Ta dokument je mišljen zgolj kot dokumentacijsko orodje in institucije za njegovo vsebino ne prevzemajo nobene odgovornosti

►B ►C1 **ODLOČBA KOMISIJE**

z dne 16. oktobra 2009

o vzpostavitvi ukrepov za pospeševanje uporabe postopkov po elektronski poti s pomočjo „enotnih kontaktnih točk“ po Direktivi 2006/123/ES Evropskega parlamenta in Sveta o storitvah na notranjem trgu

(notificirano pod dokumentarno številko C(2009) 7806)

(Besedilo velja za EGP)

(2009/767/ES) ◄

(UL L 274, 20.10.2009, str. 36)

spremenjen z:

		Uradni list		
		št.	stran	datum
►M1	Sklep Komisije 2010/425/EU z dne 28. julija 2010	L 199	30	31.7.2010
►M2	Uredba Komisije (EU) št. 519/2013 z dne 21. februarja 2013	L 158	74	10.6.2013

popravljena z:

►C1 Popravek, UL L 299, 14.11.2009, str. 18 (2009/767/ES)
►C2 Popravek, UL L 4, 7.1.2011, str. 6 (2009/767/ES)

▼B
▼C1

ODLOČBA KOMISIJE

z dne 16. oktobra 2009

o vzpostavitvi ukrepov za pospeševanje uporabe postopkov po elektronski poti s pomočjo „enotnih kontaktnih točk“ po Direktivi 2006/123/ES Evropskega parlamenta in Sveta o storitvah na notranjem trgu

(notificirano pod dokumentarno številko C(2009) 7806)

(Besedilo velja za EGP)

(2009/767/ES)

KOMISIJA EVROPSKIH SKUPNOSTI JE –

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti,

ob upoštevanju Direktive 2006/123/ES Evropskega parlamenta in Sveta z dne 12. decembra 2006 o storitvah na notranjem trgu ([1]) in zlasti člena 8(3) Direktive,

ob upoštevanju naslednjega:

(1) Obveznosti upravne poenostavitve, ki jih državam članicam nalaga poglavje II Direktive 2006/123/ES, zlasti člena 5 in 8 tega poglavja, vključujejo obveznost poenostavitve postopkov in formalnosti, ki veljajo za začetek opravljanja in opravljanje storitvene dejavnosti, in obveznost zagotovitve, da lahko te postopke in formalnosti ponudniki storitev opravijo enostavno na daljavo in po elektronski poti s pomočjo „enotnih kontaktnih točk“.

(2) Zaključek postopkov in formalnosti s pomočjo „enotnih kontaktnih točk“ mora biti mogoč čezmejno med državami članicami, kot to določa člen 8 Direktive 2006/123/ES.

(3) Za izpolnjevanje obveznosti poenostavitve postopkov in formalnosti ter za pospeševanje čezmejne uporabe „enotnih kontaktnih točk“ morajo postopki po elektronski poti temeljiti na enostavnih rešitvah, vključno z uporabo elektronskih podpisov. V primerih, ko se po ustrezni oceni tveganja konkretnih postopkov in formalnosti šteje, da je potrebna visoka raven varnosti ali enakovrednost z lastnoročnim podpisom, se lahko od ponudnikov storitev za določene postopke in formalnosti zahtevajo napredni elektronski podpisi, ki temeljijo na kvalificiranem potrdilu, z napravo za varno tvorjenje podpisa ali brez nje.

([1]) UL L 376, 27.12.2006, str. 36.

▼C1

(4) Okvir Skupnosti za elektronski podpis je bil vzpostavljen z Direktivo Evropskega parlamenta in Sveta 1999/93/ES z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis ([1]). Da se pospeši učinkovita čezmejna uporaba naprednih elektronskih podpisov, ki temeljijo na kvalificiranem potrdilu, je treba povečati zaupanje v te elektronske podpise, ne glede na državo članico, v kateri ima podpisnik ali overitelj, ki izda kvalificirano potrdilo, sedež. To je mogoče doseči tako, da so informacije, potrebne za preverjanje elektronskih podpisov, lažje dosegljive v zanesljivi obliki, zlasti informacije v zvezi z overitelji, ki so nadzorovani/akreditirani v državi članici, in v zvezi s storitvami, ki jih nudijo.

(5) Treba je zagotoviti, da države članice s pomočjo skupnega modela omogočijo javni dostop do teh informacij, da se pospeši njihova uporaba in zagotovi ustrezna raven podrobnosti, ki prejemnikom omogoča potrjevanje elektronskega podpisa –

SPREJELA NASLEDNJO ODLOČBO:

Člen 1

Uporaba in sprejem elektronskih podpisov

1. Če je to upravičeno na podlagi ustrezne ocene povezanega tveganja in je v skladu s členom 5(1) in (3) Direktive 2006/123/ES, lahko države članice zahtevajo, da ponudnik storitev za dokončanje določenih postopkov in formalnosti s pomočjo enotnih kontaktnih točk po členu 8 Direktive 2006/123/ES uporabi napredne elektronske podpise, ki temeljijo na kvalificiranem potrdilu, z napravo za varno tvorjenje podpisa ali brez nje, kot je to določeno in urejeno z Direktivo 1999/93/ES.

2. Države članice sprejmejo vsak napredni elektronski podpis, ki temelji na kvalificiranem potrdilu, z napravo za varno tvorjenje podpisa ali brez nje, za dokončanje postopkov in formalnosti iz odstavka 1, brez poseganja v možnost držav članic, da omejijo ta sprejem na napredne elektronske podpise, ki temeljijo na kvalificiranem potrdilu in so oblikovani z napravo za varno tvorjenje podpisa, če je to v skladu z oceno tveganja iz odstavka 1.

3. Države članice sprejem naprednih elektronskih podpisov, ki temeljijo na kvalificiranem potrdilu, z napravo za varno tvorjenje podpisa ali brez nje, ne pogojujejo z zahtevami, ki ovirajo takšno uporabo postopkov s strani ponudnikov storitev po elektronski poti s pomočjo enotnih kontaktnih točk.

([1]) UL L 13, 19.1.2000, str. 12.

▼C1

4. Odstavek 2 državam članicam ne preprečuje sprejema elektronskih podpisov, ki niso napredni elektronski podpisi, ki temeljijo na kvalificiranem potrdilu, z napravo za varno tvorjenje podpisa ali brez nje.

Člen 2

Vzpostavitev, vzdrževanje in objava zanesljivih seznamov

1. Vsaka država članica v skladu s tehničnimi specifikacijami iz Priloge vzpostavi, vzdržuje in objavi „zanesljiv seznam“, ki vsebuje minimalne informacije v zvezi z overitelji, ki izdajajo kvalificirana potrdila javnosti ter so nadzorovani in akreditirani s strani države.

▼M1

2. Države članice v skladu s specifikacijami, določenimi v Prilogi, vzpostavijo in objavijo zanesljiv seznam v berljivi obliki in obliki, primerni za strojno obdelavo.

2a. Države članice svoje zanesljive sezname v obliki, primerni za strojno obdelavo, elektronsko podpišejo in prek varnega kanala objavijo vsaj zanesljive sezname v berljivi obliki, da se tako zagotovita avtentičnost in celovitost seznamov.

3. Države članice Komisiji sporočijo naslednje informacije:

(a) organe, odgovorne za vzpostavitev, vzdrževanje in objavo zanesljivega seznama v berljivi obliki in obliki, primerni za strojno obdelavo;

(b) lokacije, kjer je zanesljivi seznam objavljen v berljivi obliki in v obliki, primerni za strojno obdelavo;

(c) potrdilo javnega ključa, ki se je uporabilo za izvedbo varnega kanala, prek katerega je objavljen zanesljivi seznam v berljivi obliki, oz. v primeru, da je berljiva oblika elektronsko podpisana, potrdilo javnega ključa, ki se je uporabilo za podpis;

(d) potrdilo javnega ključa, ki se je uporabilo za elektronski podpis na zanesljivem seznamu v obliki, primerni za strojno obdelavo;

(e) vse spremembe informacij iz točk (a) do (d).

4. Komisija prek varnega kanala do overjenega spletnega strežnika vsem državam članicam zagotovi dostop do informacij iz odstavka 3, ki so jih predložile države članice, tako v berljivi obliki kot tudi obliki, primerni za strojno obdelavo.

▼C1

Člen 3

Začetek veljavnosti

Ta odločba začne veljati 28. decembra 2009.

Člen 4

Naslovniki

Ta odločba je naslovljena na države članice.

▼C1

PRILOGA

TEHNIČNE SPECIFIKACIJE ZA SKUPNI MODEL ZA „ZANESLJIVI SEZNAM NADZOROVANIH/AKREDITIRANIH OVERITELJEV“

UVOD

1. **Splošno**

Namen skupnega modela za „Zanesljivi seznam nadzorovanih/akreditiranih overiteljev“ držav članic je vzpostaviti skupen način, na katerega države članice zagotovijo informacije o statusu nadzora/akreditacije storitev overjanja s strani overiteljev ([1]) (CSP), ki so nadzorovani/akreditirani zaradi skladnosti z zadevnimi določbami Direktive 1999/93/ES. To vključuje zagotavljanje preteklih informacij o statusu nadzora/akreditacije nadzorovanih/akreditiranih storitev overjanja.

Obvezne informacije na zanesljivem seznamu (TL) morajo zajemati najmanj informacije o nadzorovanih/akreditiranih overiteljih, ki izdajajo kvalificirana potrdila (QC) ([2]) v skladu z določbami iz Direktive 1999/93/ES (členi 3.3, 3.2 in 7.1(a)), vključno z informacijami o kvalificiranih potrdilih, ki podpirajo elektronski podpis, in o tem, ali je podpis oblikovan z napravo za varno tvorjenje podpisa (SSCD) ([3]).

Prostovoljno je na nacionalni ravni v zanesljivi seznam mogoče vključiti dodatne informacije o drugih nadzorovanih/akreditiranih overiteljih, ki ne izdajajo kvalificiranih potrdil, vendar nudijo storitve, povezane z elektronskimi podpisi (npr. o overiteljih, ki nudijo storitve časovnega žigosanja in izdajajo žetone časovnega žiga, o overiteljih, ki izdajajo nekvalificirana potrdila itd.).

