Käesolev dokument on vaid dokumenteerimisvahend ja institutsioonid ei vastuta selle sisu eest

►B ►C1 **KOMISJONI OTSUS,**

16. oktoober 2009,

millega kehtestatakse meetmed elektrooniliste haldustoimingute kasutamise lihtsustamiseks ühtsete kontaktpunktide kaudu, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis 2006/123/EÜ teenuste kohta siseturul

(teatavaks tehtud numbri K(2009) 7806 all)

(EMPs kohaldatav tekst)

(2009/767/EÜ) ◄

(ELT L 274, 20.10.2009, lk 36)

Muudetud:

		Euroopa Liidu Teataja		
		nr	lehekülg	kuupäev
►M1	Komisjoni Otsus 2010/425/EL, 28. juuli 2010	L 199	30	31.7.2010

Parandatud:

►C1 Parandus, ELT L 299, 14.11.2009, lk 18 (2009/767/EÜ)
►C2 Parandus, ELT L 4, 7.1.2011, lk 6 (2009/767/EÜ)

▼B
▼C1

KOMISJONI OTSUS,

16. oktoober 2009,

millega kehtestatakse meetmed elektrooniliste haldustoimingute kasutamise lihtsustamiseks ühtsete kontaktpunktide kaudu, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis 2006/123/EÜ teenuste kohta siseturul

(teatavaks tehtud numbri K(2009) 7806 all)

(EMPs kohaldatav tekst)

(2009/767/EÜ)

EUROOPA ÜHENDUSTE KOMISJON,

võttes arvesse Euroopa Ühenduse asutamislepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 12. detsembri 2006. aasta direktiivi 2006/123/EÜ teenuste kohta siseturul, ([1]) eriti selle artikli 8 lõiget 3,

ning arvestades järgmist:

(1) Liikmesriikidele direktiivi 2006/123/EÜ II peatüki, eriti selle artiklite 5 ja 8 kohaselt pandud haldustoimingute lihtsustamise kohustused hõlmavad kohustust lihtsustada haldustoiminguid ja -formaalsusi, mida rakendatakse teenuste osutamise valdkonnale juurdepääsuks või selles valdkonnas tegutsemiseks, ning kohustust tagada, et teenuseosutajad saaksid neid haldustoiminguid ja -formaalsusi hõlpsasti täita vahemaa tagant ja elektrooniliste vahendite abil ühtsete kontaktpunktide kaudu.

(2) Liikmesriikidevahelisi piiriüleseid haldustoiminguid ja -formaalsusi peab olema võimalik täita ühtsete kontaktpunktide kaudu vastavalt direktiivi 2006/123/EÜ artikli 8 sätetele.

(3) Et täita haldustoimingute ja -formaalsuste lihtsustamise kohustust ja hõlbustada ühtsete kontaktpunktide piiriülest kasutamist, peavad elektroonilised haldustoimingud põhinema lihtsatel lahendustel, mis hõlmab ka elektrooniliste allkirjade kasutamist. Kui konkreetsete haldustoimingute ja -formaalsuste kohta tehtud asjakohase riskianalüüsi tulemusel peetakse vajalikuks kõrget turvalisust või elektroonilise allkirja võrdväärsust käsitsi kirjutatud allkirjaga, võib teenuseosutajatelt teatavate haldustoimingute ja -formaalsuste täitmisel nõuda kvalifitseeritud sertifikaadil põhinevaid täiustatud elektroonilisi allkirju, mis on antud turvalise allkirja andmise vahendiga või ilma selleta.

([1]) ELT L 376, 27.12.2006, lk 36.

▼C1

(4) Ühenduse elektrooniliste allkirjade raamistik kehtestati Euroopa Parlamendi ja nõukogu 13. detsembri 1999. aasta direktiivis 1999/93/EÜ elektroonilisi allkirju käsitleva ühenduse raamistiku kohta ([1]). Et soodustada kvalifitseeritud sertifikaadil põhinevate täiustatud elektrooniliste allkirjade tulemuslikku piiriülest kasutamist, tuleb tõsta usaldust nende elektrooniliste allkirjade suhtes, olenemata sellest, millises liikmesriigis asub allakirjutaja või kvalifitseeritud sertifikaadi väljastanud sertifitseerimisteenuse osutaja. Seda on võimalik saavutada, muutes elektrooniliste allkirjade tõendamiseks vajaliku teabe usaldusväärsel kujul kergemini kättesaadavaks, pidades eelkõige silmas teavet liikmesriigis järelevalvealuste/akrediteeritud sertifitseerimisteenuse osutajate ja nende poolt pakutavate teenuste kohta.

(5) Oluline on tagada, et liikmesriigid teeksid kõnealuse teabe avalikult kättesaadavaks ühtse vormi kaudu, mis lihtsustab teabe kasutamist ja tagab selle piisava detailsuse, mis võimaldab vastuvõtval poolel elektroonilist allkirja tõendada,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Elektrooniliste allkirjade kasutamine ja tunnustamine

1. Kui see on asjakohase riskianalüüsi tulemusel ja kooskõlas direktiivi 2006/123/EÜ artikli 5 lõigetega 1 ja 3 põhjendatud, võivad liikmesriigid nõuda teatavate haldustoimingute ja -formaalsuste täitmisel direktiivi 2006/123/EÜ artikli 8 kohaste ühtsete kontaktpunktide kaudu, et teenusosutaja kasutaks kvalifitseeritud sertifikaadil põhinevaid täiustatud elektroonilisi allkirju, mis on antud direktiivis 1999/93/EÜ määratletud ja reguleeritud turvalise allkirja andmise vahendiga või ilma selleta.

2. Liikmesriigid tunnustavad lõikes 1 osutatud haldustoimingute ja -formaalsuste täitmisel kõiki kvalifitseeritud sertifikaadil põhinevaid täiustatud turvalise allkirja andmise vahendiga või ilma selleta antud elektroonilisi allkirju, kuid see ei välista liikmesriikide võimalust piirata nende elektrooniliste allkirjade tunnustamist kvalifitseeritud sertifikaadil põhinevate täiustatud turvalise allkirja andmise vahendiga antud elektroonilistele allkirjadele, kui see on kooskõlas lõikes 1 osutatud riskianalüüsi tulemustega.

3. Liikmesriigid ei kohalda kvalifitseeritud sertifikaadil põhinevate täiustatud turvalise allkirja andmise vahendiga või ilma selleta antud elektrooniliste allkirjade tunnustamisel nõudeid, mis takistavad teenuseosutajatel ühtsete kontaktpunktide kaudu elektrooniliste haldustoimingute kasutamist.

([1]) EÜT L 13, 19.1.2000, lk 12.

▼C1

4. Lõige 2 ei takista liikmesriike tunnustamast teisi elektroonilisi allkirju peale kvalifitseeritud sertifikaadil põhinevate täiustatud turvalise allkirja andmise vahendiga või ilma selleta antud elektrooniliste allkirjade.

Artikkel 2

Usaldusnimekirjade koostamine, haldamine ja avaldamine

1. Iga liikmesriik peab koostama, haldama ja avaldama lisas esitatud tehnilistele nõuetele vastava usaldusnimekirja, mis sisaldab miinimumteavet liikmesriigi järelevalvealuste/akrediteeritud sertifitseerimisteenuse osutajate kohta, kes väljastavad üldsusele nõuetekohaseid sertifikaate, ning seda nimekirja haldama.

▼M1

2. Liikmesriigid koostavad ja avaldavad nii inimesele loetava kui ka masinloetava usaldusnimekirja vastavalt lisas sätestatud nõuetele.

2a. Liikmesriigid allkirjastavad oma masinloetava usaldusnimekirja elektrooniliselt ja avaldavad vähemalt mõne turvakanali kaudu inimesele loetava usaldusnimekirja, et tagada selle autentsus ja terviklikkus.

3. Liikmesriigid edastavad komisjonile järgmise teabe:

a) inimesele loetava ja masinloetava usaldusnimekirja versiooni koostamise, haldamise ja avaldamise eest vastutav(ad) asutus(ed);

b) inimesele loetava ja masinloetava usaldusnimekirja versiooni avaldamise koht;

c) avaliku võtme sertifikaat sellise turvakanali jaoks, mille kaudu inimesele loetav usaldusnimekiri avaldatakse, või – kui inimesele loetav usaldusnimekiri on elektrooniliselt allkirjastatud – selle allkirjastamisel kasutatava avaliku võtme sertifikaat;

d) avaliku võtme sertifikaat, mida kasutatakse masinloetava usaldusnimekirja elektroonilisel allkirjastamisel;

e) kõik muudatused punktides a–d esitatud teabes.

4. Komisjon teeb kõigile liikmesriikidele kasutaja serveri ja autenditud veebiserveri vaheliste turvakanalite kaudu kättesaadavaks lõikes 3 osutatud teabe, mille liikmesriigid on esitanud nii inimesele loetaval kujul kui ka allkirjastatult, masinloetaval kujul.

▼C1

Artikkel 3

Kohaldamine

Käesolevat otsust kohaldatakse alates 28. detsembrist 2009.

Artikkel 4

Adressaadid

Käesolev otsus on adresseeritud liikmesriikidele.

▼C1

LISA

TEHNILISED NÕUDED JÄRELEVALVEALUSTE/AKREDITEERITUD SERTIFITSEERIMISTEENUSE OSUTAJATE USALDUSNIMEKIRJA ÜHTSE VORMI KOOSTAMISEKS

EESSÕNA

1. **Üldteave**

Liikmesriikide järelevalvealuste/akrediteeritud sertifitseerimisteenuse osutajate usaldusnimekirja ühtse vormi eesmärk on kehtestada ühtne kord, mille alusel liikmesriigid peavad esitama teavet selliste sertifitseerimisteenuse osutajate (*Certification Service Providers* – CSPs) ([1]) sertifitseerimisteenuste järelevalve-/akrediteerimisolekute kohta, kelle järelevalvet nad teostavad või kelle nad on akrediteerinud, et tagada direktiivi 1999/93/EÜ asjaomaste sätete järgimine. See hõlmab ka varasema teabe esitamist järelevalvealuste/akrediteeritud sertifitseerimisteenuste järelevalve-/akrediteerimisoleku kohta.

Usaldusnimekirjas (*Trusted List* – TL) esitatav kohustuslik teave peab sisaldama miinimumteavet direktiivi 1999/93/EÜ sätetega (artikli 3 lõikega 3, artikli 3 lõikega 2 ja artikli 7 lõike 1 punktiga a) kooskõlas kvalifitseeritud sertifikaate (*Qualified Certificates* – QCs) ([2]) väljastavate järelevalvealuste/akrediteeritud CSPde kohta, sealhulgas teavet elektroonilist allkirja toetava QC kohta ning selle kohta, kas allkiri luuakse turvalise allkirja andmise vahendiga (*Secure Signature Creation Device* – SSCD) ([3]) või ilma selleta.

Liikmesriik võib vabatahtlikult oma riiklikus usaldusnimekirjas esitada täiendavat teavet teiste järelevalvealuste/akrediteeritud CSPde kohta, kes ei väljasta QCsid, kuid osutavad elektrooniliste allkirjadega seotud teenuseid (nt ajatempliteenuseid osutavad ja ajatempleid väljastavad CSPd, mittekvalifitseeritud mittenõuetekohaseid sertifikaate väljastavad CSPd jne).

Kõnealuse teabe põhieesmärk on toetada kvalifitseeritud sertifikaadi poolt toetatavate kvalifitseeritud elektrooniliste allkirjade (*Qualified Electronic Signatures* – QES) ja täiustatud elektrooniliste allkirjade (*Advanced Electronic Signatures* – AdES) ([4]) ([5]) ([6]) tõendamist.

Kavandatav ühtne vorm on kooskõlas rakendusega, mis tuleneb Euroopa Telekommunikatsiooni Standardite Instituudi tehnilise spetsifikaadi 102 231 (*European Telecommunication Standards Institute Technical Specification* – ETSI TS 102 231) ([7]) nõuetest, mida kasutatakse selliste nimekirjade koostamisel, avaldamisel, paigutamisel, juurdepääsu loomisel, autentimisel ja usaldusväärsuse tagamisel.

([1]) Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 11 määratlusele.
([2]) Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 10 määratlusele.
([3]) Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 6 määratlusele.
([4]) Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 2 määratlusele.
([5]) Käesolevas dokumendis kasutatakse kõikjal akronüümi „$AdES_{QC}$” QC poolt toetatava AdES tähistamiseks.
([6]) Juhime tähelepanu sellele, et on olemas mitu lihtsatel täiustatud elektroonilistel allkirjadel põhinevat elektroonilist teenust, mille piiriülest kasutamist tuleks samuti lihtsustada tingimusel, et toetavad sertifitseerimisteenused (nt mittekvalifitseeritud sertifikaatide väljastamine) moodustavad osa järelevalvealustest/akrediteeritud teenustest, mida liikmesriik kajastab oma usaldusnimekirja vabatahtliku teabe osas.
([7]) ETSI TS 102 231 – *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information*.

▼C1

2. **Juhised usaldusnimekirja kirjete redigeerimiseks**

2.1. *Järelevalvealustele/akrediteeritud sertifitseerimisteenustele suunatud TL*

Ühtses nimekirjas sisalduvad asjaomased sertifitseerimisteenused ja sertifitseerimisteenuse osutajad

Liikmesriigi usaldusnimekiri on selliste sertifitseerimisteenuse osutajate sertifitseerimisteenuste järelevalve-/akrediteerimisolekute loetelu, kelle järelevalvet asjaomane liikmesriik teostab või kelle ta on akrediteerinud, et tagada direktiivi 1999/93/EÜ asjaomaste sätete järgimine.

Sellises usaldusnimekirjas peavad sisalduma:

— kõik direktiivi 1999/93/EÜ artikli 2 lõikes 11 määratletud **sertifitseerimisteenuse osutajad**, st üksused või juriidilised või füüsilised isikud, kes väljastavad sertifikaate või osutavad muid elektrooniliste allkirjadega seotud teenuseid;

— **kes on järelevalvealused/akrediteeritud** direktiivi 1999/93/EÜ asjaomaste sätete järgimise tagamiseks.

Direktiivis 1999/93/EÜ sisalduvate, eelkõige asjaomaste CSPde ja nende järelevalve- / vabatahtlikkusel põhinevate akrediteerimissüsteemidega seotud määratluste ja sätete käsitlemisel tuleb eristada kahte CSPde rühma, nimelt üldsusele QCsid väljastavad CSPd (CSPQC) ja CSPd, kes ei väljasta üldsusele QCsid, kuid pakuvad muid elektrooniliste allkirjadega seotud (kõrval)teenuseid:

— **QCsid väljastavad CSPd:**

  — nende järelevalvet peab teostama nende asukohaks olev liikmesriik (kui nad asuvad mõnes liikmesriigis) ja nad võivad olla ka akrediteeritud direktiivi 1999/93/EÜ sätete järgimise tagamiseks, sealhulgas I lisa (nõuded QCdele) ja II lisa (nõuded QCsid väljastavatele CSPdele) nõuetega. Liikmesriigis akrediteeritud QCsid väljastavad CSPd peavad siiski alluma ka selle liikmesriigi asjaomasele järelevalvesüsteemile, välja arvatud juhul, kui nad ei asu selles liikmesriigis;

  — kohaldatav järelevalvesüsteem (vastavalt „vabatahtlikkusel põhinev akrediteerimissüsteem”) on määratletud direktiivis 1999/93/EÜ, eriti selle artikli 3 lõikes 3, artikli 8 lõikes 1, artiklis 11, põhjenduses 13 (vastavalt artikli 2 lõikes 13, artikli 3 lõikes 2, artikli 7 lõike 1 punktis a, artikli 8 lõikes 1, artiklis 11, põhjendustes 4 ja 11–13) ja peab vastama seal sätestatud asjaomastele nõuetele;

— **QCsid mitteväljastavad CSPd:**

  — need võivad alluda vabatahtlikkusel põhinevale akrediteerimissüsteemile (mis on määratletud direktiivis 1999/93/EÜ ja on sellega vastavuses) ja/või riiklikult määratletud tunnustatud heakskiitmissüsteemile, mida rakendatakse siseriiklikel alustel, et kontrollida direktiivi sätete ja vajadusel siseriiklike normide järgimist sertifitseerimisteenuste osutamisel (direktiivi artikli 2 lõike 11 tähenduses);

  — mõnele sertifitseerimisteenuse osutamise tulemusel tekkivale või väljastatavale füüsilisele või binaarsele (loogilisele) objektile võib anda erikvalifikatsiooni, lähtudes nende vastavusest siseriiklikult kehtestatud normidele ja nõuetele, kuid tõenäoliselt piirdub sellise kvalifikatsiooni tähendus üksnes siseriikliku tasandiga.

