Šis dokumentas yra skirtas tik informacijai, ir institucijos nėra teisiškai atsakingos už jo turinį

►**B** ►**C1** **KOMISIJOS SPRENDIMAS**

2009 m. spalio 16 d.

kuriuo 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

(pranešta dokumentu Nr. C(2009) 7806)

(Tekstas svarbus EEE)

(2009/767/EB) ◄

(OL L 274, 2009 10 20, p. 36)

iš dalies keičiamas:

		Oficialusis leidinys		
		Nr.	puslapis	data
►**M1**	Komisijos sprendimas 2010/425/ES, 2010 m. liepos 28 d.	L 199	30	2010 7 31

pataisytas:

►**C1** Klaidų ištaisymas, OL L 299, 2009 11 14, p. 18 (2009/767/EB)
►**C2** Klaidų ištaisymas, OL L 4, 2011 1 7, p. 6 (2009/767/EB)

▼B
▼C1

KOMISIJOS SPRENDIMAS

2009 m. spalio 16 d.

kuriuo 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

(pranešta dokumentu Nr. C(2009) 7806)

(Tekstas svarbus EEE)

(2009/767/EB)

EUROPOS BENDRIJŲ KOMISIJA,

atsižvelgdama į Europos bendrijos steigimo sutartį,

atsižvelgdama į 2006 m. gruodžio 12 d. Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje [1], ypač jos 8 straipsnio 3 dalį,

kadangi:

(1) Direktyvos 2006/123/EB II skyriuje, pirmiausia jo 5 ir 8 straipsniuose, valstybėms narėms nustatyti administracinio supaprastinimo įpareigojimai, įskaitant įpareigojimą supaprastinti procedūras ir formalumus, taikomus norint įgyti teisę verstis paslaugų teikimo veikla ir vykdant šią veiklą, ir įpareigojimą užtikrinti, kad tas procedūras ir formalumus paslaugų teikėjai galėtų lengvai atlikti nuotoliniu būdu ir elektroninėmis priemonėmis, naudodamiesi kontaktinių centrų paslaugomis.

(2) Naudojantis kontaktinių centrų paslaugomis, šias procedūras ir formalumus turi būti įmanoma atlikti už valstybių narių teritorijų ribų, kaip nustatyta Direktyvos 2006/123/EB 8 straipsnyje.

(3) Kad būtų galima įvykdyti įpareigojimą supaprastinti procedūras ir formalumus ir sudaryti palankesnes sąlygas už valstybių narių teritorijų ribų naudotis kontaktinių centrų paslaugomis, elektroninėmis priemonėmis atliekamos procedūros turi būti pagrįstos paprastais sprendimais, įskaitant su elektroninių parašų naudojimu susijusius spendimus. Jei, tinkamai įvertinus su konkrečiomis procedūromis ir formalumais susijusią riziką, manoma, kad būtina užtikrinti aukšto lygio apsaugą arba rašytinio parašo atitiktį, gali būti reikalaujama, kad paslaugų teikėjai, atlikdami tam tikras procedūras arba formalumus, naudotų saugesnius elektroninius parašus, pagrįstus kvalifikuotu sertifikatu ir kuriamus naudojant saugią parašo formavimo įrangą arba jos nenaudojant.

[1] OL L 376, 2006 12 27, p. 36.

▼C1

(4) Bendrijos elektroninių parašų pagrindai nustatyti 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvoje 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos ([1]). Siekiant padėti veiksmingai tarpvalstybiniu mastu naudoti saugius elektroninius parašus, pagrįstus kvalifikuotu sertifikatu, turėtų būti sustiprintas pasitikėjimas šiais elektroniniais parašais, kad ir kokioje valstybėje narėje būtų įsisteigęs pasirašantis asmuo arba kvalifikuotą sertifikatą išduodantis sertifikavimo paslaugų teikėjas. Tą galima pasiekti suteikiant galimybę lengviau gauti patikimos informacijos, reikalingos elektroniniam parašui patikrinti, pirmiausia informacijos apie sertifikavimo paslaugų teikėjus, kuriuos prižiūri ir (arba) yra akreditavusi valstybė narė, ir apie jų teikiamas paslaugas.

(5) Būtina užtikrinti, kad valstybės narės, naudodamos bendrąją formą, šią informaciją skelbtų viešai ir taip palengvintų naudojimąsi šia informacija bei užtikrintų tinkamą išsamumo lygį, kad gavėjas galėtų įsitikinti elektroninio parašo tikrumu,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Elektroninių parašų naudojimas ir pripažinimas

1. Jeigu tai pagrįsta remiantis tinkamu susijusios rizikos vertinimu ir laikantis Direktyvos 2006/123/EB 5 straipsnio 1 ir 3 dalių, valstybės narės, norėdamos pagal Direktyvos 2006/123/EB 8 straipsnį atlikti tam tikras procedūras ir formalumus naudodamosi kontaktinių centrų paslaugomis, gali reikalauti, kad paslaugų teikėjas naudotų saugius elektroninius parašus, pagrįstus kvalifikuotu sertifikatu ir sukurtus naudojant saugią parašo formavimo įrangą arba jos nenaudojant, kaip nustatyta ir reglamentuojama Direktyvoje 1999/93/EB.

2. Valstybės narės pripažįsta visus saugius elektroninius parašus, pagrįstus kvalifikuotu sertifikatu ir sukurtus naudojant saugią parašo formavimo įrangą arba jos nenaudojant, naudojamus atliekant pirmoje dalyje nurodytas procedūras ir formalumus, išsaugodamos galimybę pripažinti tik saugius elektroninius parašus, pagrįstus kvalifikuotu sertifikatu ir sukurtus naudojant saugią parašo formavimo įrangą, jei tai pagrįsta pirmoje dalyje nurodytu rizikos vertinimu.

3. Valstybės narės nepripažįsta saugių elektroninių parašų, pagrįstų kvalifikuotu sertifikatu ir sukurtų naudojant saugią parašo formavimo įrangą arba jos nenaudojant, laikydamosi reikalavimų, kuriais paslaugų teikėjams neleidžiama atlikti procedūrų elektroninėmis priemonėmis, naudojantis kontaktinių centrų paslaugomis.

([1]) OL L 13, 2000 1 19, p. 12.

▼C1

4. 2 dalimi valstybėms narėms nedraudžiama pripažinti elektroninių parašų, jei tai nėra saugūs elektroniniai parašai, pagrįsti kvalifikuotu sertifikatu ir sukurti naudojant saugią parašo formavimo įrangą arba jos nenaudojant.

2 straipsnis

Patikimų sąrašų sudarymas, tvarkymas ir skelbimas

1. Kiekviena valstybė narė pagal priede pateiktas technines specifikacijas sudaro, tvarko ir skelbia patikimą sąrašą, kuriame pateikiama būtina informacija apie tos valstybės narės prižiūrimus ir (arba) akredituotus sertifikavimo paslaugų teikėjus, visuomenei išduodančius kvalifikuotus sertifikatus.

▼M1

2. Valstybės narės pagal priede nustatytas technines specifikacijas sudaro ir paskelbia ir žmonėms suprantamos, ir techninėmis priemonėmis apdorojamos formos patikimą sąrašą.

2a. Kad būtų užtikrintas patikimo sąrašo autentiškumas ir vientisumas, valstybės narės elektroniniu būdu pasirašo techninėmis priemonėmis apdorojamą savo patikimo sąrašo versiją ir saugiu kanalu paskelbia bent žmonėms suprantamos formos patikimą sąrašą.

3. Valstybės narės Komisijai pateikia tokią informaciją:

a) įstaiga ar įstaigos, atsakinga (-os) už žmonėms suprantamos ir techninėmis priemonėmis apdorojamos formos patikimo sąrašo sudarymą, tvarkymą ir skelbimą;

b) žmonėms suprantamos ir techninėmis priemonėmis apdorojamos formos patikimo sąrašo skelbimo vietos;

c) viešojo rakto sertifikatas, naudojamas kanalo, kuriuo skelbiamas žmonėms suprantamos formos patikimas sąrašas, saugumui užtikrinti, arba, jei žmonėms suprantamas sąrašas pasirašytas elektroniniu būdu, jam pasirašyti naudojamas viešojo rakto sertifikatas;

d) viešojo rakto sertifikatas, naudojamas techninėmis priemonėmis apdorojamos formos patikimam sąrašui pasirašyti elektroniniu būdu;

e) visi a–d punktuose nurodytos informacijos pakeitimai.

4. Komisija saugiu prieigos prie patvirtinto žiniatinklio serverio kanalu visoms valstybėms narėms pateikia 3 dalyje nurodytą valstybių narių perduotą informaciją ir žmonėms suprantama, ir pasirašyta techninėmis priemonėmis apdorojama forma.

▼C1

3 straipsnis

Taikymas

Šis sprendimas taikomas nuo 2009 m. gruodžio 28 d.

4 straipsnis

Adresatai

Šis sprendimas skirtas valstybėms narėms.

▼C1

PRIEDAS

PATIKIMO PRIŽIŪRIMŲ IR (ARBA) AKREDITUOTŲ SERTIFIKAVIMO PASLAUGŲ TEIKĖJŲ SĄRAŠO BENDROSIOS FORMOS TECHNINĖS SPECIFIKACIJOS

ĮVADAS

1. **Bendrosios nuostatos**

Valstybių narių patikimo prižiūrimų ir (arba) akredituotų sertifikavimo paslaugų teikėjų sąrašo bendrosios formos paskirtis – nustatyti bendrą būdą, kuriuo kiekviena valstybė narė teiktų informaciją apie sertifikavimo paslaugų teikėjų ([1]) (SPT), jos prižiūrimų ir (arba) akredituotų siekiant užtikrinti atitinkamų Direktyvos 1999/93/EB nuostatų laikymąsi, teikiamų sertifikavimo paslaugų priežiūros ir (arba) akreditacijos statusą. Be kitos informacijos taip pat teikiama istorinė informacija apie prižiūrimų ir (arba) akredituotų sertifikavimo paslaugų priežiūros ir (arba) akreditacijos statusą.

Į privalomą patikimo sąrašo (PS) informaciją turi būti įtraukta būtiniausia informacija apie prižiūrimus ir (arba) akredituotus SPT, išduodančius kvalifikuotus sertifikatus (KS) ([2]) pagal Direktyvos 1999/93/EB nuostatas (3 straipsnio 3 dalį, 3 straipsnio 2 dalį ir 7 straipsnio 1 dalies a punktą), įskaitant informaciją apie KS, kuriuo patvirtinamas elektroninis parašas, ir apie tai, ar parašas kuriamas naudojant saugią parašo formavimo įrangą (SPFĮ) ([3]).

Be to, nacionaliniu lygmeniu sudaromame patikimame sąraše savanoriškai gali būti teikiama papildoma informacija apie kitus prižiūrimus ir (arba) akredituotus SPT, neišduodančius KS, tačiau teikiančius paslaugas, susijusias su elektroniniais parašais (pvz., apie SPT, teikiančius laiko fiksavimo paslaugas ir išduodančius laiko fiksavimo žymas; apie SPT, išduodančius nekvalifikuotus sertifikatus, ir t. t.).

Ši informacija pirmiausia skirta padėti įsitikinti kvalifikuotų elektroninių parašų (KEP) ir saugių elektroninių parašų (SEP) ([4]), patvirtinamų kvalifikuotu sertifikatu, tikrumu ([5]), ([6]).

Siūloma bendroji forma atitinka įgyvendinimo nuostatas, pagrįstas ETSI TS 102 231 nustatytomis specifikacijomis ([7]), taikomomis sudarant ir skelbiant tokius sąrašus, nurodant jų vietą, suteikiant galimybę jais naudotis, nustatant jų tikrumą ir patikimumą.

([1]) Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 11 punkte.
([2]) Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 10 punkte.
([3]) Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 6 punkte.
([4]) Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 2 punkte.
([5]) Šiame dokumente SEP, patvirtinamas KS, sutrumpintai žymimas SEP_{KS}.
([6]) Būtina atkreipti dėmesį į tai, kad įvairiomis elektroninėmis paslaugomis, pagrįstomis paprastu SEP, tarpvalstybiniu mastu taip pat būtų lengviau naudotis, jei papildomos sertifikavimo paslaugos (pvz., nekvalifikuotų sertifikatų išdavimas) būtų įtrauktos į prižiūrimas ir (arba) akredituotas paslaugas, apie kurias valstybės narės patikimame sąraše savanoriškai teikia informaciją.
([7]) ETSI TS 102 231 – „Elektroniniai parašai ir infrastruktūros (EPI). Suderintos patikimumo užtikrinimo paslaugų statuso informacijos teikimas“ (angl. *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information*).

▼C1

2. **PS įrašų redagavimo gairės**

2.1. *PS, skirtas prižiūrimoms ir (arba) akredituotoms sertifikavimo paslaugoms*

Bendras atitinkamų sertifikavimo paslaugų ir sertifikavimo paslaugų teikėjų sąrašas

Valstybės narės patikimas sąrašas apibrėžiamas kaip Sertifikavimo paslaugų teikėjų, kuriuos, siekdama užtikrinti atitinkamų Direktyvos 1999/93/EB nuostatų laikymąsi, prižiūri ir (arba) yra akreditavusi nurodyta valstybė narė, teikiamų sertifikavimo paslaugų priežiūros ir (arba) akreditacijos statuso sąrašas.

Į tokį patikimą sąrašą turi būti įtraukti:

— **visi sertifikavimo paslaugų teikėjai**, iš kurių kiekvienas, kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 11 punkte, yra „subjektas arba juridinis ar fizinis asmuo, kuris išduoda sertifikatus arba teikia kitas paslaugas, susijusias su elektroniniais parašais“,

— **prižiūrimi ir (arba) akredituoti** siekiant užtikrinti atitinkamų Direktyvos 1999/93/EB nuostatų laikymąsi.

Svarstant Direktyvoje 1999/93/EB nustatytas apibrėžtis ir nuostatas, pirmiausia susijusias su atitinkamais SPT ir jų priežiūros ir (arba) savanoriškos akreditacijos sistemomis, galima išskirti dvi SPT grupes: SPT, kurie visuomenei išduoda KS (SPT_{KS}), ir SPT, kurie KS visuomenei neišduoda, tačiau teikia „kitas (papildomas) paslaugas, susijusias su elektroniniais parašais“.

— **KS išduodantys SPT:**

— Juos turi prižiūrėti valstybė narė, kurioje jie yra įsisteigę (jei jie įsisteigę valstybėje narėje); be to, jie gali būti akredituoti siekiant užtikrinti Direktyvos 1999/93/EB nuostatų, įskaitant I priede nustatytus reikalavimus (KS reikalavimus) ir II priede nustatytus reikalavimus (reikalavimus KS išduodantiems SPT), laikymąsi. Be to, SPT, išduodantiems KS ir akredituotiems valstybėje narėje, turi būti taikoma atitinkama tos valstybės narės priežiūros sistema, nebent jie nėra įsisteigę toje valstybėje narėje.

— Turi būti nustatyta taikytina priežiūros sistema (arba atitinkama savanoriškos akreditacijos sistema), atitinkanti Direktyvoje 1999/93/EB, pirmiausia 3 straipsnio 3 dalyje, 8 straipsnio 1 dalyje, 11 straipsnyje ir 13 konstatuojamoje dalyje (arba atitinkamai 2 straipsnio 13 dalyje, 3 straipsnio 2 dalyje, 7 straipsnio 1 dalies a punkte, 8 straipsnio 1 dalyje, 11 straipsnyje, 4 ir 11–13 konstatuojamose dalyse), nustatytus atitinkamus reikalavimus.

— **KS neišduodantys SPT:**

— Jiems gali būti taikoma savanoriškos akreditacijos sistema (apibrėžta Direktyvoje 1999/93/EB ir atitinkanti jos nuostatas) ir (arba) nacionaliniu lygmeniu apibrėžta pripažinta patvirtinimo schema, įgyvendinama nacionaliniu lygmeniu siekiant užtikrinti, kad būtų prižiūrima, kaip laikomasi šios direktyvos nuostatų ir galbūt nacionalinių nuostatų, susijusių su sertifikavimo paslaugų teikimu (atsižvelgiant į šios direktyvos 2 straipsnio 11 punktą).

— Kai kuriems fiziniams arba dvejetainiams (loginiams) objektams, sukurtiems arba parengtiems teikiant sertifikavimo paslaugą, gali būti suteikta tam tikra kvalifikacija remiantis jų atitiktimi nacionalinėms nuostatoms ir reikalavimams, tačiau ji veikiausiai turės reikšmės tik nacionaliniu lygmeniu.

▼C1

Valstybės narės patikimame sąraše turi būti pateikta būtiniausia informacija apie prižiūrimus ir (arba) akredituotus SPT, visuomenei išduodančius kvalifikuotus sertifikatus (KS) pagal Direktyvos 1999/93/EB nuostatas (3 straipsnio 3 dalį, 3 straipsnio 2 dalį ir 7 straipsnio 1 dalies a punktą), informacija apie KS, kuriuo patvirtinamas elektroninis parašas, ir apie tai, ar parašas kuriamas naudojant saugią parašo formavimo įrangą.

Nacionaliniu lygmeniu sudaromame patikimame sąraše savanoriškai gali būti teikiama papildoma informacija apie kitas prižiūrimas ir (arba) akredituotas paslaugas, kurias teikia SPT, visuomenei neišduodantys KS (pvz., SPT, teikiantys laiko fiksavimo paslaugas ir išduodantys laiko fiksavimo žymas; SPT, išduodantys nekvalifikuotus sertifikatus, ir t. t.).

Patikimo sąrašo paskirtis:

— registruoti ir teikti patikimą informaciją apie sertifikavimo paslaugų teikėjų, kuriuos, siekdama užtikrinti atitinkamų Direktyvos 1999/93/EB nuostatų laikymąsi, prižiūri ir (arba) yra akreditavusi valstybė narė, atsakinga už sąrašo sudarymą ir tvarkymą, teikiamų sertifikavimo paslaugų priežiūros ir (arba) akreditacijos statusą,

— padėti įsitikinti elektroninių parašų, patvirtinamų teikiant prižiūrimas ir (arba) akredituotas į sąrašą įtrauktų SPT sertifikavimo paslaugas, tikrumu.