Te informacije so namenjene predvsem podpori potrjevanja kvalificiranih elektronskih podpisov (QES) in naprednih elektronskih podpisov (AdES) ([4]), ki temeljijo na kvalificiranem potrdilu ([5]) ([6]).

Predlagani skupni model je skladen z izvajanjem, ki temelji na specifikacijah ETSI TS 102 231 ([7]), ki se uporabljajo za obravnavanje vzpostavitve, objave, lokacije, dostopa, avtentifikacije in zaupanja v takšne sezname.

([1]) Kot je opredeljeno v členu 2.11 Direktive 1999/93/ES.
([2]) Kot je opredeljeno v členu 2.10 Direktive 1999/93/ES.
([3]) Kot je opredeljeno v členu 2.6 Direktive 1999/93/ES.
([4]) Kot je opredeljeno v členu 2.2 Direktive 1999/93/ES.
([5]) Za napredni elektronski podpis, ki temelji na kvalificiranem potrdilu, se v nadaljevanju uporablja kratica „$AdES_{QC}$“.
([6]) Obstaja več elektronskih storitev, ki temeljijo na enostavnem AdES, katerih čezmejna uporaba bi prav tako bila pospešena, pod pogojem, da so podporne storitve overjanja (npr. izdajanje nekvalificiranih potrdil) del nadzorovanih/akreditiranih storitev, ki jih država članica vključi v prostovoljni del informacij v zanesljivem seznamu.
([7]) ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

2. **Smernice za urejanje vnosov v zanesljivi seznam**

2.1. *Zanesljivi seznam nadzorovanih/akreditiranih storitev overjanja*

Zadevne storitve overjanja in overitelji na enem seznamu

Zanesljivi seznam države članice je opredeljen kot „seznam statusov nadzora/akreditacije storitev overjanja s strani overiteljev, ki jih referenčna država članica nadzoruje/akreditira za skladnost z zadevnimi določbami Direktive 1999/93/ES“.

Takšen zanesljivi seznam mora zajemati:

— **vse overitelje**, kot so opredeljeni v členu 2.11 Direktive 1999/93/ES, tj. „subjekt, fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z elektronskim podpisom“,

— **ki so nadzorovani/akreditirani** za skladnost z zadevnimi določbami iz Direktive 1999/93/ES.

Pri obravnavi opredelitev in določb iz Direktive 1999/93/ES, zlasti v zvezi z zadevnimi overitelji in njihovimi prostovoljnimi sistemi nadzora/akreditacije, je mogoče razlikovati med dvema skupinama overiteljev, in sicer overitelji, ki izdajajo kvalificirana potrdila javnosti (CSP_{QC}), in overitelji, ki ne izdajajo kvalificiranih potrdil javnosti, temveč zagotavljajo „druge (pomožne) storitve, povezane z elektronskimi podpisi“:

— **Overitelji, ki izdajajo kvalificirana potrdila:**

— Nadzorovati jih mora tista država članica, v kateri imajo sedež (če imajo sedež v državi članici EU), in so lahko akreditirani tudi za skladnost z določbami iz Direktive 1999/93/ES, vključno z zahtevami Priloge I (zahteve za kvalificirana potrdila) in zahtevami Priloge II (zahteve za overitelje, ki izdajajo kvalificirana potrdila). Overitelji, ki izdajajo kvalificirana potrdila in so akreditirani v državi članici, morajo še vedno spadati v ustrezen sistem nadzora te države članice, razen če nimajo sedeža v tej državi članici.

— Veljavni sistem „nadzora“ (oziroma prostovoljni sistem „akreditacije“) je opredeljen in mora izpolnjevati ustrezne zahteve Direktive 1999/93/ES, zlasti zahteve v členih 3.3, 8.1 in 11 ter uvodni izjavi 13 (oziroma členih 2.13, 3.2, 7.1(a), 8.1 in 11 ter uvodnih izjavah 4 in 11 do 13).

— **Overitelji, ki ne izdajajo kvalificiranih potrdil:**

— Lahko spadajo v prostovoljni sistem „akreditacije“ (kot je opredeljen v Direktivi 1999/93/ES in skladno s to direktivo) in/ali v nacionalno opredeljeno „priznano shemo potrjevanja“, ki se izvaja na nacionalni ravni za nadzor skladnosti z določbami iz Direktive in po možnosti z nacionalnimi določbami v zvezi z zagotavljanjem storitev overjanja (v smislu člena 2.11 Direktive).

— Nekateri fizični ali binarni (logični) objekti, ustvarjeni ali izdani kot posledica zagotavljanja storitev overjanja, so lahko upravičeni do posebne „kvalifikacije“ na podlagi njihove skladnosti z določbami in zahtevami na nacionalni ravni, vendar je pomen takšne „kvalifikacije“ verjetno omejen izključno na nacionalno raven.

▼C1

Zanesljivi seznam države članice mora nuditi najmanj informacije o nadzorovanih/akreditiranih overiteljih, ki izdajajo kvalificirana potrdila (QC) javnosti v skladu z določbami iz Direktive 1999/93/ES (členi 3.3, 3.2 in 7.1(a)), informacije o kvalificiranih potrdilih, ki podpirajo elektronski podpis, in o tem, ali je podpis oblikovan z napravo za varno tvorjenje podpisa (SSCD).

Prostovoljno je na nacionalni ravni v zanesljivi seznam mogoče vključiti dodatne informacije o drugih nadzorovanih/akreditiranih storitvah overiteljev, ki ne izdajajo kvalificiranih potrdil javnosti (npr. o overiteljih, ki nudijo storitve časovnega žigosanja in izdajajo žetone časovnega žiga, o overiteljih, ki izdajajo nekvalificirana potrdila itd.).

Namen zanesljivega seznama je:

— popisati in nuditi zanesljive informacije o statusu nadzora/akreditacije storitev overjanja s strani overiteljev, ki jih nadzira/akreditira država članica, ki je odgovorna za pripravo in posodabljanje seznama zaradi skladnosti z zadevnimi določbami iz Direktive 1999/93/ES,

— olajšati potrjevanje elektronskih podpisov, ki temeljijo na navedenih nadzorovanih/akreditiranih storitvah overjanja navedenih overiteljev.

Enotna zbirka vrednosti statusa nadzora/akreditacije

Vsaka država članica mora vzpostaviti in vzdrževati enoten zanesljivi seznam, ki navaja status nadzora in/ali akreditacije tistih storitev overjanja s strani overiteljev, ki jih država članica nadzoruje/akreditira.

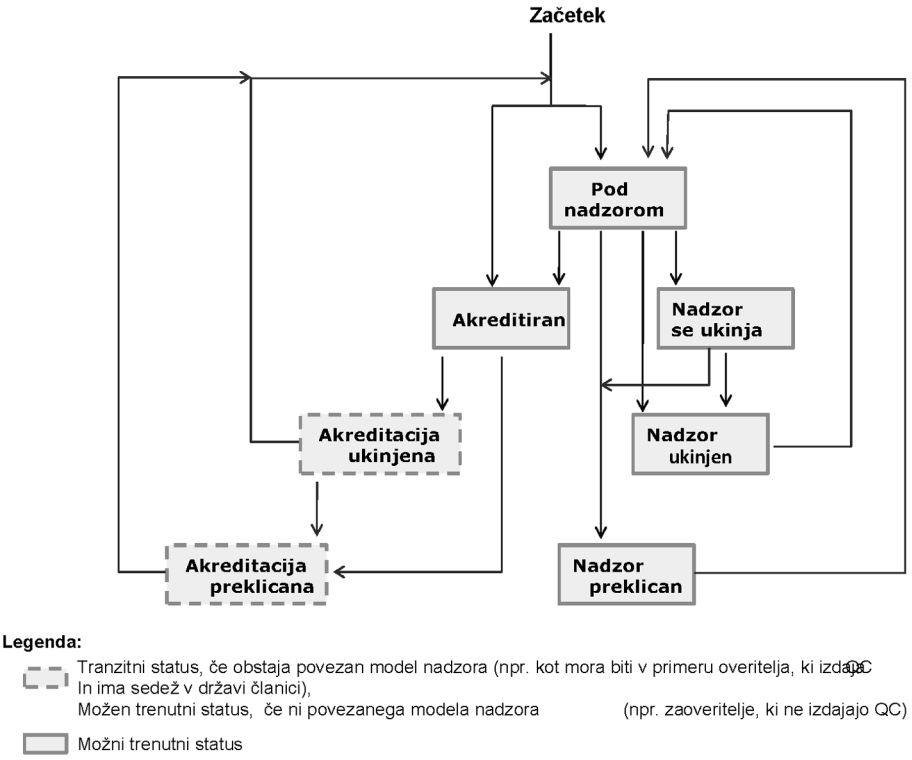
Dejstvo, da je storitev trenutno nadzorovana ali akreditirana, je del trenutnega statusa. Poleg tega je lahko status nadzora ali akreditacije „v teku“, „se ukinja“, „ukinjen“ ali celo „preklican“. V času obstoja storitve overjanja se lahko njen status spremeni iz statusa nadzora v status akreditacije in obratno ([1]).

Naslednja slika 1 opisuje pričakovani tok za eno storitev overjanja med možnima statusoma nadzora/akreditacije:

([1]) Npr. overitelj s sedežem v državi članici, ki nudi storitve overjanja in ga na začetku nadzoruje država članica (nadzorni organ), se lahko po določenem času odloči za prostovoljno akreditacijo za trenutno nadzorovane storitve overjanja. Nasprotno se lahko overitelj v drugi državi članici odloči, da ne bo prenehal opravljati akreditiranih storitev overjanja, temveč da bo status akreditacije zamenjal s statusom nadzora, npr. zaradi poslovnih in/ali gospodarskih razlogov.

▼C1

Pričakovani tok statusa nadzora/akreditacije za storitev overitelja



Slika 1

Overitelj, ki izdaja kvalificirana potrdila, mora biti nadzorovan (če ima sedež v državi članici) in je lahko prostovoljno akreditiran. „Trenutna vrednost statusa“ takšne storitve, ki je navedena v zanesljivem seznamu, je lahko katera koli od zgoraj prikazanih vrednosti. Vendar pa je treba poudariti, da morata imeti statusa „akreditacija ukinjena“ in „akreditacija preklicana“ vrednosti „tranzitnega statusa“ samo v primeru CSP_{QC} s sedežem v državi članici, saj morajo biti te storitve nadzorovane že same po sebi (tudi če niso oziroma niso več akreditirane).