▼C1

Liikmesriigi usaldusnimekiri peab andma üldsusele miinimumteavet kooskõlas direktiivi 1999/93/EÜ sätetega (artikli 3 lõikega 3, artikli 3 lõikega 2 ja artikli 7 lõike 1 punktiga a) QCsid väljastavate järelevalvealuste/akrediteeritud CSPde kohta, teavet elektroonilist allkirja toetavate QCde kohta ja selle kohta, kas allkiri on loodud turvalise allkirja andmise vahendiga või ilma selleta.

Liikmesriik võib vabatahtlikult oma siseriiklikus usaldusnimekirjas esitada täiendavat teavet üldsusele QCsid mitteväljastavate CSPde poolt osutatavate teiste järelevalvealuste/akrediteeritud teenuste kohta (nt ajatempliteenuseid osutavad ja ajatempleid väljastavad CSPd, mittekvalifitseeritud sertifikaate väljastavad CSPd jne).

Usaldusnimekirja eesmärk on järgmine:

— koguda ja esitada usaldusväärset teavet selliste sertifitseerimisteenuse osutajate sertifitseerimisteenuste järelevalve-/akrediteerimisoleku kohta, kelle järelevalvet nimekirja koostamise ja haldamise eest vastutav liikmesriik teostab või kelle ta on akrediteerinud, et tagada direktiivi 1999/93/EÜ asjaomaste sätete järgimine;

— lihtsustada elektrooniliste allkirjade tõendamist, mida toetavad nimekirja kantud CSPde poolt pakutavad nimekirja kantud järelevalvealused/-akrediteeritud sertifitseerimisteenused.

Järelevalve-/akrediteerimisoleku väärtuste ühtne kogum

Iga liikmesriik peab koostama ühe TLi ja seda haldama, et viidata liikmesriigi järelevalvealuste/akrediteeritud CSPde poolt osutatavate sertifitseerimisteenuste järelevalve- ja/või akrediteerimisolekule.

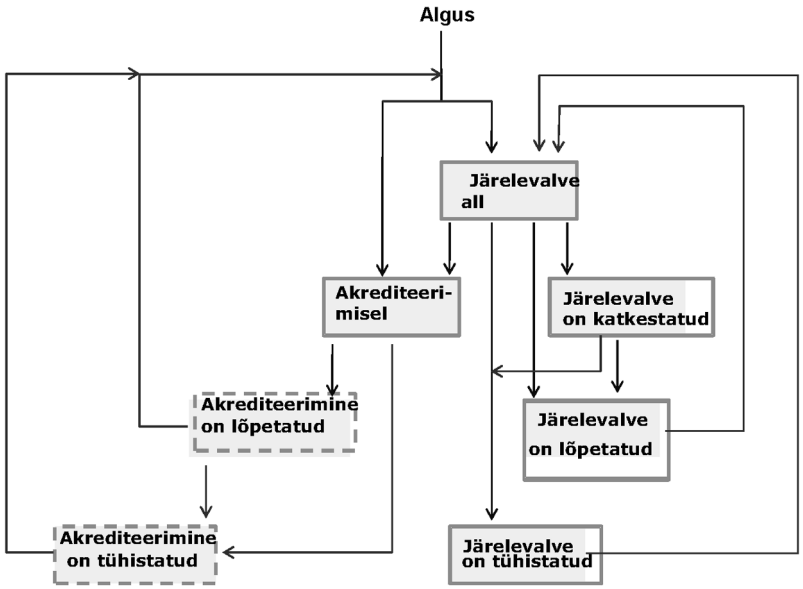
Asjaolu, et teenus on järelevalve all või akrediteerimisel, on osa teenuse hetkeolekust. Lisaks sellele võib järelevalve- või akrediteerimisolek olla „jätkuv", „katkestatud", „lõpetatud" või isegi „tühistatud". Sama sertifitseerimisteenus võib oma eluea jooksul liikuda järelevalveolekust akrediteerimisolekusse ja vastupidi ([1]).

Järgneval joonisel 1 on kujutatud ühe sertifitseerimisteenuse eeldatav liikumine võimalike järelevalve-/akrediteerimisolekute vahel:

([1]) Nt sertifitseerimisteenuse osutaja, kes asub liikmesriigis, mis pakub algselt liikmesriigi (järelevalveasutuse) poolt järelevalvatavat sertifitseerimisteenust, võib pärast teatava aja möödumist otsustada, et ta laseb hetkel järelevalve all oleva sertifitseerimisteenuse suhtes teostada vabatahtlikkusel põhineva akrediteerimise. Seevastu võib teises liikmesriigis asuv sertifitseerimisteenuse osutaja otsustada, et ta ei lõpeta akrediteeritud sertifitseerimisteenuse osutamist, vaid viib selle akrediteerimisolekust järelevalveolekusse, nt ärilistel ja/või majanduslikel põhjustel.

▼C1

Ühe ertifitseerimisteenuse eeldatav liikumine järelevalve-/akrediteerimisolekute vahel



Legend:

Üleminekuolek, kui on olemas seotud järelevalvemudel (nt QCsid väljastava CSP puhul, kui viimane asub liikmesriigis). Võimalik hetkeolek, kui ei ole seotud järelevalvemudelit, (nt QCsid mitteväljastava CSP puhul).

Võimalik hetkeolek

Joonis 1

QCsid väljastava sertifitseerimisteenuse järelevalvet peab teostama (kui seda osutatakse liikmesriigis) ja seda võib vabatahtlikult akrediteerida. Sellise usaldusnimekirjas oleva teenuse hetkeoleku väärtus võib olla mis tahes eespool kirjeldatud olekuväärtus. Kuid tuleb märkida, et olekud „akrediteerimine lõpetatud" ja „akrediteerimine tühistatud" peavad olema mõlemad üleminekuväärtused üksnes liikmesriigis osutatavate CSP_{QC} teenuste puhul, kuna nende teenuste järelevalvet tuleb igal juhul teostada (isegi kui neid ei akrediteerita või enam ei akrediteerita).

Liikmesriigid, kes kehtestavad või on kehtestanud riiklikult määratletud tunnustatud heakskiitmissüsteemi(d), mida rakendatakse riigisiseselt selleks, et kontrollida QCsid mitteväljastavate CSPde teenuste vastavust direktiivi 1999/93/EÜ sätetele ja võimalikele siseriiklikele normidele sertifitseerimisteenuste osutamisel (direktiivi artikli 2 lõike 11 tähenduses), peavad liigitama sellise(d) kinnitamise skeemi(d) kahte järgmisse kategooriasse:

— vabatahtlikkusel põhinev akrediteerimine, mis on määratletud ja reguleeritud direktiivis 1999/93/EÜ (artikli 2 lõige 13, artikli 3 lõige 2, artikli 7 lõike1 punkt a, artikli 8 lõige 1, artikkel 11, põhjendused 4 ja 11–13);

— järelevalve, mis on nõutav direktiivis 1999/93/EÜ ja mida rakendatakse siseriiklike normide ja nõuete alusel kooskõlas siseriiklike õigusaktidega.

▼C1

Seega võib QCsid mitteväljastav sertifitseerimisteenus olla järelevalvealune või vabatahtlikult akrediteeritav. Sellise usaldusnimekirjas oleva teenuse hetkeoleku väärtuseks võib olla mis tahes eespool kirjeldatud olekuväärtus (vt joonis 1).

Usaldusnimekiri peab sisaldama teavet selle aluseks oleva(te) järelevalve-/-akrediteerimissüsteemide(de) kohta, eelkõige järgmist:

— teavet kõigi CSP_{QC}de suhtes kohaldatava järelevalvesüsteemi kohta;

— vajaduse korral teavet kõigi CSP_{QC}de suhtes kohaldatava siseriikliku vabatahtlikkusel põhineva akrediteerimissüsteemi kohta;

— vajaduse korral teavet kõigi QCsid mitteväljastavate CSPde suhtes kohaldatava järelevalvesüsteemi kohta;

— vajaduse korral teavet kõigi QCsid mitteväljastavate CSPde suhtes kohaldatava siseriikliku vabatahtlikkusel põhineva akrediteerimissüsteemi kohta;

Kaks viimast teaberühma on seotud osapoolte jaoks eriti olulised selleks, et hinnata selliste järelevalve-/akrediteerimissüsteemide kvaliteedi ja turvalisuse taset, mida siseriiklikul tasandil QCsid mitteväljastavate CSPde suhtes kohaldatakse. Kui TLis esitatakse teavet QCsid mitteväljastavate CSPde poolt osutatavate teenuste järelevalve-/akrediteerimisoleku kohta, tuleb eespool nimetatud teaberühmad esitada TLi tasemel, kasutades *Scheme Information* URI (*Uniform Resource Identifier*) välja (punkt 5.3.7 – liikmesriikide poolt esitatav teave), *Scheme type/community/rule*s välja (punkt 5.3.9 – kasutades kõigi liikmesriikide jaoks ühist teksti ja liikmesriigi valikulist eriteavet) ja TSL *policy/legal notice* välja (punkt 5.3.11 – kõigi liikmesriikide jaoks ühine tekst, viidates direktiivile 1999/93/EÜ, koos kõigi liikmesriikide võimalusega lisada oma teksti/viiteid). Vajaduse korral ja kui see on nõutav (nt et eristada mitut kvaliteedi/turvalisuse taset) võib teenuse tasemel esitada täiendavat teavet kvalifikatsiooni kohta, mis on määratletud QCsid mitteväljastavate CSPde puhul siseriiklike järelevalve-/akrediteerimissüsteemide tasemel, kasutades *additionalServiceInformation* laienduse välja (punkt 5.8.2), mis on *Service information extension* välja (punkt 5.5.9) osa. Täpsem teave tehniliste nõuete kohta on esitatud I peatüki üksikasjalikes kirjeldustes.

Olenemata sellest, et liikmesriigis võivad sertifitseerimisteenuste järelevalve ja akrediteerimisega tegeleda eraldi asutused, eeldatakse, et ühe sertifitseerimisteenuse jaoks kasutatakse vaid ühte kirjet (mis on tuvastatav tema teenuse digitaalse tunnusena vastavalt ETSI TSile 102 231) ([1]) ja et selle järelevalve-/akrediteerimisolekut ajakohastatakse. Eespool käsitletud olekute tähendust kirjeldatakse I peatüki üksikasjalike tehniliste nõuete punktis 5.5.4.

2.2. *TLi kirjed, mille eesmärk on lihtsustada QESi ja $AdES_{QC}$-i tõendamist*

TLi loomise kõige olulisem osa on TLi kohustusliku osa koostamine, milleks on QCsid väljastava CSP teenuste nimekiri, et kajastada õigesti iga sellise QCsid väljastava sertifitseerimisteenuse osutaja täpset sertifikaatide väljastamise seisu ja tagada, et igas kandes esitatav teave oleks piisav QES ja $AdES_{QC}$-i tõendamise lihtsustamiseks (kui see on ühendatud CSP poolt selles kirjes loetletud sertifitseerimisteenuse alusel väljastatud lõppkasutaja kvaliteedisertifikaadi sisuga).

([1]) ETSI TS 102 231 – *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information*.

▼C1

Kuni kvalifitseeritud sertifikaadil puudub tõeliselt koostalitlusvõimeline ja piiriülene profiil, võiks nõutav teave sisaldada muud teavet peale ühe juursertifitseerija ((*Root*) CA) teenuse digitaalse tunnuse, eelkõige teavet väljastatud sertifikaadi QC oleku tuvastamiseks ja teavet selle kohta, kas toetatud allkirjad on loodud SSCD toel või mitte. Liikmesriigis TLi koostamiseks, redigeerimiseks ja haldamiseks määratud asutus (st süsteemioperaator vastavalt ETSI TSile 102 231) peab seepärast võtma arvesse iga väljastatud QC hetkeprofiili ja sertifikaadi sisu iga TLis sisalduva CSP_{QC} kohta.

Ideaalis peaks igas väljastatud QCs sisalduma ETSI määratletud QcCompliance'i ([1]) tunnus, kui on väidetud, et tegemist on QCga, ning ETSI määratletud QcSSCD tunnus, kui on väidetud, et sertifikaati toetab turvalise allkirja andmise vahend e-allkirjade loomiseks ja/või et iga väljastatud QC sisaldab ühte ETSI TSis 101 456 ([2]). määratletud sertifitseerimispoliitika objektiidentifikaatorit (*QCP/QCP + certificate policy Object Identifiers (OIDs))*. QCsid väljastavate CSPde poolt viidetena erinevate standardite kasutamine, selliste standardite laialdane tõlgendamine ja puudulikud teadmised mõne normatiivse tehnilise nõude või standardi olemasolu ja prioriteetsuse kohta on põhjustanud erinevused praegu väljastatavate QCde tegelikus sisus (nt ETSIs määratletud QC tunnuste kasutamine või mittekasutamine) ja see takistab vastuvõtvatel pooltel allakirjutaja sertifikaati (ja seotud ketti/teed) usaldada, et hinnata vähemalt masinloetavalt, kas e-allkirja toetav sertifikaat on väidetavalt QC ja kas see on seotud SSCDga, mille abil e-allkiri loodi.

Kirjete *Service type identifier (Sti), Service name (Sn)* ja *Service digital identity (Sdi)* ([3]) täitmine kirjes *Service information extensions (Sie)* esitatud teabega võimaldab kavandatava TLi ühtsel vormil täielikult kindlaks teha nimekirja kantud QCsid väljastava CSP poolt väljastatud kvalifitseeritud sertifikaadi tüübi ja esitada teavet selle kohta, kas sertifikaati toetab SSCD või mitte (kui see teave puudub väljastatud QCl). Selle kirjega on muidugi seotud spetsiifiline teave *Service current status (Scs)*. Seda on kirjeldatud allpool esitatud joonisel 2.

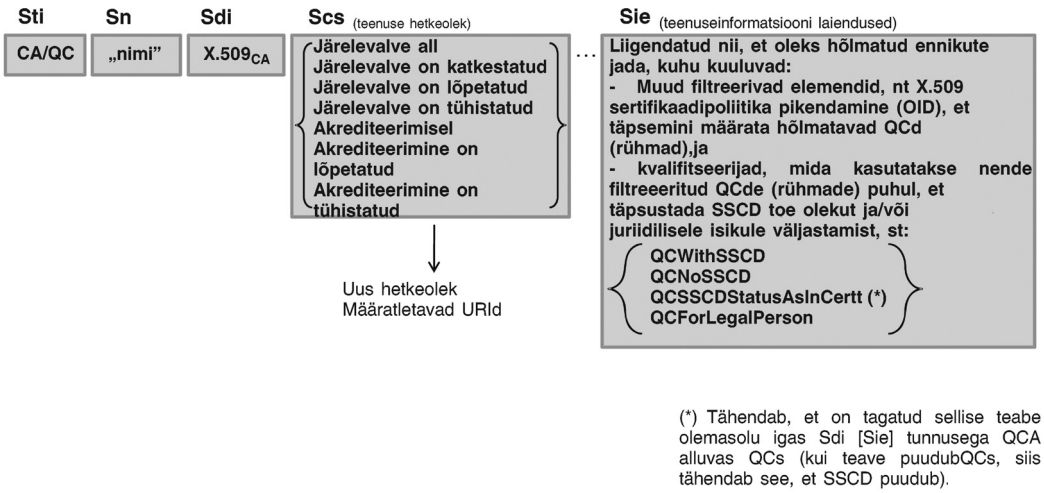
Teenuse nimekirja kandmine üksnes *(Root)* CA *Sdi* esitamise teel tähendab, et on tagatud (QCsid väljastava CSP, aga ka selle CSP järelevalve/akrediteerimise eest vastutava järelevalve-/akrediteerimisasutuse poolt), et iga selle (*Root*) CA hierarhia alusel väljastatud lõppkasutaja sertifikaat sisaldab piisavalt ETSI määratletud ja masintöödeldavat teavet, mille alusel hinnata, kas tegemist on QCga või mitte ja kas seda toetab SSCD või mitte. Näiteks juhul, kui viimane väide ei vasta tõele (nt QC-l ei ole ETSI standardiseeritud masintöödeldavat viidet selle kohta, kas sertifikaati toetab SSCD), võib üksnes selle (*Root*) CA *Sdi* nimekirja kandmise puhul eeldada vaid seda, et selle (*Root*) CA hierarhia alusel väljastatud QCsid ei toeta ükski SSCD. Et eeldada seda, et neid QCsid toetab SSCD, tuleb sellele faktile viitamiseks kasutada *Sie*-d (see näitab ka, et seda tagab QCsid väljastav CSP ja selle järelevalvet teostab / seda akrediteerib vastavalt järelevalve- või akrediteerimisasutus).