Bendras priežiūros ir (arba) akreditacijos statuso reikšmių rinkinys

Kiekvienoje valstybėje narėje turi būti sudaromas ir tvarkomas vienas bendras PS, kuriame nurodomas valstybės narės prižiūrimų ir (arba) akredituotų SPT teikiamų sertifikavimo paslaugų priežiūros ir (arba) akreditacijos statusas.

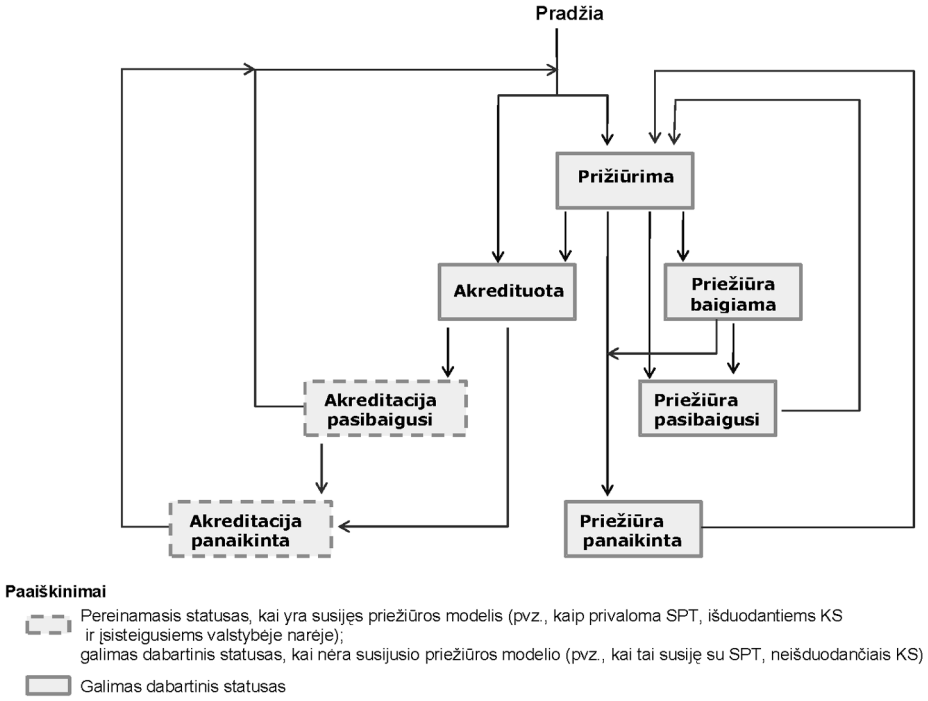
Tai, kad paslauga yra prižiūrima arba akredituota, yra vienas iš dabartinio statuso aspektų. Be to, priežiūra arba akreditacija gali būti galiojanti, baigiama, pasibaigusi ar netgi panaikinta. Kol yra teikiama, ta pati sertifikavimo paslauga iš prižiūrimos gali tapti akredituota ir atvirkščiai ([1]).

Toliau pateiktame 1 paveiksle parodyta galima tos pačios sertifikavimo paslaugos priežiūros ir (arba) akreditacijos statuso kaita:

([1]) Pvz., valstybėje narėje įsisteigęs sertifikavimo paslaugų teikėjas, teikiantis sertifikavimo paslaugą, kuri iš pradžių buvo prižiūrima tos valstybės narės (priežiūros įstaigos), po tam tikro laiko gali nuspręsti gauti savanorišką prižiūrimos sertifikavimo paslaugos akreditaciją. Ir atvirkščiai – kitoje valstybėje narėje veikiantis sertifikavimo paslaugų teikėjas gali nuspręsti nenutraukti akredituotos sertifikavimo paslaugos teikimo, tačiau, pvz., verslo ir (arba) ekonominiais sumetimais gali pakeisti paslaugos statusą, akredituotą paslaugą pakeisdamas prižiūrima.

▼C1

Galima SPT paslaugos priežiūros ir (arba) akreditacijos statuso kaita



1 pav.

Sertifikavimo paslauga, kurią teikiant išduodamas KS, turi būti prižiūrima (jei jos teikėjas įsisteigęs valstybėje narėje) ir gali būti savanoriškai akredituota. Tokios į patikimą sąrašą įtrauktos paslaugos statuso reikšmė – dabartinė statuso reikšmė – gali būti bet kuri iš pirmiau nurodytų statuso reikšmių. Tačiau reikia paminėti, kad statuso reikšmės „Akreditacija pasibaigusi“ ir „Akreditacija panaikinta“ kaip pereinamojo statuso reikšmės turi būti naudojamos tik tuo atveju, jei tai SPT_{KS} paslaugos, kurių teikėjas įsisteigęs valstybėje narėje, nes paprastai reikalaujama, kad tokios paslaugos būtų prižiūrimos (net jeigu jos nėra akredituotos arba jeigu jų akreditacija yra pasibaigusi).

Reikalaujama, kad valstybės narės, nustačiusios arba nustatančios nacionaliniu mastu pripažintą (-as) patvirtinimo schemą (-as), įgyvendinamą (-as) nacionaliniu lygmeniu ir skirtą (-as) prižiūrėti, kad KS neišduodančių SPT teikiamos paslaugos atitiktų Direktyvos 1999/93/EB nuostatas ir galimas nacionalines nuostatas, susijusias su sertifikavimo paslaugų teikimu (atsižvelgiant į šios direktyvos 2 straipsnio 11 punktą), priskirtų šią (šias) patvirtinimo schemą (-as) kuriai nors iš šių dviejų kategorijų:

— savanoriška akreditacija, apibrėžta ir reglamentuojama Direktyvoje 1999/93/EB (2 straipsnio 13 punktas, 3 straipsnio 2 dalis, 7 straipsnio 1 dalies a punktas, 8 straipsnio 1 dalis, 11 straipsnis, 4 ir 11–13 konstatuojamosios dalys),

— priežiūra, nustatyta Direktyvoje 1999/93/EB ir įgyvendinama pagal nacionalines nuostatas ir reikalavimus, laikantis nacionalinių teisės aktų.

▼C1

Taigi sertifikavimo paslauga, kurią teikiant neišduodami KS, gali būti prižiūrima arba savanoriškai akredituota. Tokios į patikimą sąrašą įtrauktos paslaugos statuso reikšmė – dabartinė statuso reikšmė – gali būti bet kuri iš pirmiau nurodytų statuso reikšmių (žr. 1 paveikslą).

Patikimame sąraše turi būti pateikta informacija apie pamatinę (-es) priežiūros ir (arba) akreditacijos schemą (-as), pirmiausia:

— informacija apie priežiūros sistemą, taikomą kiekvienam SPT_{KS},

— jei reikia, informacija apie nacionalinę savanoriškos akreditacijos schemą, taikomą kiekvienam SPT_{KS},

— jei reikia, informacija apie priežiūros sistemą, taikoma kiekvienam KS neišduodančiam SPT,

— jei reikia, informacija apie nacionalinę savanoriškos akreditacijos schemą, taikomą kiekvienam KS neišduodančiam SPT.

Paskutinieji du informacijos rinkiniai yra ypač svarbūs, kad susijusios šalys galėtų įvertinti tokių priežiūros ir (arba) akreditacijos sistemų, nacionaliniu lygmeniu taikomų KS neišduodantiems SPT, kokybę ir saugumą. Kai patikimame sąraše teikiama informacija apie KS neišduodančių SPT teikiamų paslaugų priežiūros ir (arba) akreditacijos statusą, minėtieji informacijos rinkiniai PS lygmeniu teikiami naudojant „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 valstybės narės teikiama neprivaloma specifinė informacija) ir „PUPSS politika ir (arba) teisinė informacija“ (5.3.11 punktas – visoms valstybėms narėms bendras tekstas, susietas su Direktyva 1999/93/EB; be to, kiekviena valstybė narė gali pateikti papildomą jai svarbų tekstą ir (arba) nuorodų). Papildoma su kvalifikacija susijusi informacija, nustatyta pagal nacionalines priežiūros ir (arba) akreditacijos sistemas, taikomas KS neišduodantiems SPT, apie kiekvieną paslaugą gali būti teikiama, kai reikia ir reikalaujama (pvz., norint išskirti keletą kokybės ir (arba) saugumo lygmenų), naudojant plėtinį „Papildoma informacija apie paslaugą“ (angl. *additionalServiceInformation*) (5.8.2 punktas), kuris yra „Informacijos apie paslaugą plėtinys“ (angl. *Service information extension*) dalis (5.5.9 punktas). Daugiau informacijos apie atitinkamas technines specifikacijas pateikta I skyriuje pateiktose išsamiose specifikacijose.

Nors valstybėje narėje už sertifikavimo paslaugų priežiūrą ir akreditaciją gali būti atsakingos kelios tos valstybės narės institucijos, reikalaujama, kad vienai sertifikavimo paslaugai būtų naudojamas tik vienas įrašas (identifikuojamas pagal „Paslaugos skaitmeninį identifikatorių“ (angl. *Service digital identity*), nustatytą ETSI TS 102 231 ([1]) ir kad tos paslaugos priežiūros ir (arba) akreditacijos statusas būtų atitinkamai atnaujinamas. Pirmiau nurodytos statuso reikšmės yra aprašytos tam skirtame I skyriuje pateiktų išsamių techninių specifikacijų 5.5.4 punkte.

2.2. *PS įrašai, skirti padėti įsitikinti KEP ir SEP_{KS} tikrumu*

Svarbiausias PS kūrimo etapas – privalomos PS dalies, t. y. kiekvieno KS išduodančio SPT teikiamų paslaugų sąrašo, sudarymas siekiant teisingai nurodyti tikslų kiekvienos tokios sertifikavimo paslaugos, kurią teikiant išduodamas KS, teikimo statusą, ir užtikrinti, kad kiekviename įraše pateiktos informacijos pakaktų padėti įsitikinti KEP ir SEP_{KS} tikrumu (kartu remiantis galutinio subjekto KS, kurį, teikdamas šiame įraše nurodytą sertifikavimo paslaugą, išdavė SPT, turiniu).

([1]) ETSI TS 102 231 – „Elektroniniai parašai ir infrastruktūros (EPI). Suderintos patikimumo užtikrinimo paslaugų statuso informacijos teikimas“ (angl. *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information*).

▼C1

Kadangi nėra ištiesuderinto tarptvalstybinio KS aprašo, gali būti, kad į reikiamą informaciją bus įtraukta ne bendros (pagrindinės) SI „Paslaugos skaitmeninio identifikatoriaus“ informacija, o kita informacija, pirmiausia informacija apie išduoto sertifikato KS statusą ir tai, ar patvirtinami parašai kuriami naudojant SPFĮ. Todėl valstybės narės įstaiga, kuriai pavesta sudaryti, redaguoti ir tvarkyti PS (t. y. schemos operatorius, kaip nustatyta ETSI TS 102 231), turi atsižvelgti į kiekvieno kiekvienam į PS įtrauktam SPT_{KS} išduoto KS galiojantį aprašą ir sertifikato turinį.

Būtų geriausia, kad, kai tvirtinama, kad tai yra KS, į kiekvieną išduodamą KS būtų įrašomas ETSI nustatytas KS atitikties (angl. *QcCompliance*) ([1]) patvirtinimas, o kai tvirtinama, kad elektroniniams parašams (angl. *eSignatures*), kurie patvirtinami KS, kurti naudojama SPFĮ, – ETSI nustatytas KS SPFĮ (angl. *QcSSCD*) patvirtinimas, ir (arba) kad į kiekvieną išduodamą KS būtų įrašomas vienas iš KSP/KSP+ (angl. *QCP/QCP+*) sertifikatų politikos objektų identifikatorių (angl. *Object Identifiers*, OID), nustatytų ETSI TS 101 456 ([2]). KS išduodantys SPT rėmėsi skirtingais standartais, šie standartai buvo įvairiai interpretuojami ir trūko žinių apie kai kurių norminių techninių specifikacijų arba standartų buvimą ir taikymo pirmenybę, todėl faktinis šiuo metu išduodamų KS turinys (pvz., tai, ar naudojami ETSI nustatyti KS patvirtinimai) nevienodas ir sertifikatus gaunančios šalys negali pasikliauti tik pasirašančio asmens sertifikatu (ir susijusia grandine ar keliu), norėdamos bent techninėmis priemonėmis įvertinti, ar sertifikatas, kuriuo patvirtinamas elektroninis parašas, yra teikiamas kaip KS, ir ar jis susijęs su SPFĮ, kurią naudojant buvo sukurtas elektroninis parašas.

Į laukus „Paslaugos rūšies identifikatorius“ (angl. *Service type identifier*, „Sti“), „Paslaugos pavadinimas“ (angl. *Service name*, „Sn“) ir „Paslaugos skaitmeninis identifikatorius“ (angl. *Service digital identity*, „Sdi“) ([3]) įrašius informaciją, pateiktą lauke „Informacijos apie paslaugą plėtiniai“ (angl. *Service information extensions*, „Sie“), galima pagal siūlomą bendrąją PS formą išsamiai apibrėžti konkretų kvalifikuoto sertifikato, kurį išdavė į sąrašą įtrauktas KS išduodantis SPT, tipą ir pateikti informacijos apie tai, ar jis patvirtinamas naudojant SPFĮ (jei tokia informacija išduotame KS nepateikta). Be abejo, su šiuo įrašu susiejama konkreti dabartinio paslaugos statuso (angl. *Service current status*, „Scs“) informacija. Tai parodyta toliau pateiktame 2 paveiksle.

Paslaugos įtraukimas į sąrašą nurodant tik (pagrindinės) SI „Sdi“ reikštų, kad užtikrinama (užtikrina ne tik KS išduodantis SPT, bet ir priežiūros ir (arba) akreditacijos įstaiga, atsakinga už šio SPT priežiūrą ir (arba) akreditaciją), jog visuose galutinio subjekto sertifikatuose, išduotuose prižiūrint šiai (pagrindinei) SI (pagal tam tikrą hierarchiją), pateikiama pakankamai ETSI nustatytos ir techninėmis priemonėmis apdorojamos informacijos, kad būtų galima įvertinti, ar tai KS ir ar jis patvirtinamas naudojant SPFĮ. Pvz., jeigu pastarasis teiginys neteisingas (pvz., kvalifikuotame sertifikate nepateikta ETSI standartizuotos, techninėmis priemonėmis apdorojamos informacijos apie tai, ar šis KS patvirtinamas naudojant SPFĮ), sąraše nurodžius tik tos (pagrindinės) SI „Sdi“, galima daryti tik išvadą, kad KS, išduodami pagal šią (pagrindinės) SI hierarchiją, netvirtinami naudojant SPFĮ. Kad būtų galima teigti, jog šie KS patvirtinami naudojant SPFĮ, tai turėtų būti nurodyta naudojant „Sie“ (tai kartu rodo, jog tai užtikrina KS išduodantis SPT, prižiūrimas ir (arba) akredituotas priežiūros arba akreditacijos įstaigos).

([1]) Žr. ETSI TS 101 862 – „Elektroniniai parašai ir infrastruktūros (EPI). Kvalifikuoto sertifikato profilis“ (angl. *Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile*).

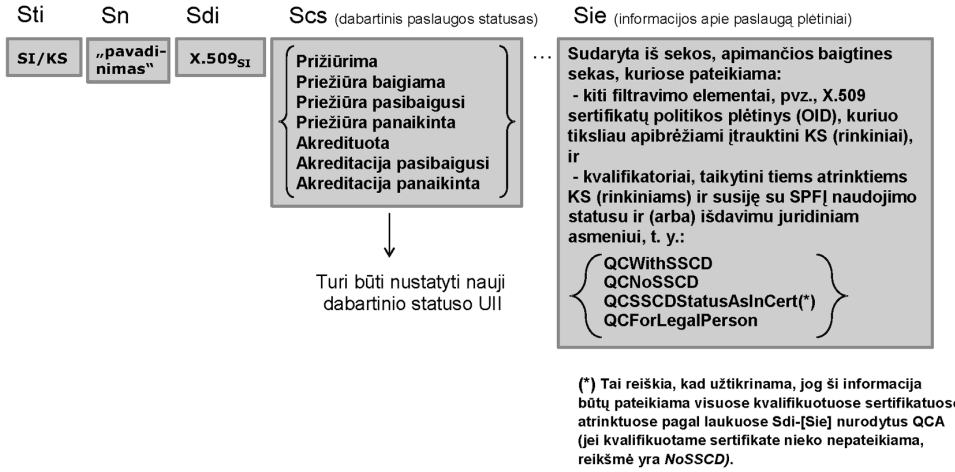
([2]) ETSI TS 101 456 – „Elektroniniai parašai ir infrastruktūros (EPI). Strateginiai reikalavimai, keliami kvalifikuotus sertifikatus išduodantiems sertifikavimo paslaugų teikėjams“ (angl. *Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates*).

([3]) T.y. bent SI, išduodančios KS, arba pagal sertifikavimo kelią aukštesnės SI išduodamą X.509 v3 sertifikatą.

▼C1

Bendrieji principai – Redagavimo taisyklės – SPT_{KS} įrašai (į sąrašą įtrauktos paslaugos)

Į sąrašą įtraukto SPT_{KS} paslaugos įrašas



2 pvz.

Į sąrašą įtraukto KS išduodančio SPT teikiamos paslaugos įrašas patikimame sąraše, rengiamame PUPSS forma

Pagal šias PS bendrosios formos techninės specifikacijas paslaugos įraše galima naudoti penkių pagrindinių informacijos dalių derinį:

— „Paslaugos rūšies identifikatorius“ („Sti“), kuriuo pvz., nurodoma KS išduodanti SI, (SI/KS (angl. *CA/QC*)),

— „Paslaugos pavadinimas“ („Sn“),

— „Paslaugos skaitmeninio identifikatoriaus“ („Sdi“) informacija, kuria nurodoma į sąrašą įtraukta paslauga, pvz., KS išduodančios SI X.509v3 sertifikatas (būtinasis reikalavimas),

— jei tai SI/KS paslauga, neprivaloma „Informacijos apie paslaugą plėtinių“ („Sie“) informacija, leidžianti įtraukti seką, sudarytą iš vienos arba daugiau baigtinių sekų, iš kurių kiekvienoje nurodoma:

  — kriterijai, taikytini papildomai apibrėžti (atrinkti filtravimo būdu) pagal „Sdi“ apibrėžtą sertifikavimo paslaugą, kad būtų galima tiksliai nustatyti paslaugą (t. y. kvalifikuotų sertifikatų rinkinį), apie kurią reikalaujama pateikti arba apie kurią pateikta papildomos informacijos, susijusios su informacija apie SPFĮ naudojimą (ir (arba) išdavimą juridiniam asmeniui); ir

  — susijusi informacija (kvalifikatoriai, angl. *qualifiers*) apie tai, ar šis papildomai apibrėžtas kvalifikuotų sertifikatų teikimo paslaugų rinkinys teikiamas naudojant SPFĮ arba ar ši susijusi informacija yra KS dalis, rengiama standartizuota, techninėmis priemonėmis apdorojama forma, ir (arba) informacija apie tai, ar šie KS išduodami juridiniams asmenims (paprastai tariama, kad KS išduodami tik fiziniams asmenims);

▼C1

— šiam paslaugos įrašui skirta informacija apie dabartinį statusą, pateikiant informaciją apie:

— tai, ar tai prižiūrima, ar akredituota paslauga; ir

— konkretų priežiūros ir (arba) akreditacijos statusą.