Zahteva se, da države članice, ki vzpostavljajo ali so vzpostavile nacionalno opredeljeno „priznano shemo potrjevanja“, uvedeno na nacionalni ravni za nadzor skladnosti storitev overiteljev, ki ne izdajajo kvalificiranih potrdil, z določbami iz Direktive 1999/93/ES in z morebitnimi nacionalnimi določbami v zvezi z zagotavljanjem storitev overjanja (v smislu člena 2.11 Direktive), razvrstijo takšne sheme potrjevanja v naslednji kategoriji:

— „prostovoljna akreditacija“, kot je opredeljena in urejena v Direktivi 1999/93/ES (členi 2.13, 3.2, 7.1(a), 8.1, 11 ter uvodne izjave 4 in 11 do 13),

— „nadzor“, kot ga zahteva Direktiva 1999/93/ES ter se izvaja z nacionalnimi določbami in zahtevami v skladu z nacionalno zakonodajo.

▼C1

Overitelj, ki ne izdaja kvalificiranih potrdil, je lahko nadzorovan ali prostovoljno akreditiran. „Trenutna vrednost statusa“ takšne storitve, ki je navedena v zanesljivem seznamu, je lahko katera koli od zgoraj prikazanih vrednosti (glej sliko 1).

Zanesljivi seznam mora vsebovati informacije o osnovni shemi nadzora/akreditacije, zlasti:

— informacije o sistemu nadzora, ki velja za katerega koli CSP_{QC},

— informacije, kadar je to primerno, o nacionalni „prostovoljni shemi akreditacije“, ki velja za kateri koli CSP_{QC},

— informacije, kadar je to primerno, o sistemu nadzora, ki velja za katerega koli overitelja, ki ne izdaja kvalificiranih potrdil,

— informacije, kadar je to primerno, o nacionalni „prostovoljni shemi akreditacije“, ki velja za katerega koli overitelja, ki ne izdaja kvalificiranih potrdil.

Zadnja dva niza informacij sta izjemno pomembna za to, da stranke ocenijo raven kakovosti in varnosti takšnih sistemov nadzora/akreditacije, ki na nacionalni ravni veljajo za overitelje, ki ne izdajajo kvalificiranih potrdil. Če je v zanesljivem seznamu podana informacija o statusu nadzora/akreditacije v zvezi s storitvami overiteljev, ki ne izdajajo kvalificiranih potrdil, se zgoraj navedeni nizi informacij vključijo v zanesljivi seznam s pomočjo „Scheme information URI“ (klavzula 5.3.7 – informacije, ki jih zagotovijo države članice), „Scheme type/community/rules“ (klavzula 5.3.9 – s pomočjo besedila, ki je enako za vse države članice, in neobveznih posebnih informacij, ki jih zagotovi država članica) in „TSL policy/legal notice“ (klavzula 5.3.11 – besedilo, ki je enako za vse države članice s sklicevanjem na Direktivo 1999/93/ES, skupaj z možnostjo za vsako državo članico, da doda besedilo/reference, specifične za državo članico). Dodatne informacije o „kvalifikaciji“, opredeljene na ravni nacionalnih sistemov nadzora/akreditacije za overitelje, ki ne izdajajo kvalificiranih potrdil, se lahko zagotovijo na ravni storitve, če je to primerno in potrebno (npr. za razlikovanje med več ravnmi kakovosti/varnosti), s pomočjo razširitve „additionalServiceInformation“ (klavzula 5.8.2) kot dela „Service information extension“ (klavzula 5.5.9). Dodatne informacije o ustreznih tehničnih specifikacijah so navedene v podrobnih specifikacijah v poglavju I.

Čeprav so lahko za nadzor in akreditacijo storitev overjanja pristojni različni organi države članice, se pričakuje, da bo za posamezno storitev overjanja uporabljen samo en vnos (opredeljen s „Service digital identity“ po ETSI TS 102 231 [1]) in da bo njen status nadzora/akreditacije posodobljen v skladu s tem. Pomen zgoraj opisanih statusov je opisan v zadevni klavzuli 5.5.4 podrobnih tehničnih specifikacij v poglavju I.

2.2. *Vnosi v zanesljivi seznam, ki so namenjeni olajšanju potrjevanja QES in $AdES_{QC}$*

Najpomembnejši del priprave zanesljivega seznama je vzpostavitev obveznega dela zanesljivega seznama, in sicer „seznama storitev“ za overitelja, ki izdaja kvalificirana potrdila, da se pravilno odraža natančno stanje izdajanja vsakega overitelja, ki izdaja kvalificirana potrdila, in da se zagotovi, da so informacije, posredovane pri vsakem vnosu, zadostne za olajšanje potrjevanja kvalificiranih elektronskih podpisov in $AdES_{QC}$ (ko so združene z vsebino kvalificiranega potrdila končne entitete, ki ga izda overitelj po storitvi overjanja, navedeni v tem vnosu).

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

▼C1

Če ni resnično interoperabilnega in čezmejnega profila za kvalificirana potrdila, lahko zahtevane informacije vključujejo tudi druge informacije, ki niso informacije o „Service digital identity“ posameznega (korenskega) CA, zlasti informacije, ki opredeljujejo status QC izdanega potrdila, ter podatek, ali so bili podprti podpisi oblikovani s SSCD. Organ v državi članici, ki je imenovan za vzpostavitev, urejanje in vzdrževanje zanesljivega seznama (tj. upravljavec sheme po ETSI TS 102 231), mora zato upoštevati trenutni profil in vsebino potrdila v vsakem izdanem kvalificiranem potrdilu, po overiteljih, ki izdajajo kvalificirana potrdila, vključenih v zanesljivi seznam.

Najbolje bi bilo, da bi vsako izdano kvalificirano potrdilo vsebovalo s strani ETSI opredeljeno izjavo QcCompliance ([1]), kadar naj bi šlo za QC, in da bi vključevalo s strani ETSI opredeljeno izjavo QcSSCD, kadar naj bi bilo podprto s SSCD za ustvarjanje e-podpisov, in/ali da bi vsako izdano kvalificirano potrdilo vključevalo eno od identifikacijskih oznak (OID) politike potrdila QCP/QCP+, opredeljeno v ETSI TS 101 456 ([2]). Ker so overitelji, ki izdajajo kvalificirana potrdila, za reference uporabljali različne standarde, ker so bili ti standardi zelo različno tolmačeni in zaradi pomanjkanja ozaveščenosti o obstoju in prednostne razvrstitve nekaterih normativnih tehničnih specifikacij ali standardov, je prišlo do razlik v dejanski vsebini trenutno izdanih QC (npr. uporaba oziroma neuporaba s strani ETSI opredeljenih izjav QC), kar pa posledično strankam prejemnicam preprečuje, da bi se zanesle na potrdilo podpisnika (in povezano verigo/pot) za oceno, vsaj v strojno berljivi obliki, ali je potrdilo, ki podpira e-podpis, kvalificirano potrdilo in ali je povezano s SSCD, s katero je bil e-podpis ustvarjen.

Z vnašanjem informacij, navedenih v polju „Service information extensions“ („Sie“), v polja „Service type identifier“ („Sti“), „Service name“ („Sn“) in „Service digital identity“ („Sdi“) ([3]), omogoča predlaganemu skupnemu modelu zanesljivega seznama, da v celoti določi posebno vrsto kvalificiranega potrdila, ki ga je izdal na seznamu naveden overitelj, ki izdaja kvalificirana potrdila, in da zagotovi informacije o tem, ali je podprto s SSCD (če tega podatka ni v izdanem QC). S tem vnosom je seveda povezan poseben podatek o „Service current status“ („Scs“). To je prikazano v spodnji sliki 2.

Navedba storitve zgolj z navedbo „Sdi“ (korenskega) CA bi pomenila, da je zagotovljeno (s strani overitelja, ki izdaja kvalificirana potrdila, in tudi s strani organa nadzora/akreditacije, ki je odgovoren za nadzor/akreditacijo tega overitelja), da vsako potrdilo končne entitete, izdano po tem (korenskem) CA (hierarhija), vsebuje dovolj s strani ETSI opredeljenih informacij, ki jih je mogoče strojno obdelati, da se oceni, ali gre za kvalificirano potrdilo in ali ga podpira SSCD. Če ta trditev ne drži (npr. kvalificirano potrdilo ne vsebuje s strani ETSI standardizirane navedbe, ki jo je mogoče strojno obdelati, o tem, da je podprto s SSCD), je mogoče zgolj z navedbo „Sdi“ tega (korenskega) CA domnevati samo, da kvalificirana potrdila, izdana po tej (korenski) CA hierarhiji, niso podprta s SSCD. Da se kvalificirana potrdila štejejo za podprta s SSCD, je treba za navedbo tega dejstva uporabiti „Sie“ (to tudi pomeni, da to potrjuje overitelj, ki izdaja kvalificirana potrdila in ga nadzoruje/akreditira organ nadzora oziroma akreditacije).