([1]) Viide ETSI TSile 101 862 – *Electronic Signatures and Infrastructures* (ESI): *Qualified Certificate Profile*.

([2]) ETSI TS 101 456 – *Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates*.

([3]) St vähemalt väljastava QCA või sertifitseerimistee ülataseme CA X.509v3 sertifikaat.

▼C2



Joonis 2

Nimekirja kantud, QCsid väljastava CSP teenusekirje TSLi formaati rakendatud TLis

▼C1

Käesolevad TLi ühtse vormi tehnilised nõuded võimaldavad kasutada teenusekirjel teabe viie põhiosa kombinatsiooni:

— *Service type identifier (Sti)*, nt tuvastab QCsid väljastava CA (CA/QC);

— *Service name (Sn)*;

— *Service digital identity (Sdi)* teave nimekirja kantud teenuse tuvastamiseks, nt QCsid väljastava CA X.509v3 sertifikaat (vähemalt);

— CA/QC teenuste kohta valikuline *Service information extensions (Sie)* teave, mis võimaldab ühe või enama enniku jada hõlmamist, kus iga enniku puhul on esitatud järgmine:

  — kriteeriumid, mida kasutatakse selleks, et *Sdi* alusel tuvastatava sertifitseerimisteenuse hulgast täpsemalt tuvastada (filtreerida) teenus (st kvalifitseeritud sertifikaatide rühm), mille puhul nõutakse/esitatakse lisateavet seoses SSCD toele viitamisega (ja/või juriidilisele isikule väljastamisega), ja

  — seotud teave (kvalifitseerijad) selle kohta, kas täpsemalt tuvastatud kvalifitseeritud sertifikaatide teenuste rühma toetab SSCD või mitte, või kas see seotud teave on QC osa standardiseeritud masintöödeldaval kujul, ja/või teave selle kohta, et selliseid QCsid väljastatakse juriidilistele isikutele (vaikimisi loetakse neid väljastatuks üksnes füüsilistele isikutele);

▼C1

— teave selle teenusekirje hetkeoleku kohta, kus on kirjas järgmine:

— kas tegemist on järelevalvealuse või akrediteeritud teenusega ja

— järelevalve/akrediteerimise olek.

2.3. *CSP_{QC} teenuste kirjete redigeerimise ja kasutamise juhised*

Redigeerimise üldjuhised on järgmised.

1. Kui on tagatud (garanteeritud CSP_{QC} poolt ja järelevalve-/akrediteerimisasutuse järelevalve all / akrediteeritud), et nimekirja kantud *Sdi* tunnusega teenuse puhul sisaldab mõni SSCD poolt toetatav QC ETSIs määratletud kvalifitseeritud sertifikaadile vastavuse tunnust (*QcCompliance statement*) ja sisaldab QcSSCD tunnust ja/või QCP + objekti identifikaatorit (*Object Identifier* – OID), siis on sobiva *Sdi* kasutamine piisav ja *Sie* välja võib kasutada vabal valikul ning see ei pea sisaldama teavet SSCD toe kohta.

2. Kui on tagatud (garanteeritud CSP_{QC} poolt ja järelevalve-/akrediteerimisasutuse järelevalve all / akrediteeritud), et nimekirja kantud *Sdi* tunnusega teenuse puhul sisaldab mõni SSCD poolt mitte toetatav QC kas kvalifitseeritud sertifikaadile vastavuse tunnust ja/või QCP OIDd, ja see ei peaks sisaldama QcSSCD tunnust või QCP + OIDd, siis on sobiva *Sdi* kasutamine piisav ja *Sie* välja võib kasutada vabal valikul ja see ei pea sisaldama teavet SSCD toe kohta (see tähendab, et seda ei toeta SSCD).

3. Kui on tagatud (garanteeritud CSP_{QC} poolt ja järelevalve-/akrediteerimisasutuse järelevalve all / akrediteeritud), et nimekirja kantud *Sdi* tunnusega teenuse puhul sisaldab mõni QC kvalifitseeritud sertifikaadile vastavuse tunnust ja mõnda sellist QCd peaks toetama SSCD ja mõnda mitte (nt seda võib eristada erinevate CSP sertifitseerimispoliitika objektiidentifikaatoritega (*Certificate Policy* OID) või muu QCs sisalduva CSP teabe kaudu, kas otseselt või kaudselt, masintöödeldavalt või mitte), kuid see ei sisalda EI QcSSCD tunnust EGA ETSI QCP(+) OIDd, siis võib sobiva *Sdi* kasutamine olla ebapiisav JA *Sie* välja tuleb kasutada selleks, et viidata selgelt teabele SSCD toe kohta koos võimaliku laiendatud teabega, et tuvastada hõlmatud sertifikaatide rühma. Sel juhul tuleb ilmselt *Sie* välja kasutades lisada erinevad SSCD toe informatsiooni väärtused sama *Sdi* puhul.

4. Kui on tagatud (garanteeritud CSP_{QC} poolt ja järelevalve-/akrediteerimisasutuse järelevalve all / akrediteeritud), et nimekirja kantud *Sdi* tunnusega teenuse puhul ei sisalda mõni QC ühtegi kvalifitseeritud sertifikaadile vastavuse tunnust, QCP OIDd, QcSSCD tunnust ega QCP + OIDd, kuid on tagatud, et mõned nendest *Sdi* alusel väljastatud lõppkasutaja sertifikaatidest peaksid olema QCd ja/või toetatavad SSCDde poolt ja mõned mitte (nt seda võib eristada erinevate CSP_{QC} sertifitseerimispoliitika objektiidentifikaatoritega või muu QCs sisalduva CSP_{QC} teabe kaudu kas otseselt või kaudselt, masintöödeldult või mitte), siis võib sobiva *Sdi* kasutamine olla ebapiisav JA Sie välja tuleb kasutada selge teabe lisamiseks SSCD toe kohta. Sel juhul tuleb ilmselt *Sie* välja kasutades lisada erinevad SSCD *support information* values sama *Sdi* puhul.

▼C1

Vaikimisi peab usaldusnimekirja kantud CSP puhul olema ühe X.509v3 sertifikaadi kohta üks teenusekirje, kui tegemist on CA/QC tüüpi sertifitseerimisteenusega, st sertifitseerimisasutus väljastab (otse) QCsid. Mõnes hoolikalt kavandatud olukorras ja hoolikalt juhitud ja toetatud tingimustel võib liikmesriigi järelevalveasutus/akrediteerimisasutus otsustada, et ta kasutab juur- või ülataseme sertifitseerija (*Root or Upper level* CA) (st sertifitseerimisasutus, mis ei anna välja otseselt lõppkasutaja QCsid, vaid sertifitseerib CAde hierarhiat kuni CAni, mis väljastab lõppkasutajale QCsid) X.509v3 sertifikaati nimekirja kantud CSP teenuste loetelu ühe kirje *Sdi*-na. Sellise X.509v3 *Root* CA või *Upper* CA kasutamise puhul TLi teenuste kirjete *Sdi* väärtustena tuleb hoolikalt kaaluda selle tagajärgi (eeliseid ja puudusi) ja seda peavad toetama liikmesriigid. Lisaks sellele peavad liikmesriigid üldisest põhimõttest lubatud erandi kasutamisel esitama vajaliku dokumentatsiooni, et hõlbustada sertifitseerimistee loomist ja kontrollimist.

Redigeerimise üldjuhiste illustreerimiseks võib tuua järgmise näite. Olukorras, kus CSP_{QC} kasutab *Root* CAd, mille alusel mitu CAd väljastavad kvalifitseeritud ja mittekvalifitseeritud sertifikaate, kuid mille puhul QCd sisaldavad vaid *QcCompliance* tunnust, mitte aga viidet selle kohta, kas seda toetab SSCD või mitte, tähendab *Root* CA *Sdi* nimekirja kandmine eespool selgitatud eeskirjade kohaselt üksnes seda, et mitte ühtegi selle *Root* CA hierarhia alusel väljastatud QCd EI toeta SSCD. Kui neid QCsid tegelikult SSCD toetab, soovitatakse tungivalt kasutada tulevikus väljastatavate QCde puhul QcSSCD tunnust. Vahepealsel ajal (kuni viimane kõnealust teavet mittesisaldav QC on aegunud) peaks TSL kasutama *Sie* välja ja sellega seotud *Qualifications* laiendust, nt filtreerides sertifikaate eri CSP_{QC} poolt määratletud OIDde kaudu, mida võimaluse korral kasutavad CSP_{QC}-d selleks, et eristada erinevaid QCde tüüpe (millest mõni on SSCD poolt toetatav ja mõni mitte), ja lisades selge SSCD *support information*'i nende filtreeritud sertifikaatide puhul, kasutades *Qualifications* laiendust.

Käesolevatele tehnilistele nõuetele vastava usaldusnimekirja TSLi rakendusel põhineva elektroonilise allkirja rakenduste, teenuste või toodete **kasutamise üldjuhised** on järgmised:

CA/QC *Sti* kirje (sarnaselt CA/QC kirjele, mida täpsemalt kirjeldatakse *Root* CA/QC-na, mille puhul kasutatakse *Sie* teenuse lisainformatsiooni laiendust)

— viitab sellele, et *Sdi* tunnusega CA poolt (sarnaselt CA hierarhias alates *Sdi* tunnusega juursertifitseerijast (*Root* CA)) väljastatavad kõik lõppkasutaja sertifikaadid on QCd **tingimusel**, et nii on väidetud sertifikaadil, kasutades sobivaid kvaliteedisertifikaadi tunnuseid (*QcStatements*) (st QcC, QcSSCD) ja/või ETSI poolt määratletud QCP(+) OIDsid (ja seda tagab järelevalve-/akrediteerimisasutus, vt eespool esitatud redigeerimise üldjuhiseid).

Märkus: kui puudub *Sie Qualifications* teave või kui lõppkasutaja sertifikaati, mis on väidetavalt QC, ei ole täpsemalt tuvastatud seotud Sie kirje kaudu, siis teostatakse QCs leitavat masintöödeldava teabe järelevalvet / seda akrediteeritakse, et see oleks täpne. See tähendab, et oleks tagatud, et sobivate *QcStatement*'ide (st QcC, QcSSCD) ja/või ETSI määratletud QCP(+) OIDde kasutamine (või mittekasutamine) on kooskõlas CSPQC poolt väidetuga;

▼C1

— **ja KUI** *Sie Qualifications* teave on olemas, siis lisaks eespool nimetatud vaikimisi kasutamise tõlgendamise eeskirjale tuleb neid sertifikaate, mida tuvastatakse selle *Sie Qualifications* kirje kasutamise kaudu, mis on loodud sertifikaatide rühma täpsemalt tuvastava filtrite jada põhimõttel ja mis annab lisateavet selle kohta, kas on tegemist SSCD *support*'i ja/või *Legal person as subject*'iga (nt sertifikaadid, mis sisaldavad eri OIDd sertifitseerimispoliitika laienduses ja/või millel on eri *Key usage muster*, ja/või mis on filtreeritud, kasutades eriväärtust, mis ilmneb ühel konkreetsel sertifikaadi väljal või laiendusel jne) käsitleda vastavalt järgmisele kvalifitseerijate rühmale, mis kompenseerib teabe puudumist asjaomases QCs, st:

— et viidata SSCD toele:

  — QCWithSSCD kvalifitseerija väärtus, mis tähendab „SSCD poolt toetatav QC”, või

  — QCNoSSCD kvalifitseerija väärtus, mis tähendab „SSCD poolt mittetoetatav QC”, või

  — QCSSCD*StatusAsInCert* kvalifitseerija väärtus, mis tähendab, et on tagatud, et teave SSCD toe kohta sisaldub iga QC puhul selles CA/QC kirjes *Sdi-Sie* alusel esitatud teabes;

JA/VÕI

— et viidata juriidilisele isikutele väljastamisele:

  — QC*ForLegalPerson* kvalifitseerija väärtus, mis tähendab „sertifikaat on väljastatud juriidilisele isikule”.

2.4. *CA/QC teenuseid toetavad teenused, mis ei ole CA/QC Sdi osa*

Juhtumid, mil sertifikaaditühistusnimistute (CRLs – *Certificate Revocation Lists*) ja OCSP (*Online Certificate Status Protocol* – onlain kehtivuskinnituse teenuse alusprotokoll) kehtivuskinnitused on allkirjastatud peale QCsid väljastava CA (CA/QC) võtmete muude võtmetega, peaksid samuti olema hõlmatud. Seda võib lahendada nii, et need teenused on loetletud sellistena TLi TSLi rakenduses (st teenusetüübi identifikaatoriga, mis on täpsemalt kirjeldatud *additionalServiceInformation* laienduse abil, mis kajastab OCSP või CRL teenust QCde pakkumise osana, nt vastavalt OCSP/QC või CRL/QC teenuse tüübiga), kuna neid teenuseid võib käsitleda järelevalvealuste/akrediteeritud kvalifitseeritud teenuste osana, mis on seotud QC sertifitseerimisteenuste osutamisega. Muidugi tuleb OCSP responderеid või CRLi väljastajaid, kelle sertifikaate allkirjastavad CAd nimekirja kantud CA/QC teenuse hierarhia alusel, käsitleda „kehtivatena” ja kooskõlas nimekirja kantud CA/QC teenuse olekuväärtusega.

Sarnast nõuet võib kohaldada mittekvalifitseeritud sertifikaate (CA/PKC (avaliku võtme sertifikaat – *Public Key Certificate*) teenuse tüüpi) väljastavate sertifitseerimisteenuste suhtes, kasutades vaikimisi ETSI TSi 102 231 OCSP ja CRL teenuse tüüpe.

Juhime tähelepanu sellele, et TLi TSL rakenduses PEAVAD sisalduma tühistusteenused, kui asjakohane teave puudub lõppsertifikaatide AIA (sertifitseerija juurdepääs teabele – *Authority Info Access*) väljal või kui seda ei ole allkirjastanud CA, mis on üks nimekirja kantud CAdest.

2.5. *Koostalitlusvõimelise QC profiili väljaarendamine*

Vastavalt põhimõttele tuleb teenuste kirjete arvu (erinevaid *Sdi*-sid) nii palju kui võimalik vähendada. See peab aga olema tasakaalus nende teenuste korrektse tuvastamisega, mis on seotud QCde väljastamisega ja usaldusväärse teabe pakkumisega selle kohta, kas need QCd on SSCD poolt toetatavad või mitte, kui see teave puudub väljastatud QC-l.

▼C1

Ideaalis peaks Sie välja ja *Qualifications* laienduse kasutamine olema (rangelt) piiratud nende sel viisil lahendatavate erijuhtumitega, kuna QCd peaksid sisaldama piisavalt teavet väidetava kvalifitseeritud oleku kohta ja väidetava SSCD toe või selle puudumise kohta.

Liikmesriigid peaksid võimalikult palju julgustama koostalitlusvõimeliste QC profiilide juurutamist ja kasutamist.

3. **Usaldusnimekirja ühtse vormi struktuur**

Kavandatav liikmesriigi usaldusnimekirja ühtne vorm ehitatakse üles järgmiste teabeliikide kaupa:

1) teave usaldusnimekirja ja selle väljastamissüsteemi kohta;

2) väljade jada, mis sisaldab selget tuvastusteavet iga selle süsteemi alusel järelevalvealuse/akrediteeritud CSP kohta (see jada on valikuline, st kui seda ei kasutata, loetakse nimekirja tühjaks, mis tähendab, et seotud liikmesriigis ei teostata CSPde järelevalvet ega akrediteerita neid usaldusnimekirja ulatust arvestades);

3) iga nimekirja kantud CSP puhul väljade jada, mis sisaldab selget tuvastusteavet CSP poolt osutatava järelevalvealuse/akrediteeritud sertifitseerimisteenuse kohta (selles jadas peab olema vähemalt üks kirje);

4) iga nimekirja kantud järelevalvealuse/akrediteeritud sertifitseerimisteenuse puhul teenuse hetkeoleku tuvastamine ja selle oleku ajalugu.

QCsid väljastava CSPga seoses tuleb nimekirja kantava järelevalvealuse/akrediteeritud sertifitseerimisteenuse selgeks tuvastamiseks arvesse võtta olukordi, kus kvalifitseeritud sertifikaat ei sisalda piisavalt teavet selle kvalifitseeritud oleku kohta, võimaliku SSCD toe kohta, eriti selleks, et arvestada täiendavat asjaolu, et enamik (kommertsalustel töötavaid) CSPsid kasutavad ainult ühte sertifikaate väljastavat kvalifitseeritud CAd, kes väljastab nii kvalifitseeritud kui ka mittekvalifitseeritud lõppkasutaja sertifikaatide eri tüüpe.