2.3. *SPT_{KS} paslaugų įrašų redagavimo ir naudojimo gairės*

Toliau pateikiamos **bendrosios redagavimo gairės**.

1. Jei užtikrinama (garantija, suteikta SPT_{KS} ir prižiūrima arba akredituota priežiūros įstaigos (PĮ) arba akreditacijos įstaigos (AĮ)), kad į sąrašą įtrauktos pagal „Sdi“ identifikuotos paslaugos kvalifikuotame sertifikate, kuris patvirtinamas naudojant SPFĮ, būtų pateikiamas ETSI nustatytas KS atitikties patvirtinimas, taip pat KS SPFĮ patvirtinimas ir (arba) KSP + objekto identifikatorius (OID), pakanka naudoti atitinkamą „Sdi“, o laukas „Sie“ gali būti naudojamas pasirinktinai, ir jame nebūtina pateikti informacijos apie SPFĮ naudojimą.

2. Jei užtikrinama (garantija, suteikta SPT_{KS} ir prižiūrima arba akredituota PĮ arba AĮ), kad į sąrašą įtrauktos pagal „Sdi“ identifikuotos paslaugos kvalifikuotame sertifikate, kuris nepatvirtinamas naudojant SPFĮ, būtų pateikiamas KS atitikties patvirtinimas ir (arba) KSP OID, ir jei šiame sertifikate nenumatyta teikti KS SPFĮ patvirtinimo arba KSP + OID, tuomet pakanka naudoti atitinkamą „Sdi“, o laukas „Sie“ gali būti naudojamas pasirinktinai, ir jame nebūtina pateikti informacijos apie SPFĮ naudojimą (tai reiškia, kad išduodant KS, SPFĮ nenaudojamas).

3. Jei užtikrinama (garantija, suteikta SPT_{KS} ir prižiūrima arba akredituota PĮ arba AĮ), kad į sąrašą įtrauktos pagal „Sdi“ identifikuotos paslaugos kvalifikuotame sertifikate būtų pateikiamas KS atitikties patvirtinimas, ir jei kai kuriuos iš šių KS numatoma patvirtinti naudojant SPFĮ, o kai kuriuos – ne (pvz., šie skirtumai gali atsirasti dėl to, kad įvairūs SPT naudoja specifinius sertifikatų politikos OID, arba dėl kitos sertifikavimo paslaugų teikėjų kvalifikuotuose sertifikatuose teikiamos specifinės informacijos, kuri gali būti teikiama tiesiogiai arba netiesiogiai, gali būti apdorojama techninėmis priemonėmis arba ne), tačiau jame neteikiamas NEI KS SPFĮ patvirtinimas, NEI ETSI KSP(+) OID, tuomet gali nepakakti naudoti atitinkamą „Sdi“ IR turi būti naudojamas laukas „Sie“, kuriame būtų pateikiama aiški informacija apie SPFĮ naudojimą ir galima papildoma informacija, skirta sertifikatų rinkiniui, kuriam tai taikoma, identifikuoti. Šiuo tikslu naudojant lauką „Sie“, pagal tą patį „Sdi“ veikiausiai reikės pateikti skirtingas „Informacijos apie SPFĮ naudojimą reikšmes“ (angl. *SSCD support information values*).

4. Jei užtikrinama (garantija, suteikta SPT_{KS} ir prižiūrima arba akredituota PĮ arba AĮ), kad į sąrašą įtrauktos pagal „Sdi“ identifikuotos paslaugos kvalifikuotame sertifikate nebūtų teikiamas KS atitikties patvirtinimas, KSP OID, KS SPFĮ patvirtinimas arba KSP + OID, tačiau užtikrinama, kad kai kurie iš šių galutinių subjektų sertifikatų, išduodamų pagal šį „Sdi“, būtų KS ir (arba) kad juos išduodant būtų naudojama SPFĮ, o kai kurie nebūtų KS ir nebūtų patvirtinami naudojant SPFĮ (pvz., šie skirtumai gali atsirasti dėl to, kad įvairūs SPT_{KS} naudoja specifinius sertifikatų politikos OID, arba dėl kitos SPT_{KS} kvalifikuotuose sertifikatuose teikiamos specifinės informacijos, kuri gali būti teikiama tiesiogiai arba netiesiogiai, gali būti apdorojama techninėmis priemonėmis arba ne), tuomet nepakanka naudoti atitinkamą „Sdi“ IR turi būti naudojamas laukas „Sie“ aiškiai informacijai apie SPFĮ naudojimą pateikti. Šiuo tikslu naudojant lauką „Sie“, pagal tą patį „Sdi“ veikiausiai reikės pateikti skirtingas „Informacijos apie SPFĮ naudojimą reikšmes“.

▼C1

Paprastai taikomas numatytasis principas, kad į patikimą sąrašą įtraukiant SPT, vienam X.509v3 sertifikatui, išduodamam SI/KS tipo sertifikavimo paslaugai, t. y. sertifikavimo institucijos, (tiesiogiai) išduodančios KS, teikiamai paslaugai, turi būti pateikiamas vienas paslaugos įrašas. Tam tikromis tiksliai numatytomis aplinkybėmis ir rūpestingai kontroliuojamomis sąlygomis valstybės narės priežiūros arba akreditacijos įstaiga gali nuspręsti naudoti pagrindinės arba aukštesniojo lygmens SI (t. y. sertifikavimo institucijos, tiesiogiai neišduodančios galutiniams subjektams skirtų KS, bet patvirtinančios SI hierarchiją nuo viršaus iki SI, išduodančių KS galutiniams subjektams) X.509v3 sertifikatą kaip į sąrašą įtrauktų SPT teikiamų paslaugų sąraše esančio vienintelio įrašo „Sdi“. Valstybės narės turi išsamiai apsvarstyti ir patvirtinti šių pagrindinės arba aukštesniojo lygmens SI X.509v3 sertifikatų naudojimo PS paslaugų įrašų „Sdi“ vertėms pateikti padarinius (pranašumus ir trūkumus). Be to, valstybė narė, taikydama šią leidžiamą numatytojo principo išimtį, privalo pateikti reikiamus dokumentus, padedančius nustatyti sertifikavimo kelią ir tikrinimo būdą.

Bendrosioms redagavimo gairėms paaiškinti galima pateikti tokį pavyzdį: jei SPT_{KS} naudojasi paslaugomis, teikiamomis vienos pagrindinės SI, kurios vadovaujamos kelios SI išduoda kvalifikuotus ir nekvalifikuotus sertifikatus, o jai išduodamuose kvalifikuotuose sertifikatuose pateikiamas tik KS atitikties patvirtinimas, tačiau nenurodoma, ar KS patvirtinami naudojant SPFĮ, pagal pirmiau išaiškintas taisykles tik pagrindinės SI „Sdi“ pateikimas reikštų, kad visi pagal šios pagrindinės SI hierarchiją išduoti KS NETVIRTINAMI naudojant SPFĮ. Jie šie KS iš tiesų patvirtinami naudojant SPFĮ, primygtinai rekomenduojama kvalifikuotuose sertifikatuose, kuries bus išduodami ateityje, naudoti KS SPFĮ patvirtinimą. Kol kas (kol baigsis paskutinio KS, kuriame ši informacija neteikiama, galiojimas), patikimumo užtikrinimo paslaugų statuso sąraše turėtų būti naudojamas laukas „Sie“ ir susijęs plėtinys „Kvalifikacijos“ (angl. *Qualifications*), pavyzdžiui, sertifikatai turėtų būti filtruojami naudojant specialius SPT_{KS} nustatytus OID, kuriuos SPT_{KS} galbūt naudoja įvairių tipų KS atskirti, (kai kurie iš jų patvirtinami naudojant SPFĮ, o kai kurie – ne) ir, naudojant plėtinį „Kvalifikatoriai“, pateikiama su tais filtravimo būdu atrinktais sertifikatais susijusi tiksli informacija apie SPFĮ naudojimą.

Toliau pateikiamos **bendrosios** elektroninio parašo taikymo priemonių, paslaugų arba produktų, pagrįstų patikimo sąrašo rengimu PUPSS forma pagal šias technines specifikacijas, **naudojimo gairės**.

SI/KS įrašas „Sti“ (ir panašus SI/KS įrašas, toliau vadinamas „pagrindinės SI/KS“ (angl. *RootCA/QC*), daromas naudojant „Sie“ plėtinį „Papildoma informacija apie paslaugą“ (angl. *additionalServiceInformation*):

— rodo, kad pagal „Sdi“ identifikuojamų SI (taip pat SI, priklausančių hierarchijai, kuri prasideda nuo pagal „Sdi“ identifikuojamos pagrindinės SI (angl. *RootCA*)) visi galutiniam subjektui išduoti sertifikatai yra KS, **jeigu** sertifikate tvirtinama, kad jie tokie yra, naudojant atitinkamus KS patvirtinimus (t. y. KS atitikties, KS SPFĮ) ir (arba) ETSI nustatytus KSP(+) OID (ir kad tai užtikrina priežiūros arba akreditacijos įstaiga; žr. pirmiau pateiktas bendrąsias redagavimo gaires),

Pastaba: jei lauke „Sie“ informacija apie kvalifikaciją neteikiama arba jei galutiniam subjektui išduotas sertifikatas, teikiamas kaip KS, papildomai neapibrėžtas susijusiame „Sie“ įraše, tuomet kvalifikuotame sertifikate teikiama techninėmis priemonėmis apdorojama informacija turi būti prižiūrima ir (arba) akredituota siekiant užtikrinti jos tikslumą. Tai reiškia, kad užtikrinama, jog atitinkami KS patvirtinimai (t. y. KS atitikties, KS SPFĮ) ir (arba) ETSI nustatyti KSP(+) OID naudojami (arba nenaudojami) pagal tai, ką tvirtina SPT_{KS},

▼C1

— **ir JEIGU** lauke „Sie“ pateikta informacija apie kvalifikaciją, tada, be pirmiau minėtos numatytosios naudojimo aiškinimo taisyklės, šie sertifikatai, identifikuojami naudojant šį lauko „Sie“ kvalifikacijos įrašą, sudaromą iš kelių filtrų, kuriais tiksliau identifikuojamas sertifikatų rinkinys ir pateikiama papildomos informacijos apie SPFĮ naudojimą ir (arba) juridinį asmenį kaip subjektą (pvz., tie sertifikatai, kurių sertifikatų politikos plėtinyje nurodytas tam tikras OID ir (arba) kuriems nustatytas tam tikras raktų naudojimo modelis, ir (arba) kurie filtruojami naudojant tam tikrą reikšmę, nurodytą kuriame nors konkrečiame sertifikato lauke arba plėtinyje, ir t. t.), turi būti vertinami pagal toliau nurodytą kvalifikatorių, kompensuojančių informacijos trūkumą atitinkamame KS, rinkinį, t. y.:

— siekiant nurodyti, ar naudojama SPFĮ:

— kvalifikatoriaus reikšmė „QCWithSSCD“, reiškianti, kad KS patvirtinamas naudojant SPFĮ, arba

— kvalifikatoriaus reikšmė „QCNoSSCD“, reiškianti, kad KS netvirtinamas naudojant SPFĮ, arba

— kvalifikatoriaus reikšmė „QCSSCDStatusAsInCert“, reiškianti, kad užtikrinama, jog visuose KS informacija apie SPFĮ naudojimą būtų pateikta šio SI/KS įrašo laukuose „Sdi“–„Sie“;

IR (ARBA)

— siekiant nurodyti, kad sertifikatas išduodamas juridiniam asmeniui:

— kvalifikatoriaus reikšmė „QCForLegalPerson“, reiškianti, kad sertifikatas išduotas juridiniam asmeniui.

2.4. *Paslaugos, padedančios teikti SI/KS paslaugas, tačiau nesusijusios su SI/KS lauku „Sdi“*

Taip pat reikėtų įtraukti atvejus, kai panaikinamų sertifikatų sąrašų (angl. *Certificate Revocation Lists*, CRL) ir interneto sertifikatų statuso protokolo (angl. *Online Certificate Status Protocol*, OCSP) atsakai pasirašomi naudojant raktus, gautus ne iš KS išduodančios SI (SI/KS). Tai galima padaryti šias paslaugas įtraukiant į patikimą sąrašą, rengiamą PUPSS forma (t. y. naudojant paslaugos rūšies identifikatorių, papildomai apibūdintą naudojant plėtinį „Papildoma informacija apie paslaugą“, kuriame nurodoma, kad OCSP arba CRL paslauga teikiama išduodant KS, pvz., atitinkamai nurodant paslaugos tipą OCSP/KS arba CRL/KS), nes galima tarti, kad šios paslaugos yra prižiūrimų ir (arba) akredituotų paslaugų, susijusių su KS sertifikavimo paslaugų teikimu, dalis. Be abejo, OCSP atsakovai arba CRL teikėjai, kurių sertifikatus pasirašo SI, priklausiančios tam tikrai į sąrašą įtrauktos SI/KS paslaugos hierarchijai, turi būti pripažinti teisėtais ir atitinkančiais SI/KS paslaugos, kuri yra įtraukta į sąrašą, statuso reikšmę.

Panaši nuostata gali būti taikoma sertifikavimo paslaugoms, kurias teikiant išduodami nekvalifikuoti sertifikatai (teikiant SI/VRS (angl. *CA/PKC*) rūšies paslaugas), naudojant numatytąsias ETSI TS 102 231 OCSP ir CRL paslaugų rūšis.

Atminkite, kad į patikimą sąrašą, rengiamą PUPSS forma, TURI būti įtrauktos atšaukimo paslaugos, taikomos, kai galutinių sertifikatų lauke AIA nepateikta reikiama informacija arba kai nėra į sąrašą įtrauktos SI parašo.

2.5. *Perėjimas prie sąveikaus KS aprašo*

Iš esmės reikia pamėginti kuo labiau sumažinti paslaugų įrašų (skirtingų „Sdi“) skaičių. Kita vertus, būtina užtikrinti tikslų tų paslaugų, kurios yra susijusios su KS išdavimu ir patikimos informacijos apie tai, ar KS patvirtinami naudojant SPFĮ, teikimu, kai šios informacijos išduotame KS nėra, identifikavimą.

▼C1

Būtų geriausia, kad laukas „Sie“ ir plėtinys „Kvalifikacija“ (griežtai) būtų naudojami tik tais specifiniais atvejais, kuriais reikia taikyti šį sprendimą, nes kvalifikuotame sertifikate turėtų būti pateikiama pakankamai informacijos apie deklaruotą kvalifikaciją ir deklaruotą SPFĮ naudojimą.

Valstybės narės turėtų kaip galima geriau užtikrinti, kad būtų priimti ir naudojami sąveikūs KS aprašai.

3. **Patikimo sąrašo bendrosios formos struktūra**

Siūloma valstybės narės patikimo sąrašo bendroji forma bus suskirstyta į šias informacijos kategorijas:

1. informacija apie patikimą sąrašą ir jo rengimo schemą;

2. laukų, kuriuose pateikiama aiški identifikavimo informacija apie kiekvieną pagal minėtą schemą prižiūrimą ir (arba) akredituotą SPT, seka (ši seka neprivaloma, t. y. jei ji nenaudojama, bus tariama, kad sąrašas tuščias, o tai reikš, kad susijusioje valstybėje narėje nėra nė vieno prižiūrimo arba akredituoto SPT, patenkančio į patikimo sąrašo taikymo sritį);

3. kiekvienam į sąrašą įtrauktam SPT skirta laukų, kuriuose aiškiai identifikuojama SPT teikiama prižiūrima ir (arba) akredituota sertifikavimo paslauga, seka (turi būti bent vienas šios sekos įrašas);

4. kiekvienos į sąrašą įtrauktos prižiūrimos ir (arba) akredituotos sertifikavimo paslaugos dabartinio statuso identifikavimo informacija ir šio statuso istorija.

Jei tai KS išduodantys SPT, aiškiai identifikuojant prižiūrimą ir (arba) akredituotą sertifikavimo paslaugą, kuri bus įtraukta į sąrašą, būtina apsvarstyti atvejus, kai kvalifikuotame sertifikate pateikiama nepakankamai informacijos apie jo kvalifikaciją ir galimybę jį patvirtinti naudojant SPFĮ, o pirmiausia reikia išspręsti klausimą, susijusį su tuo, kad daugelis (komercinių) SPT galutiniams subjektams skirtiems įvairių rūšių kvalifikuotiems ir nekvalifikuotiems sertifikatams parengti naudojasi vienos kvalifikuotos sertifikatus išduodančios SI paslaugomis.

Sąraše teikiamų įrašų, skirtų kiekvienam pripažintam SPT, skaičių galima sumažinti tada, kai yra viena ar keletas aukštesniųjų SI tarnybų, pvz., priklausančių komercinei SI hierarchijai nuo pagrindinės SI iki sertifikatus išduodančių SI. Tačiau net ir tokiais atvejais būtina taikyti ir palaikyti principą, kad būtų užtikrintas aiškus SPT_{KS} sertifikavimo paslaugos ryšys su sertifikatų, identifikuotinų kaip KS, rinkiniu.