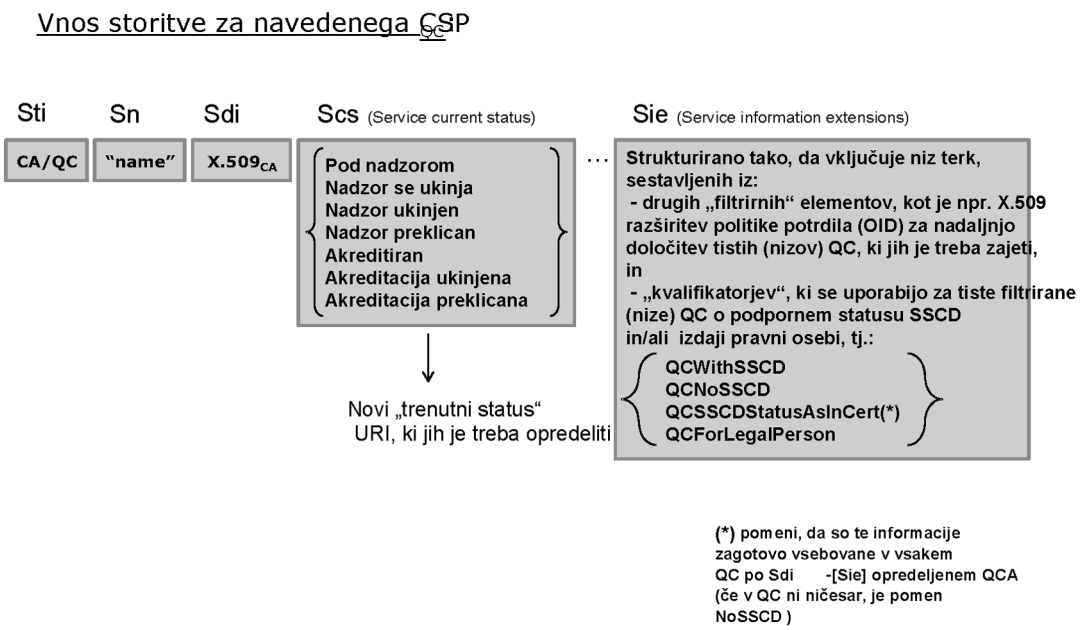
([1]) Glej ETSI TS 101 862 – Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.

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

([3]) Tj., najmanj, potrdilo X.509v3 izdajatelja QCA ali višjega CA v verigi overjanja.

▼C1

Splošna načela – Pravila urejanja – CSP_{QC} vnosi (navedene storitve)



Slika 2

Vnos storitve za navedenega CSP, ki izdaja QC, v TL, izvedenem v formatu TSL

Veljavne tehnične specifikacije za skupni model TL omogočajo uporabo kombinacije petih glavnih delov informacij v vnosu storitve:

— „Service type identifier“ („Sti“), npr. opredeljuje CA, ki izdaja QC („CA/QC“),

— „Service name“ („Sn“),

— podatek „Service digital identity“ („Sdi“) opredeljuje navedeno storitev, npr. potrdilo X.509v3 (najmanj) za CA, ki izdaja QC,

— za storitve CA/QC, neobvezne informacije „Service information extensions“ („Sie“), ki omogočajo vključitev niza ene ali več terk, pri čemer vsaka terka nudi:

  — merila za nadaljnjo opredelitev (filter), po „Sdi“ opredeljeni storitvi overjanja, tiste storitve (tj. niz kvalificiranih potrdil), za katero se zahtevajo/zagotovijo dodatne informacije v zvezi z navedbo podpore SSCD (in/ali izdajo pravni osebi), in

  — povezane informacije („kvalifikatorji“) o tem, ali je ta nadalje opredeljeni niz kvalificiranih potrdil podprt s SSCD oziroma ali so te povezane informacije del QC po standardizirani obliki, ki jo je mogoče strojno obdelati, in/ali informacije v zvezi z dejstvom, da se takšna QC izdajo pravnim osebam (načeloma se šteje, da se izdajo samo fizičnim osebam).

▼C1

— Informacije o „trenutnem statusu“ za ta vnos storitve, ki zagotavljajo informacije:

— o tem, ali gre za nadzorovano ali akreditirano storitev, in

— o samem statusu nadzora/akreditacije.

2.3. *Smernice za urejanje in uporabo vnosov storitev CSP_{QC}*

Splošne smernice za urejanje so:

1. Če je zagotovljeno (jamstvo, ki ga zagotovi CSP_{QC} in nadzoruje/akreditira nadzorni organ (SB)/akreditacijski organ (AB)), da za navedeno storitev, opredeljeno s „Sdi“, vsako QC, podprto s SSCD, vsebuje s strani ETSI opredeljeno izjavo QcCompliance in izjavo QcSSCD in/ali identifikacijsko oznako (OID) QCP+, potem zadostuje uporaba ustreznega „Sdi“, polje „Sie“ pa se lahko uporabi kot možna izbira in ni nujno, da vsebuje informacije o podpori SSCD.

2. Če je zagotovljeno (jamstvo, ki ga zagotovi CSP_{QC} in nadzoruje/akreditira SB/AB), da za navedeno storitev, opredeljeno s „Sdi“, vsako QC, ki ni podprto s SSCD, vsebuje bodisi izjavo QcCompliance in/ali QCP OID in je takšno, da se šteje, da ne vsebuje izjave QcSSCD ali QCP+ OID, potem zadostuje uporaba ustreznega „Sdi“, polje „Sie“ pa se lahko uporabi kot možna izbira in ni nujno, da vsebuje informacije o podpori SSCD (kar pomeni, da ni podprto s SSCD).

3. Če je zagotovljeno (jamstvo, ki ga zagotovi CSP_{QC} in nadzoruje/akreditira SB/AB), da za navedeno storitev, opredeljeno s „Sdi“, vsako QC vsebuje izjavo QcCompliance, in da so nekatera od teh QC podprta s SSCD (npr. to se lahko razlikuje glede na različne OID politike potrdila, specifične za CSP, ali druge za CSP specifične informacije, neposredno ali posredno, z možnostjo strojne obdelave ali ne), vendar NE VSEBUJE niti izjave QcSSCD niti ETSI QCP(+) OID, potem uporaba ustreznega „Sdi“ ne zadostuje IN se v polje „Sie“ vnesejo izrecne informacije o podpori SSCD, skupaj z morebitno razširitvijo informacij, da se opredeli zajeti niz potrdil. To zelo verjetno zahteva vključitev različnih „vrednosti informacij o podpori SSCD“ za isti „Sdi“, če se uporablja polje „Sie“.

4. Če je zagotovljeno (jamstvo, ki ga zagotovi CSP_{QC} in nadzoruje/akreditira SB/AB), da za navedeno storitev, opredeljeno s „Sdi“, QC ne vsebuje izjave QcCompliance, QCP OID, izjave QcSSCD ali QCP+ OID, vendar je zagotovljeno, da se nekatera izmed teh potrdil končnih entitet, izdana po tem „Sdi“, štejejo za QC in/ali kot podprta s SSCD (npr. to se lahko razlikuje glede na različne OID politike potrdila, specifične za CSP_{QC} ali druge za CSP_{QC} specifične informacije v QC, neposredno ali posredno, z možnostjo strojne obdelave ali ne), potem uporaba ustreznega „Sdi“ ne zadostuje IN je treba uporabiti polje „Sie“ za vključitev izrecnih informacij o podpori SSCD. To zelo verjetno zahteva vključitev različnih „vrednosti informacij o podpori SSCD“ za isti „Sdi“, če se uporablja polje „Sie“.

▼C1

Načeloma mora za navedenega CSP na zanesljivem seznamu obstajati en vnos storitve za potrdilo X.509v3 za storitev overjanja CA/QC, tj. za overitelja potrdila (CA), ki (neposredno) izdaja QC. V nekaterih skrbno nadzorovanih okoliščinah in skrbno nadzorovanih pogojih se lahko nadzorni organ/akreditacijski organ države članice odloči za uporabo potrdila X.509v3 CA korenske ali višje ravni (tj. overitelja potrdila, ki ne izdaja QC neposredno končnim entitetam, temveč potrjuje hierarhijo CA vse do CA, ki izdajajo QC končnim entitetam) kot „Sdi“ posameznega vnosa na seznam storitev navedenega CSP. Države članice morajo skrbno preučiti in potrditi posledice (prednosti in slabosti) uporabe takšnega potrdila X.509v3 korenskega CA ali višjega CA kot vrednosti „Sdi“ vnosov storitev na TL. Poleg tega morajo države članice pri uporabi te dovoljene izjeme od splošnega načela zagotoviti potrebno dokumentacijo za pospešitev vzpostavitve in potrditve verige overjanja.

Za ponazoritev splošnih smernic urejanja je mogoče podati naslednji primer: v okviru CSP_{QC}, ki uporablja en korenski CA, po katerem več CA izdaja kvalificirana in nekvalificirana potrdila, vendar za katerega QC vsebujejo le izjavo QcCompliance in ne navajajo, ali so QC podprti s SSCD, bi zgolj navedba „Sdi“ korenskega CA pomenila, po zgoraj pojasnjenih pravilih, da QC, izdan po tej korenski hierarhiji CA, NI podprt s SSCD. Če so ta QC dejansko podprta s SSCD, se močno priporoča, da se v prihodnosti v QC uporabi izjava QcSSCD. Medtem (dokler ne poteče veljavnost zadnjega QC, ki ne vsebuje te informacije) pa mora TSL uporabljati polje „Sie“ in povezano razširitev „kvalifikacije“, npr. filtriranje potrdil s pomočjo posebnih OID, ki jih opredeli CSP_{QC} in jih morebiti uporablja za razlikovanje med različnimi vrstami QC (nekateri so podprti s SSCD, drugi pa ne), in vključno z izrecnimi „informacijami o podpori SSCD“ v zvezi s temi filtriranimi potrdili s pomočjo „kvalifikatorjev“.

Splošne smernice za uporabo aplikacij, storitev ali proizvodov za elektronsko podpisovanje, ki temeljijo na izvajanju TSL zanesljivega seznama v skladu z zadevnimi tehničnimi specifikacijami, so naslednje:

Vnos „CA/QC“„Sti“ (podobno vnos CA/QC, ki je nadalje opredeljen kot „korenski CA/QC“ s pomočjo „Sie“ razširitve additionalServiceInformation)

— pomeni, da so s strani „Sdi“ opredeljenega CA (podobno v hierarhiji CA, začenši s korenskim CA, opredeljenim s „Sdi“) vsa izdana potrdila končnim entitetam kvalificirana potrdila, **pod pogojem**, da je to navedeno v potrdilu s pomočjo ustreznih QcStatement (tj. QcC, QcSSCD) in/ali s strani ETSI opredeljenih QCP(+) OID (in to zagotavlja nadzorni/akreditacijski organ, glej zgornje „splošne smernice za urejanje“).