Nimekirja kirjete arvu ühe tunnustatud CSP kohta võib vähendada, kui on olemas üks või mitu *Upper* CA teenust, nt CAde ärilise hierarhia olukorras alates *Root* CAst kuni sertifikaate väljastava CAni. Kuid isegi nendel juhtudel tuleb säilitada ja tagada põhimõtte täitmine, mille kohaselt peab olema tagatud selge seos CSP_{QC} sertifitseerimisteenuse ja QCdena tuvastatavate sertifikaatide rühma vahel.

1. *Teave usaldusnimekirja ja selle väljastussüsteemi kohta*

Sellesse kategooriasse kuulub järgmine teave:

— usaldusnimekirja **märgend**, mis hõlbustab usaldusnimekirja tuvastamist elektrooniliste otsingute käigus ja samuti nimekirja eesmärkide kinnitamist, kui nimekiri on inimesele loetaval kujul;

— usaldusnimekirja **formaat ja formaadi versiooni tuvastaja**;

— usaldusnimekirja **järjenumber (või redaktsiooninumber)**;

— teave **usaldusnimekirja tüübi** kohta (nt selleks, et tuvastada asjaolu, et kõnealune usaldusnimekiri sisaldab teavet selliste CSPde poolt osutatavate sertifitseerimisteenuste järelevalve-/akrediteerimisoleku kohta, kelle järelevalvet asjaomane liikmesriik teostab või kelle ta on akrediteerinud, et tagada direktiivi 1999/93/EÜ sätete järgimine);

▼C1

— teave **usaldusnimekirja omaniku** kohta (nt usaldusnimekirja koostamise, turvalise avaldamise ja haldamisega tegeleva liikmesriigi asutuse nimi, aadress, kontaktandmed jne);

— teave usaldusnimekirja aluseks oleva(te) **järelevalve-/akrediteerimissüsteemi (de)** kohta, mis hõlmab muu hulgas järgmisi andmeid:

  — riik, kus seda kohaldatakse,

  — teave või viide selle kohta, kust võib leida teavet süsteemi(de) kohta (süsteemi mudel, eeskirjad, kriteeriumid, piirkond, kus seda kohaldatakse, tüüp jne),

  — (varasema) teabe säilitamise aeg;

— usaldusnimekirja **põhimõtted ja/või juriidiline klausel, kohustused, vastutused**;

— usaldusnimekirja **väljastamise kuupäev ja kellaaeg ja järgmine kavandatav uuendus**.

2. *Selge tuvastusteave iga süsteemi alusel tunnustatava CSP kohta*

See teaberühm sisaldab vähemalt järgmisi andmeid:

— CSP organisatsiooni nimi, mida kasutatakse ametlike juriidiliste kannete puhul (see võib sisaldada CSP organisatsiooni UIDd vastavalt liikmesriigi tavadele);

— CSP aadress ja kontaktandmed;

— lisateave CSP kohta, mis on vahetult kättesaadav või on lisatud viide, kust sellist teavet saab alla laadida.

3. *Iga nimekirja kantud CSP puhul väljade jada, mis sisaldab selget tuvastusteavet CSP poolt osutatava ja direktiivi 1999/93/EÜ alusel järelevalvatava/akrediteeritud sertifitseerimisteenuse kohta*

See teaberühm sisaldab nimekirja kantud CSP iga sertifitseerimisteenuse kohta vähemalt järgmisi andmeid:

— sertifitseerimisteenuse tüübi identifikaator (nt identifikaator, mis näitab, et CSP poolt osutatava järelevalvealuse/akrediteeritud sertifitseerimisteenuse puhul on tegemist QCde väljastamisega sertifitseerimisasutuse poolt);

— sertifitseerimisteenuse (kaubamärk) nimi;

— sertifitseerimisteenuse selge kordumatu identifikaator;

— lisateave sertifitseerimisteenuse kohta (nt vahetult kättesaadav teave või lisatud viide, kust sellist teavet saab alla laadida, teave teenusele juurdepääsu kohta);

— CA/QC teenuste puhul valikuline informatsiooniennikute jada, kus iga ennik sisaldab järgmist:

  i) kriteeriumid, mida kasutatakse selleks, et *Sdi* alusel tuvastatava sertifitseerimisteenuse hulgast täpsemalt tuvastada (filtreerida) teenus (st kvalifitseeritud sertifikaatide rühm), mille puhul nõutakse/esitatakse lisateavet seoses SSCD toele viitamisega (ja/või juriidilisele isikule väljastamisega); ja

  ii) seotud teave (kvalifitseerijad) selle kohta, kas täpsemalt tuvastatud kvalifitseeritud sertifikaatide teenuste rühma toetab SSCD või mitte või kas see seotud teave on QC osa standardiseeritud masintöödeldaval kujul, ja/või teave selle kohta, et selliseid QCsid väljastatakse juriidilistele isikutele (vaikimisi loetakse neid väljastatuks üksnes füüsilistele isikutele).

▼C1

4. *Iga nimekirja kantud sertifitseerimisteenuse puhul teenuse hetkeoleku tuvastamine ja selle oleku ajalugu*

See teaberühm sisaldab vähemalt järgmisi andmeid:

— hetkeoleku identifikaator;

— hetkeoleku alguskuupäev ja -kellaaeg;

— varasem teave oleku kohta.

4. **Mõisted ja lühendid**

Käesolevas dokumendis kasutatakse järgmisi mõisteid ja akronüüme:

Mõiste	Akronüüm	Määratlus
Sertifitseerimisteenuse osutaja	CSP	Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 11 määratlusele.
Sertifitseerimisasutus	CA	Sertifitseerimisasutus on sertifitseerimisteenuse osutaja ja ta võib kasutada lõppkasutaja sertifikaatide väljastamiseks erinevaid tehnilisi CAde isiklikke signeerimisvõtmeid, millest igaühel on seotud sertifikaat. CA on ühe või mitme kasutaja poolt usaldatav sertifikaatide loomise ja määratlemise asutus. Sertifitseerimisasutus võib lisaks luua kasutaja võtmeid (ETSI TS 102 042). CA peaks olema tuvastatav CA sertifikaadi väljastaja väljal oleva tuvastusteabe kaudu, mis on seotud CA isikliku signeerimisvõtmega seotud avaliku võtmega (sertifitseerimisega), mida CA tegelikult kasutab kasutajasertifikaatide väljastamiseks. CA-l võib olla mitu signeerimisvõtit. Iga CA signeerimisvõti on kordumatult tuvastatud kordumatu identifikaatoriga, mis on CA sertifikaadi avaliku võtme identifikaatori välja osa.
Kvalifitseeritud sertifikaate väljastav sertifitseerimisasutus	CA/QC	CA, mis vastab direktiivi 1999/93/EÜ II lisas sätestatud nõuetele ja väljastab kvalifitseeritud sertifikaate, mis vastavad direktiivi 1999/93/EÜ I lisas sätestatud nõuetele.
Sertifikaat	Sertifikaat	Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 9 määratlusele.
Kvalifitseeritud sertifikaat	QC	Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 10 määratlusele.
Allakirjutaja	Allakirjutaja	Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 3 määratlusele
Järelevalve	Järelevalve	Mõistet „järelevalve” kasutatakse direktiivi 1999/93/EÜ artikli 3 lõike 3 tähenduses. Direktiivis on nõutud, et liikmesriigid kehtestaksid sobiva süsteemi, mis võimaldab valvata riigi territooriumil asuvate ja üldsusele kvalifitseeritud sertifikaate väljastavate sertifitseerimisteenuste osutajate järele, tagades direktiivis sätestatud nõuete täitmise järelevalve.
Vabatahtlikkusel põhinev akrediteerimine	Akrediteerimine	Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 13 määratlusele.
Usaldusnimekiri	TL	Mõiste tähistab nimekirja, mis näitab selliste sertifitseerimisteenuse osutajate pakutava sertifitseerimisteenuse järelevalve-/akrediteerimisolekut, kelle järele asjaomane liikmesriik valvab või kelle ta on akrediteerinud, et tagada direktiivi 1999/93/EÜ sätete järgimine.

▼C1

Mõiste	Akronüüm	Määratlus
Usaldusteenuse oleku nimekiri	TSL	Allkirjastatud nimekirja vorm, mida kasutatakse usaldusteenuse oleku kohta teabe esitamise alusena vastavalt ETSI TSi 102 231 nõuetele.
Usaldusteenus		Teenus, mis tõstab usaldust ja kindlust elektrooniliste tehingute suhtes (mille puhul kasutatakse tavaliselt, kuid mitte tingimata, krüpteerimistehnikaid või mis on seotud konfidentsiaalse materjaliga) (ETSI TS 102 231).
Usaldusteenuse osutaja	TSP	Asutus, mis osutab ühte või mitut (elektroonilist) usaldusteenust. (Seda mõistet kasutatakse laiemas tähenduses kui CSPd.)
Usaldusteenuse märk	TrST	Füüsiline või binaarne (loogiline) objekt, mis tekib või väljastatakse usaldusteenuse kasutamise tulemusel. Binaarsed TrSTd on näiteks sertifikaadid, CRLd, ajatemplid ja OCSP kehtivuskinnitused.
Kvalifitseeritud elektrooniline allkiri	QES	Täiustatud elektrooniline allkiri, mida toetab kvalifitseeritud sertifikaat ja mis on loodud direktiivi 1999/93/EÜ artiklis 2 määratletud turvalise allkirja andmise vahendiga.
Täiustatud elektrooniline allkiri	AdES	Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 2 määratlusele.
Kvalifitseeritud sertifikaadiga toetatav täiustatud elektrooniline allkiri	$AdES_{QC}$	Mõiste tähistab elektroonilist allkirja, mis vastab AdES nõuetele ja mida toetab direktiivi 1999/93/EÜ artiklis 2 määratletud QC.
Turvalise allkirja andmise vahend	SSCD	Vastavalt direktiivi 1999/93/EÜ artikli 2 lõike 6 määratlusele.

I PEATÜKK

JÄRELEVALVEALUSE/AKREDITEERITUD SERTIFITSEERIMISTEENUSE OSUTAJATE USALDUSNIMEKIRJA ÜHTSE VORMI ÜKSIKASJALIK KIRJELDUS

Dokumendi järgmises osas tuleb võtmesõnu TULEB, EI TOHI, KOHUSTUSLIK, PEAB, EI PEA, PEAKS, EI PEAKS, SOOVITATAV, VÕIB ja VALIKULINE tõlgendada vastavalt kommentaarinõudes (*Request for Comments* – RFC) 2119 ([1]) esitatud kirjeldusele.

►**M1** Käesolevad nõuded põhinevad ETSI TS 102 231 punktis v.3.1.2 sätestatud tingimustel ja nõuetel. Kui käesolevas kirjelduses ei ole sätestatud erinõudeid, siis PEAB kohaldama täielikult ETSI TS 102 231 punkti v.3.1.2 nõudeid. ◄ Kui käesolevas kirjelduses on sätestatud erinõuded, PEAB neid käsitama vastavate ETSI TSi 102 231 nõuete suhtes ülimuslikena, kusjuures nende täitmisel tuleb võtta aluseks ETSI TSis 102 231 esitatud vorminõuded. Käesolevas kirjelduses ja ETSI TSi 102 231 nõuetes esinevate lahknevuste korral PEAB normdokumendiks võtma käesoleva kirjelduse.

([1]) *Internet Engineering Task Force Request for Comments – IETF RFC 2119: Key words for use in RFCs to indicate Requirements Levels.*

▼C1

Keeleabi PEAB rakendama ja pakkuma vähemalt inglise keeles (EN) ja võimaluse korral lisaks ühes või enamas riigikeeles.

Kuupäevale ja kellaajale viitamisel PEAB lähtuma ETSI TSi 102 231 punktist 5.1.4.

URIde kasutamine PEAB olema kooskõlas ETSI TSi 102 231 punktiga 5.1.5.

Teave usaldusnimekirja väljastamise süsteemi kohta

Tag

TSL *tag* (punkt 5.2.1)

See väli on KOHUSTUSLIK ja see PEAB olema kooskõlas ETSI TSi 102 231 punktiga 5.2.1.

▼M1

_____

▼C1

Scheme Information

TSL *version identifier* (punkt 5.3.1)

See väli on KOHUSTUSLIK ja see peab olema määratud arvuga 3 (täisarv).

TSL *sequence number* (punkt 5.3.2)

▼M1

See väli on KOHUSTUSLIK. Selles PEAB olema esitatud TSLi järjenumber. Alates numbrist „1” TSLi esimeses redaktsioonis PEAB seda täisarvulist väärtust kasvatama igas järgmises TSLi redaktsioonis. Kui eespool nimetatud tunnust „TSL version identifier” kasvatatakse, siis EI TOHI nimetatud väärtust taas arvuni „1” taandada.

▼C1

TSL *type* (punkt 5.3.3)

▼M1

See väli on KOHUSTUSLIK ning sellel peab olema esitatud TSLi tüüp. See PEAB olema määratud http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic).

▼C1

Märkus: et täita ETSI TSi 102 231 punkti 5.3.3 nõudeid ja osutada konkreetsele TSLi tüübile, kui viidatakse käesoleva kirjelduse olemasolule, mis reguleerib liikmesriikide usaldusnimekirja [1] TSL rakenduse koostamist ja võimaldab parseril kindlaks teha, millist järgmiste väljade [2] vormi eeldada, kui nendel väljadel on konkreetsed (või alternatiivsed) tähendused vastavalt esindatavale TSLi tüübile (sel juhul on tegemist liikmesriigi usaldusnimekirjaga), PEAB registreerima eespool esitatud URI ja kirjeldama seda järgmiselt:

[1] st selliste sertifitseerimisteenuse osutajate sertifitseerimisteenuste kontrolli-/akrediteerimisoleku nimekiri, kelle üle asjaomane liikmesriik teostab järelevalvet või kelle ta on akrediteerinud, et tagada direktiivi 1999/93/EÜ asjaomaste sätete järgimine (lühidalt „usaldusnimekiri”).

[2] St väljad, mida on kirjeldatud ETSI TSis 102 231 – *Electronic Signatures and Infrastructures* – ESI: *Provision of harmonized Trust-service status information*, mis on profileeritud käesoleva kirjeldusega, et täpsustada liikmesriikide usaldusnimekirja koostamise nõudeid.

▼M1

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

▼C1

Kirjeldus: selliste sertifitseerimisteenuse osutajate sertifitseerimisteenuste järelevalve-/akrediteerimisoleku nimekirja TSL rakendus, kelle järele asjaomane TSL rakendust omav liikmesriik valvab või kelle ta on akrediteerinud, et tagada direktiivi 1999/93/EÜ asjaomaste sätete järgimine.

Scheme operator name (punkt 5.3.4)

See väli on KOHUSTUSLIK. Selles PEAB olema esitatud riigi usaldusnimekirja koostamise, avaldamise ja haldamisega tegeleva liikmesriigi asutuse nimi. Selles PEAB olema esitatud ametlik nimi, mille all tegutseb nimetatud asutusega seotud juriidiline isik või volitatud üksus (nt riigiasutus). See PEAB olema nimi, mida kasutatakse ametlike juriidiliste kannete või lubade puhul ja millele adresseeritakse kõik ametlikud teated. See PEAB olema mitmekeelsete märgistringide jada ning PEAB olema rakendatav inglise keeles (EN), mis on kohustuslik keel ja võimaluse korral lisaks ühes või enamas riigikeeles.

Märkus: riigil VÕIB olla eraldi järelevalve- ja akrediteerimisasutus ja isegi täiendavad asutused mis tahes seotud tegevuste elluviimiseks. ►M1 Iga liikmesriik määrab ise oma riigi TLi TSL-rakenduse süsteemioperaatori. ◄ Eeldatakse, et nii järelevalve- ja akrediteerimisasutusel kui ka süsteemioperaatoril (kui need on eraldiseisvad asutused) on igaühel oma vastutusvaldkonnad ja kohustused. Iga selline olukord, kus järelevalve, akrediteerimise või operatiivküsimuste eest vastutab mitu asutust, PEAB olema selgelt kajastatud ja sellisena tuvastatav TLi osaks olevas süsteemi käsitlevas teabes, sealhulgas *Scheme information* URI väljal (punkt 5.3.7) viidatud teabes süsteemi kohta.

Iga selline olukord, kus järelevalve, akrediteerimise või operatiivküsimuste eest vastutab mitu asutust, PEAB olema selgelt kajastatud ja sellisena tuvastatav TLi osaks olevas süsteemi käsitlevas teabes, sealhulgas Scheme information URI väljal (punkt 5.3.7) viidatud teabes süsteemi kohta.