1. *Informacija apie patikimą sąrašą ir jo rengimo schemą*

Šioje kategorijoje pateikiama tokia informacija:

— patikimo sąrašo **žyma**, padedanti identifikuoti patikimą sąrašą vykdant elektroninę paiešką ir skirta jo paskirčiai patvirtinti, kai sąrašas teikiamas žmonėms suprantama forma,

— patikimo sąrašo **formatas ir formato versijos identifikatorius**,

— patikimo sąrašo **eilės (arba laidos) numeris**,

— patikimo sąrašo **tipo informacija** (pvz., skirta nustatyti, ar tai patikimas sąrašas, kuriame pateikiama informacija apie nurodytos valstybės narės prižiūrimų ir (arba) akredituotų, siekiant užtikrinti, kad būtų laikomasi Direktyvos 1999/93/EB nuostatų, SPT teikiamų sertifikavimo paslaugų priežiūros ir (arba) akreditacijos statusą),

▼C1

— patikimo sąrašo **tvarkytojo informacija** (pvz., valstybės narės įstaigos, atsakingos už patikimo sąrašo sudarymą, saugų skelbimą ir tvarkymą, pavadinimas, adresas, informacija ryšiams ir t. t.),

— **informacija apie pamatinę (-es) priežiūros ir (arba) akreditacijos schemą (-as)**, su kuriomis patikimas sąrašas yra siejamas, įskaitant bent šią informaciją:

  — šalis, kurioje schema taikoma,

  — informacija apie tai, kur galima rasti informacijos apie schemą (-as), arba tokios vietos nuoroda (schemos modelis, taisyklės, kriterijai, naudotojai, tipas ir t. t.),

  — (istorinės) informacijos saugojimo laikotarpis,

— su patikimu sąrašu susijusi **politika ir (arba) teisinė informacija, įsipareigojimai, atsakomybė**,

— patikimo sąrašo **paskelbimo data ir laikas, kitas numatomas atnaujinimas**.

2. *Aiški identifikavimo informacija apie kiekvieną pagal schemą pripažįstamą SPT*

Šiame informacijos rinkinyje pateikiama bent ši informacija:

— SPT organizacijos pavadinimas, naudojamas oficialiuose teisiniuose registruose (pagal valstybėje narėje taikomą tvarką tai gali būti ir SPT organizacijos UID),

— SPT adresas ir informacija ryšiams,

— papildoma informacija apie SPT, pateikiama tiesiogiai arba nurodant vietą, iš kurios tą informaciją galima atsisiųsti.

3. *Kiekvienam į sąrašą įtrauktam SPT skirta laukų, kuriuose aiškiai identifikuojama SPT teikiama pagal Direktyvą 1999/93/EB prižiūrima ir (arba) akredituota sertifikavimo paslauga, seka*

Šiame informacijos rinkinyje apie kiekvieną į sąrašą įtraukto SPT teikiamą sertifikavimo paslaugą pateikiama bent ši informacija:

— sertifikavimo paslaugos rūšies identifikatorius (pvz., identifikatorius, nurodantis, kad SPT teikiama prižiūrima ir (arba) akredituota sertifikavimo paslauga yra sertifikavimo institucijos teikiama KS išdavimo paslauga),

— sertifikavimo paslaugos (prekės) pavadinimas;

— aiškus unikalus sertifikavimo paslaugos identifikatorius,

— papildoma informacija apie sertifikavimo paslaugą (pvz., pateikiama tiesiogiai arba nurodant vietą, iš kurios tą informaciją galima atsisiųsti, taip pat paslaugos prieinamumo informacija).

— Jei tai SI/KS paslaugos, neprivaloma seka, sudaryta iš baigtinių informacijos sekų, iš kurių kiekvienoje nurodoma:

  i) kriterijai, taikytini papildomai apibrėžti (atrinkti filtravimo būdu) lauke „Sdi“ apibrėžtą sertifikavimo paslaugą, kad būtų galima nustatyti konkrečią paslaugą (t. y. kvalifikuotų sertifikatų rinkinį), apie kurią reikia pateikti arba apie kurią pateikta papildomos informacijos apie SPFĮ naudojimą (ir (arba) sertifikato išdavimą juridiniam asmeniui); ir

  ii) susiję kvalifikatoriai, kuriais pateikiama informacijos apie tai, ar šis su papildomai apibrėžta paslauga susijęs kvalifikuotų sertifikatų rinkinys patvirtinamas naudojant SPFĮ, ir (arba) informacija apie tai, ar šie KS išduodami juridiniam asmeniui (paprastai tariama, kad KS išduodami fiziniams asmenims).

▼C1

4. *Kiekvienos į sąrašą įtrauktos sertifikavimo paslaugos dabartinio statuso identifikavimo informacija ir šio statuso istorija*

Šiame informacijos rinkinyje pateikiama bent ši informacija:

— dabartinio statuso identifikatorius,

— dabartinio statuso galiojimo pradžios data ir laikas,

— istorinė informacija apie šį statusą.

4. **Apibrėžtys ir santrumpos**

Šiame dokumente taikomos šios apibrėžtys ir akronimai:

Terminas	Akronimas	Apibrėžtis
Sertifikavimo paslaugų teikėjas	SPT	Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 11 punkte.
Sertifikavimo institucija	SI	SI – tai SPT, kuris, išduodamas galutiniam subjektui skirtus sertifikatus, gali naudoti keletą techninių SI privačių parašo raktų, iš kurių kiekvienas susietas su tam tikru sertifikatu. SI yra institucija, kuriai vienas arba daugiau naudotojų patiki rengti ir priskirti sertifikatus. Neprivaloma tvarka sertifikavimo institucija gali kurti naudotojų raktus [ETSI TS 102 042]. SI turėtų būti identifikuojama pagal identifikavimo informaciją, pateiktą SI sertifikato, susijusio su (patvirtinimo) viešuoju raktu, kuris yra susietas su SI privačiu parašo raktu ir kurį SI iš tiesų naudoja subjektų sertifikatams išduoti, lauke „Sertifikatą išduodantis asmuo“ (angl. *Issuer*). SI gali turėti keletą parašo raktų. Kiekvienas SI parašo raktas išskirtinai identifikuojamas unikaliu identifikatoriumi, kuris yra SI sertifikato lauko „Institucijos rakto identifikatorius“ (angl. *Authority Key Identifier*) dalis.
Kvalifikuotus sertifikatus išduodanti sertifikavimo institucija	SI/KS	SI, atitinkanti Direktyvos 1999/93/EB II priede nustatytus reikalavimus ir išduodanti kvalifikuotus sertifikatus, atitinkančius Direktyvos 1999/99/EB I priede nustatytus reikalavimus.
Sertifikatas	Sertifikatas	Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 9 punkte.
Kvalifikuotas sertifikatas	KS	Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 10 punkte.
Pasirašantis asmuo	Pasirašantis asmuo	Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 3 punkte.
Priežiūra	Priežiūra	Terminas „priežiūra“ vartojamas ta prasme, kokia jis vartojamas Direktyvoje 1999/93/EB (3 straipsnio 3 dalis). Šioje direktyvoje reikalaujama, kad kiekviena valstybė narė sukurtų tinkamą sistemą, leidžiančią prižiūrėti jos teritorijoje įsisteigusius SPT, išduodančius kvalifikuotus sertifikatus visuomenei, ir taip užtikrintų direktyvos nuostatų laikymosi priežiūrą.
Savanoriška akreditacija	Akreditacija	Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 13 punkte.
Patikimas sąrašas	PS	Sąrašas, kuriame nurodomas sertifikavimo paslaugų teikėjų, kuriuos, siekdama užtikrinti Direktyvos 1999/93/EB nuostatų laikymąsi, prižiūri ir (arba) yra akreditavusi nurodyta valstybė narė, teikiamų sertifikavimo paslaugų priežiūros ir (arba) akreditacijos statusas.

▼C1

Terminas	Akronimas	Apibrėžtis
Patikimumo užtikrinimo paslaugų statuso sąrašas	PUPSS	Pasirašyto sąrašo forma, naudojama patikimumo užtikrinimo paslaugų statuso informacijai pagal ETSI TS 102 231 nustatytas specifikacijas pateikti.
Patikimumo užtikrinimo paslauga		Paslauga, kuria didinamas elektroninių operacijų patikimumas ir pasitikėjimas šiomis operacijomis (paprastai – bet nebūtinai – atliekamomis naudojant kriptografijos technologijas arba susijusiomis su slapta medžiaga) (ETSI TS 102 231).
Patikimumo užtikrinimo paslaugų teikėjas	PUPT	Įstaiga, teikianti vieną arba daugiau (elektroninių) patikimumo užtikrinimo paslaugų (šis terminas vartojamas platesne prasme nei SPT).
Patikimumo užtikrinimo paslaugos žyma	PUPŽ	Fizinis arba dvejetainis (loginis) objektas, sukurtas arba išduotas teikiant patikimumo užtikrinimo paslaugą. Dvejetainio PUPŽ pavyzdžiai yra sertifikatai, CRL, laiko fiksavimo žymos ir OCSP atsakai.
Kvalifikuotas elektroninis parašas	KEP	SEP, patvirtintas kvalifikuotu sertifikatu ir sukurtas naudojant SPFĮ, kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnyje.
Saugus elektroninis parašas	SEP	Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 2 punkte.
Saugus elektroninis parašas, patvirtintas kvalifikuotu sertifikatu	SEP_{KS}	Elektroninis parašas, atitinkantis SEP reikalavimus ir patvirtintas kvalifikuotu sertifikatu, kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnyje.
Saugi parašo formavimo įranga	SPFĮ	Kaip apibrėžta Direktyvos 1999/93/EB 2 straipsnio 6 punkte.

I SKYRIUS

PATIKIMO PRIŽIŪRIMŲ IR (ARBA) AKREDITUOTŲ SERTIFIKAVIMO PASLAUGŲ TEIKĖJŲ SĄRAŠO BENDROSIOS FORMOS IŠSAMIOS SPECIFIKACIJOS

Šioje dokumento dalyje raktiniai žodžiai „PRIVALO“, „NEPRIVALO“, „PRIVALOMAS“, „TURI“, „NETURI“, „TURĖTŲ“, „NETURĖTŲ“, „REKOMENDUOJAMA“, „GALI“ ir „NEPRIVALOMAS“ turi būti suprantami taip, kaip aprašyta RFC 2119 ([1]).

►M1 Šios specifikacijos pagrįstos specifikacijomis ir reikalavimais, nustatytais ETSI TS 102 231 v.3.1.2. Jei šiose specifikacijose konkretus reikalavimas nenurodytas, TURI būti taikomi visi ETSI TS 102 231 v.3.1.2 nustatyti reikalavimai. ◄ Jei šiose specifikacijose pateikiami konkretūs reikalavimai, jiems TURI būti teikiama pirmenybė prieš atitinkamus ETSI TS 102 231 nustatytus reikalavimus ir jie turi būti papildomi formato specifikacijomis, nustatytomis ETSI TS 102 231. Jei šios specifikacijos prieštarauja ETSI TS 102 231 specifikacijoms, kaip norminės TURI būti taikomos šios specifikacijos.

([1]) IETF RFC 2119: „Raktiniai žodžiai, naudojami RFC būtinumo lygiams nurodyti“ (angl. *Key words for use in RFCs to indicate Requirements Levels*).

▼C1

TURI būti įdiegta galimybė pasirinkti kalbą – bent anglų (EN) ir galbūt dar vieną arba daugiau nacionalinių kalbų.

Data ir laikas TURI būti nurodomi pagal ETSI TS 102 231 5.1.4 punktą.

Unikalieji išteklių identifikatoriai (UII) TURI būti nurodomi pagal ETSI TS 102 231 5.1.5 punktą.

Informacija apie patikimo sąrašo rengimo schemą

Tag

TSL tag (5.2.1 punktas)

Šis laukas PRIVALOMAS; jis TURI atitikti ETSI TS 102 231 5.2.1 punktą.

▼M1

_____

▼C1

Scheme Information

TSL version identifier (5.3.1 punktas)

Šis laukas PRIVALOMAS; jame TURI būti įrašyta „3“ (sveikasis skaičius).

TSL sequence number (5.3.2 punktas)

▼M1

Šis laukas PRIVALOMAS. Jame TURI būti nurodytas PUPSS eilės numeris. Pirmosios PUPSS versijos eilės numeris yra „1“, po to ši sveikuoju skaičiumi išreikšta reikšmė TURI būti padidinama kiekvieną kartą, kai išleidžiama nauja PUPSS versija. Padidinus minėto „TSL version identifier“ reikšmę, šis numeris NETURI vėl tapti „1“.

▼C1

TSL type (5.3.3 punktas)

▼M1

Šis laukas PRIVALOMAS; jame nurodomas PUPSS tipas. Šio lauko reikšmė TURI būti http://uri.etsi.org/TrstSvc/eSigDir-1999–93-EC-TrustedList/TSLType/-generic (Generic).

▼C1

Pastaba: siekiant laikytis ETSI TS 102 231 5.3.3 punkto ir nurodyti konkretų PUPSS tipą, remiantis šiomis specifikacijomis, kuriomis nustatyta valstybėse narėse PUPSS forma rengiamo patikimo sąrašo ([1]) rengimo tvarka ir leidžiama taikyti tam tikrą analizės priemonę, skirtą nustatyti, kuri toliau nurodytų laukų ([2]) forma veikiausiai bus taikoma, jei, atsižvelgiant į teikiamo PUPSS tipą (šiuo atveju tai valstybės narės patikimas sąrašas), nustatyta kokia nors konkreti (arba alternatyvi) šių laukų reikšmė, minėtas konkretus UII TURI būti užregistruotas ir aprašytas, kaip nurodyta toliau:

([1]) T. y. Sertifikavimo paslaugų teikėjų, kuriuos, siekdama užtikrinti Direktyvos 1999/93/EB nuostatų laikymąsi, prižiūri ir (arba) yra akreditavusi nurodyta valstybė narė, teikiamų sertifikavimo paslaugų priežiūros ir (arba) akreditacijos statuso sąrašas (trumpiau – patikimas sąrašas).

([2]) T. y. laukai, nurodyti ETSI TS 102 231 – „Elektroniniai parašai ir infrastruktūros (EPI). Suderintos patikimumo užtikrinimo paslaugų statuso informacijos teikimas“ (angl. *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information*) ir trumpai apibūdinti šiose specifikacijose, skirtose patikimo sąrašo rengimo tvarkai valstybėse narėse nustatyti.

▼M1

UII: URI: (Generic) http://uri.etsi.org/TrstSvc/eSigDir-1999–93-EC-TrustedList/TSLType/generic

▼C1

Aprašas. PUPSS forma rengiamas sertifikavimo paslaugų teikėjų, kuriuos, siekdama užtikrinti, kad būtų laikomasi atitinkamų 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvos 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos nuostatų, tiesioginės (savanoriškos arba teisės aktais nustatytos) priežiūros tvarka prižiūri ir (arba) yra akreditavusi nurodyta valstybė narė, tvarkanti PUPSS forma rengiamą sąrašą, teikiamų sertifikavimo paslaugų priežiūros ir (arba) akreditacijos statuso sąrašas.

Scheme operator name (5.3.4 punktas)

Šis laukas PRIVALOMAS. Jame TURI būti nurodytas valstybės narės įstaigos, atsakingos už nacionalinio patikimo sąrašo sudarymą, skelbimą ir tvarkymą, pavadinimas. Jame TURI būti nurodytas oficialus pavadinimas, kurį naudodamas susijęs juridinis asmuo arba įgaliotasis asmuo (pvz., Vyriausybės administracinė agentūra), susijęs su šia įstaiga, vykdo veiklą. Tai PRIVALO būti pavadinimas, naudojamas oficialiame teisiniame registre arba įgaliojime ir siunčiant oficialius pranešimus. Šis pavadinimas TURI būti sudarytas iš įvairiakalbių ženklų eilučių sekos ir turi būti užrašytas anglų (EN) kalba, kaip privaloma, ir galbūt viena arba daugiau nacionalinių kalbų.

Pastaba. Šalyje GALI būti atskiros priežiūros ir akreditacijos įstaigos ir netgi papildomos įstaigos, vykdančios įvairią susijusią einamąją veiklą. Kiekviena valstybė narė pati paskiria PUPSS forma rengiamo valstybės narės patikimo sąrašo schemos operatorių. ►M1 Kiekviena valstybė narė pati paskiria PUPSS forma rengiamo valstybės narės patikimo sąrašo „Scheme Operator“ (schemos operatorių). ◄

Patikimo sąrašo dalyje, kurioje pateikiama informacija apie schemą, taip pat teikiant specifinę schemos informaciją, kuri nurodoma naudojant schemos informacijos UII, TURI būti nuosekliai išdėstytos ir nurodytos visos aplinkybės, kuriomis už priežiūrą, akreditaciją arba veiklos aspektus atsakingos atskiros įstaigos (5.3.7 punktas).

▼M1

PUPSS pasirašo nurodytas „Scheme Operator“ (schemos operatorius) (5.3.4 punktas).

▼C1

Scheme operator address (5.3.5 punktas)

Šis laukas PRIVALOMAS. Jame TURI būti nurodytas juridinio asmens arba įgaliotosios organizacijos, nurodytos lauke „Scheme operator name“ (5.3.4 punktas), pašto ir elektroninio pašto adresas. Šiame lauke TURI būti nurodytas „PostalAddress“ (t. y. namo numeris, gatvė, vietovė, [sritis arba rajonas], [pašto kodas] ir ISO 3166–1 dviejų raidžių šalies kodas), kaip nurodyta 5.3.5.1 punkte, ir „ElectronicAddress“ (t. y. e. paštas ir (arba) interneto svetainės UII), kaip nurodyta 5.3.5.2 punkte.

Scheme name (5.3.6 punktas)

Šis laukas PRIVALOMAS; jame nurodomas schemos pavadinimas. Šis pavadinimas TURI būti sudarytas iš įvairiakalbių ženklų eilučių sekos (privaloma kalba – anglų (EN), taip pat gali būti naudojama viena arba daugiau nacionalinių kalbų), sudaromos taip:

▼C1

— versijoje anglų (EN) kalba TURI būti ženklų eilutė, kurios struktūra tokia:

CC:EN_name_value,

kur:

– CC = ISO 3166–1 dviejų raidžių šalies kodas, nurodytas lauke „Schemos teritorija“ (angl. *Scheme territory*, 5.3.10 punktas),

– : = naudojamas kaip skyriklis,

▼M1

- „EN_name_value“ = Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State's laws.

▼C1

— versijose valstybės narės nacionalinėmis kalbomis TURI būti ženklų eilutė, kurios struktūra tokia:

CC:name_value,

kur:

– CC = ISO 3166–1 dviejų raidžių šalies kodas, nurodytas lauke „Schemos teritorija“ (5.3.10 punktas),

– : = naudojamas kaip skyriklis,

– name_value = pirmiau nurodyto pavadinimo anglų kalba (EN_name_value) oficialus vertimas į nacionalinę kalbą.