Opomba: če ni navedene informacije „Sie“„kvalifikacija“ ali če potrdilo končne entitete, ki naj bi bilo QC, ni „nadalje opredeljeno“ s povezanim vnosom „Sie“, se točnost informacij v QC, „ki jih je mogoče strojno obdelati“, nadzoruje/akreditira. To pomeni, da je uporaba (ali neuporaba) ustreznih QcStatement (tj. QcC, QcSSCD) in/ali s strani ETSI opredeljenih QCP(+) OID zagotovo v skladu s podatki, ki jih navaja CSP_{QC},

▼C1

— **in ČE** je navedena informacija „Sie“„kvalifikacija“, je treba poleg zgornjega pravila za razlago upoštevati tista potrdila, ki so opredeljena s pomočjo tega vnosa „Sie“„kvalifikacija“, ki je sestavljen po načelu niza „filtrov“, ki nadalje opredeljujejo sklop potrdil in zagotavljajo dodatne informacije o „podpori SSCD“ in/ali „pravni osebi kot subjektu“ (npr. tista potrdila, ki vsebujejo posebno OID v razširitvi politike potrdila, in/ali ki imajo poseben vzorec „uporabe ključa“, in/ali so filtrirana s pomočjo posebne vrednosti, ki se pojavi v določenem polju ali razširitvi itd.), in sicer v skladu z naslednjim nizom „kvalifikatorjev“, ki nadomeščajo pomanjkanje informacij v ustreznem QC, tj.:

— navedba podpore SSCD:

  — vrednost kvalifikatorja „QCWithSSCD“ pomeni „QC, podprt s SSCD“, ali

  — vrednost kvalifikatorja „QCNoSSCD“ pomeni „QC, ki ni podprt s SSCD“, ali

  — vrednost kvalifikatorja „QCSSCDStatusAsInCert“ pomeni, da so informacije o podpori SSCD zagotovo vsebovane v vseh QC pod informacijami „Sdi“-„Sie“ v tem vnosu CA/QC,

  in/ali

— navedba izdaje pravni osebi:

  — vrednost kvalifikatorja „QCForLegalPerson“ pomeni „potrdilo, izdano pravni osebi“.

2.4. *Storitve, ki podpirajo storitve „CA/QC“, vendar niso del „CA/QC“„Sdi“*

Zajeti je treba tudi primere, ko so odzivi CRL in OCSP podpisani s ključi, ki niso ključi CA, ki izdajajo QC („CA/QC“). To je mogoče zajeti s seznamom tistih storitev v izvajanju TSL zanesljivega seznama (tj. s „Service type identifier“, ki je nadalje opredeljen z razširitvijo „additionalServiceInformation“, ki odraža OCSP ali storitev CRL kot del zagotavljanja QC, npr. z vrsto storitve „OCSP/QC“ ali „CRL/QC“), saj je te storitve mogoče obravnavati kot del nadzorovanih/akreditiranih „kvalificiranih“ storitev, povezanih z zagotavljanjem storitev overjanja QC. Seveda je treba strežnike OCSP ali izdajatelje CRL, katerih potrdila podpišejo CA po hierarhiji navedene storitve CA/QC, obravnavati kot „veljavne“ in skladne z vrednostjo statusa navedene storitve CA/QC.

Podobno velja za storitve overjanja, ki izdajajo nekvalificirana potrdila (vrsta storitve „CA/PKC“) s pomočjo privzetih vrst storitev ETSI TS 102 231 OCSP in CRL.

Izvajanje TSL zanesljivega seznama MORA vsebovati storitve preklica, če povezane informacije niso prisotne v polju AIA končnega potrdila ali če ni podpisa CA, ki je eden od navedenih CA.

2.5. *Korak proti interoperabilnemu profilu QC*

Na splošno si je treba prizadevati za kar največjo poenostavitev (zmanjšanje) števila vnosov storitev (različne „Sdi“). To je treba uravnavati s pravilno identifikacijo storitev, ki so povezane z izdajanjem QC in zagotavljanjem zaupanja vrednih informacij o tem, ali so ta QC podprta s SSCD, če izdano QC ne vsebuje te informacije.

▼C1

V idealnih razmerah bi morala biti uporaba polja „Sie“ in razširitve „kvalifikacija“ (strogo) omejena na tiste specifične primere, ki jih je treba rešiti na ta način, saj bi morali QC vsebovati dovolj informacij v zvezi z navedenim kvalificiranim statusom in navedeno (ne)podporo SSCD.

Države članice bi morale v največji možni meri uveljaviti sprejetje in uporabo interoperabilnih profilov QC.

3. **Struktura skupnega modela za zanesljivi seznam**

Predlagani skupni model za zanesljivi seznam držav članic bo razdeljen v naslednje kategorije informacij:

1. informacije o zanesljivem seznamu in shemi izdajanja;

2. niz polj z jasnimi identifikacijskimi informacijami o vsakem nadzorovanem/akreditiranem CSP po shemi (ta niz je neobvezen, tj. če se ne uporablja, se seznam šteje za praznega, kar pomeni, da CSP niso nadzorovani ali akreditirani v povezani državi članici v okviru zanesljivega seznama);

3. za vsak navedeni CSP niz polj z jasno identifikacijo nadzorovane/akreditirane storitve overjanja, ki jo nudi CSP (ta niz mora imeti najmanj en vnos);

4. za vsako navedeno nadzorovano/akreditirano storitev overjanja identifikacijo trenutnega statusa storitve in zgodovino tega statusa.

V okviru CSP, ki izdaja QC, mora jasna identifikacija nadzorovane/akreditirane storitve overjanja, ki se navede na seznamu, upoštevati primere, ko v kvalificiranem potrdilu ni na voljo dovolj informacij o „kvalificiranem“ statusu, morebitni podpori SSCD in zlasti za obravnavo dodatnega dejstva, da večina (komercialnih) CSP uporablja enega kvalificiranega CA za izdajo več vrst potrdil končnim entitetam, kvalificiranih in nekvalificiranih.

Število vnosov na seznamu za priznanega CSP je mogoče zmanjšati, kjer obstaja ena ali več storitev višjih CA, npr. v okviru komercialne hierarhije CA od korenskih CA pa vse do CA izdajateljev. Vendar pa je treba celo v teh primerih ohraniti in zagotoviti jasno povezavo med storitvijo overjanja CSP_{QC} in nizom potrdil, namenjenih opredelitvi kot QC.

1. *Informacije o zanesljivem seznamu in o shemi izdajanja*

V to kategorijo spadajo naslednje informacije:

— **oznaka** zanesljivega seznama, ki olajša opredelitev zanesljivega seznama med elektronskim iskanjem in za potrjevanje namenov v berljivi obliki,

— **format in identifikator različice formata** zanesljivega seznama,

— **zaporedna številka (številka izdaje)** zanesljivega seznama,

— **informacije o vrsti** zanesljivega seznama (npr. za opredelitev dejstva, da ta zanesljivi seznam nudi informacije o statusu nadzora/akreditacije storitev overjanja s strani overiteljev (CSP), ki jih referenčna država članica nadzoruje/akreditira za skladnost z določbami iz Direktive 1999/93/ES),

▼C1

— **informacije o imetniku** zanesljivega seznama (npr. ime, naslov, kontaktni podatki itd. za organ države članice, ki je pristojen za vzpostavitev, varno objavo in vzdrževanje zanesljivega seznama),

— **informacije o osnovni shemi nadzora/akreditacije**, s katero je zanesljivi seznam povezan, med drugim:

  — država, na katero se nanaša,

  — informacije o lokaciji ali sklic nanjo, kjer je mogoče najti informacije o shemi (model sheme, pravila, merila, veljavna skupnost, vrsta itd.),

  — obdobje hrambe (preteklih) informacij,

— **obvestilo o politiki in/ali pravno obvestilo, obveznosti, odgovornosti** zanesljivega seznama,

— **datum in čas izdaje** zanesljivega seznama **ter naslednja predvidena posodobitev**.

2. *Jasne informacije o identifikaciji glede vsakega CSP, priznanega s shemo*

Ta niz informacij vsebuje vsaj naslednje:

— ime organizacije CSP, kot se uporablja v uradnih sodnih registrih (to lahko vključuje UID organizacije CSP po praksah držav članic),

— naslov in kontaktne podatke CSP,

— dodatne informacije o CSP, vključene neposredno ali s sklicem na lokacijo, s katere je te informacije mogoče prenesti.

3. *Za vsak navedeni CSP niz polj z jasno identifikacijo storitve overjanja, ki jo nudi CSP in je nadzorovana/akreditirana v okviru Direktive 1999/93/ES*

Ta sklop informacij vključuje za vsako storitev overjanja navedenega CSP najmanj naslednje:

— identifikator vrste storitve overjanja (npr. identifikator, ki navaja, da je nadzorovana/akreditirana storitev overjanja s strani overitelja (CSP) overitelj potrdila (CA), ki izdaja QC),

— (trgovsko) ime te storitve overjanja,

— jasen edinstven identifikator storitve overjanja,

— dodatne informacije o storitvi overjanja (npr. neposredno vključene ali vključene s sklicem na lokacijo, s katere je informacije mogoče prenesti, informacije o dostopu v zvezi s storitvijo),

— za storitve CA/QC, neobvezen niz terk informacij, pri čemer vsaka terka navaja

  (i) merila, v okviru po „Sdi“ opredeljene storitve overjanja, za nadaljnjo opredelitev (filter) storitve (tj. niz kvalificiranih potrdil), za katero se zahtevajo/zagotovijo dodatne informacije v zvezi z navedbo podpore SSCD (in/ali izdajo pravni osebi); in

  (ii) povezane „kvalifikatorje“, ki zagotavljajo informacije o tem, ali je niz kvalificiranih potrdil iz te nadalje opredeljene storitve podprt s SSCD, in/ali informacije o tem, ali se takšni QC izdajajo pravnim osebam (načeloma se izdajajo fizičnim osebam).

▼C1

4. *Za vsako navedeno storitev overjanja identifikacijo trenutnega statusa storitve in zgodovino tega statusa*

Ta niz informacij vsebuje vsaj naslednje:

— identifikator trenutnega statusa,

— datum in čas začetka trenutnega statusa,

— pretekle informacije o tem statusu.