▼M1

Määratud süsteemioperaator (punkt 5.3.4) on üksus, kes allkirjastab TSLi.

▼C1

Scheme operator address (punkt 5.3.5)

See väli on KOHUSTUSLIK. Selles PEAB olema esitatud *Scheme operator name* väljal (punkt 5.3.4) tuvastatava juriidilise isiku või volitatud organisatsiooni aadress teabe edastamiseks nii posti teel kui ka elektrooniliselt. Selles PEAB sisalduma nii *PostalAddress* (st tänava nimi, asukoht, (riik või piirkond), (postiindeks) ning standardile ISO 3166-1 vastav kahetäheline riigikood) vastavalt punktile 5.3.5.1 kui ka *ElectronicAddress* (st e-posti aadress ja/või veebilehe URI) vastavalt punktile 5.3.5.2.

Scheme name (punkt 5.3.6)

See väli on KOHUSTUSLIK ning sellel peab olema näidatud, millise nime all süsteem tegutseb. See PEAB olema mitmekeelsete märgistringide jada, (kus EN on kohustuslik keel, millele lisandub võimaluse korral üks või enam riigikeelt), mis on määratletud järgmiselt:

▼C1

— EN-versioon PEAB olema märgistring, mis on struktureeritud järgmiselt:

CC:EN_name_value

kus

— „CC” = standardile ISO 3166-1 vastav kahetäheline riigikood, mida kasutatakse *Scheme territory* väljal (punkt 5.3.10);

— „:” = kasutatakse eraldajana;

▼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

— mis tahes liikmesriigi keeleversioon PEAB olema märgistring, mis on struktureeritud järgmiselt:

CC:name_value

kus

— „CC” = standardile ISO 3166-1 vastav kahetäheline riigikood, mida kasutatakse *Scheme territory* väljal (punkt 5.3.10);

— „:” = kasutatakse eraldajana;

— „name_value” = eespool esitatud „EN_name_value” riigikeelne ametlik tõlge.

Süsteemi nimi on nõutav üksnes selleks, et tuvastada nime järgi *Scheme information* URI väljal viidatud süsteem ning tagada, et juhul, kui süsteemioperaator opereerib rohkem kui ühte kava, siis on igaühele neist antud erinev nimi.

Liikmesriigid ja süsteemioperaatorid PEAVAD tagama, et kui liikmesriik või süsteemioperaator opereerib rohkem kui ühte kava, siis on igaühele neist antud erinev nimi.

Scheme information URI (punkt 5.3.7)

See väli on KOHUSTUSLIK ning sellel PEAVAD olema esitatud URI(d), kust kasutajad (sõltuvad osapooled) võivad saada teavet süsteemi kohta (kus EN on kohustuslik keel, millele lisandub võimaluse korral üks või enam riigikeelt). See PEAB olema mitmekeelsete viitade jada (kus EN on kohustuslik keel, millele lisandub võimaluse korral üks või enam riigikeelt). Viidatud URI(d) PEAVAD viima teabeallikani, kust leida asjakohast teavet skeemi kohta (*appropriate information about the scheme*).

Asjakohane teave skeemi kohta PEAB sisaldama vähemalt järgmist:

— kõigi liikmesriikide puhul ühtset tutvustavat üldteavet usaldusnimekirja ulatuse ja tausta ning selle aluseks oleva(te) järelevalve-/-akrediteerimisüsteemi(de) kohta. Ühtne tekst, mida tuleb kasutada, on järgmine:

▼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, etc.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis."

— teavet usaldusnimekirja aluseks oleva(te) järelevalve-/akrediteerimisüsteemi (de) kohta, eelkõige ([1]):

— teave kõigi CSP_{QC}-de suhtes kohaldatava järelevalvesüsteemi kohta;

([1]) Kaks viimast teaberühma on kasutajate jaoks eriti olulised selleks, et hinnata selliste järelevalve-/akrediteerimissüsteemide kvaliteedi ja turvalisuse taset. Nimetatud teaberühmad tuleb esitada usaldusnimekirja tasemel, kasutades käesolevat *Scheme information* URI välja (punkt 5.3.7 – liikmesriikide poolt esitatav teave), *Scheme type/community/rules* välja (punkt 5.3.9 – kasutades kõigi liikmesriikide jaoks ühtset teksti) ja „TSL policy/legal notice" välja (punkt 5.3.11 – kõigi liikmesriikide jaoks ühtne tekst, milles viidatakse direktiivile 1999/93/EÜ koos kõigi liikmesriikide võimalusega lisada liikmesriigi jaoks septsiifilist teksti/viiteid). Vajaduse korral ja kui see on nõutav (nt et eristada mitut kvaliteedi/turvalisuse taset) võib esitada täiendavat teavet QCsid mitteväljastavate CSPde siseriiklike järelevalve-/akrediteerimissüsteemide kohta teenuse tasemel, kasutades *Scheme service definition* URI välja (punkt 5.5.6).

▼C1

— vajaduse korral teave kõigi CSP_{QC}-de suhtes kohaldatava siseriikliku vabatahtlikkusel põhineva akrediteerimise süsteemi kohta;

— vajaduse korral teave kõigi QCsid mitteväljastavate CSPde suhtes kohaldatava järelevalvesüsteemi kohta;

— vajaduse korral teave kõigi QCsid mitteväljastavate CSPde suhtes kohaldatava siseriikliku vabatahtlikkusel põhineva akrediteerimise süsteemi kohta;

— see teave PEAB sisaldama iga eespool loetletud süsteemi kohta vähemalt järgmist:

— üldist kirjeldust;

— teavet protsessi kohta, mida järgib järelevalve-/akrediteerimisasutus CSPde järelevalve/akrediteerimise korral ja mida järgivad CSPd nende järelevalve/akrediteerimise korral;

— teavet kriteeriumide kohta, mille alusel CSPde järelevalvet teostatakse / neid akrediteeritakse;

— vajaduse korral teavet mõne sertifitseerimisteenuse osutamise tulemusel tekkiva või väljastatava füüsilise või binaarse (loogilise) objekti erikvalifikatsioonide kohta, mis on antud, lähtudes nende vastavusest siseriiklikult kehtestatud normide ja nõuetega, mis hõlmab ka sellise kvalifikatsiooni ja sellega seotud siseriiklike normide ja nõuete tähendust.

Liikmesriik VÕIB vabatahtlikult esitada täiendavat teavet oma süsteemi kohta. See teave PEAB sisaldama järgmist:

— teavet kriteeriumide ja eeskirjade kohta, mida kasutatakse järelevalve teostajate / audiitorite valikul ja selle kohta, kuidas nad CSPde järelevalvet teostavad (kontrollivad) / neid akrediteerivad (auditeerivad);

— muud kontakt- ja üldteavet süsteemi toimimise kohta.

Status determination approach (punkt 5.3.8)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud oleku määramise viisi identifikaator. Selleks PEAB kasutama konkreetset URIt, mille aadress ja kirjeldus on järgmised:

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

Kirjeldus: nimekirja kantud teenuste oleku määrab süsteemioperaator või tema esindaja asjakohase süsteemi alusel, mida kohaldatakse viidatud liikmesriigis, kes lubab teostada oma territooriumil asutatud (või vabatahtlikkusel põhineva akrediteerimise puhul kolmandas riigis asutatud) ja vastavalt direktiivi 1999/93/EÜ artikli 3 lõikele 3 (vastavalt artikli 3 lõikele 2 või artikli 7 lõike 1 punktile a) üldsusele kvalifitseeritud sertifikaate väljastatavate sertifitseerimisteenuse osutajate järelevalvet (ja vajaduse korral vabatahtlikkusel põhinevat akrediteerimist) ja kes lubab vajaduse korral teostada järelevalvet / vabatahtlikkusel põhinevat akrediteerimist kvalifitseeritud sertifikaate mitteväljastavate sertifitseerimisteenuse osutajate suhtes vastavalt riiklikult määratletud ja kehtestatud tunnustatud heakskiitmissüsteemi(de)le, mida rakendatakse siseriiklikel alustel, et kontrollida QCsid mitteväljastavate CSPde poolt osutatavate teenuste vastavust direktiivi 1999/93/EÜ sätetega ja võimaluse korral laiemalt selliste sertifitseerimisteenuste suhtes kohaldatavate siseriiklike sätetega.

▼C1

Scheme type/community/rules (punkt 5.3.9)

See väli on KOHUSTUSLIK ning sellel PEAVAD sisalduma vähemalt järgmised registreeritud URId:

— kõigi liikmesriikide usaldusnimekirjade jaoks ühine URI, mis viitab kirjeldavale tekstile, mida PEAB kasutama kõigi usaldusnimekirjade puhul:

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

— millega väljendatakse liikmesriigi süsteemi osalemist (tuvastatav TSL type välja (punkt 5.3.3) ja *Scheme name* välja (punkt 5.3.6) kaudu) üldises süsteemis (st TSL nimekirjade viited kõigile liikmesriikidele, kes avaldavad ja haldavad TLi TSLi kujul);

— kust kasutajad pääsevad ligi põhimõtetele/eeskirjadele, mille suhtes PEAB nimekirja kantud teenuseid hindama ja mille alusel võib määratleda TSLi tüüpi (vt punkt 5.3.3);

— kust kasutajad leiavad kirjelduse, kuidas kasutada ja tõlgendada usaldusnimekirja TSL rakenduse sisu. Need kasutuseeskirjad PEAVAD olema ühtsed kõigi liikmesriikide usaldusnimekirjade puhul, olenemata nimekirja kantud teenuse tüübist ja järelevalve-/akrediteerimissüsteemi(de)st.

Kirjeldav tekst:

„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, etc.) 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 „Root CA/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, etc.). 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 2009/767/EC for further details on the fields, description and meaning for the TSL implementation of the Member States' Trusted Lists.”

▼C1

— Iga liikmesriigi usaldusnimekirja URI, mis viitab kirjeldavale tekstile, mida PEAB kohaldama selle liikmesriigi TLi suhtes:

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

kus CC = standardile ISO 3166-1 vastav kahetäheline riigikood, mida kasutatakse *Scheme territory* väljal (punkt 5.3.10),

— kust kasutajad pääsevad ligi põhimõtetele/eeskirjadele, mille suhtes PEAB nimekirja kantud teenuseid hindama vastavalt liikmesriigi asjaomastele järelevalvesüsteemile ja vabatahtlikkusel põhinevatele akrediteerimissüsteemidele;

— kust kasutajad võivad leida asjaomase liikmesriigi kirjelduse selle kohta, kuidas kasutada ja tõlgendada usaldusnimekirja TSL rakenduse sisu QCde väljastamisega mitteseotud sertifitseerimisteenuste puhul. Seda võib kasutada selleks, et viidata QCsid mitteväljastavate CSPdega seotud siseriiklike järelevalve-/akrediteerimissüsteemide võimalikule detailsusele ja sellele, kuidas kasutada Scheme service definition URI (punkt 5.5.6) ja *Service information extension* välju sellel eesmärgil.

Liikmesriigid VÕIVAD määratleda täiendavaid URIsid lisaks eespool nimetatud liikmesriigi URI-le (st URId, mis on eristatavad sellest hierarhilisest URIst).

Scheme territory (punkt 5.3.10)

Käesoleva kirjelduse kohaldamisel on see väli KOHUSTUSLIK ja selles PEAB olema näidatud, millises riigis on see süsteem kehtestatud (standardile ISO 3166-1 vastav kahetäheline riigikood).

TSL policy/legal notice (punkt 5.3.11)

Käesoleva kirjelduse kohaldamisel on see väli KOHUSTUSLIK ja selles PEAVAD olema esitatud süsteemi põhimõtted või peab olema näidatud süsteemi juriidiline staatus või selles riigis süsteemi suhtes kohaldatavad juriidilised nõuded, kus süsteem on kehtestatud ja/või mis tahes piirangud ja tingimused, mille alusel TLi hallatakse ja avaldatakse.

See PEAB ole mitmekeelne märgistring (lihttekst), mis koosneb kahest osast:

— esimene, kohustuslik osa, mis on ühine kõigi liikmesriikide TLide puhul (kus EN on kohustuslik keel, millele lisandub võimaluse korral üks või enam riigikeelt), kus on viidatud, et kohaldatav õigusraamistik on direktiiv 1999/93/EÜ ja selle vastav rakenduskord liikmesriigi õigusaktides, millele on viidatud *Scheme Territory* väljal.

Ühtse teksti ingliskeelne versioon:

„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.”

Tekst liikmesriikide keel(t)es: [eespool esitatud ingliskeelse teksti ametlik tõlge (ametlikud tõlked)].

▼C1

— Teine, valikuline osa, mis on iga TLi puhul erinev (kus EN on kohustuslik keel, millele lisandub võimaluse korral üks või enam riigikeelt), kus viidatakse kohaldatavatele siseriiklikele õiguslikele raamistikele (nt eelkõige seoses QCsid mitteväljastavate CSPde siseriiklike järelevalve-/-akrediteerimissüsteemidega).

Historical information period (punkt 5.3.12)

See väli on KOHUSTUSLIK ning sellel PEAB olema näidatud, millise perioodi kohta (täisarv) esitatakse TSLis varasemat teavet. See täisarvuline väärtus peab olema esitatud päevade arvuna ja käesoleva kirjelduse puhul PEAB see arv olema 3 653 või üle selle (st liikmesriikide TLi TSL rakendus PEAB sisaldama varasemat teavet vähemalt kümne aasta kohta). Suuremate väärtuste puhul tuleks võtta arvesse andmete säilitamisega seotud juriidilisi nõudeid *Scheme Territory* väljal (punkt 5.3.10) viidatud liikmesriigis.

Pointers to other TSLs (punkt 5.3.13)

Käesoleva kirjelduse kohaldamisel on see väli KOHUSTUSLIK ja selles PEAB sisalduma selle olemasolu korral viide ETSI TSile 102 231 vastavale Euroopa Komisjoni koostatud linkide (viidete) loetelule, mis on suunatud liikmesriikide usaldusnimekirjade kõigile TSL rakendustele. ETSI TSi 102 231, punkti 5.3.13 nõudeid kohaldatakse, kui antakse luba valikulise digitaalse tunnuse kasutamiseks, mis esindab viidatud TSLi väljastajat ja mis on vormistatud vastavalt punktile 5.5.3.

Märkus: enne Euroopa Komisjoni poolt koostatud ETSI TSile 102 231 vastava liikmesriikide TLide TSLi rakenduste juurde suunavate linkide loetelu kasutusse-võtmist EI TOHI seda välja kasutada.

List issue date and time (punkt 5.3.14)

See väli on KOHUSTUSLIK ning sellel PEAVAD olema esitatud TSLi väljastamise kuupäev ja kellaaeg (kasutada koordineeritud maailmaaega (*Coordinated Universal Time* – UTC) ehk *Zulu* aega), kasutades ETSI TSi 102 231 punktis 5.1.4 sätestatud kuupäeva ja kellaaja väärtust.

Next update (punkt 5.3.15)

See väli on KOHUSTUSLIK ning sellel PEAVAD olema esitatud kuupäev ja kellaaeg (kasutada koordineeritud maailmaaega (*Coordinated Universal Time* – UTC) ehk *Zulu* aega), millal hiljemalt peab olema väljastatud järgmine TSL, või on see jäetud tühjaks, viidates suletud TSLile (kasutades ETSI TSi 102 231 punktis 5.1.4 sätestatud kuupäeva ja kellaaja väärtust).

Kui süsteemiga hõlmatud TSP või teenuse olekus vahepealseid muutusi ei toimu, TULEB TSL uuesti väljastada selleks ajaks, kui viimase väljastatud TSLi kehtivus lõpeb.

Käesoleva kirjelduse kohaldamisel EI TOHI erinevus *Next update* kuupäeva ja kellaaja ning *List issue date and time* vahel olla suurem kui **kuus (6)** kuud.

▼C1

Distribution points (punkt 5.3.16)

See väli on VALIKULINE. Kui seda kasutatakse, siis PEAVAD sellel olema näidatud kohad, kus on avaldatud kehtiv TLi TSL rakendus ja kust võib leida kehtiva TSLi uuendusi. Kui on märgitud mitu jaotuspunkti, PEAVAD nad kõik andma kehtiva TSLi või selle uuendatud versiooni identsed koopiad. Kui seda välja kasutatakse, siis vormindatakse see stringide mittetühja jadana, kus iga string vastab RFCle 3986 ([1]).