Reikalaujama, kad lauke „Scheme information URI“ nurodyta schema turėtų unikalų pavadinimą ir būtų užtikrinta, kad tuo atveju, jei schemos operatorius valdo daugiau kaip vieną schemą, kiekvienai iš jų būtų duotas skirtingas pavadinimas.

Valstybės narės ir schemų operatoriai TURI užtikrinti, kad tuo atveju, jei valstybė narė arba schemos operatorius valdo daugiau kaip vieną schemą, kiekvienai iš jų būtų duotas skirtingas pavadinimas.

Scheme information URI (5.3.7 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodytas (-i) UII, pagal kurį (-iuos) naudotojai (susijusios šalys) gali gauti specifinės informacijos apie schemą (privaloma kalba – anglų (EN), taip pat gali būti naudojama viena arba daugiau nacionalinių kalbų). Šis laukas TURI būti sudarytas iš įvairiakalbių nuorodų sekos (privaloma kalba – anglų (EN), taip pat gali būti naudojama viena arba daugiau nacionalinių kalbų). Nurodytu (-ais) UII PRIVALO būti pateikta nuoroda į informaciją, kuria apibūdinama tinkama schemos informacija.

Į tinkamą schemos informaciją TURI būti įtraukta bent ši informacija:

— visoms valstybėms narėms vienoda bendra įvadinė informacija apie patikimo sąrašo taikymo sritį ir aplinkybes, taip pat pamatinę (-es) priežiūros ir (arba) akreditacijos schemą (-as). Bendras naudotinas tekstas yra toks:

▼C1

The present list is the TSL implementation of [*name of the relevant Member State*] „Trusted List of supervised/accredited Certification Service Providers“ providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable „supervision“ system (respectively „voluntary accreditation“ system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art.2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, ir t. t.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

— Specifinė informacija apie pamatinę (-es) priežiūros ir (arba) akreditacijos schemą (-as), pirmiausia ([1]):

— informacija apie priežiūros sistemą, taikomą kiekvienam SPT_{KS},

([1]) Paskutinieji du informacijos rinkiniai yra ypač svarbūs, kad susijusios šalys galėtų įvertinti tokių priežiūros ir (arba) akreditacijos sistemų kokybę ir saugumą. Šie informacijos rinkiniai PS lygmeniu teikiami naudojant esamą „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/teisinė informacija“ (5.3.11 punktas – visoms valstybėms narėms bendras tekstas, susietas su Direktyva 1999/93/EB; be to, kiekviena valstybė narė gali pateikti papildomą jai svarbų tekstą ir (arba) nuorodų). Papildoma informacija apie nacionalines priežiūros ir (arba) akreditacijos sistemas, taikomas KS neišduodantiems sertifikavimo paslaugų teikėjams, apie kiekvieną paslaugą gali būti teikiama, kai reikia ir reikalaujama (pvz., norint išskirti keletą kokybės ir (arba) saugumo lygmenų), naudojant „Schemos paslaugos apibrėžties UII“ (5.5.6 punktas).

▼C1

— jei reikia, informacija apie nacionalinę savanoriškos akreditacijos schemą, taikomą kiekvienam SPT_{KS},

— jei reikia, informacija apie priežiūros sistemą, taikoma kiekvienam KS neišduodančiam SPT,

— jei reikia, informacija apie nacionalinę savanoriškos akreditacijos schemą, taikomą kiekvienam KS neišduodančiam SPT.

— Teikiant šią specifinę informaciją apie kiekvieną pirmiau nurodytą pamatinę schemą, TURI būti pateikta bent tokia informacija:

— bendras aprašas,

— informacija apie procedūrą, kurią priežiūros ir (arba) akreditacijos įstaiga taiko, kad užtikrintų SPT priežiūrą ir (arba) akreditaciją ir kurią taiko prižiūrimi ir (arba) akredituoti SPT,

— informacija apie kriterijus, pagal kuriuos SPT yra prižiūrimi ir (arba) akredituojami.

— Jei reikia, specifinė informacija apie konkrečias kvalifikacijas, kurios kai kuriems fiziniams arba dvejetainiams (loginiams) objektams, sukurtiems arba parengtiems teikiant sertifikavimo paslaugą, gali būti suteiktos remiantis jų atitiktimi nacionalinėms nuostatoms ir reikalavimams, įskaitant informaciją apie tokios kvalifikacijos reikšmę ir susijusias nacionalines nuostatas ir reikalavimus.

Be to, savanoriškai GALI būti teikiama papildoma specifinė valstybės narės informacija apie schemą. Teikiant šią informacija, TURI būti nurodoma:

— informaciją apie kriterijus ir taisykles, taikomas prižiūrėtojams ir (arba) auditoriams atrinkti ir nustatyti, kaip jie turėtų prižiūrėti (kontroliuoti) ir (arba) akredituoti (audituoti) SPT,

— kita informacija ryšiams ir bendra informacija apie schemos veikimą.

Status determination approach (5.3.8 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodytas statuso nustatymo metodo identifikatorius. TURI būti naudojamas toliau nurodytas specialus UII, užregistruotas ir aprašytas, kaip nurodyta toliau:

UII: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/-appropriate

Aprašas. Į sąrašą įtrauktų paslaugų statusą nustato schemos operatorius arba šis statusas nustatomas jo vardu, taikant atitinkamą nurodytos valstybės narės sistemą, leidžiančią užtikrinti sertifikavimo paslaugų teikėjų, įsisteigusių jos teritorijoje (arba, jei tai savanoriška akreditacija, – trečiojoje šalyje) ir visuomenei pagal Direktyvos 1999/93/EB 3 straipsnio 3 dalį (arba atitinkamai pagal 3 straipsnio 2 dalį arba 7 straipsnio 1 dalies a punktą) išduodančių kvalifikuotus sertifikatus, priežiūrą (ir, jei reikia, savanorišką akreditaciją) ir, jei reikia, leidžiančią užtikrinti sertifikavimo paslaugų teikėjų, neišduodančių kvalifikuotų sertifikatų, priežiūrą ir (arba) savanorišką akreditaciją pagal nacionaliniu mastu nustatytą (-as) ir įdiegtą (-ą) pripažintą (-as) patvirtinimo schemą (-as), nacionaliniu mastu taikomą (-as) siekiant užtikrinti, kad būtų prižiūrima, ar KS neišduodančių SPT teikiamos paslaugos atitinka nuostatas, išdėstytas Direktyvoje 1999/93/EB ir galbūt papildytas nacionalinėmis nuostatomis dėl tokių sertifikavimo paslaugų teikimo.

▼C1

Scheme type/community/rules (5.3.9 punktas)

Šis laukas PRIVALOMAS; jame TURI būti pateikti bent šie registruoti UII:

— visų valstybių narių patikimiems sąrašams bendras UII kaip nuoroda į aiškinamąjį tekstą, kuris TURI būti taikomas visiems PS:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

— šiame tekste nurodomas valstybės narės schemos (nurodytos naudojant laukus „TSL type“ (5.3.3 punktas) ir „Scheme name“ (5.3.6 punktas)) priklausymas schemų schemai (t. y. PUPSS, kuriame pateikiamas nuorodų į visas valstybes nares, skelbiančias ir tvarkančias PUPSS forma rengiamą PS, sąrašas),

— jame naudotojai gali rasti politiką ir (arba) taisykles, pagal kurias TURI būti vertinamos į sąrašą įtrauktos paslaugos ir pagal kurias galima nustatyti PUPSS tipą (žr. 5.3.3 punktą),

— jame naudotojai gali rasti aprašą, kaip naudoti ir aiškinti PUPSS forma rengiamo patikimo sąrašo turinį. Šios naudojimo taisyklės TURI būti bendros visų valstybių narių patikimiems sąrašams, nepaisant to, kokios rūšies paslauga įtraukiama į sąrašą ir kokia (-ios) priežiūros ir (arba) akreditacijos sistema (-os) taikoma (-os).

Aprašas:

„Participation in a scheme

Each Member State must create a „Trusted List of supervised/accredited Certification Service Providers“ providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The present TSL implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's TSL implementation of their Trusted List, compiled by the European Commission.

Policy/rules for the assessment of the listed services

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

▼C1

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable „supervision“ system (respectively „voluntary accreditation“ system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art.2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, ir t. t.) may be included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a „voluntary accreditation“ system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined „recognised approval scheme“ implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Art. 2.11 of the Directive). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific „qualification“ on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a „qualification“ is likely to be limited solely to the national level.

Interpretation of the TSL implementation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision 2009/767/EC are as follows:

A „CA/QC“„Service type identifier“ („Sti“) entry (similarly a CA/QC entry further qualified as being a „RootCA/QC“ through the use of „Service information extension“ („Sie“) additionalServiceInformation extension)

— indicates that from the „Service digital identifier“ („Sdi“) identified CA (similarly within the CA hierarchy starting from the „Sdi“ identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) **provided** that it is claimed as such in the certificate through the use of appropriate ETSI TS 101 862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101 456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C1

Note: if no „Sie“„Qualification“ information is present or if an end-entity certificate that is claimed to be a QC is not „further identified“ through a related „Sie“ entry, then the „machine-processable“ information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— **and IF**„Sie“„Qualification“ information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this „Sie“„Qualification“ entry, which is constructed on the principle of a sequence of „filters“ further identifying a set of certificates, must be considered according to the associated „qualifiers“ providing some additional information regarding „SSCD support“ and/or „Legal person as subject“ (e.g. those 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.). Those qualifiers are part of the following set of „qualifiers“ used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

— to indicate the nature of the SSCD support:

— „QCWithSSCD“ qualifier value meaning „QC supported by an SSCD“, or

— „QCNoSSCD“ qualifier value meaning „QC not supported by an SSCD“, or

— „QCSSCDStatusAsInCert“ qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the „Sdi“-„Sie“ provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

— „QCForLegalPerson“ qualifier value meaning „Certificate issued to a Legal Person“

The general interpretation rule for any other „Sti“ type entry is that the listed service named according to the „Sn“ field value and uniquely identified by the „Sdi“ field value has a current supervision/accreditation status according to the „Scs“ 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 Technical specifications for a Common Template for the „Trusted List of supervised/accredited Certification Service Providers“ in the Annex of Commission Decision [reference to the actual Decision] for further details on the fields, description and meaning for the TSL implementation of the Member States’ Trusted Lists.“

▼C1

— specifinis kiekvienos valstybės narės patikimo sąrašo UII kaip nuoroda į aiškinamąjį tekstą, kuris TURI būti taikomas šios valstybės narės patikimam sąrašui:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC

kur CC – ISO 3166–1 dviejų raidžių šalies kodas, nurodytas lauke „Schemos teritorija“ (5.3.10 punktas),

— šiame tekste naudotojai gali rasti specifinę nurodytos valstybės narės politiką ir (arba) taisykles, pagal kurias, laikantis valstybės narės atitinkamos priežiūros sistemos ir savanoriškos akreditacijos schemų reikalavimų, TURI būti vertinamos į sąrašą įtrauktos paslaugos,

— jame naudotojai gali rasti specifinį nurodytos valstybės narės aprašą, kaip naudoti ir aiškinti PUPSS forma rengiamo patikimo sąrašo turinį, susijusį su sertifikavimo paslaugomis, kurias teikiant neišduodami KS. Šis tekstas gali būti naudojamas galimam nacionalinių priežiūros ir (arba) akreditacijos sistemų, susijusių su KS neišduodančiais SPT, hierarchijos lygiui nurodyti, taip pat nurodyti, kaip šiuo tikslu naudojami laukai „Pagal schemą teikiamos paslaugos apibrėžties UII“ (angl. *Scheme service definition URI*) (5.5.6 punktas) ir „Informacijos apie paslaugą plėtinys“.

Valstybės narės, remdamosi minėtu specifiniu valstybės narės UII, GALI nustatyti papildomus UII (t. y. UII, nustatomus remiantis šiuo specifiniu hierarchiniu UII).

Scheme territory (5.3.10 punktas)

Pagal šias specifikacijas šis laukas yra PRIVALOMAS; jame TURI būti nurodyta šalis, kurioje taikoma schema (ISO 3166–1 dviejų raidžių šalies kodas).

TSL policy/legal notice (5.3.11 punktas)

Pagal šias specifikacijas šis laukas yra PRIVALOMAS; jame TURI būti nurodyta schemos politika arba pateiktas pranešimas 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 tvarkomas ir skelbiamas PS.

Tai TURI būti įvairiakalbių ženklų eilutė (paprastojo teksto), sudaryta iš dviejų dalių:

— pirmosios – privalomosios – dalies, kuri yra bendra visų valstybių narių patikimiems sąrašams (privaloma kalba – anglų (EN), taip pat gali būti naudojama viena arba daugiau nacionalinių kalbų); šioje dalyje nurodoma, kad taikomas teisinis pagrindas yra Direktyva 1999/93/EB ir valstybės narės, nurodytos lauke „Schemos teritorija“, teisės aktų nuostatos, kuriomis įgyvendinama ši direktyva.

Bendras tekstas anglų kalba:

„The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.“

Tekstas valstybės narės nacionaline (-ėmis) kalba (-omis): [oficialus (-ūs) pirmiau nurodyto teksto anglų kalba vertimas (-ai)].

▼C1

— antroji – neprivalomoji – dalis, specifinė kiekvienam PS (privaloma kalba – anglų (EN), taip pat gali būti naudojama viena arba daugiau nacionalinių kalbų); šioje dalyje pateikiamos nuorodos į konkrečias galiojančias nacionalines teisines sistemas (pvz., pirmiausia susijusias su nacionalinėmis priežiūros ir (arba) akreditacijos schemomis, taikomomis KS neišduodantiems SPT).

Historical information period (5.3.12 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodytas laikotarpis (sveikasis skaičius), kuriuo PUPSS turi būti teikiama istorinė informacija. Ši sveiku skaičiumi išreikšta reikšmė pateikiama dienų skaičiumi; pagal šias specifikacijas ji TURI būti ne mažesnė kaip 3 653 (tai reiškia, kad PUPSS forma rengiamame valstybių narių patikimame sąraše teikiama istorinė informacija PRIVALO apimti ne trumpesnį kaip dešimties metų laikotarpį). Nurodant didesnius skaičius, reikėtų atsižvelgti į valstybės narės, nurodytos lauke „Scheme Territory“, teisinius duomenų saugojimo reikalavimus (5.3.10 punktas).

Pointers to other TSLs (5.3.13 punktas)

Pagal šias specifikacijas šis laukas yra PRIVALOMAS; jame, jei tokios informacijos yra, turi būti pateikta nuoroda į ETSI TS 102 231 reikalavimus atitinkančią formą, kurioje pateikiamas Europos Komisijos sudarytas nuorodų sąrašas su nuorodomis į visus PUPSS forma rengiamus valstybių narių patikimus sąrašus. Įgaliojant naudoti neprivalomą skaitmeninį identifikatorių, kuriuo 5.5.3 punkte nustatyta forma nurodomas nurodyto PUPSS rengėjas, taikomos ETSI TS 102 231 5.3.13 punkte nustatytos specifikacijos.

Pastaba: kol pagal ETSI TS 102 231 reikalavimus bus parengtas Europos Komisijos sudaromas nuorodų sąrašas su nuorodomis į valstybės narės PUPSS forma rengiamus PS, šis laukas NETURI būti naudojamas.

List issue date and time (5.3.14 punktas)

Šis laukas PRIVALOMAS; jame, naudojant ETSI TS 102 231 5.1.4 punkte nustatytą datos ir laiko reikšmę, TURI būti nurodyta PUPSS sudarymo data ir laikas (pasaulinis laikas, nurodytas kaip Zulu laikas).

Next update (5.3.15 punktas)

Šis laukas PRIVALOMAS; jame, naudojant ETSI TS 102 231 5.1.4 punkte nustatytą datos ir laiko reikšmę, TURI būti nurodyta kito PUPSS sudarymo data ir laikas (pasaulinis laikas, nurodytas kaip Zulu laikas) arba pateikta nulinė reikšmė, reiškianti, kad PUPSS nebenaudojamas.

Jei tarpinių PUPT arba paslaugų, kurioms taikoma schema, statuso pakeitimų nedaroma, pasibaigus paskutinio PUPSS galiojimui, TURI būti paskelbtas naujas PUPSS.

Pagal šias specifikacijas „Next update“ data ir laikas nuo „List issue date and time“ NETURI skirtis daugiau kaip **šešiais (6)** mėnesiais.

▼C1

Distribution points (5.3.16 punktas)

Šis laukas NEPRIVALOMAS. Jei jis naudojamas, jame TURI būti nurodytos vietos, kuriose skelbiamas galiojantis PUPSS forma rengiamas PS ir kuriose galima rasti galiojančio PUPSS naujinius. Jei nurodomi keli paskirstymo taškai, juose visuose PRIVALO būti pateiktos vienodos galiojančio PUPSS arba atnaujintos jo versijos kopijos. Jei šis laukas naudojamas, jo formatas turi būti netuščia eilučių seka, o kiekviena eilutė turi atitikti RFC 3986 ([1]).

Scheme extensions (5.3.17 punktas)

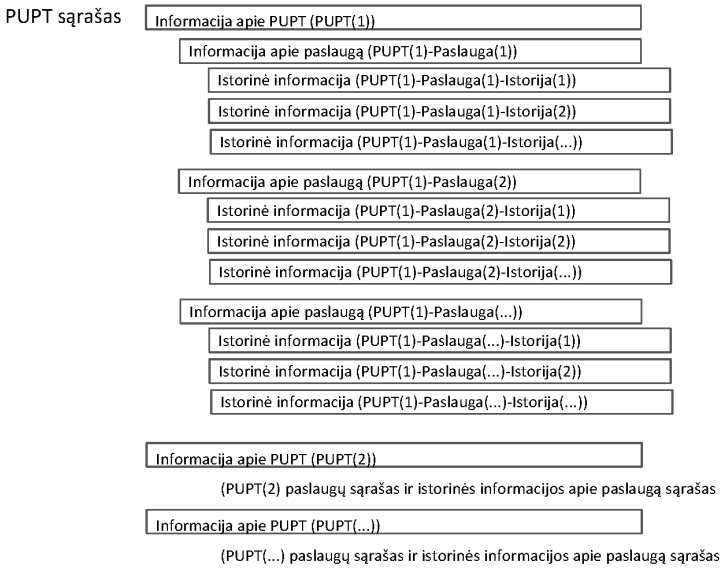
Šis laukas NEPRIVALOMAS, pagal šias specifikacijas jis nenaudojamas.