4. **Opredelitve in kratice**

Za namene tega dokumenta se uporabljajo naslednje opredelitve in kratice:

Izraz	Kratica	Opredelitev
Overitelj	CSP	Kot je opredeljeno v členu 2(11) Direktive 1999/93/ES.
Overitelj potrdila	CA	CA je CSP in lahko uporablja več zasebnih tehničnih ključev CA za podpisovanje, vsak ima povezano potrdilo, da se izdajo potrdila končnim entitetam. CA je organ, ki mu eden ali več uporabnikov zaupa ustvarjanje in dodeljevanje potrdil. Overitelj potrdila lahko ustvarja ključe uporabnikov [ETSI TS 102 042]. Šteje se, da je CA opredeljen z informacijami o identifikaciji, ki so navedene v polju Izdajatelj v potrdilu CA za (overjanje) javnega ključa, povezanega z zasebnim ključem CA za podpisovanje, ki ga CA uporablja za izdajanje potrdil subjektom. CA ima lahko več ključev za podpisovanje. Vsak ključ CA za podpisovanje je jasno opredeljen z edinstvenim identifikatorjem v polju Authority Key Identifier v potrdilu CA.
Overitelj potrdila, ki izdaja kvalificirana potrdila	CA/QC	CA, ki izpolnjuje zahteve iz Priloge II k Direktivi 1999/93/ES in izdaja kvalificirana potrdila, ki izpolnjujejo zahteve iz Priloge I k Direktivi 1999/93/ES.
Potrdilo	Potrdilo	Kot je opredeljeno v členu 2.9 Direktive 1999/93/ES.
Kvalificirano potrdilo	QC	Kot je opredeljeno v členu 2(10) Direktive 1999/93/ES.
Podpisnik	Podpisnik	Kot je opredeljen v členu 2(3) Direktive 1999/93/ES.
Nadzor	Nadzor	„Nadzor“ se uporablja v smislu Direktive 1999/93/ES (člen 3.3). Direktiva od držav članic zahteva, da vzpostavijo ustrezen sistem, ki omogoča nadzor CSP, ki imajo sedež na njihovem ozemlju in izdajajo kvalificirana potrdila javnosti, s katerim zagotavljajo nadzor skladnosti z določbami iz Direktive.
Prostovoljna akreditacija	Akreditacija	Kot je opredeljena v členu 2(13) Direktive 1999/93/ES.
Zanesljivi seznam	TL	Označuje seznam, ki navaja status nadzora/akreditacije storitev overjanja s strani overiteljev (CSP), ki jih referenčna država članica nadzira/akreditira zaradi skladnosti z določbami iz Direktive 1999/93/ES.

▼C1

Izraz	Kratica	Opredelitev
Seznam statusa varnih storitev	TSL	Oblika podpisanega seznama, ki se uporablja kot podlaga za predstavitev informacij o statusu varnih storitev v skladu s specifikacijami iz ETSI TS 102 231.
Varna storitev		Storitev, ki poveča zaupanje v elektronske transakcije (običajno, vendar ne nujno s pomočjo kriptografskih tehnik, ali ki vključuje zaupno gradivo) (ETSI TS 102 231).
Ponudnik varnih storitev	TSP	Organ, ki izvaja eno ali več varnih (elektronskih) storitev (ta izraz se uporablja v širšem smislu kot CSP).
Žeton zaupanja varnih storitev	TrST	Fizični ali binarni (logični) objekt, ustvarjen ali izdan kot rezultat uporabe varne storitve. Primeri binarnih TrST so potrdila, CRL, žetoni časovnega žiga in odzivi OCSP.
Kvalificiran elektronski podpis	QES	AdES, podprt s QC in ustvarjen s SSCD, kot je opredeljena v členu 2 Direktive 1999/93/ES.
Napreden elektronski podpis	AdES	Kot je opredeljen v členu 2(2) Direktive 1999/93/ES.
Napredni elektronski podpis, podprt s kvalificiranim potrdilom	$AdES_{QC}$	Pomeni elektronski podpis, ki izpolnjuje zahteve AdES in je podprt s QC, kot je opredeljeno v členu 2 Direktive 1999/93/ES.
Naprava za varno tvorjenje podpisa	SSCD	Kot je opredeljena v členu 2(6) Direktive 1999/93/ES.

POGLAVJE I

PODROBNE SPECIFIKACIJE ZA SKUPNI MODEL ZA „ZANESLJIVI SEZNAM NADZOROVANIH/AKREDITIRANIH OVERITELJEV“

V naslednjem delu dokumenta se ključne besede „MORA“, „NE SME“, „ZAHTEVA“, „PRIPOROČA“, „LAHKO“ in „NEOBVEZNO“ tolmačijo, kot je navedeno v RFC 2119 ([1]).

►M1 Te specifikacije temeljijo na specifikacijah in priporočilih iz ETSI TS 102 231 v.3.1.2. Če v teh specifikacijah ni navedena nobena posebna zahteva, v celoti veljajo zahteve iz ETSI TS 102 231 v.3.1.2. ◄ Če so v teh specifikacijah navedene posebne zahteve, prevladajo nad ustreznimi zahtevami iz ETSI TS 102 231, hkrati pa so dopolnjene s specifikacijami za format, opredeljenimi v ETSI TS 102 231. V primeru odstopanj med temi specifikacijami in specifikacijami iz ETSI TS 102 231, veljajo te specifikacije.

([1]) IETF RFC 2119: „Key words for use in RFCs to indicate Requirements Levels“.

▼C1

Jezikovna podpora se izvede in zagotovi vsaj v angleščini (EN) in po možnosti še v enem ali več nacionalnih jezikih.

Navedba datuma in časa je skladna s klavzulo 5.1.4 v ETSI TS 102 231.

Uporaba URI je skladna s klavzulo 5.1.5 v ETSI TS 102 231.

Informacije o shemi izdajanja zanesljivega seznama

Tag

TSL tag (klavzula 5.2.1)

To polje SE ZAHTEVA in JE skladno s klavzulo 5.2.1 v ETSI TS 102 231.

▼M1

———————

▼C1

Scheme Information

TSL version identifier (klavzula 5.3.1)

To polje SE ZAHTEVA in JE nastavljeno na „3“ (celo število).

TSL sequence number (klavzula 5.3.2)

▼M1

To polje SE ZAHTEVA. Polje podrobno opredeljuje zaporedno številko TSL. Ob prvi izdaji TSL je začetna številka „1“. Ob vsaki naslednji izdaji TSL se to število poveča. Ko se zgornji „TSL version identifier“ poveča, se to število ne povrne na vrednost „1“.

▼C1

TSL type (klavzula 5.3.3)

▼M1

To polje SE ZAHTEVA in podrobno opredeljuje vrsto TSL. Nastavi se na http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generično).

▼C1

Opomba: Za skladnost s klavzulo 5.3.3 ETSI TS 102 231 in za navedbo posebne vrste TSL, ob hkratnem sklicevanju na obstoj teh specifikacij, ki urejajo vzpostavitev izvajanja TSL zanesljivega seznama držav članic ([1]), in omogočanju razčlenjevalniku, da določi, katero obliko katerega koli od naslednjih polj ([2]) je mogoče pričakovati, kjer imajo ta polja posebne (ali alternativne) pomene glede na vrsto predstavljenega TSL (v tem primeru zanesljivi seznam države članice), se zgoraj navedeni URI registrira in opiše, kot sledi:

([1]) Tj. seznam statusa nadzora/akreditacije storitev overjanja overiteljev, ki jih referenčna država članica nadzira/akreditira zaradi skladnosti z zadevnimi določbami iz Direktive 1999/93/ES (na kratko „zanesljivi seznam“).

([2]) Pomeni polja, podrobno opredeljena v ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information in „profilirana“ s temi specifikacijami za opredelitev priprave zanesljivega seznama držav članic.

▼M1

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

▼C1

Opis: Izvajanje TSL seznama statusa nadzora/akreditacije za storitve overjanja s strani overiteljev, ki jih nadzoruje/akreditira referenčna država članica, imetnica izvajanja TSL za skladnost z zadevnimi določbami iz Direktive 1999/93/ES, s pomočjo postopka neposrednega nadzora (prostovoljnega ali regulativnega).

Scheme operator name (klavzula 5.3.4)

To polje SE ZAHTEVA. Polje podrobno opredeli ime organa države članice, ki je pristojen za vzpostavitev, objavo in vzdrževanje nacionalnega zanesljivega seznama. Polje podrobno opredeli uradno ime, pod katerim deluje povezani pravni subjekt ali pooblaščeni subjekt (npr. za vladne upravne agencije), povezan s tem organom. To MORA biti ime, ki se uporablja pri uradni pravni registraciji ali avtorizaciji in na katero se naslovi vsako uradno obvestilo. Polje je zaporedje večjezičnih nizov črk in je v angleščini kot obveznem jeziku in po možnosti v enem ali več nacionalnih jezikih.

Opomba: Država ima LAHKO ločene nadzorne in akreditacijske organe in celo dodatne organe za katere koli operativne dejavnosti. ►M1 Vsaka država članica imenuje upravljavca sheme izvajanja TSL zanesljivega seznama države članice. ◄ Pričakuje se, da bodo nadzorni organ, akreditacijski organ in upravljavec sheme (če so ti organi ločeni) imeli vsak svoje odgovornosti in obveznosti.

Vsako stanje, ko je več organov odgovornih za nadzor, akreditacijo ali delovanje, SE kot tako dosledno odraža in identificira v informacijah o shemi kot delu TL, vključno z informacijami, specifičnimi za shemo, navedenimi v „Scheme information URI“ (klavzula 5.3.7).

▼M1

Imenovani upravljavec sheme (klavzula 5.3.4) je subjekt, ki bo podpisal TSL.

▼C1

Scheme operator address (klavzula 5.3.5)

To polje SE ZAHTEVA. Polje podrobno opredeli naslov pravnega subjekta ali pooblaščene organizacije, opredeljene v polju „Scheme operator name“ (klavzula 5.3.4), za poštne in elektronske komunikacije. Vključuje tako „PostalAddress“ (tj. ulica, kraj [država ali provinca], [poštna številka] in ISO 3166-1 dvočrkovna (alfa-2) oznaka države), skladno s klavzulo 5.3.5.1, kot tudi „ElectronicAddress“ (tj. e-pošta in/ali URI spletne strani), skladno s klavzulo 5.3.5.2.