Scheme extensions (punkt 5.3.17)

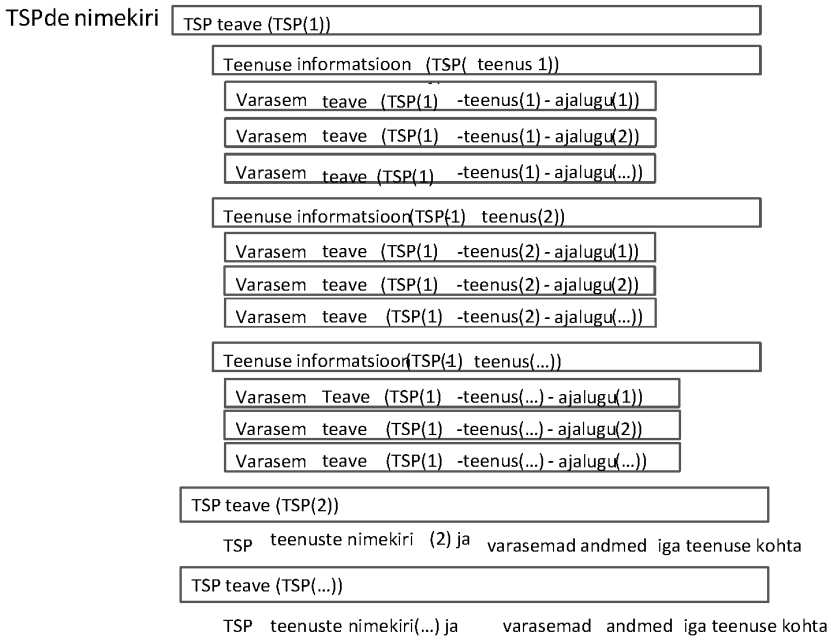
See väli on VALIKULINE ja seda ei kasutata käesoleva kirjelduse kohaldamisel.

List of Trust Service Providers

See väli on VALIKULINE.

Kui liikmesriigis ei teostata või ei teostatud CSPde järelevalvet ning neid ei akrediteerita ega akrediteeritud süsteemi alusel, siis PEAB see väli puuduma. Kuid on kokku lepitud, et isegi, kui süsteemi alusel liikmesriigis CSPde järelevalvet ei teostata ning neid ei akrediteerita, PEAVAD liikmesriigid rakendama TSLi ilma selle väljata. Mõne CSP nimekirjast puudumist TULEB mõista nii, et väljal *Scheme Territory* näidatud liikmesriigis ei teostata CSPde järelevalvet / neid ei akrediteerita.

Kui süsteemi alusel teostatakse või teostati ühe või enama CSP teenuse järelevalvet või neid akrediteeritakse või akrediteeriti, PEAB väli sisaldama jada, milles on tuvastatud ühte või mitut sellist järelevalvealust/akrediteeritud teenust osutav CSP koos andmetega iga CSP teenuse järelevalve-/akrediteerimisoleku ja oleku ajaloo kohta (allpool esitatud joonisel TSP = CSP).



([1]) IETF RFC 3986: „Uniform Resource Identifiers (URI): Generic syntax”.

▼C1

TSPde nimekiri on struktureeritud nagu eelneval joonisel kujutatud. Igal TSP-l on väljade jada, mis sisaldab teavet TSP kohta (TSP *Information*), millele järgneb teenuste loetelu. Igal nimekirja kantud teenusel on väljade jada, mis sisaldab teavet teenuse kohta (*Service Information*), ja väljade jada teenuse kinnitamise oleku ajaloo kohta (*Service approval history*).

TSP Information

TSP(1)

TSP name (punkt 5.4.1)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud süsteemi alusel CSPde teenuste järelevalvet teostava või neid akrediteeriva **juriidilise isiku** nimi. See on mitmekeelsete märgistringide jada (kus EN on kohustuslik keel, millele lisandub võimaluse korral üks või enam riigikeelt). See PEAB olema nimi, mida kasutatakse ametlike juriidiliste kannete puhul ja millele adresseeritakse kõik ametlikud teated.

TSP trade name (punkt 5.4.2)

See väli on VALIKULINE ja kui seda kasutatakse, PEAB sellel olema märgitud alternatiivne nimi, mille alusel CSP tuvastab end eriolukorras, kui ta osutab neid teenuseid, mida võib leida käesolevas TSLis tema TSP *name* (punkt 5.4.1) väljal.

Märkus: kui üks juriidilisest isikust CSP osutab teenuseid erinevate kaubamärkide all või erinevates eriolukordades, siis võib olla sama palju CSP kirjeid, kui on selliseid eriolukordi (nt nime/kaubamärgi kirjed). Teine võimalus on kanda iga CSP (juriidiline isik) nimekirja vaid üks kord ja lisada teave teenuse eriolukorra kohta. Liikmesriigi süsteemioperaator peab nõu CSPga ja lepib temaga kokku sobivaima lähenemisviisi suhtes.

TSP address (punkt 5.4.3)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud TSP *name* väljal (punkt 5.4.1) tuvastatava juriidilise isiku või volitatud organisatsiooni aadress teadete edastamiseks nii posti teel kui ka elektrooniliselt. Selles PEAB sisalduma nii *PostalAddress* (st tänava nimi, asukoht, (riik või piirkond), (postiindeks) ning standardile ISO 3166-1 vastav kahetäheline riigikood) vastavalt punktile 5.3.5.1 kui ka *ElectronicAddress* (st e-posti aadress ja/või veebilehe URI) vastavalt punktile 5.3.5.2.

TSP information URI (punkt 5.4.4)

See väli on KOHUSTUSLIK ning sellel PEAB (PEAVAD) olema esitatud URI (d), kust kasutajad (nt sõltuvad osapooled) saavad teavet CSP kohta. See PEAB olema mitmekeelsete viitade jada (kus EN on kohustuslik keel, millele lisandub võimaluse korral üks või enam riigikeelt). Viidatud URI(d) PEAB (PEAVAD) juhtima teabeni, kus on selgitatud CSP üldisi tingimusi, tavasid, juriidilisi küsimusi, klienditeeninduspoliitikat ja muud üldteavet kõigi CSP teenuste kohta, mis on loetletud TSLis sisalduvas CSP kirjes.

Märkus: kui üks juriidilisest isikust CSP osutab teenuseid erinevate kaubamärkide all või erinevates eriolukordades ja seda on kajastatud sama hulga TSP kirjetena kui on selliseid eriolukordi, siis PEAB see väli sisaldama teavet konkreetse TSP/TradeName kirje all loetletud teenusterühma kohta.

▼C1

TSP information extensions (punkt 5.4.5)

See väli on VALIKULINE ja kui seda kasutatakse, VÕIB süsteemioperaator seda kasutada kooskõlas ETSI TSi 102 231 nõuetega (punkt 5.4.5) selleks, et esitada konkreetset teavet, mida tuleb tõlgendada vastavalt konkreetse süsteemi eeskirjadele.

List of Services

See väli on KOHUSTUSLIK ning sellel PEAB sisalduma kõigi CSP tunnustatud teenuste jada ja iga teenuse kinnitamise olek (ning selle oleku ajalugu). Nimekirja peab olema kantud vähemalt üks teenus (isegi juhul, kui on olemas vaid varasem teave).

Kuna käesoleva kirjelduse alusel on KOHUSTUSLIK varasema teabe säilitamine, TULEB varasemat teavet säilitada isegi juhul, kui teenuse hetkeoleku puhul ei ole selle nimekirja kandmine üldjuhul kohustuslik (nt teenusest on loobutud). Seega PEAB CSP olema hõlmatud isegi juhul, kui selle ainus nimekirja kantud teenus on sellises olekus, et säilitada selle ajalugu.

Service Information

TSP(1) Service(1)

Service type identifier (punkt 5.5.1)

▼M1

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud teenusetüübi identifikaator vastavalt käesolevates TSLi nõuetes sisalduvale tüübile (st „/-eSigDir-1999-93-EC-TrustedList/TSLType/generic”).

▼C1

Kui nimekirja kantud teenus on seotud kvalifitseeritud sertifikaatide väljastamisega, PEAB viidatavaks URIks olema http://uri.etsi.org/TrstSvc/Svctype/CA/QC (kvalifitseeritud sertifikaate väljastav sertifitseerimisasutus).

Kui nimekirja kantud teenus on seotud usaldusteenuse märkide väljastamisega, mis ei ole QCd ega toeta QCde väljastamist, PEAB viidatavaks URIks olema üks ETSIs 102 231 määratletud ja selle punktis D.2 loetletud URIdest, mis on seotud selle väljaga. Seda nõuet TULEB kohaldada isegi nende usaldusteenuse märkide puhul, mille järelevalvet teostatakse / mida akrediteeritakse liikmesriikide õigusaktidest tulenevate mõne erinõudega vastavuse tagamiseks (nt nn kvalifitseeritud ajatemplid Saksamaal või Ungaris), viidatud URI PEAB olema üks ETSIs 102 231 määratletud ja selle punktis D.2 loetletud URIdest, mis on seotud selle väljaga (nt TSA siseriiklikult määratletud kvalifitseeritud ajatemplite puhul). Vajaduse korral VÕIB selline ajatemplite siseriiklik erinõue sisalduda teenuse kirjes ja selleks PEAB kasutama teenuse lisainformatsiooni laiendust (punkt 5.8.2) punktis 5.5.9 (*Service information extension*).

▼C1

Vaikimisi peab usaldusnimekirja kantud CSP puhul olema ühe X.509v3 sertifikaadi kohta üks teenusekirje (nt CA/QC tüüpi sertifitseerimisteenuse puhul) nimekirja kantud CSP poolt osutatavate usaldusnimekirja kantud sertifitseerimisteenuste all (nt sertifitseerimisasutus väljastab (otse) QCsid). Mõnes hoolikalt kavandatud olukorras ja hoolikalt juhitud ja toetatud tingimustel võib liikmesriigi järelevalveasutus/akrediteerimisasutus otsustada, et ta kasutab juur- või ülataseme sertifitseerija (*Root or Upper level* CA) (st sertifitseerimisasutus, mis ei anna välja otseselt lõppkasutaja QCsid, vaid sertifitseerib CAde hierarhiat kuni CAni, mis väljastab lõppkasutajale QCsid) X.509v3 sertifikaati nimekirja kantud CSP teenuste loetelu ühe kirje *Sdi*-na. Sellise X.509v3 *Root* CA *või Upper* CA kasutamise puhul TLi teenuste kirjete *Sdi* väärtustena tuleb hoolikalt kaaluda selle tagajärgi (eeliseid ja puudusi) ja seda peavad toetama liikmesriigid ([1]). Lisaks sellele PEAVAD liikmesriigid põhimõttest lubatud erandi kasutamisel esitama vajaliku dokumentatsiooni, et hõlbustada sertifitseerimistee loomist ja kontrollimist.

Märkus: sarnaselt OCSP responderite ja CRL väljastajatele, mis on CSP_{QC} sertifitseerimisteenuste osa ja mille puhul peab kasutama eraldi võtmepaare vastavalt OCSP kehtivuskinnituste ja CRLide allkirjastamiseks, VÕIB TSPsid kanda ka käesolevasse TSLi vormi, kasutades järgmist URIde kombinatsiooni:

— „*Service type identifier*” (punkt 5.5.1) väärtus:

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

mis on kombineeritud järgmise *Service information extension* (punkt 5.5.9) teenuse lisainformatsiooni laienduse (punkt 5.8.2) väärtusega:

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

kirjeldus: sertifitseerimisoleku pakkuja, mis opereerib OCSP-serverit kvalifitseeritud sertifikaate väljastava CSP teenuse osana;

— „*Service type identifier*” (punkt 5.5.1) väärtus:

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

mis on kombineeritud järgmise *Service information extension* (punkt 5.5.9) teenuse lisainformatsiooni laienduse (punkt 5.8.2) väärtusega:

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

kirjeldus: sertifitseerimisoleku pakkuja, mis opereerib CRLi kvalifitseeritud sertifikaate väljastava CSP teenuse osana;

— „*Service type identifier*” (punkt 5.5.1) väärtus:

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

([1]) *Root* CA X.509v3 sertifikaadi kasutamine *Sdi* väärtusena nimekirja kantud teenuse puhul sunnib süsteemioperaatorit käsitlema kogu sellise *Root* CA alla kuuluvat sertifitseerimisteenuste rühma „järelevalve-/akrediteerimisoleku” suhtes tervikuna. Nt mis tahes oleku muutus, mida nõuab üks CA nimekirja kantud juurhierarhias, sunnib tegema selle oleku muudatuse kogu hierarhias.

▼C1

mis on kombineeritud järgmise *Service information extension* (punkt 5.5.9) teenuse lisainformatsiooni laienduse (punkt 5.8.2) väärtusega:

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

kirjeldus: juursertifitseerimisasutus, kelle juurest võib viia sertifitseerimistee kvalifitseeritud sertifikaate väljastava sertifitseerimisasutuseni;

— „*Service type identifier*" (punkt 5.5.1) väärtus:

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

mis on kombineeritud järgmise *Service information extension* (punkt 5.5.9) teenuse lisainformatsiooni laienduse (punkt 5.8.2) väärtusega:

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

kirjeldus: ajatempliteenus, mis on sellise kvalifitseeritud sertifikaate väljastava sertifitseerimisteenuse osutaja teenuse osa, mis väljastavad TSTsid, mida saab kasutada kvalifitseeritud allkirja kontrolliprotsessis, et kindlaks teha ja pikendada allkirja kehtivust, kui QC on tühistatud või kehtivuse kaotanud.

Service name (punkt 5.5.2)

See väli on KOHUSTUSLIK ning sellel PEAB olema näidatud, millise nime all TSP *name* (punkt 5.4.1) väljal tuvastatav CSP *Service type identifier* (punkt 5.5.1) väljal tuvastatavat teenust osutab. See PEAB olema mitmekeelsete märgistringide jada, (kus EN on kohustuslik keel, millele lisandub võimaluse korral üks või enam riigikeelt).

Service digital identity (punkt 5.5.3)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud vähemalt üks digitaalne identifikaator, mis on ainulaadne teenuse puhul, mille tüüp on esitatud *Service type identifier* (punkt 5.5.1) väljal ja millega on võimalik teenust selgelt tuvastada.

Käesoleva kirjelduse kohaldamisel PEAB sellel väljal kasutatav digitaalne identifikaator olema vastav X.509v3 sertifikaat, mis on avalik võti (avalikud võtmed), mida vastav CSP kasutab teenuse osutamisel, mille tüüp on esitatud *Service type identifier* (punkt 5.5.1) väljal (st *Root* CA/QC poolt kasutatav võti, mida kasutatakse sertifikaatide allkirjastamiseks [1]) või ajatemplite väljastamiseks või CRLide allkirjastamiseks või OCSP kehtivuskinnituste allkirjastamiseks). Seda seotud X.509v3 sertifikaati PEAB kasutama minimaalselt nõutava digitaalse identifikaatorina (mis on CSP poolt nimekirja kantud teenuste osutamiseks kasutatav (ad) avalik(ud) võti/võtmed). Täiendavaid identifikaatoreid VÕIB kasutada järgmiselt, kuid need kõik PEAVAD viitama samale tunnusele (st seotud X.509v3 sertifikaadile):

[1] See võib olla lõppkasutaja sertifikaate väljastava CA (nt CA/PKC, CA/QC) sertifikaat või usaldusväärse *Root* CA sertifikaat, millest võib leida tee kuni lõppkasutaja kvalifitseeritud sertifikaatideni. Olenevalt sellest, kas kõnelaust teavet ja teavet, mis on leitav igast nimetatud usaldusväärse *Root* CA poolt väljastatud lõppkasutaja sertifikaadist, on võimalik kasutada mis tahes kvalifitseeritud sertifikaadi vastavate omaduste selgeks määramiseks, võib tekkida vajadus kõnealuse teabe (*Service digital identity*) täiendamiseks *Service information extensions*'is sisalduvate andmetega (vt punkt 5.5.9).

▼C1

a) sertifikaadi eraldusnimi (*distinguished name* – DN), mida saab kasutada *Service type identifier* (punkt 5.5.1) väljal esitatud CSP teenuse elektrooniliste allkirjade kontrollimiseks;

b) seotud avaliku võtme identifikaator (st X.509v3 *SubjectKeyIdentifier* või SKI väärtus);

c) seotud avalik võti.

Vaikimisi EI TOHI digitaalne identifikaator (st seotud X.509v3 sertifikaat) üldiselt esineda usaldusnimekirjas enam kui üks kord, st selles PEAB olema üks kirje ühe X.509v3 sertifikaadi kohta usaldusnimekirja kantud CSP poolt osutatavate nimekirja kantud sertifitseerimisteenuste alla kuuluva sertifitseerimisteenuse puhul. Seevastu ühte X.509v3 sertifikaati PEAB kasutama ühes teenusekirjes *Sdi* väärtusena.