List of Trust Service Providers

Šis laukas NEPRIVALOMAS.

Jei valstybėje narėje pagal schemą prižiūrimų ir (arba) akredituotų SPT nėra arba nebuvo, šis laukas NETURI būti teikiamas. Tačiau sutarta, kad net jei valstybėje narėje nėra pagal schemą prižiūrimų ir (arba) akredituotų SPT, valstybės narės TURI parengti PUPSS be šio lauko. Jei sąraše nenurodytas nė vienas SPT, TURI būti suprantama, kad šalyje, nurodytoje lauke „Schemos teritorija“, prižiūrimų ir (arba) akredituotų SPT nėra.

Jeigu pagal schemą yra arba buvo prižiūrimos ir (arba) akredituotos viena arba daugiau SPT paslaugų, šiame lauke TURI būti pateikta seka, kurioje nurodomas kiekvienas SPT, teikiantis vieną arba daugiau tų prižiūrimų ir (arba) akredituotų paslaugų, taip pat išsami informacija apie kiekvienos SPT paslaugos priežiūros ir (arba) akreditacijos statusą ir statuso istorija (toliau pateiktame paveiksle PUPT = SPT).



([1]) IETF RFC 3986: „Universalusis išteklių identifikatorius (URI). Bendroji sintaksė“ (angl. *Uniform Resource Identifiers (URI): Generic syntax*).

▼C1

PUPT sąrašas sudaromas taip, kaip pavaizduota pirmiau pateiktame paveiksle. Pateikiama kiekvieno PUPT laukų, kuriuose saugoma informacija apie PUPT („TSP Information“), seka ir paslaugų sąrašas. Taip pat pateikiama kiekvienos tokios į sąrašą įtrauktos paslaugos laukų, kuriuose saugoma informacija apie paslaugą („Service Information“), seka ir laukų, kuriuose pateikiama paslaugos patvirtinimo statuso istorija („Service approval history“), seka.

TSP Information

PUPT(1)

TSP name (5.4.1 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodytas **juridinio asmens**, atsakingo už SPT paslaugas, kurios yra arba buvo prižiūrimos arba akredituotos pagal schemą, pavadinimas. Tai įvairiakalbių ženklų eilučių seka (privaloma kalba – anglų (EN), taip pat gali būti naudojama viena arba daugiau nacionalinių kalbų). Tai PRIVALO būti pavadinimas, naudojamas oficialiuose teisiniuose registruose ir siunčiant oficialius pranešimus.

TSP trade name (5.4.2 punktas)

Šis laukas NEPRIVALOMAS; jei jis naudojamas, jame TURI būti nurodytas kitas pavadinimas, kuriuo SPT vadinasi teikdamas tas paslaugas, kurios yra nurodytos PUPSS ir susietos su jo įrašu „PUPT pavadinimas“ (5.4.1 punktas).

Pastaba: jei vienas SPT juridinis asmuo teikia paslaugas naudodamas įvairius prekės pavadinimus arba įvairiomis specifinėmis aplinkybėmis, SPT įrašų gali būti tiek, kiek yra tų specifinių aplinkybių (pvz., pavadinimo ir (arba) prekės pavadinimo įrašų). Kita galimybė – kiekvieną SPT (juridinį asmenį) sąraše nurodyti tik vieną kartą ir pateikti konkrečią informaciją apie paslaugos teikimo aplinkybes. Dėl tinkamiausio būdo valstybės narės schemos operatorius turi pasitarti su SPT ir priimti bendrą sprendimą.

TSP address (5.4.3 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodytas juridinio asmens arba įgaliotosios organizacijos, nurodytos lauke „TSP name“ (5.4.1 punktas), pašto ir elektroninio pašto adresas. Šiame lauke TURI būti nurodytas „PostalAddress“ (t. y. namo numeris, gatvė, vietovė, [sritis arba rajonas], [pašto kodas] ir ISO 3166–1 dviejų raidžių šalies kodas), kaip nurodyta 5.3.5.1 punkte, ir „ElectronicAddress“ (t. y. e. paštas ir (arba) interneto svetainės UII), kaip nurodyta 5.3.5.2 punkte.

TSP information URI (5.4.4 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodytas (-i) UII, pagal kurį (-iuos) naudotojai (pvz., susijusios šalys) gali gauti specifinės informacijos apie SPT. Šis laukas TURI būti sudarytas iš įvairiakalbių nuorodų sekos (privaloma kalba – anglų (EN), taip pat gali būti naudojama viena arba daugiau nacionalinių kalbų). Nurodytu (-ais) UII PRIVALO būti pateikta nuoroda į informaciją apie SPT bendrąsias veiklos sąlygas, jo taikomą praktiką, teisinius klausimus, klientų aptarnavimo politiką ir kitą bendrą informaciją apie visas jo paslaugas, nurodytas PUPSS ir susietas su atitinkamu SPT įrašu.

Pastaba: jei vienas SPT juridinis asmuo teikia paslaugas naudodamas įvairius prekės pavadinimus arba įvairiomis specifinėmis aplinkybėmis, ir padaryta tiek PUPT įrašų, kiek yra tų specifinių aplinkybių, šiame lauke TURI būt pateikta informacija apie specifinį paslaugų, nurodytų sąraše ir susietų su PUPT ir (arba) prekės pavadinimo įrašu, rinkinį.

▼C1

TSP information extensions (5.4.5 punktas)

Šis laukas NEPRIVALOMAS; jei jis teikiamas, schemos operatorius, laikydamasis ETSI TS 102 231 specifikacijų (5.4.5 punktas), GALI jį naudoti specifinei informacijai, aiškinamai pagal konkrečios schemos taisykles, pateikti.

List of Services

Šis laukas PRIVALOMAS; jame TURI būti pateikta seka, kurioje nurodoma kiekviena pripažinta SPT teikiama paslauga ir jos patvirtinimo statusas (ir to statuso istorija). Turi būti nurodyta bent viena paslauga (net jei saugoma informacija yra tik istorinė).

Kadangi pagal šias specifikacijas PRIVALOMA saugoti istorinę informaciją apie sąraše nurodomas paslaugas, ši istorinė informacija PRIVALO būti saugoma net ir tokiu atveju, jei atsižvelgiant į dabartinį paslaugos statusą įprastai jos nereikėtų įtraukti į sąrašą (pvz., jei paslauga buvo atšaukta). Taigi kad būtų išsaugota istorija, SPT PRIVALO būti įtrauktas į sąrašą, net jei jo vienintelės sąraše nurodomos paslaugos statusas yra toks, kaip minėta.

Service Information

►C2 *TSP(1) Service(1)* ◄

Service type identifier (5.5.1 punktas)

▼M1

Šis laukas PRIVALOMAS; jame TURI būti nurodytas paslaugos rūšies identifikatorius, atitinkantis šių PUPSS specifikacijų tipą (t. y. „/eSigDir-1999–93-EC-TrustedList/TSLType/generic“).

▼C1

Jei sąraše nurodyta paslauga yra susijusi su kvalifikuotų sertifikatų išdavimu, TURI būti nurodomas UII http://uri.etsi.org/TrstSvc/Svctype/CA/QC (kvalifikuotus sertifikatus išduodanti sertifikavimo institucija).

Jei sąraše nurodyta paslauga yra susijusi su patikimumo užtikrinimo paslaugos žymomis, kurios nėra KS ir kurias teikiant KS neišduodami, TURI būti nurodomas vienas iš UII, nustatytų ETSI 102 231 ir nurodytų D.2 punkte, susijusiame su šiuo lauku. Ši nuostata TURI būti taikoma ir toms patikimumo užtikrinimo paslaugos žymoms, kurios yra prižiūrimos ir (arba) akredituotos siekiant užtikrinti atitiktį tam tikroms specifinėms kvalifikacijoms, nustatytoms valstybių narių nacionaliniuose teisės aktuose (pvz., Vokietijoje arba Vengrijoje naudojamiems kvalifikuotiems laiko fiksavimo ženklams); TURI būti nurodomas vienas iš UII, nustatytų ETSI 102 231 ir nurodytų D.2 punkte, susijusiame su šiuo lauku (pvz., laiko fiksavimo institucija, išduodanti nacionaliniu mastu nustatytas kvalifikuotas laiko fiksavimo žymas). Jei taikoma, ši specifinė nacionalinė patikimumo užtikrinimo paslaugų žymų kvalifikacija GALI būti nurodyta paslaugos įraše; šiuo tikslu 5.5.9 punkte („Informacijos apie paslaugą plėtinys“) TURI būti naudojamas plėtinys „Papildoma informacija apie paslaugą“ (5.8.2 punktas).

▼C1

Paprastai taikomas numatytasis principas, kad sąraše nurodant į patikimą sąrašą įtrauktų SPT (pvz., sertifikavimo institucijos, (tiesiogiai) išduodančios KS) teikiamas sertifikavimo paslaugas, TURI būti nurodomas vienas vieno X.509v3 sertifikato (pvz., išduodamo SI/KS tipo sertifikavimo paslaugai) įrašas. Tam tikromis tiksliai numatytomis aplinkybėmis ir rūpestingai kontroliuojamomis ir patvirtintomis sąlygomis valstybės narės priežiūros arba akreditacijos įstaiga GALI nuspręsti naudoti pagrindinės arba aukštesniojo lygmens SI (pvz., sertifikavimo institucijos, tiesiogiai neišduodančios galutiniams subjektams skirtų KS, bet patvirtinančios SI hierarchiją nuo viršaus iki SI, išduodančių KS galutiniams subjektams) X.509v3 sertifikatą, kaip į sąrašą įtrauktų SPT teikiamų paslaugų sąraše esančio vienintelio įrašo „Sdi“. Valstybės narės turi išsamiai apsvarstyti ir patvirtinti šių pagrindinės arba aukštesniojo lygmens SI X.509v3 sertifikatų naudojimo patikimame sąraše nurodytų paslaugų įrašų „Sdi“ vertėms pateikti padarinius (pranašumus ir trūkumus) ([1]). Be to, valstybės narės, taikydamos šią leidžiamą numatytojo principo išimtį, PRIVALO pateikti reikiamus dokumentus, padedančius nustatyti sertifikavimo kelią ir atlikti patikras.

Pastaba: naudojant toliau nurodytą UII derinį, šioje PUPSS formoje taip pat GALI būti nurodyti tokie PUPT, kaip OCSP atsakovai arba CRL teikėjai, kurie dalyvauja teikiant SPT_{KS} sertifikavimo paslaugas ir privalo naudoti atskirų raktų poras, kad pasirašytų atitinkamai OCSP atsakus ir CRL:

— „Paslaugos rūšies identifikatoriaus“ (5.5.1 punktas) reikšmė

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

derinama su toliau nurodyta „Informacijos apie paslaugą plėtinio“ (5.5.9 punktas) „Papildoma informacija apie paslaugą“ (5.8.2 punktas) reikšme

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Aprašas – sertifikato statuso teikėjas, naudojantis OCSP tarnybinę stotį kvalifikuotus sertifikatus išduodančio sertifikavimo paslaugų teikėjo paslaugai teikti.

— „Paslaugos rūšies identifikatoriaus“ (5.5.1 punktas) reikšmė

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

derinama su toliau nurodyta „Informacijos apie paslaugą plėtinio“ (5.5.9 punktas) „Papildoma informacija apie paslaugą“ (5.8.2 punktas) reikšme

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Aprašas – sertifikato statuso teikėjas, naudojantis CRL kvalifikuotus sertifikatus išduodančio sertifikavimo paslaugų teikėjo paslaugai teikti.

— „Paslaugos rūšies identifikatoriaus“ (5.5.1 punktas) reikšmė

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

([1]) Naudodamas pagrindinės SI X.509v3 sertifikatus sąraše nurodytų paslaugų įrašų „Sdi“ vertėms perteikti, schemos operatorius, atsižvelgdamas į priežiūros ir (arba) akreditacijos statusą, turės visas pagrindinei SI vadovaujant teikiamas sertifikavimo paslaugas vertinti kaip visumą. Pvz., dėl kokio nors statuso pakeitimo, reikalingo atskirai SI pagal sąraše nurodytą pagrindinę hierarchiją, statusas pasikeis visoje hierarchijoje.

▼C1

derinama su toliau nurodyta „Informacijos apie paslaugą plėtinio“ (5.5.9 punktas) „Papildoma informacija apie paslaugą“ (5.8.2 punktas) reikšme

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Aprašas – pagrindinė sertifikavimo institucija, nuo kurios galima nustatyti sertifikavimo kelią iki kvalifikuotus sertifikatus išduodančios sertifikavimo institucijos.

— „Paslaugos rūšies identifikatoriaus“ (5.5.1 punktas) reikšmė

http://uri.etsi.org/TrstSvc/Svctype/TSA

derinama su toliau nurodyta „Informacijos apie paslaugą plėtinio“ (5.5.9 punktas) „Papildoma informacija apie paslaugą“ (5.8.2 punktas) reikšme

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Aprašas – laiko fiksavimo paslauga, teikiama teikiant sertifikavimo paslaugų teikėjo, išduodančio kvalifikuotus sertifikatus, paslaugą, kurią teikiant išduodama laiko fiksavimo žyma (LFŽ), kurią galima naudoti taikant kvalifikuoto parašo patikros procedūrą, siekiant įsitikinti parašo tikrumu ir pratęsti jo galiojimą, kai KS panaikinamas arba baigiasi jo galiojimas.

Service name (5.5.2 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodytas pavadinimas, kurį naudodamas lauke „TSP name“ (5.4.1 punktas) nurodytas SPT teikia paslaugą, nurodytą lauke „Service type identifier“ (5.5.1 punktas). Šis laukas TURI būti sudarytas iš įvairiakalbių ženklų eilučių sekos (privaloma kalba – anglų (EN), taip pat gali būti naudojama viena arba daugiau nacionalinių kalbų).

Service digital identity (5.5.3 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodytas bent vienas unikalus paslaugos, kurios rūšis nurodyta lauke „Service type identifier“ (5.5.1 punktas), skaitmeninis identifikatorius, pagal kurį galima aiškiai identifikuoti paslaugą.

Pagal šias specifikacijas šiame lauke naudojamas skaitmeninis identifikatorius TURI būti atitinkamas X.509v3 sertifikatas, teikiamas kaip viešasis (-ieji) raktas (-ai), kurį (-iuos) SPT naudoja teikdamas paslaugą, kurios rūšis nurodyta lauke „Service type identifier“ (5.5.1 punktas) (t. y. raktas, kurį naudoja pagrindinė SI/KS, arba raktas, naudojamas sertifikatams pasirašyti ([1]) arba laiko fiksavimo žymoms išduoti, arba CRL ar OCSP atsakams pasirašyti). Šis susijęs X.509v3 sertifikatas TURI būti naudojamas kaip būtinasis skaitmeninis identifikatorius (teikiamas kaip viešasis (-ieji) raktas (-ai), kurį (-iuos) SPT naudoja teikdamas sąraše nurodytą paslaugą). GALI būti naudojami papildomi toliau nurodyti identifikatoriai, tačiau visi jie PRIVALO būti susieti su tuo pačiu identifikatoriumi (t. y. su atitinkamu X.509v3 sertifikatu):

([1]) Tai gali būti SI, išduodančios galutiniam subjektui skirtus sertifikatus (pvz., SI/VRS, SI/KS), sertifikatas **arba** patikimos pagrindinės SI, nuo kurios galima atsekti kelią iki galutiniam subjektui skirtų kvalifikuotų sertifikatų, sertifikatas. Atsižvelgiant į tai, ar šią informaciją ir informaciją, teikiamą kiekvienam galutiniam subjektui skirtame sertifikate, išduotame vadovaujant šiai patikimai pagrindinei SI, galima naudoti siekiant aiškiai nustatyti atitinkamas bet kurio kvalifikuoto sertifikato ypatybes, šią informaciją („Paslaugos skaitmeninis identifikatorius“) gali reikėti papildyti „Informacijos apie paslaugą plėtinių“ duomenimis (žr. 5.5.9 punktą).

▼C1

a) sertifikato išskirtinis pavadinimas (IP), kuris gali būti naudojamas su SPT paslauga, nurodyta lauke „Service type identifier“ (5.5.1 punktas), susijusiems elektroniniams parašams tikrinti;

b) susijęs viešojo rakto identifikatorius (t. y. X.509v3 „Subjekto rakto identifikatoriaus“ (angl. *SubjectKeyIdentifier*) arba SKI reikšmė);

c) susijęs viešasis raktas.

Paprastai taikomas numatytasis principas, kad patikimame sąraše skaitmeninis identifikatorius (t. y. susijęs X.509v3 sertifikatas) NETURI būti teikiamas daugiau kaip vieną kartą, t. y. vienam X.509v3 sertifikatui, kuris išduodamas sertifikavimo paslaugai kaip vienai iš sąraše nurodytų sertifikavimo paslaugų, kurias teikia į patikimą sąrašą įtrauktas SPT, TURI būti teikiamas vienas įrašas. Ir atvirkščiai – viename paslaugos įraše „Sdi“ reikšmei nurodyti TURI būti naudojamas tik vienas X.509v3 sertifikatas.

Pastaba (1). Minėtasis bendras numatytasis principas gali būti netaikomas tik tokiu atveju, jei išduodant įvairių tipų patikimumo užtikrinimo paslaugų žymas, kurioms taikomos skirtingos priežiūros ir (arba) akreditacijos schemos, naudojamas vienas X.509v3 sertifikatas, pvz., kai SPT, pagal atitinkamą priežiūros sistemą išduodamas KS arba išduodamas nekvalifikuotus sertifikatus, kurių priežiūros ir (arba) akreditacijos statusas yra skirtingas, naudoja vieną X.509v3 sertifikatą. Šiuo atveju pagal minėtą pavyzdį turėtų būti naudojami du įrašai su skirtingomis „Sti“ reikšmėmis (pvz., pagal pateiktą pavydį – atitinkamai SI/KS ir SI/VRS) ir ta pačia „Sdi“ reikšme (susijęs X.509v3 sertifikatas).