Scheme name (klavzula 5.3.6)

To polje SE ZAHTEVA in podrobno opredeli ime, pod katerim shema deluje. Ime je zaporedje večjezičnih nizov črk (v angleščini kot obveznem jeziku in po možnosti v enem ali več nacionalnih jezikih) in je opredeljeno, kot sledi:

▼C1

— Angleška različica je niz črk, sestavljen na naslednji način:

CC:EN_ime_vrednost

pri čemer je:

— „CC“ = ISO 3166-1 dvočrkovna (alfa-2) oznaka države, ki se uporablja v polju „Scheme territory“ (klavzula 5.3.10),

— „:“ = se uporablja kot ločevalnik,

▼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

— Različica v nacionalnem jeziku države članice je niz črk, sestavljen, kot sledi:

CC:name_value

pri čemer je:

— „CC“ = ISO 3166-1 dvočrkovna (alfa-2) oznaka države, ki se uporablja v polju „Scheme territory“ (klavzula 5.3.10),

— „:“ = se uporablja kot ločevalnik,

— „name_value“ = uradni prevod zgornje „EN_name_value“ v nacionalni jezik. Prevod v slovenski jezik: „Seznam statusov nadzora/akreditacije storitev overjanja s strani overiteljev, ki jih referenčna država članica upravljavca sheme nadzira/akreditira zaradi skladnosti z zadevnimi določbami iz Direktive 1999/93/ES“.

Ime sheme mora nedvoumno poimensko določati shemo, ki jo navaja „Scheme information URI“, in tudi zagotavljati, da v primeru, če upravljavec sheme upravlja več shem, te sheme nosijo vsaka svoje ime.

Države članice in upravljavci shem zagotovijo, da v primeru, ko država članica ali upravljavec sheme upravlja več shem, vsaka shema nosi svoje ime.

Scheme information URI (klavzula 5.3.7)

To polje SE ZAHTEVA in podrobno opredeli URI(-je), na katerem(-ih) lahko uporabniki (odvisne stranke) pridobijo za shemo specifične informacije (pri čemer je angleščina obvezni jezik, lahko pa se vključi tudi enega ali več nacionalnih jezikov). Polje je zaporedje večjezičnih kazalcev (v angleščini kot obveznem jeziku ter po možnosti v enem ali več nacionalnih jezikih). Navedeni URI MORAJO zagotavljati pot do informacij, ki podajajo „ustrezne informacije o shemi“.

„Ustrezne informacije o shemi“ vključujejo najmanj naslednje:

— Splošne uvodne informacije, ki so skupne vsem državam članicam, v zvezi z obsegom in okvirom zanesljivega seznama ter z osnovnimi shemami nadzora/akreditacije. To splošno besedilo se uporablja, kot sledi:

▼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."

— Posebne informacije o osnovnih shemah nadzora/akreditacije, zlasti ([1]):

— informacije o sistemu nadzora, ki velja za katerega koli CSP_{QC},

([1]) Zadnja dva sklopa informacij sta izjemno pomembna za to, da odvisne stranke ocenijo raven kakovosti in varnosti takšnih sistemov nadzora/akreditacije. Ta dva sklopa informacij se zagotovita na ravni zanesljivega seznama s pomočjo trenutne „Scheme information URI" (klavzula 5.3.7 – informacije, ki jih zagotovi država članica), „Scheme type/community/rules" (klavzula 5.3.9 – s pomočjo besedila, ki je enako za vse države članice) in „TSL policy/legal notice" (klavzula 5.3.11 – besedilo, ki je enako za vse države članice s sklicevanjem na Direktivo 1999/93/ES, skupaj z možnostjo, da vsaka država članica doda besedilo/reference, specifične za državo članico). Dodatne informacije o nacionalnih sistemih nadzora/akreditacije za overitelje, ki ne izdajajo kvalificiranih potrdil, se lahko zagotovijo na ravni storitve, če je to primerno in potrebno (npr. za razlikovanje med več ravnmi kakovosti/varnosti) s pomočjo „Scheme service definition URI" (klavzula 5.5.6).

▼C1

— informacije, kadar je to primerno, o nacionalni prostovoljni shemi akreditacije, ki velja za katerega koli CSP_{QC},

— informacije, kadar je to primerno, o sistemu nadzora, ki velja za katerega koli overitelja, ki ne izdaja kvalificiranih potrdil,

— informacije, kadar je to primerno, o nacionalni prostovoljni shemi akreditacije, ki velja za katerega koli overitelja, ki ne izdaja kvalificiranih potrdil.

— Te posebne informacije za vsako zgoraj navedeno osnovno shemo vključujejo najmanj:

— splošni opis,

— informacije o postopku, ki ga uporablja organ nadzora/akreditacije za nadzor/akreditacijo overiteljev, in overitelji, ki se nadzirajo/akreditirajo,

— informacije o merilih, po katerih se nadzirajo/akreditirajo CSP.

— Posebne informacije, kadar je to primerno, o posebnih „kvalifikacijah“ nekaterih fizičnih ali binarnih (logičnih) objektov, ustvarjenih ali izdanih kot posledica zagotavljanja storitev overjanja, ki so lahko upravičeni do posebne „kvalifikacije“ na podlagi njihove skladnosti z določbami in zahtevami na nacionalni ravni, vključno s pomenom takšne „kvalifikacije“ ter povezanimi nacionalnimi določbami in zahtevami.

Prostovoljno JE MOGOČE dodati dodatne specifične informacije države članice o shemi. To vključuje:

— informacije o merilih in pravilih, ki se uporabljajo za izbiro nadzornikov/revizorjev in za opredelitev, kako so CSP nadzorovani (kontrolirani)/akreditirani (revidirani),

— druge kontaktne in splošne informacije, ki veljajo za delovanje sheme.

Status determination approach (klavzula 5.3.8)

To polje SE ZAHTEVA in podrobno opredeli identifikator pristopa za določanje statusa. Uporabi se naslednji posebni URI, registriran in opisan, kot sledi:

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

Opis: Status navedenih storitev določi upravljavec sheme oziroma nekdo drug v njegovem imenu po ustreznem sistemu za referenčno državo članico, ki omogoča „nadzor“ (in, kadar je to primerno, „prostovoljno akreditacijo“) nad overitelji, ki imajo sedež na njenem ozemlju (ali v tretji državi v primeru „prostovoljne akreditacije“) in izdajajo kvalificirana potrdila javnosti v skladu s členom 3.3 (oziroma členom 3.2 ali 7.1(a)) Direktive 1999/93/ES, ter ki omogoča, kadar je to primerno, „nadzor/prostovoljno akreditacijo“ overiteljev, ki ne izdajajo kvalificiranih potrdil, v skladu z nacionalno opredeljenimi in vzpostavljenimi „priznanimi shemami potrjevanja“, uvedenimi na nacionalni ravni za nadzor skladnosti storitev overiteljev, ki ne izdajajo kvalificiranih potrdil, z določbami iz Direktive 1999/93/ES in z možnimi nacionalnimi določbami v zvezi z zagotavljanjem takšnih storitev overjanja.

▼C1

Scheme type/community/rules (klavzula 5.3.9)

To polje SE ZAHTEVA in vsebuje najmanj naslednje registrirane URI:

— URI, ki je skupen vsem zanesljivim seznamom držav članic, s kazalcem na opisno besedilo, ki velja za vse TL:

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

— Z njim je označena udeležba sheme države članice (opredeljena z „TSL type“ (klavzula 5.3.3) in „Scheme name“ (klavzula 5.3.6)) v shemi shem (tj. kazalci seznama TSL na vse države članice, ki objavljajo in vzdržujejo zanesljivi seznam v obliki TSL).

— Kjer lahko uporabniki pridobijo politiko/pravila, po katerih se ocenijo storitve, vključene v seznam, in s katerimi je mogoče določiti vrsto TSL (glej klavzulo 5.3.3).

— Kjer lahko uporabniki pridobijo navodila o tem, kako uporabljati in tolmačiti vsebino izvajanja TSL zanesljivega seznama. Ta pravila za uporabo so skupna za vse zanesljive sezname držav članic, ne glede na vrsto navedene storitve in sistem(-e) nadzora/akreditacije.

Opisno besedilo:

„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 ‚RootCA/QC' through the use of ‚Service information extension' (‚Sie') additionalServiceInformation extension)

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

▼C1

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

— **and IF**‚Sie',Qualification' information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this ‚Sie',Qualification' entry, which is constructed on the principle of a sequence of ‚filters' further identifying a set of certificates, must be considered according to the associated ‚qualifiers' providing some additional information regarding ‚SSCD support' and/or ‚Legal person as subject' (e.g. those certificates containing a specific OID in the Certificate Policy extension, and/or having a specific ‚Key usage' pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, 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

— URI, ki je specifičen za vsak zanesljiv seznam države članice, s kazalcem na opisno besedilo, ki velja za TL te države članice:

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

pri čemer je CC = ISO 3166-1 dvočrkovna (alfa-2) oznaka države, ki se uporablja v polju „Scheme territory“ (klavzula 5.3.10).

— Kjer lahko uporabniki pridobijo posebno politiko/pravila referenčne države članice, v skladu s katerimi se storitve, vključene v seznam, ocenijo v skladu z ustreznim sistemom nadzora in prostovoljnimi shemami akreditacije države članice.

— Kjer lahko uporabniki pridobijo navodila, specifična za referenčno državo članico, o tem, kako uporabiti in tolmačiti vsebino izvajanja TSL zanesljivega seznama v zvezi s storitvami overjanja, ki niso povezane z izdajanjem QC. To je mogoče uporabiti za navedbo morebitne razčlenjenosti v nacionalnih sistemih nadzora/akreditacije, povezanih s CSP, ki ne izdajajo QC, in za način, kako se v ta namen uporabita „Scheme service definition URI“ (klavzula 5.5.6). in polje „Service information extension“.

Države članice LAHKO opredelijo dodatne URI iz zgoraj navedenega URI, specifičnega za državo članico (tj. URI, opredeljene iz tega hierarhičnega specifičnega URI).

Scheme territory (klavzula 5.3.10)

V okviru teh specifikacij se to polje ZAHTEVA in podrobno opredeljuje državo, v kateri je shema vzpostavljena (ISO 3166-1 dvočrkovna (alfa-2) oznaka države).