Märkus 1: ainus olukord, mil võib mitte kohaldada eespool nimetatud üldist põhimõtet, tekib juhul, kui ühte X.509v3 sertifikaati kasutatakse erinevate usaldusteenuste märkide väljastamisel, mille suhtes kehtivad erinevad järelevalve-/akrediteerimissüsteemid. Näiteks, kui CSP kasutab ühtset X.509v3 sertifikaati ühelt poolt sobiva järelevalvesüsteemi alusel QCde väljastamisel ja teiselt poolt mittekvalifitseeritud sertifikaatide väljastamisel erineva järelevalve-/akrediteerimisoleku all. Selle juhtumi ja näite puhul kasutatakse kahte erineva *Sti* väärtusega (nt esitatud näite puhul vastavalt CA/QC ja CA/PKC) ja sama *Sdi* väärtusega (seotud X.509v3 sertifikaat) kirjet.

Rakendused on sõltuvad ASN.1st või XMLst ja need PEAVAD olema kooskõlas ETSI TSi 102 231 nõuetega (ASN.1 kohta vt ETSI TSi 102 231 A lisa ja XML kohta vt ETSI TSi 102 231 B lisa).

Märkus 2: kui tuvastatava teenusekirjega seoses on vaja esitada täiendavat kvalifikatsiooniteavet, siis PEAB süsteemioperaator vajaduse korral kaaluma *Service information extension* välja (punkt 5.5.9) *additionalServiceInformation* laienduse (punkt 5.8.2) kasutamist vastavalt sellise kvalifikatsiooniteabe esitamise vajadusele. Lisaks sellele võib skeemioperaator kasutada valikuliselt punkti 5.5.6 (*Scheme service definition* URI).

S e r v i c e c u r r e n t s t a t u s (punkt 5.5.4)

▼C2

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud teenuse oleku identifikaator, kasutades ühte järgmistest URIdest:

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

— **Supervision of Service in Cessation (järelevalve on katkestatud)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/-supervisionincessation);

— **Supervision Ceased (järelevalve on lõpetatud)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— **Supervision Revoked (järelevalve on tühistatud)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked);

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

— **Accreditation Ceased (akrediteerimine on lõpetatud)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— **Accreditation Revoked (akrediteerimine on tühistatud)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

Eespool nimetatud olekuid PEAB käesoleva usaldusnimekirja nõuete kohaldamisel tõlgendama järgmiselt:

— ***Under Supervision:*** TSP *name* väljal (punkt 5.4.1) tuvastatava sertifitseerimisteenuse osutaja (CSP) poolt osutatav Service digital identity väljal (punkt 5.5.3) tuvastatav teenus on hetkel Scheme territory väljal (punkt 5.3.10) tuvastatava CSP asukohaks oleva liikmesriigi järelevalve all, et teha kindlaks, kas teenus on kooskõlas direktiivi 1999/93/EÜ sätetega;

▼M1

— ***Supervision of Service in Cessation:*** „TSP name" väljal (punkt 5.4.1) näidatud CSP poolt „Service digital identity" väljal (punkt 5.5.3) näidatud teenuse osutamine on hetkel katkestatud, kuid selle üle teostatakse siiski järelevalvet, kuni järelevalve lõpetatakse või tühistatakse. Kui vastutuse selle katkestusetapi kindlustamise eest on võtnud üle „TSP name" väljal näidatud juriidilise isiku asemel mõni teine juriidiline isik, PEAB selle uue või varuks oleva juriidilise isiku (varu-CSP) nimi olema esitatud teenusekirje punktis „Scheme service definition URI" (punkt 5.5.6) ja „TakenOverBy" laiendis (punkt L.3.2);

▼C1

— ***Supervision Ceased:*** järelevalvehindamise kehtivusaeg on lõppenud ilma *Service digital identity* väljal (punkt 5.5.3) tuvastatava teenuse ümberhindamiseta. Teenus ei ole hetkeoleku kuupäevast alates enam järelevalve all, kuna on teada, et teenuse osutamine on lõpetatud;

— ***Supervision Revoked:*** vastavalt eelnevalt teostatud järelevalvele ei suuda CSP teenus ega võibolla ka CSP ise täita jätkuvalt direktiivi 1999/93/EÜ sätteid, mis on määratletud *Scheme territory* väljal (punkt 5.3.10) tuvastatava CSP asukohaks oleva liikmesriigi poolt. Seepärast tuli teenuse osutamine lõpetada ja seda tuleks lugeda lõpetatuks eespool nimetatud põhjusel.

Märkus 1: oleku väärtus *Supervision Revoked* võib olla lõplik olek isegi juhul, kui CSP lõpetab siis täielikult oma tegevuse. Sel juhul ei ole vajadust liikuda *Supervision of Service in Cessation* või Supervision Ceased olekusse. Tegelikult on ainsaks viisiks, kuidas muuta *Supervision Revoked* olekut, taastada vastavus direktiiviga 1999/93/EÜ vastavalt TLi omava liikmesriigi asjaomasele kehtivale järelevalvesüsteemile ja omandada uuesti olek *Under Supervision*. Olek *Supervision of Service in Cessation* või olek *Supervision Ceased* tekib vaid siis, kui CSP ise otse lõpetab järelevalvealuste teenuste osutamise, mitte aga siis, kui järelevalve on tühistatud;

— ***Accredited:*** akrediteerimisasutus on akrediteerimiseks vajaliku hindamise läbi viinud Scheme territory väljal (punkt 5.3.10) tuvastava liikmesriigi nimel ja väljal *Service digital identity* (punkt 5.5.3) tuvastatav, väljal TSP name (punkt 5.4.1) tuvastatava CSP [1] poolt osutatav teenus loetakse direktiivi 1999/93/EÜ sätetega kooskõlas olevaks.

[1] Juhime tähelepanu sellele, et see akrediteeritud CSP võib asuda mõnes muus liikmesriigis peale TLi TSL rakenduse „Scheme territory" väljal tuvastatava liikmesriigi või kolmanda riigi (vt direktiivi 1999/93/EÜ artikli 7 lõike 1 punkt a).

▼C1

Märkus 2: kui seda olekut kasutatakse *Scheme territory*'l (punkt 5.3.10) asuva QCsid väljastava CSP puhul, TULEB olekuid *Accreditation Revoked* ja *Accreditation Ceased* lugeda üleminekuolekuteks ja neid EI TOHI kasutada *Service current status* väärtusena, sest kui neid kasutatakse, PEAB neile vahetult järgnema *Service approval history information* või *Service current status* puhul olek *Under supervision*, millele järgneb tõenäoliselt mõni muu eespool määratletud ja joonisel 1 kujutatud järelevalveolek. Kui seda olekut kasutatakse QCsid mitteväljastava CSP puhul ja kui on olemas vaid seotud vabatahtlikkusel põhineva akrediteerimise süsteem, millega ei ole seotud järelevalvesüsteem, või kui seda kasutatakse QCsid väljastava CSP puhul, kusjuures CSP ei asu *Scheme territory*'l (punkt 5.3.10) (nt kolmandas riigis), VÕIB olekuid *Accreditation Revoked* ja *Accreditation Ceased kasutada Service current status* väärtusena:

— ***Accreditation Ceased:*** akrediteerimiseks vajaliku hindamise kehtivusaeg on lõppenud ilma *Service digital identity* väljal (punkt 5.5.3) tuvastatava teenuse ümberhindamise teostamiseta;

— ***Accreditation Revoked:*** olles eelnevalt tunnistatud skeemi kriteeriumidega vastavaks, ei suuda väljal TSP *name* (punkt 5.4.1) tuvastatava sertifitseerimisteenuse osutaja (CSP) poolt osutatav *Service digital identity* väljal (punkt 5.5.3) tuvastatav teenus ega võibolla ka CSP ise täita enam direktiivi 1999/93/EÜ sätteid.

Märkus 3: täpselt samu olekuväärtusi tuleb kasutada QCsid väljastatavate CSPde ja QCsid mitteväljastatavate CSPde puhul (nt TSTsid väljastavad ajatempliteenuste osutajad, mittekvalifitseeritud sertifikaate väljastavad CSPd jne). *Service Type identifier* välja (punkt 5.5.1) kasutatakse selleks, et eristada kohaldatavaid järelevalve-/akrediteerimissüsteeme.

Märkus 4: vajaduse ja nõudmise korral (nt erinevate kvaliteedi/turvalisuse tasemete eristamiseks) VÕIB QCsid mitteväljastavate CSPde kohta teenuse tasandil esitada täiendavat olekuga seotud kvalifikatsiooniteavet, mis on määratletud siseriiklike järelevalve-/akrediteerimissüsteemide tasandil. Süsteemioperaator PEAB kasutama *Service information extension* välja (punkt 5.5.9) *additionalServiceInformation* laiendust (punkt 5.8.2) vastavalt sellise täiendava kvalifikatsiooniteabe eesmärgile. Lisaks sellele võib süsteemioperaator kasutada valikuliselt punkti 5.5.6 (*Scheme service definition* URI).

Current status starting date and time (punkt 5.5.5)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud kuupäev ja kellaaeg, mil kinnituse hetkeolek hakkas kehtima (kuupäeva ja kellaaja väärtus vastavalt ETSI TSi 102 231 punkti 5.1.4 määratlusele).

Scheme service definition URI (punkt 5.5.6)

See väli on VALIKULINE ning selle kasutamisel PEAB (PEAVAD) sellel olema esitatud URI(d), kust sõltuvad osapooled saavad süsteemioperaatori pakutavat teenusega seotud teavet, mitmekeelsete viitade jadana (kus EN on kohustuslik keel, millele lisandub võimaluse korral üks või enam riigikeelt).

Viidatud URI(d) PEAB (PEAVAD) nende kasutamise korral juhtima teabeni, kus on kirjeldatud süsteemis määratletud teenust. See VÕIB vajaduse korral sisaldada eelkõige järgmist teavet:

a) varu-CSP tunnusele viitav URI, kui teenuse järelevalve on katkestatud, mistõttu on kaasatud varu-CSP (vt punkt 5.5.4 – *Service current status*);

▼C1

b) URI viidetega dokumentidele, kust võib leida lisateavet mõne riiklikult määratletud erikvalifikatsiooni kasutamise kohta järelevalvealuse/akrediteeritud usaldusteenuse märgi pakkumise teenuse puhul kooskõlas *Service information extension* välja (punkt 5.5.9) kasutamisega koos *additionalServiceInformation*'iga vastavalt punktile 5.8.2.

Service supply points (punkt 5.5.7)

See väli on VALIKULINE ning sellel PEAB (PEAVAD) olema esitatud URI(d), kust seotud osapooled pääsevad teenusele ligi märgistringide jada kaudu, mille süntaks PEAB olema kooskõlas RFCga 3986.

TSP service definition URI (punkt 5.5.8)

See väli on VALIKULINE ning selle kasutamisel PEAB (PEAVAD) olema esitatud URI(d), kust seotud osapooled saavad teavet TSP pakutava teenuse kohta märgistringide jadana (kus EN on kohustuslik keel, millele lisandub võimaluse korral üks või enam riigikeelt). Viidatud URI(d) PEAB (PEAVAD) juhtima teabeni, kus on kirjeldatud TSP määratletud teenust.

Service information extensions (punkt 5.5.9)

Käesolevate kirjelduse kohaldamisel on see väli VALIKULINE, kuid see PEAB olemas olema juhul, kui Service digital identity väljal (punkt 5.5.3) esitatud teave ei ole piisav selleks, et selgelt tuvastada kõnealuse teenuse osutamisel väljastatavaid kvalifitseeritud sertifikaate ja/või ei võimalda seotud kvalifitseeritud sertifikaatides sisalduv teave tuvastada masintöötluse teel, kas SSCD toetab QCd või mitte ([1]).

Kui käesoleva kirjelduse kohaldamisel on see KOHUSTUSLIK, nt CA/QC teenuste puhul, PEAB kasutama valikulist *Service information extensions (Sie)* teabevälja ja selle struktureerima vastavalt ETSI TSi 102 231 L.2.1 lisas määratletud *Qualifications* laiendusele ühe või mitme enniku jadana, millest iga ennik sisaldab järgmist teavet:

— (filtrid) teave, mida kasutatakse, et täpsemalt tuvastada Sdi tunnusega sertifitseerimisteenuse all seda konkreetset teenust (st kvalifitseeritud sertifikaatide rühma), mille puhul nõutakse/esitatakse lisateavet SSCD toe olemasolu või selle puudumise (ja/või juriidilisele isikule väljastamise) kohta; ning

— seotud teave (kvalifitseerijad) selle kohta, kas seda täpsemalt tuvastatud kvalifitseeritud sertifikaatide teenusterühma toetab SSCD või mitte (kui see teave on QCSSCD*StatusAsInCert*, mis tähendab, et kõnealune seotud teave on kvalifitseeritud sertifikaadi osa ETSI standardiseeritud masintöödeldaval kujul), ([2]) ja/või teave selle kohta, et neid QCsid väljastatakse juriidilistele isikutele (vaikimisi loetakse neid väljastatuks üksnes füüsilistele isikutele).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD) tähendab, et CSP tagab ja liikmesriik (selle järelevalve- või akrediteerimisasutus) teostab järelevalvet (järelevalvemudel) või auditeerib (akrediteerimismudel), et teenuse (QCA) alusel väljastatud iga QC, mis on tuvastatav *Service digital identity* väljal (punkt 5.5.3) ja täpsemalt tuvastatav eespool kirjeldatud (filtrite) teabe abil, mida kasutatakse Sdi tunnusega sertifitseerimisteenuse all selle täpse kvalifitseeritud sertifikaatide rühma täpsemaks tuvastamiseks, mille puhul see lisateave on nõutav seoses SSCD toe olemasolu või puudumisega, **ON** SSCD toega (st sertifikaadis avaliku võtmega seotud isiklikku võtit hoitakse turvalise allkirja andmise vahendis vastavalt direktiivi 1999/93/EÜ III lisale).

([1]) Vt käesoleva dokumendi 2.2. jagu.

([2]) See viitab ETSIs määratletud QcCompliance tunnuse, QcSSCD tunnuste (ETSI TS 101 862) või QCP/QCP + ETSIs määratletud OID (ETSI TS 101 456) asjakohasele kombinatsioonile.

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD) tähendab, et CSP tagab ja liikmesriik (selle järelevalve- või akrediteerimisasutus) teostab järelevalvet (järelevalvemudel) või auditeerib (akrediteerimismudel), et teenuse (*Root* CA/QC või CA/QC) alusel väljastatud iga QC, mis on tuvastatav *Service digital identity* väljal (punkt 5.5.3) ja täpsemalt tuvastatav eespool kirjeldatud (filtrite) teabe abil, mida kasutatakse Sdi tunnusega sertifitseerimisteenuse all selle täpse kvalifitseeritud sertifikaatide rühma täpsemaks tuvastamiseks, mille puhul see lisateave on nõutav seoses SSCD toe olemasolu või puudumisega, **EI OLE** SSCD toega (st sertifikaadis avaliku võtmega seotud isiklikku võtit **EI** hoita turvalise allkirja andmise vahendis vastavalt direktiivi 1999/93/EÜ III lisale).

— **QCSSCD*StatusAsInCert*** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert) tähendab, et CSP tagab ja liikmesriik (selle järelevalve- või akrediteerimisasutus) teostab järelevalvet (järelevalvemudel) või auditeerib (akrediteerimismudel), et teenuse (*Root* CA/QC või CA/QC) alusel väljastatud iga QC, mis on tuvastatav *Service digital identity* väljal (punkt 5.5.3) ja täpsemalt tuvastatav eespool kirjeldatud (filtrite) teabe abil, mida kasutatakse Sdi tunnusega sertifitseerimisteenuse all selle täpse kvalifitseeritud sertifikaatide rühma täpsemaks tuvastamiseks, mille puhul see lisateave on nõutav seoses SSCD toe olemasolu või puudumisega, PEAB sisaldama masintöödeldavat teavet selle kohta, kas QC on SSCD toega või mitte.

— **QC*ForLegalPerson*** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson) tähendab, et CSP tagab ja liikmesriik (selle järelevalve- või akrediteerimisasutus) teostab järelevalvet (järelevalvemudel) või auditeerib (akrediteerimismudel), et teenuse (QCA) alusel väljastatud iga QC, mis on tuvastatav *Service digital identity* väljal (punkt 5.5.3) ja täpsemalt tuvastatav eespool kirjeldatud (filtrite) teabe abil, mida kasutatakse Sdi tunnusega sertifitseerimisteenuse all selle täpse kvalifitseeritud sertifikaatide rühma täpsemaks tuvastamiseks, mille puhul see lisateave on nõutav seoses juriidilisele isikule väljastamisega, **ON** väljastatud juriidilistele isikutele.