Įgyvendinimo būdas priklauso nuo to, ar naudojama ASN.1, ar XML, ir TURI atitikti ETSI TS 102 231 specifikacijas (jei naudojama ASN.1, žr. ETSI TS 102 231 A priedą, jei XML – ETSI TS 102 231 B priedą).

Pastaba (2). Jei reikia pateikti papildomos informacijos apie kvalifikaciją, susijusią su tam tikru paslaugos įrašu, kai tinka, schemos operatorius, atsižvelgdamas į tokios papildomos informacijos apie kvalifikaciją teikimo tikslą, TURI apsvarstyti galimybę naudoti lauko „Service information extension“ (5.5.9 punktas) plėtinį „Papildoma informacija apie paslaugą“ (5.8.2 punktas). Be to, schemos operatorius savanoriškai gali naudoti 5.5.6 punktą („Pagal schemą teikiamos paslaugos apibrėžties UII“).

Service current status (5.5.4 punktas)

Šis laukas PRIVALOMAS; jame, naudojant vieną iš toliau nurodytų UII, TURI būti nurodytas paslaugos statuso identifikatorius:

▼C2

— Under Supervision (prižiūrima) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision);

— Supervision of Service in Cessation (paslaugos priežiūra baigiama) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/-supervisionincessation);

— Supervision Ceased (priežiūra pasibaigusi) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— Supervision Revoked (priežiūra panaikinta) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked;

— Accredited (akredituota) (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited);

— Accreditation Ceased (akreditacija pasibaigusi) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— Accreditation Revoked (akreditacija panaikinta) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

Pagal šias patikimo sąrašo specifikacijas pirmiau nurodytos statuso reikšmės TURI būti aiškinamos taip:

– ***prižiūrima***– sertifikavimo paslaugų teikėjo (SPT), nurodyto lauke „TSP name“ (5.4.1 punktas), teikiamą paslaugą, nurodytą lauke „Service digital identity“ (5.5.3 punktas), siekdama užtikrinti Direktyvos 1999/93/EB nuostatų laikymąsi, dabar prižiūri lauke „Scheme territory“ (5.3.10 punktas) nurodyta valstybė narė, kurioje yra įsisteigęs SPT;

▼M1

- ***Paslaugos priežiūra baigiama***– lauke „TSP name“ (5.4.1 punktas) nurodytas SPT baigia teikti lauke „Service digital identity“ (5.5.3 punktas) nurodytą paslaugą, tačiau ta paslauga vis dar prižiūrima, kol priežiūra bus nutraukta arba panaikinta. Jei atsakomybę už šį baigiamąjį etapą prisiėmė ne lauke „TSP name“ nurodytas juridinis asmuo, šio naujo arba atsarginio juridinio asmens (atsarginio SPT) identifikatorius TURI būti nurodytas šios paslaugos įrašo lauke „Scheme service definition URI“ (5.5.6 punktas) ir plėtinyje „TakenOverBy“ (L.3.2 punktas);

▼C1

– ***priežiūra pasibaigusi***– užtikrinant priežiūrą atliekamo vertinimo galiojimas baigėsi, o naujas lauke „Service digital identity“ (5.5.3 punktas) nurodytos paslaugos vertinimas neatliktas. Nuo dabartinio statuso įsigaliojimo dienos paslauga nebeprižiūrima, nes tariama, kad su šia paslauga susijusios operacijos nebeatliekamos;

– ***priežiūra panaikinta***– lauke „Scheme territory“ (5.3.10 punktas) nurodyta valstybė narė, kurioje yra įsisteigęs SPT, nustatė, kad anksčiau prižiūrėta SPT teikiama paslauga ir galbūt pats SPT nebeatitinka Direktyvos 1999/93/EB nuostatų. Todėl pareikalauta, kad su paslauga susijusios operacijos būtų nutrauktos, ir dėl šios priežasties turi būti tariama, kad paslaugos teikimas nutrauktas.

Pastaba (1). Statuso reikšmė „Priežiūra panaikinta“ gali būti galutinė, net jei SPT vėliau visiškai nutraukia veiklą; tokiu atveju nebūtina šį statusą pakeisti statusu „Paslaugos priežiūra baigiama“ arba „Priežiūra pasibaigusi“. Iš tiesų vienintelis būdas pakeisti statusą „Priežiūra panaikinta“ yra vėl pradėti laikytis Direktyvos 1999/93/EB nuostatų, kurių nebuvo laikomasi, atsižvelgiant į atitinkamą priežiūros sistemą, galiojančią PS tvarkančioje valstybėje narėje, ir susigrąžinti statusą „Prižiūrima“. Statusas „Paslaugos priežiūra baigiama“ arba „Priežiūra pasibaigusi“ naudojamas tik tada, kai SPT pats nustoja teikti susijusias prižiūrimas paslaugas, o ne tada, kai priežiūra panaikinama.

– ***akredituota***– akreditacijos įstaiga valstybės narės, nurodytos lauke „Schemos teritorija“ (5.3.10 punktas), vardu atliko vertinimą ir nustatė, kad sertifikavimo paslaugų teikėjo ([1]), nurodyto lauke „TSP name“ (5.4.1 punktas), teikiama paslauga, nurodyta lauke „Service digital identity“ (5.5.3 punktas), atitinka Direktyvos 1999/93/EB nuostatas.

([1]) Atminkite, kad šis akredituotas SPT gali būti įsisteigęs ne valstybėje narėje, kuri nurodyta PUPSS forma rengiamo PS lauke „Schemos teritorija“, o kitoje valstybėje narėje arba trečiojoje šalyje (žr. Direktyvos 1999/93/EB 7 straipsnio 1 dalies a punktą).

▼C1

Pastaba (2). Kai tai susiję su KS išduodančiais SPT, įsisteigusiais „Scheme territory“ (5.3.10 punktas), statuso reikšmės „Akreditacija panaikinta“ ir „Akreditacija pasibaigusi“ PRIVALO būti laikomos pereinamojo statuso reikšmėmis ir PRIVALO būti nenaudojamos kaip dabartinio paslaugos statuso reikšmės, nes, kai jos naudojamos, lauke „Informacija apie paslaugos patvirtinimo istoriją“ (angl. *Service approval history information*) arba lauke „Dabartinis paslaugos statusas“ jos turi būti nedelsiant pakeistos statuso reikšme „Prižiūrima“ ir galbūt kita priežiūros statuso reikšme, apibrėžta pirmiau ir nurodyta 1 paveiksle. Kai tai susiję su KS neišduodančiais SPT ir kai yra tik susijusi savanoriškos akreditacijos schema, bet nėra susijusios priežiūros schemos, arba kai tai susiję su KS išduodančiais SPT, kurie nėra įsisteigę „Scheme territory“ (5.3.10 punktas) (pvz., įsisteigę trečiojoje šalyje), minėtos statuso reikšmės „Akreditacija panaikinta“ ir „Akreditacija pasibaigusi“ GALI būti naudojamos kaip dabartinio paslaugos statuso reikšmės.

– ***akreditacija pasibaigusi***– suteikiant akreditaciją atliekamo vertinimo galiojimas baigėsi, o naujas lauke „Service digital identity“ (5.5.3 punktas) nurodytos paslaugos vertinimas neatliktas;

– ***akreditacija panaikinta***– sertifikavimo paslaugų teikėjo (SPT), nurodyto lauke „TSP name“ (5.4.1 punktas), teikiama paslauga, nurodyta lauke „Service digital identity“ (5.5.3 punktas), ir galbūt pats SPT, pirmiau atitikę schemos kriterijus, nebeatitinka Direktyvos 1999/93/EB nuostatų.

Pastaba (3). Sertifikavimo paslaugų teikėjams, išduodantiems KS, ir sertifikavimo paslaugų teikėjams, neišduodantiems KS (pvz., laiko fiksavimo paslaugos teikėjams, išduodantiems LFŽ, sertifikavimo paslaugų teikėjams, išduodantiems nekvalifikuotus sertifikatus, ir t. t.), turi būti taikomos tokios pačios statuso reikšmės. Taikomoms priežiūros ir (arba) akreditacijos sistemoms išskirti turi būti naudojamas „Service Type identifier“ (5.5.1 punktas).

Pastaba (4). Kai reikia ir reikalaujama (pvz., norint išskirti keletą kokybės ir (arba) saugumo lygmenų), apie kiekvieną paslaugą GALI būti teikiama papildoma su statusu susijusi informacija apie kvalifikaciją, nustatyta pagal nacionalines priežiūros ir (arba) akreditacijos sistemas, taikomas KS neišduodantiems sertifikavimo paslaugų teikėjams. Šiai papildomai su kvalifikacija susijusiai informacijai pateikti schemų operatoriai TURI naudoti lauko „Service information extension“ (5.5.9 punktas) plėtinį „Papildoma informacija apie paslaugą“ (5.8.2 punktas). Be to, schemos operatorius savanoriškai gali naudoti 5.5.6 punktą („Pagal schemą teikiamos paslaugos apibrėžties UII“)

Current status starting date and time (5.5.5 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodyta dabartinio patvirtinimo statuso įsigaliojimo data ir laikas (naudojant datos ir laiko reikšmę, kurios reikalavimai nustatyti ETSI TS 102 231 5.1.4 punkte).

Scheme service definition URI (5.5.6 punktas)

Šis laukas NEPRIVALOMAS; jei jis teikiamas, jame TURI būti nurodytas (-i) UII, kurį (-iuos) naudodamos susijusios šalys gali gauti schemos operatoriaus įvairiakalbių nuorodų sekos pavidalu (privaloma kalba – anglų (EN), taip pat gali būti naudojama viena arba daugiau nacionalinių kalbų) teikiamos specifinės informacijos apie paslaugą.

Jei šis laukas naudojamas, nurodytu (-ais) UII PRIVALO būti pateikta nuoroda į informaciją, apibūdinančią paslaugą, kaip nurodyta pagal schemą. Pirmiausia, jei tinka, GALI būti teikiama ši informacija:

a) UII, kuriuo nurodomas atsarginio SPT, jei paslaugos priežiūra baigiama ir į šį procesą įtraukiamas atsarginis SPT, identifikatorius (žr. „Service current status“, 5.5.4 punktas);

▼C1

b) UII, kuriuo nurodomi dokumentai, kuriuose, atsižvelgiant į lauko „Informacijos apie paslaugą plėtinys“ (5.5.9 punktas) plėtinio „Papildoma informacija apie paslaugą“, apibrėžto 5.8.2 punkte, naudojimą, teikiama papildoma informacija apie tam tikros nacionaliniu mastu nustatytos specifinės kvalifikacijos taikymą prižiūrimai ir (arba) akredituotai patikimumo užtikrinimo paslaugos žymos teikimo paslaugai.

Service supply points (5.5.7 punktas)

Šis laukas NEPRIVALOMAS; jei jis teikiamas, jame, naudojant ženklų eilučių, kurių sintaksė PRIVALO atitikti RFC 3986, seką, TURI būti nurodytas (-i) UII, kurį (-iuos) naudodamos susijusios šalys gali pasinaudoti paslauga.

TSP service definition URI (5.5.8 punktas)

Šis laukas NEPRIVALOMAS; jei jis teikiamas, jame TURI būti nurodytas (-i) UII, kurį (-iuos) naudodamos susijusios šalys gali gauti įvairiakalbių nuorodų sekos pavidalu PUPT teikiamos specifinės informacijos apie paslaugą (privaloma kalba – anglų (EN), taip pat gali būti naudojama viena arba daugiau nacionalinių kalbų). Nurodytu (-ais) UII PRIVALO būti pateikta nuoroda į informaciją, apibūdinančią paslaugą, kaip nurodė PUPT.

Service information extensions (5.5.9 punktas)

Pagal šias specifikacijas šis laukas NEPRIVALOMAS, tačiau TURI būti teikiamas, kai informacijos, pateiktos lauke „Service digital identity“ (5.5.3 punktas), nepakanka, kad būtų galima aiškiai identifikuoti kvalifikuotus sertifikatus, išduodamus teikiant šią paslaugą, ir (arba) kai remiantis informacija, pateikta atitinkamuose kvalifikuotuose sertifikatuose, neįmanoma techninėmis priemonėmis nustatyti, ar KS patvirtinamas naudojant SPFĮ ([1]).

Pagal šias specifikacijas, kai tai PRIVALOMA, pvz., jei tai SI/KS paslaugos, neprivalomas informacijos laukas „Service information extensions“ („Sie“) TURI būti naudojamas ir sudaromas pagal plėtinio „Kvalifikacijos“ reikalavimus, nustatytus ETSI TS 102 231 L priedo 3.1 skirsnyje, teikiant vieną arba daugiau baigtinių sekų, iš kurių kiekvienoje nurodoma:

— (filtrų) informacija, naudotina pagal „Sdi“ apibrėžtai sertifikavimo paslaugai papildomai apibrėžti, kad būtų galima nustatyti konkrečią paslaugą (t. y. kvalifikuotų sertifikatų rinkinį), apie kurią reikia pateikti arba apie kurią pateikta papildomos informacijos apie SPFĮ (ne)naudojimą (ir (arba) sertifikato išdavimą juridiniam asmeniui); ir

— susijusi informacija (kvalifikatoriai) apie tai, ar šis papildomai apibrėžtas paslaugų, kurias teikiant išduodami kvalifikuoti sertifikatai, rinkinys patvirtinamas naudojant SPFĮ (kai ši informacija yra „QCSSCDStatusAsInCert“, tai reiškia, kad ši susijusi informacija yra KS dalis, rengiama ETSI standartizuota, techninėmis priemonėmis apdorojama forma ([2]), ir (arba) informacija apie tai, ar šie KS išduodami juridiniam asmeniui (paprastai tariama, kad KS išduodami tik fiziniams asmenims).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD) – tai reiškia, kad SPT užtikrina, o valstybė narė (atitinkamai jos priežiūros arba akreditacijos įstaiga) kontroliuoja (pagal priežiūros modelį) arba tikrina (pagal akreditacijos modelį), jog visi KS, išduoti teikiant paslaugą (QCA), nurodytą lauke „Service digital identity“ (5.5.3 punktas) ir papildomai apibrėžtą naudojant minėtą (filtrų) informaciją, naudojamą pagal „Sdi“ apibrėžtai sertifikavimo paslaugai papildomai apibrėžti, siekiant nustatyti konkretų kvalifikuotų sertifikatų, apie kuriuos reikia pateikti su SPFĮ naudojimu susijusios papildomos informacijos, rinkinį, **YRA** patvirtinami naudojant SPFĮ (t. y. privatusis raktas, susietas su viešuoju sertifikate pateiktu raktu, yra saugomas saugioje parašo formavimo įrangoje, atitinkančioje Direktyvos 1999/93/EB III priede nustatytus reikalavimus);

([1]) Žr. šio dokumento 2.2 skirsnį.

([2]) Tai reiškia atitinkamą ETSI nustatyto KS atitikties patvirtinimo, KS SPFĮ patvirtinimų [ETSI TS 101 862] arba ETSI nustatytų KSP/KSP + OID [ETSI TS 101 456] derinį.

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD) – tai reiškia, kad SPT užtikrina, o valstybė narė (atitinkamai jos priežiūros arba akreditacijos įstaiga) kontroliuoja (pagal priežiūros modelį) arba tikrina (pagal akreditacijos modelį), jog visi KS, išduodami teikiant paslaugą (pagrindinės SI/KS arba SI/KS), nurodytą lauke „Service digital identity“ (5.5.3 punktas) ir papildomai apibrėžtą naudojant minėtą (filtrų) informaciją, naudojamą pagal „Sdi“ apibrėžtai sertifikavimo paslaugai papildomai apibrėžti, siekiant nustatyti konkretų kvalifikuotų sertifikatų, apie kuriuos reikia pateikti su SPFĮ naudojimu susijusios papildomos informacijos, rinkinį, **NĖRA** tvirtinami naudojant SPFĮ (t. y. privatusis raktas, susietas su viešuoju sertifikate pateiktu raktu, **nėra** saugomas saugioje parašo formavimo įrangoje, atitinkančioje Direktyvos 1999/93/EB III priede nustatytus reikalavimus).

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert) – tai reiškia, kad SPT užtikrina, o valstybė narė (atitinkamai jos priežiūros arba akreditacijos įstaiga) kontroliuoja (pagal priežiūros modelį) arba tikrina (pagal akreditacijos modelį), jog visuose KS, išduodamuose teikiant paslaugą (SI/KS), nurodytą lauke „Service digital identity“ (5.5.3 punktas) ir papildomai apibrėžtą naudojant minėtą (filtrų) informaciją, naudojamą pagal „Sdi“ apibrėžtai sertifikavimo paslaugai papildomai apibrėžti, siekiant nustatyti konkretų kvalifikuotų sertifikatų, apie kuriuos reikia pateikti su SPFĮ naudojimu susijusios papildomos informacijos, rinkinį, PATEIKIAMA techninėmis priemonėmis apdorojama informacija apie tai, ar KS patvirtinamas naudojant SPFĮ;

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson) – tai reiškia, kad SPT užtikrina, o valstybė narė (atitinkamai jos priežiūros arba akreditacijos įstaiga) kontroliuoja (pagal priežiūros modelį) arba tikrina (pagal akreditacijos modelį), jog visi KS, išduodami teikiant paslaugą (QCA), nurodytą lauke „Service digital identity“ (5.5.3 punktas) ir papildomai apibrėžtą naudojant minėtą (filtrų) informaciją, naudojamą pagal „Sdi“ apibrėžtai sertifikavimo paslaugai papildomai apibrėžti, siekiant nustatyti konkretų kvalifikuotų sertifikatų, apie kuriuos reikia pateikti papildomos informacijos, ar jie išduodami juridiniam asmeniui, rinkinį, **YRA** išduodami juridiniams asmenims.

Jei paslaugos rūšis yra http://uri.etsi.org/TrstSvc/Svctype/CA/QC, šie kvalifikatoriai turi būti naudojami tik kaip plėtinys.

Šis laukas priklauso nuo įgyvendinimo priemonės (ASN.1 arba XML), jis PRIVALO atitikti specifikacijas, pateiktas ETSI TS 102 231 L priedo 3.1 skirsnyje.

▼M1

Jei naudojama XML, konkretus šios papildomos informacijos turinys turi būti koduojamas naudojant xsd rinkmenas, pateiktas ETSI TS 102 231 C priede.

