritmas,
- sertifikato maišos vertė,
- žmonėms suprantama forma turi būti lengvai išspausdinama,
- žmonėms suprantama forma turi būti pasirašyta arba patvirtinta spaudu schemas operatoriaus, remiantis PDF pažangiojo parašo reikalavimais, nurodytais Komisijos įgyvendinimo sprendimo (ES) 2015/1505 1 ir 3 straipsniuose.

⁽¹⁾ RFC 5280: interneto X.509 PKI sertifikatas ir CRL profilis.

⁽²⁾ RFC 3739: interneto X.509 PKI: kvalifikuoto sertifikato profilis.

II PRIEDAS

VALSTYBIŲ NARIŲ PRANEŠIMŲ FORMA

Informacija, kurią valstybės narės turi pranešti pagal šio sprendimo 4 straipsnio 1 dalį, apima šiuos duomenis ir visus jų pakeitimus:

- 1) Valstybė narė, naudojant ISO 3166-1 ⁽¹⁾ dviejų raidžių kodą, išskyrus šias išimtis:
 - a) Jungtinės Karalystės šalies kodas yra „UK“.
 - b) Graikijos šalies kodas yra „EL“.
- 2) Įstaiga (-os), atsakinga (-os) už patikimų sąrašų formos, kurią galima tvarkyti automatizuotomis priemonėmis, ir žmonėms suprantamos formos sudarymą, tvarkymą ir skelbimą:
 - a) Schemos operatoriaus pavadinimas: pateikta informacija turi būti identiška (skirti didžiąsias ir mažąsias raides) patikimame sąraše pateiktam schemos operatoriaus pavadinimui visomis kalbomis, naudojamomis patikimame sąraše.
 - b) Neprivaloma informacija, skirta Komisijos vidaus naudojimui tik tuo atveju, jei reikėtų susisiekti su atitinkama įstaiga (ši informacija nebus skelbiama EK sudarytame patikimų sąrašų suvestiniame sąraše):
 - schemos operatoriaus adresas,
 - atsakingo (-ų) asmens (-ų) kontaktiniai duomenys (vardas, pavardė, telefonas, e. pašto adresas).
- 3) Vieta, kur paskelbta forma, tinkama patikimam sąrašui tvarkyti automatizuotomis priemonėmis (*esamo patikimo sąrašo skelbimo vieta*).
- 4) Vieta, kur patikimas sąrašas atitinkamais atvejais paskelbtas žmonėms suprantama forma (*esamo patikimo sąrašo skelbimo vieta*). Jei patikimas sąrašas žmonėms suprantama forma nebeskelbiamas, tai turi būti nurodyta.
- 5) Viešųjų raktų sertifikatai, atitinkantys privačius raktus, kurie gali būti naudojami siekiant elektroniniu būdu pasirašyti arba užantspauduoti formą, tinkamą patikimam sąrašui automatizuotomis priemonėmis tvarkyti, ir patikimų sąrašų žmonėms suprantamą formą: šie sertifikatai turi būti pateikti kaip slaptojo pašto protokolo Base64 pagrindu šifruoti DER sertifikatai. Pranešant apie pasikeitusius duomenis papildoma informacija pridedama atvejais, kai naujas sertifikatas pakeičia konkretų Komisijos sąraše esantį sertifikatą, ir atvejais, kai pranešamas sertifikatas pridedamas prie esamo (-ų) sertifikato (-ų) jo (jų) nepakeisdamas.
- 6) Pagal 1–5 punktus praneštų duomenų pateikimo data.

Pagal 1, 2 (a papunktį), 3, 4 ir 5 punktus pranešti duomenys turi būti įtraukti į Europos Komisijos sudarytą patikimų sąrašų suvestinį sąrašą, pakeičiant anksčiau praneštą informaciją, įtrauktą į suvestinį sąrašą.

⁽¹⁾ ISO 3166-1: „Šalių ir jų regionų pavadinimų kodai. 1 dalis. Šalių kodai“.