Neid kvalifitseerijaid kasutatakse vaid laiendusena, kui teenusetüüp on http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

See väli on rakendusel põhinev (ASN.1 või XML) ja see PEAB olema kooskõlas ETSI TSi 102 231 L.3.1 lisa nõuetega.

▼M1

XML-rakenduse puhul peab sellise lisateabe sisu olema kodeeritud, kasutades ETSI TS 102 231 lisas C esitatud xsd-faile.

▼C1

Service Approval History

Käesoleva kirjelduse kohaldamisel on see väli VALIKULINE, kuid see PEAB olemas olema juhul, kui *Historical information period* (punkt 5.3.12) ei ole null. Seega käesoleva kirjelduse kohaselt PEAB süsteem säilitama varasemat teavet. Juhul, kui varasemat teavet kavatsetakse säilitada, kuid teenusel ei ole hetkeolekule eelnevat ajalugu (st süsteemioperaator ei ole säilitanud esimest registreeritud olekut või varasemat teavet), PEAB see väli olema tühi. Muudel juhtudel PEAB iga TSP teenuse hetkeolekusse tehtava muudatuse puhul, mis leidis aset ETSI TSi 102 231 punktis 5.3.12 sätestatud varasema teabe perioodil, olema esitatud teave eelmise kinnitamise oleku kohta oleku muutuse kuupäeva ja kellaaja (st kuupäev ja kellaaeg, mil hakkas kehtima järgmine kinnitamise olek) kahanevas järjestuses.

▼C1

See PEAB olema varasema teabe jada vastavalt allpool määratletule.

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

Service type identifier (punkt 5.6.1)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud TSP *Service Information – Service type identifier* (punkt 5.5.1) väljal kasutatud formaadi ja tähendusega teenusetüübi identifikaator.

Service name (punkt 5.6.2)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud nimi, mille all CSP osutas TSP *Service Information – Service name* (punkt 5.5.2) väljal kasutatud formaadi ja tähendusega TSP *Service Information – Service type identifier* (punkt 5.5.1) väljal tuvastatavat teenust. Selles punktis ei nõuta sama nime, mis on esitatud punktis 5.5.2. Nime muutus VÕIB olla üks selliseid olukordi, mille puhul on nõutav uus olek.

▼M1

Service digital identity (punkt 5.6.3)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud vähemalt üks digitaalne tunnus (st X.509v3 sertifikaat), mida kasutatakse „TSP Service Information – Service digital identity" väljal (punkt 5.5.3) ETSI TS 102 231 kohases formaadis ja tähenduses (vt punkt 5.5.3).

Märkus. Teenust käsitlevas Sdi punktis 5.5.3 kasutatava X.509v3 sertifikaadi väärtuse puhul peab usaldusnimekirjas olema ainult üks teenusekirje „Sti:Sie/-additionalServiceInformation" väärtuse kohta. Teave Sdi (punkt 5.6.3) kohta, mida kasutatakse teenusekirjega seotud teenuse kinnitamise oleku ajalugu käsitlevas teabes, ja teave Sdi (punkt 5.5.3) kohta, mida kasutatakse kõnealuses teenusekirjes, PEAVAD olema ühe ja sama X.509v3 sertifikaadi väärtuse kohta. Kui nimekirjas oleva teenuse Sdi muutub (st X.509v3 sertifikaadi uuendamine või uuesti tippimine nt CA/PKC või CA/QC jaoks) või sellele luuakse uus Sdi, ja isegi kui sellega seotud Sti, Sn ja (Sie) jaoks jäävad väärtused samaks, PEAB Scheme Operator looma eelmisest erineva teenusekirje.

▼C1

Service previous status (punkt 5.6.4)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud teenuse eelneva oleku identifikaator TSP *Service Information – Service current status* (punkt 5.5.4) väljal kasutatud formaadi ja tähendusega.

Previous status starting date and time (punkt 5.6.5)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud kuupäev ja kellaaeg, mil hakkas kehtima kõnealune eelnev olek TSP *Service Information – Service current status starting date and time* (punkt 5.5.5) väljal kasutatud formaadi ja tähendusega.

Service information extensions (punkt 5.6.6)

See väli on VALIKULINE ning seda võivad kasutada süsteemioperaatorid, et esitada teenuse kohta teavet TSP *Service Information – Service information extensions* väljal (punkt 5.5.9) kasutatud formaadi ja tähendusega.

▼C1

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

Sama ka TSP(1) *Service*(1)*History*(2) (enne *History* 1) kohta

…

TSP(1) Service(2)

Sama ka TSP(1)*Service* 2 kohta (vajadusel)

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

…

TSP(2) Information

Sama ka TSP 2 kohta (vajadusel)

Sama ka TSP 2 *Service* 1 kohta

Sama ka TSP 2 *Service* 1 History 1 kohta

…

▼M1

Signed TSL

Käesolevate nõuete ja eelkõige IV peatüki alusel koostatud, inimesele loetava usaldusnimekirja TSLi PEAKS allkirjastama „Scheme operator name" väljaga (punkt 5.3.4), et tagada nimekirja autentsus ja terviklikkus ([1]). Allkirja formaat PEAKS olema PAdES part 3 (ETSI TS 102 778–3), ([2]) kuid VÕIB olla ka PAdES part 2 (ETSI TS 102 778–2) ([3]) konkreetse usaldusmudeli puhul, mis on loodud usaldusnimekirjade allkirjastamiseks kasutatavate sertifikaatide avaldamise teel.

Käesoleva kirjelduse alusel koostatud, masinloetava usaldusnimekirja TSLi PEAB allkirjastama „Scheme operator name" väljaga (punkt 5.3.4), et tagada nimekirja autentsus ja terviklikkus. Käesoleva kirjelduse alusel koostatud, masinloetav usaldusnimekirja TSL PEAB olema XML-formaadis ning PEAB vastama ETSI TS 102 231 lisades B ja C sätestatud nõuetele.

Allkirja formaat PEAB olema XAdES BES või EPES, nagu on ette nähtud ETSI TS 101 903 nõuetes XML-rakenduste kohta. Selline elektroonilise allkirja teostus PEAB vastama ETSI TS 102 231 lisas B ([4]) sätestatud nõuetele. Kõnealuse allkirja suhtes kohaldatavad täiendavad üldnõuded on esitatud järgmistes jagudes.

▼C1

Scheme identification (punkt 5.7.2)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud süsteemioperaatori antud viide, millega on kordumatult tuvastatav käesolevates nõuetes kirjeldatud süsteem ja koostatud TSL, ning allkirja arvutus PEAB seda hõlmama. See peaks eeldatavasti olema märgistring või bitistring.

([1]) Kui inimesele loetav usaldusnimekirja TSL ei ole allkirjastatud, PEAB selle autentsuse ja terviklikkuse tagama asjakohase sidekanali kaudu, millel on samaväärne turvalisuse tase. Selleks soovitatakse kasutada TLSi (IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2" ja liikmesriik PEAB TLS-kanali sertifikaadi sõrmejälje TSLi kasutajatele kättesaadavaks tegema ribaväliselt.

([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]) Süsteemioperaatori kaitsmine sertifikaadi allkirjastamisel ühel ETSI TSis 101 903 sätestatud viisidest on kohustuslik ja ds:keyInfo peaks võimaluse korral sisaldama asjakohast sertifitseerimisahelat.

▼M1

Käesoleva kirjelduse kohaldamisel PEAB määratud viide sisaldama „TSL type” välja (punkt 5.3.3), „Scheme name” välja (punkt 5.3.6) ja süsteemioperaatori poolt TSLi elektrooniliseks allkirjastamiseks kasutatava sertifikaadi SubjectKeyIdentifier laienduse väärtust.

▼C1

Signature algorithm identifier (punkt 5.7.3)

See väli on KOHUSTUSLIK ning sellel PEAB olema esitatud krüptograafiline algoritm, mida on kasutatud allkirja loomiseks. Olenevalt kasutatavast algoritmist, VÕIVAD selle välja puhul olla nõutavad lisaparameetrid. Allkirja arvutus PEAB seda välja hõlmama.

Signature value (punkt 5.7.4)

See väli on KOHUSTUSLIK ning sellel PEAB sisalduma digitaalallkirja tegelik väärtus. Allkirja arvutus PEAB hõlmama kõiki TSLi väljasid (välja arvatud allkirja väärtus ise).

TSL extensions (punkt 5.8)

expiredCertsRevocationInfo laiendus (punkt 5.8.1)

See laiendus on VALIKULINE. Kui seda kasutatakse, PEAB tegema seda kooskõlas ETSI TSi 102 231 punktis 5.8.1 sätestatud nõuetega.

additionalServiceInformation laiendus (punkt 5.8.2)

Kui kasutatakse seda VALIKU laiendust, PEAB seda tegema üksnes teenuse tasandil ja üksnes punktis 5.5.9 määratletud väljal (*Service information extension*). Seda kasutatakse teenuse kohta lisateabe esitamiseks. See PEAB olema ühe või mitme enniku jada, millest iga ennik sisaldab järgmist teavet:

a) lisateavet tuvastav URI, nt:

   — URI, milles on viidatud mõnele riiklikult määratletud erikvalifikatsioonile järelevalvealuse/akrediteeritud usaldusteenuse märgi pakkumise teenuse puhul, nt:

      — turvalisuse/kvaliteedi detailsuse tase, mis on seotud siseriikliku järelevalve-/akrediteerimissüsteemiga QCsid mitteväljastavate CSPde puhul (nt RGS */**/*** Prantsusmaal, teatavate QCsid väljastavate CSPde suhtes siseriiklike õigusaktidega kehtestatud järelevalve eristaatus Saksamaal), vt punkti 5.5.4 – *Service current status* – märkus 4;

      — või juriidiline eristaatus järelevalvealuse/akrediteeritud usaldusteenuse märgi pakkumise suhtes (nt riiklikult määratletud kvalifitseeritud TST nagu Saksamaal või Ungaris);

      — või *Sdi* väljal esitatud X.509v3 sertifikaadis oleva eripoliitika identifikaatori tähendus;

   — või *Service type identifier* välja punktis 5.5.1 kirjeldatud registreeritud URI, mille eesmärk on täpsemalt kirjeldada *Sti* tunnusega teenust, mis on QCsid väljastava sertifitseerimisteenuse osutaja teenuse osa (nt OCSP-QC, CRL-QC ja *Root* CA-QC);

b) valikuline string, mis sisaldab teenuseinformatsiooni väärtust, mille tähendus on esitatud skeemis (nt *, ** või ***);

c) mis tahes skeemi formaadis esitatud valikuline lisateave.

▼**M1**

URI mahavõtmise tulemuseks PEAKS olema sellise inimesele loetava teabe saamine (vähemalt inglise ja tõenäoliselt ka ühes või mitmes vastava riigi keeles), mida peetakse asjakohaseks ja piisavaks selleks, et sellele toetuv osaline saaks laiendusest aru, ja mis eelkõige selgitaks asjakohaste URIde tähendust, täpsustades võimalikke serviceInformation'i väärtusi ja iga väärtuse tähendust.

Qualifications Extension (punkt L.3.1)

Kirjeldus. See väli on VALIKULINE, kuid see PEAB olema olemas, kui selle kasutamine on KOHUSTUSLIK, nt RootCA/QC või CA/QC teenuste puhul ja kui

— „Service digital identity" väljal esitatud teave ei ole piisav selle teenusega väljastatavate kvalifitseeritud sertifikaatide selgeks tuvastamiseks;

— seotud kvalifitseeritud sertifikaatides sisalduv teave ei võimalda masintöötluse teel tuvastada, kas SSCD toetab QCd või mitte.

Kui seda teenuse taseme laiendust kasutada, siis TOHIB seda kasutada ainult „Service information extension" (punkt 5.5.9) väljal määratletud väljal ja see PEAB vastama ETSI TS 102 231 lisas L.3.1 sätestatud nõuetele.

TakenOverBy Extension (punkt L.3.2)

Kirjeldus. Käesolev laiendus on VALIKULINE, kuid PEAB olema olemas, kui teenuse, mis kuulus enne CSP õigusliku vastutuse alla, võtab üle teine TSP ja see on ette nähtud selleks, et kinnitada ametlikult teenuse õigusliku vastutuse alla kuuluvust ning võimaldada kontrollival tarkvaral kasutajale mõningaid juriidilisi üksikasju kuvada. Käesolevas laienduses esitatud teave PEAB olema kooskõlas sellega seotud punkti 5.5.6 kasutamisega ja PEAB vastama ETSI TS 102 231 lisa L.3.2 nõuetele.

▼**M1**

II PEATÜKK

Liikmesriigid kasutavad oma usaldusnimekirjade koostamisel:

väiketähelisi keelekoode ja suurtähelisi riigikoode;

keele- ja riigikoode vastavalt järgmisele tabelile.

Kui on olemas ladinakeelne variant (koos täpse keelekoodiga), lisatakse transliteratsioon ladina tähestikku koos järgmises tabelis esitatud vastavate keelekoodidega.

Lühinimi (algkeeles)	Lühinimi (inglise keeles)	Riigikood	Keelekood	Märkused	Transliteratsioon ladina tähestikku
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	Euroopa Liidu soovitatud riigikood	el-Latn
España	Spain	ES	es	samuti katalaani (ca), baski (eu), galiitsia (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**

Lühinimi (algkeeles)	Lühinimi (inglise keeles)	Riigikood	Keelekood	Märkused	Transliteratsioon ladina tähestikku
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Euroopa Liidu soovitatud riigikood	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstei-n	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Transliteratsioon ladina tähestikku: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

_____

▼C1

IV PEATÜKK

USALDUSNIMEKIRJA TSL RAKENDUSE INIMESELE LOETAVA VORMI NÕUDED

Usaldusnimekirja TSL rakenduse inimesele loetav (HR) vorm PEAB olema avalikult kättesaadav elektrooniliste kanalite kaudu. See PEAKS olema esitatud ISO 32000 standardile vastava dokumendina porditavas dokumendiformaadis (*Portable Document Format* – PDF), mis PEAB olema vormindatud vastavalt PDF/A profiilile (ISO 19005).

PDF/A profiilil põhineva usaldusnimekirja TSL rakenduse HR vormi sisu PEAKS vastama järgmistele nõuetele:

▼M1

— inimesele loetava usaldusnimekirja pealkiri saadakse järgmiste elementide ühendamisel:

  — soovi korral liikmesriigi lipu kujutis;

  — tühik;

  — riigi lühinimi algkeel(t)es (nagu on esitatud II peatüki tabeli esimeses veerus);

  — tühik;

  — „(”;

  — riigi lühinimi inglise keeles (nagu on esitatud II peatüki tabeli teises veerus) sulgudes;

  — „):” sulgeva ümarsulu ja eraldajana;

  — tühik;

  — „Trusted List”;

  — soovi korral liikmesriigi süsteemioperaatori logo;

▼C1

— HR vormi struktuur PEAKS kajastama ETSI TSi 102 231 5.1.2. jaos kirjeldatud loogilist mudelit;

— igal olemasoleval väljal PEAKS olema näidatud ja esitatud:

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

  — välja väärtus (nt CA/QC);

  — vajaduse korral välja väärtuse tähendus (kirjeldus), eelkõige nagu on esitatud ETSI TSi 102 231 D lisas või käesoleva kirjelduse registreeritud URI(des) (nt avaliku võtme sertifikaate väljastav sertifitseerimisasutus);

  — vajaduse korral mitu loomuliku keele versiooni vastavalt usaldusnimekirja TSL rakenduses esitatule.

— HR vormis PEAKSID olema esitatud vähemalt järgmised *Service digital identity* väljal olevad digitaalsete sertifikaatide väljad ja neile vastavad väärtused:

  — versioon;

  — seerianumber;

  — allkirja algoritm;

  — väljaandja;

  — kehtiv alates;

  — kehtiv kuni;

  — subjekt;

▼C1

— avalik võti;

— sertifitseerimispoliitika;

— subjektivõtme identifikaator (*Subject Key Identifier*);

— CRLi jaotuspunktid;

— avaliku võtme identifikaator;

— võtmekasutus;

— põhipiirangud;

— pöidlajälje algoritm;

— pöidlajälg.

— HR vorm PEAKS olema kergesti prinditav.

— HR vormi VÕIB allkirjastada elektrooniliselt. Allkirjastamise korral PEAB süsteemioperaator vormi allkirjastama vastavalt samadele allkirjanõuetele, mis kehtivad usaldusnimekirja TSL rakenduse suhtes.