▼C1

Service Approval History

Šis laukas NEPRIVALOMAS, tačiau jis PRIVALO būti pateiktas, jei lauko „Historical information period“ (5.3.12 punktas) reikšmė nėra nulis. Taigi pagal šias specifikacijas taikant schemą PRIVALO būti saugoma istorinė informacija. Jei istorinę informaciją numatoma saugoti, tačiau istorinės informacijos apie ankstesnį paslaugos statusą nėra (t. y. jei tai pirmasis registruojamas statusas arba jei schemos operatorius neišsaugojo istorinės informacijos), šis laukas TURI būti paliktas tuščias. Kitu atveju kiekvieną kartą, kai per istorinės informacijos laikotarpį, nustatytą ETSI TS 102 231 5.3.12 punkte, pasikeičia PUPT teikiamos paslaugos dabartinis statusas, mažėjančia statuso pasikeitimo datos ir laiko (t. y. nurodant vėlesnio patvirtinimo statuso įsigaliojimo datą ir laiką) reikšmių tvarka TURI būti pateikta informacija apie ankstesnį patvirtinimo statusą.

▼C1

TURI būti naudojama toliau nustatyta istorinės informacijos seka.

▼C2

TSP(1) Service(1) History(1)

▼C1

Service type identifier (5.6.1 punktas)

Šis laukas PRIVALOMAS; jame TURI būti pateiktas paslaugos rūšies identifikatorius, atitinkantis lauke „TSP Service Information – Service type identifier“ (5.5.1 punktas) taikomą formą ir reikšmę.

Service name (5.6.2 punktas)

Šis laukas PRIVALOMAS; jame, naudojant „TSP Service Information – Service name“ (5.5.2 punktas) taikomą formą ir reikšmę, TURI būti nurodytas pavadinimas, kurį naudodamas SPT teikė paslaugą, nurodytą lauke „TSP Service Information – Service type identifier“ (5.5.1 punktas). Pagal šį punktą nereikalaujama, kad pavadinimas būtų toks pats, koks nurodytas 5.5.2 punkte. Pavadinimo pakeitimas GALI būti viena iš aplinkybių, kuriomis reikia suteikti naują statusą.

▼M1

Service digital identity (5.6.3 punktas)

Šis laukas PRIVALOMAS; jame ETSI TS 102 231 5.5.3 punkte nustatyta forma ir naudojant ten pat nustatytą reikšmę, TURI būti nurodytas bent vienas lauke „TSP Service Information – Service digital identity“ (5.5.3 punktas) naudojamas skaitmeninis identifikatorius (t. y. X.509v3 sertifikatas).

Pastaba. Su paslaugos 5.5.3 punkte „Sdi“ naudojama X.509v3 sertifikato reikšme turi būti susijęs vienintelis paslaugos įrašas patikimame sąraše, atitinkantis vieną „Sti:Sie/additionalServiceInformation“ reikšmę. Su paslaugos įrašu susijusioje informacijoje apie paslaugos patvirtinimo istoriją naudojama „Sdi“ (5.6.3 punktas) informacija ir tame paslaugos įraše naudojama „Sdi“ (5.5.3 punktas) informacija PRIVALO būti susijusios su ta pačia X.509v3 sertifikato reikšme. Jei keičiamas į sąrašą įtrauktos paslaugos „Sdi“ (t. y. atnaujinamas arba iš naujo pritaikomas, pavyzdžiui, CA/PKC arba CA/QC X.509v3 sertifikatas) arba sukuriamas naujas tokios paslaugos „Sdi“, net jei susijusios „Sti“, „Sn“ ir [„Sie“] reikšmės yra identiškos, „Scheme Operator“ (schemos operatorius) PRIVALO sukurti su ankstesniu nesutampantį paslaugos įrašą.

▼C1

Service previous status (5.6.4 punktas)

Šis laukas PRIVALOMAS; jame TURI būti pateiktas ankstesnio paslaugos statuso identifikatorius, atitinkantis lauke „TSP Service Information – Service current status“ (5.5.4 punktas) taikomą formą ir reikšmę.

Previous status starting date and time (5.6.5 punktas)

Šis laukas PRIVALOMAS; jame, naudojant lauke „TSP Service Information – Service current status starting date and time“ (5.5.5 punktas) taikomą formą ir reikšmę, TURI būti nurodyta ankstesnio paslaugos statuso įsigaliojimo data ir laikas.

Service information extensions (5.6.6 punktas)

Šis laukas NEPRIVALOMAS; jį schemos operatoriai GALI naudoti specifinei informacijai apie paslaugą pateikti, naudodami lauke „TSP Service Information – Service information extensions“ (5.5.9 punktas) taikomą formą ir reikšmę.

▼C2

TSP(1) Service(1) History(2)

Taip pat, kaip TSP(1) Service(1) History(2) (iki History1)

…

TSP(1) Service(2)

Taip pat, kaip TSP(1) Service 2 (jei taikoma)

TSP(1)Service(2)History(1)

…

TSP(2) Information

Taip pat, kaip TSP 2 (jei taikoma)

Taip pat, kaip TSP 2 Service 1

Taip pat, kaip TSP 2 Service 1 History 1

▼M1

Signed TSL

Siekiant užtikrinti pagal šias specifikacijas, visų pirma pagal IV skyrių sudaryto žmonėms suprantamos PUPSS formos patikimo sąrašo autentiškumą ir vientisumą, šį sąrašą TURĖTŲ pasirašyti asmuo, nurodytas lauke „Scheme operator name“ (5.3.4 punktas) ([1]). Parašo formatas TURĖTŲ būti „PAdES part 3“ (ETSI TS 102 778–3 ([2])), bet GALI būti ir „PAdES part 2“ (ETSI TS 102 778–2 ([3])), jei taikomas specialus patikimumo užtikrinimo modelis, nustatytas paskelbiant patikimiems sąrašams pasirašyti naudojamus sertifikatus.

Siekiant užtikrinti pagal šias specifikacijas sudaryto techninėmis priemonėmis apdorojamos PUPSS formos patikimo sąrašo autentiškumą ir vientisumą, šį sąrašą TURI pasirašyti asmuo, nurodytas lauke „Scheme operator name“ (5.3.4 punktas). Pagal šias specifikacijas sudaryto techninėmis priemonėmis apdorojamos PUPSS formos patikimo sąrašo formatas TURI būti XML ir atitikti ETSI TS 102 231 B ir C prieduose pateiktas specifikacijas.

Parašo formatas TURI būti XAdES BES arba EPES, kaip nustatyta XML formato sąrašų ETSI TS 101903 specifikacijose. Toks elektroninis parašas TURI atitikti ETSI TS 102 231 B priede išdėstytus reikalavimus ([4]). Papildomi bendrieji tokio parašo reikalavimai išdėstyti paskesniuose skirsniuose.

▼C1

Scheme identification (5.7.2 punktas)

Šis laukas PRIVALOMAS; jame TURI būti pateikta schemos operatoriaus nustatyta nuoroda, kuria išskirtinai identifikuojama šiose specifikacijose ir parengtame PUPSS aprašyta schema; šis laukas PRIVALO būti įtrauktas nustatant parašo reikšmę. Numatyta, kad tai bus ženklų eilutė arba bitų eilutė.

([1]) Jei žmonėms suprantama TSL forma parengtas patikimas sąrašas nepasirašomas, jo autentiškumą ir vientisumą PRIVALOMA užtikrinti naudojant tinkamą lygiaverčio saugumo lygio ryšio kanalą. Tuo tikslu rekomenduojama naudoti TLS (IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2“), o valstybė narė PRIVALO atitinkamu kanalu nesinaudojantiems TSL naudotojams pateikti TLS kanalo kontrolinį sertifikato kodą.

([2]) ETSI TS 102 778–3 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778–2 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic – Profile based on ISO 32000–1.

([4]) Schemos operatoriaus parašo sertifikatas turi būti apsaugotas parašu vienu iš ETSI TS 101 903 nustatytų būdų, o „ds:keyInfo“, jei taikoma, turėtų būti atitinkama sertifikatų seka.

▼M1

Pagal šias specifikacijas į nustatytąją nuorodą TURI būti įtraukti šie elementai: „TSL type“ (5.3.3 punktas), „Scheme name“ (5.3.6 punktas) ir sertifikato, kurį schemos operatorius naudoja elektroniniu būdu pasirašydamas PUPSS, plėtinio „SubjectKeyIdentifier“ reikšmė.

▼C1

Signature algorithm identifier (5.7.3 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodytas kriptografinis algoritmas, naudojamas parašui sukurti. Atsižvelgiant į naudojamą algoritmą, šiame lauke GALI reikėti nurodyti papildomus parametrus. Šis laukas PRIVALO būti įtrauktas nustatant parašo reikšmę.

Signature value (5.7.4 punktas)

Šis laukas PRIVALOMAS; jame TURI būti nurodyta faktinė skaitmeninio parašo reikšmė. Nustatant parašo reikšmę, PRIVALO būti įtraukti visi PUPSS laukai (išskyrus pačią parašo reikšmę).

TSL extensions (5.8 punktas)

Plėtinys **expiredCertsRevocationInfo** (5.8.1 punktas)

Šis plėtinys NEPRIVALOMAS. Jei jis naudojamas, jis PRIVALO atitikti ETSI TS 102 231 5.8.1 punkte nustatytas specifikacijas.

Plėtinys **additionalServiceInformation** (5.8.2 punktas)

Šis plėtinys NEPRIVALOMAS; jei jis naudojamas, jis PRIVALO būti naudojamas tik paslaugos lygmeniu ir tik lauke, nustatytame 5.5.9 punkte („Informacijos apie paslaugą plėtinys“). Šis plėtinys naudojamas papildomai informacijai apie paslaugą pateikti. Ši informacija TURI būti teikiama kaip seka, sudaryta iš vienos arba kelių baigtinių sekų, iš kurių kiekvienoje nurodoma:

a) UII, kuriuo identifikuojama papildoma informacija, pvz.:

   — UII, kuriuo nurodoma tam tikra nacionaliniu mastu nustatyta specifinė prižiūrimos ir (arba) akredituotos patikimumo užtikrinimo paslaugos žymos teikimo paslaugos kvalifikacija, pvz.:

      — specifinis hierarchinis apsaugos ir (arba) kokybės lygis, susijęs su nacionaline priežiūros ir (arba) akreditacijos schema, taikoma KS neišduodantiems SPT (pvz., Prancūzijoje – tai RGS */**/***, Vokietijoje – specifinis priežiūros statusas, nustatytas nacionaliniais teisės aktais, taikomais tam tikriems KS išduodantiems SPT), žr. pastabą (4) dėl lauko „Service current status“, 5.5.4 punktas;

      — specifinis teisinis prižiūrimos ir (arba) akredituotos patikimumo užtikrinimo paslaugos žymos teikimo paslaugos statusas (pvz., Vokietijoje arba Vengrijoje tai yra nacionaliniu mastu nustatyta kvalifikuota LFŽ);

      — arba specifinio politikos identifikatoriaus reikšmė, nurodyta X.509v3 sertifikato „Sdi“ lauke;

   — arba registruotas UII, nurodytas lauke „Paslaugos rūšies identifikatorius“ (5.5.1 punktas), siekiant tiksliau apibrėžti paslaugos, nurodytos lauke „Sti“, sąsają su KS išduodančio sertifikavimo paslaugų teikėjo teikiama paslauga, kurios dalis yra pirmiau minėta paslauga (pvz., OCSP-KS, CRL-KS, pagrindinė SI/KS);

b) neprivaloma eilutė, kurioje pateikiama informacijos apie paslaugą (angl. *serviceInformation*) reikšmė, apibrėžta pagal schemą (pvz., *, ** arba ***);

c) bet kokia neprivaloma papildoma informacija, teikiama specifine schemos forma.

▼**M1**

Naudojantis URI TURĖTŲ būti pasiekiama žmonėms suprantama forma pateikta informacija (bent anglų kalba ir galbūt viena ar keliomis nacionalinėmis kalbomis), kuri laikoma tinkama ir pakankama, kad susijusi šalis suprastų plėtinį; joje visų pirma išaiškinama pateiktų URI reikšmė, nurodomos galimos „serviceInformation“ reikšmės ir paaiškinama kiekviena iš šių reikšmių.

Qualifications Extension (L.3.1 punktas)

Aprašas: Šis laukas NEPRIVALOMAS, tačiau TURI būti naudojamas, kai tai PRIVALOMA, pvz., kai tai susiję su „RootCA/QC“ arba „CA/QC“ paslaugomis ir kai:

— lauke „Service digital identity“ pateiktos informacijos nepakanka teikiant šią paslaugą išduodamiems kvalifikuotiems sertifikatams aiškiai identifikuoti,

— remiantis susijusiuose kvalifikuotuose sertifikatuose pateikta informacija neįmanoma techninėmis priemonėmis nustatyti, ar KS patvirtinamas naudojant SPFĮ.

Jei šis paslaugos lygio plėtinys naudojamas, jis PRIVALO būti naudojamas tik „Service information extension“ (5.5.9 punktas) apibrėžtame lauke ir TURI atitikti ETSI TS 102 231 priede L.3.1 pateiktas specifikacijas.

TakenOverBy Extension (L.3.2 punktas)

Aprašas: Šis plėtinys NEPRIVALOMAS, tačiau TURI būti naudojamas, kai atsakomybę už paslaugos teikimą, už kurį teisiškai atsakingas buvo SPT, prisiima kitas TSP; jame oficialiai nurodoma teisinė atsakomybė už paslaugos teikimą ir taip suteikiama galimybė vartotojui naudojantis tikrinimo programine įranga peržiūrėti tam tikrus teisinius duomenis. Šiame plėtinyje pateikiama informacija TURI būti suderinama su susijusiu 5.5.6 punkto naudojimu ir atitikti ETSI TS 102 231 priede L.3.2 pateiktas specifikacijas.

▼**M1**

II SKYRIUS

Rengdamos patikimus sąrašus, valstybės narės turi:

kalbų kodus nurodyti mažosiomis, o valstybių kodus – didžiosiomis raidėmis;

naudoti toliau pateiktoje lentelėje nurodytus kalbų ir valstybių kodus.

Kai naudojami lotyniški rašmenys (su tinkamu kalbos kodu), pateikiamas ir lotyniškais rašmenimis transliteruotas tekstas su toliau pateiktoje lentelėje nurodytais susijusiais kalbų kodais.

Trumpasis pavadinimas (originalo kalba)	Trumpasis pavadinimas (anglų kalba)	Valstybės kodas	Kalbos kodas	Pastabos	Transliteracija lotyniškais rašmenimis
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	ES rekomenduojamas valstybės kodas	el-Latn
España	Spain	ES	es	Taip pat katalonų (ca), baskų (eu), galisų (gl)	
France	France	FR	fr		
Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼**M1**

Trumpasis pavadinimas (originalo kalba)	Trumpasis pavadinimas (anglų kalba)	Valstybės kodas	Kalbos kodas	Pastabos	Transliteracija lotyniškais rašmenimis
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	ES rekomenduojamas valstybės kodas	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Transliteracija lotyniškais rašmenimis: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

_____

▼C1

IV SKYRIUS

ŽMONĖMS SUPRANTAMO PUPSS FORMA RENGIAMO PATIKIMO SĄRAŠO SPECIFIKACIJOS

Žmonėms suprantamo (ŽS) PUPSS forma rengiamas patikimas sąrašas PRIVALO būti skelbiamas viešai ir prieinamas elektroninėmis priemonėmis. Jis TURĖTŲ būti teikiamas kaip *Portable Document Format* (PDF) dokumentas, parengtas pagal ISO 32000, jo formatas PRIVALO atitikti PDF/A aprašą (ISO 19005).

PDF/A aprašu pagrįsto žmonėms suprantamo (ŽS) PUPSS forma rengiamo patikimo sąrašo turinys TURĖTŲ atitikti šiuos reikalavimus:

▼M1

— žmonėms suprantamos formos patikimo sąrašo pavadinimas sudaromas iš šių elementų:

  — neprivalomas valstybės narės nacionalinės vėliavos paveikslėlis,

  — tarpas,

  — trumpasis valstybės pavadinimas originalo kalba (-omis) (kaip nurodyta II skyriuje pateiktos lentelės pirmame stulpelyje),

  — tarpas,

  — „(“,

  — skliaustuose – trumpasis valstybės pavadinimas anglų kalba (kaip nurodyta II skyriuje pateiktos lentelės antrame stulpelyje),

  — „):“ – dešinysis skliaustas ir skirtukas,

  — tarpas,

  — „Trusted List“,

  — neprivalomas valstybės narės schemos operatoriaus logotipas,

▼C1

— ŽS formos struktūra TURĖTŲ atitikti loginį modelį, aprašytą ETSI TS 102 231 5.1.2 punkte,

— kiekvienas esamas laukas TURĖTŲ būti rodomas ir jame TURĖTŲ būti nurodyta:

  — lauko pavadinimas (pvz., „Paslaugos rūšies identifikatorius“),

  — lauko reikšmė (pvz., „SI/KS“),

  — lauko, jei jis naudojamas, reikšmės prasmė (aprašymas), pirmiausia atitinkanti ETSI TS 102 231 D priedą arba šias užregistruotų UII specifikacijas (pvz., „Sertifikavimo institucija, išduodanti viešojo rakto sertifikatus“),

  — jei reikia, įvairios žmonių kalbos versijos, numatytos PUPSS forma rengiamame patikimame sąraše,

— žmonėms suprantama forma TURĖTŲ būti pateikti bent toliau nurodyti laukai ir atitinkamos skaitmeninių sertifikatų lauko „Paslaugos skaitmeninis identifikatorius“ reikšmės:

  — versija,

  — serijos numeris,

  — parašo algoritmas,

  — sertifikatą išdavęs asmuo,

  — galiojimo pradžia,

  — galiojimo pabaiga,

  — subjektas,

▼C1

— viešasis raktas,

— sertifikato politika,

— subjekto rakto identifikatorius,

— CRL paskirstymo taškai,

— institucijos rakto identifikatorius,

— rakto naudojimas,

— pagrindiniai apribojimai,

— piršto atspaudo algoritmas,

— piršto atspaudas;

— ŽS forma TURĖTŲ būti lengvai išspausdinama,

— ŽS forma GALI būti pasirašyta elektroniniu būdu. Jei sąrašas pasirašomas, jį PRIVALO pasirašyti schemos operatorius, laikydamasis tų pačių parašo specifikacijų, kokios taikomos PUPSS forma rengiamam patikimam sąrašui.