TSL policy/legal notice (klavzula 5.3.11)

V okviru teh specifikacij se to polje ZAHTEVA in podrobno opredeljuje politiko sheme ali navaja obvestilo v zvezi s pravnim statusom sheme ali pravnimi zahtevami, ki jih shema izpolnjuje za pristojnost, v kateri je shema vzpostavljena, in/ali morebitne omejitve in pogoje, po katerih se TL vzdržuje in objavlja.

To je večjezični niz črk (golo besedilo), sestavljen iz dveh delov:

— prvega obveznega dela, skupnega za vse zanesljive sezname držav članic (v angleščini kot obveznem jeziku in po možnosti v enem ali več nacionalnih jezikih), ki navaja, da je veljavni pravni okvir Direktiva 1999/93/ES in njeno ustrezno izvajanje v zakonodaji države članice, navedene v polju „Scheme Territory“.

Angleška različica skupnega besedila:

„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.“

▼C1

Besedilo v slovenskem jeziku:

„Veljavni pravni okvir za zadevno izvajanje TSL zanesljivega seznama nadzorovanih/akreditiranih overiteljev za [ime zadevne države članice] je Direktiva Evropskega parlamenta in Sveta 1999/93/ES z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis in njeno izvajanje v zakonodaji [ime zadevne države članice].“

— drugega neobveznega dela, specifičnega za vsak TL (v angleščini kot obveznem jeziku in po možnosti v enem ali več nacionalnih jezikih), ki navaja sklice na posebne veljavne nacionalne pravne okvire (npr. zlasti, če se nanašajo na nacionalne sheme nadzora/akreditacije za CSP, ki ne izdajajo QC).

Historical information period (klavzula 5.3.12)

To polje SE ZAHTEVA in podrobno opredeljuje obdobje (celo število) zagotavljanja preteklih informacij v TSL. Ta celoštevilska vrednost se navede v številu dni in v okviru teh specifikacij. Vrednost je večja ali enaka 3 653 (kar pomeni, da MORA izvajanje TSL zanesljivega seznama držav članic pretekle informacije vsebovati najmanj deset let). Višje vrednosti morajo ustrezno upoštevati pravne zahteve za hrambo podatkov v državi članici, navedeni v „Scheme Territory“ (klavzula 5.3.10).

Pointers to other TSLs (klavzula 5.3.13)

V okviru teh specifikacij se to polje ZAHTEVA in vključuje, če je ta na voljo, kazalec do ETSI TS 102 231 ustreznega obrazca seznama povezav (kazalcev), ki ga sestavi Evropska komisija, do vseh izvajanj TSL zanesljivih seznamov držav članic. Specifikacije iz ETSI TS 102 231, klavzula 5.3.13, veljajo med dovoljeno uporabo neobvezne digitalne identitete, ki predstavlja izdajatelja TSL, ki je nakazan s povezavo, in je oblikovana, kot je opredeljeno v klavzuli 5.5.3.

Opomba: Med čakanjem na izvajanje s strani Evropske komisije sestavljenega seznama povezav do izvajanja TSL zanesljivih seznamov držav članic, ki je skladno z ETSI TS 102 231, se to polje NE UPORABLJA.

List issue date and time (klavzula 5.3.14)

To polje SE ZAHTEVA ter podrobno opredeljuje datum in čas (UTC izražen kot čas Z), ko je bil TSL izdan, z uporabo vrednosti datuma in časa, kot je navedeno v ETSI TS 102 231, klavzula 5.1.4.

Next update (klavzula 5.3.15)

To polje SE ZAHTEVA in podrobno opredeljuje zadnji datum in čas (UTC izražen kot čas Z), ko bo izdan naslednji TSL, oziroma se navede ničla, kar pomeni, da je TSL zaprt (z uporabo vrednosti datuma in časa, kot je določeno v ETSI TS 102 231, klavzula 5.1.4).

Če ni vmesnih sprememb statusa katerega koli TSP ali storitve, zajete v shemo, JE TREBA TSL ponovno izdati do izteka veljavnosti zadnjega izdanega TSL.

V okviru teh specifikacij razlika med datumom in časom „Next update“ in „List issue date and time“ NE presega **šestih (6)** mesecev.

▼C1

Distribution points (klavzula 5.3.16)

To polje je NEOBVEZNO. Če se uporabi, podrobno opredeljuje lokacije, kjer je objavljeno trenutno izvajanje TSL zanesljivega seznama in kjer je mogoče najti posodobitve veljavnega TSL. Če je opredeljenih več distribucijskih točk, MORAJO vse zagotavljati enake kopije veljavnega TSL ali njegovo posodobljeno različico. Če se to polje uporablja, je oblikovano kot polno zaporedje nizov, ki so vsi skladni z RFC 3986 ([1]).

Scheme extensions (klavzula 5.3.17)

To polje je NEOBVEZNO in se ne uporablja v okviru teh specifikacij.

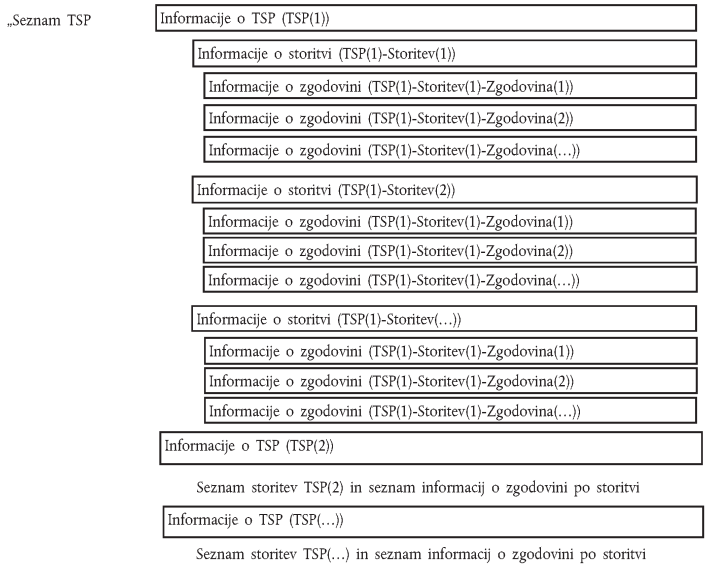
List of Trust Service Providers

To polje je NEOBVEZNO.

Če v državi članici overitelji niso oziroma niso bili nadzirani/akreditirani v okviru sheme, se to polje ne uporablja. Vendar velja, da tudi če država članica nima s shemo nadziranih ali akreditiranih overiteljev, vseeno izvaja TSL, brez uporabe tega polja. Če na seznamu ni nobenega overitelja, to pomeni, da ni overiteljev, ki bi bili nadzirani/akreditirani v državi, opredeljeni v „Scheme Territory“.

Če je oziroma je bila ena ali več storitev CSP nadzorovana/akreditirana s shemo, to polje vsebuje zaporedje, ki opredeljuje vsakega overitelja, ki zagotavlja eno ali več teh nadzorovanih/akreditiranih storitev, s podrobnostmi o statusu nadzora/akreditacije in zgodovini statusa vsake storitve CSP (TSP = CSP na spodnji sliki).

▼C2



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

▼C1

Seznam TSP je organiziran, kot je prikazano na zgornji sliki. Za vsakega TSP obstaja niz polj z informacijami o TSP („TSP Information“), ki mu sledi seznam storitev. Za vsako takšno navedeno storitev obstaja niz polj z informacijami o storitvi („Service Information“) in niz polj o zgodovini statusa odobritve storitve („Service approval history“).

TSP Information

TSP(1)

TSP name (klavzula 5.4.1)

To polje se ZAHTEVA in podrobno opredeljuje ime **pravnega subjekta**, odgovornega za storitve CSP, ki so oziroma so bile nadzorovane ali akreditirane po shemi. Polje je zaporedje večjezičnih nizov črk (v angleščini kot obveznem jeziku in po možnosti v enem ali več nacionalnih jezikih). To ime MORA biti ime, ki se uporablja v uradnih pravnih registrih in na katero bodo naslovljena uradna obvestila.

TSP trade name (klavzula 5.4.2)

To polje je NEOBVEZNO in, če se uporablja, podrobno opredeljuje drugo ime, s katerim se CSP identificira v posebnem okviru zagotavljanja storitev, ki jih je mogoče najti v tem TSL pod vnosom „TSP name“ (klavzula 5.4.1).

Opomba: Če posamezen pravni subjekt CSP zagotavlja storitve pod drugimi trgovskimi imeni ali v drugih posebnih okvirih, je lahko vnosov CSP toliko, kolikor je posebnih okvirov (npr. vnosi ime/trgovsko ime). Druga možnost je, da se vsak CSP (pravni subjekt) navede samo enkrat in zagotavlja informacije o okviru, specifičnem za storitev. O tem odloči upravitelj sheme države članice in se s CSP dogovori o najustreznejšem načinu.

TSP address (klavzula 5.4.3)

To polje se ZAHTEVA in podrobno opredeljuje naslov pravnega subjekta ali pooblaščene organizacije, opredeljene v polju „TSP name“ (klavzula 5.4.1), za poštne in elektronske komunikacije. Vključuje tako „PostalAddress“ (tj. ulica, kraj [država ali provinca], [poštna številka] in ISO 3166-1 dvočrkovna (alfa-2) oznaka države), skladno s klavzulo 5.3.5.1, kot tudi „ElectronicAddress“ (tj. e-pošta in/ali URI spletne strani), skladno s klavzulo 5.3.5.2.

TSP information URI (klavzula 5.4.4)

To polje se ZAHTEVA in podrobno opredeljuje URI, na katerih lahko uporabniki (npr. odvisne stranke) pridobijo informacije, specifične za CSP. Polje je zaporedje večjezičnih kazalcev (v angleščini kot obveznem jeziku in po možnosti v enem ali več nacionalnih jezikih). Referenčni URI MORAJO nuditi pot do informacij, ki opisujejo splošne pogoje CSP, njegove prakse, pravna vprašanja, politiko varstva strank in druge splošne informacije, ki veljajo za vse storitve, navedene v vnosu CSP v TSL.

Opomba: Če posamezen pravni subjekt CSP zagotavlja storitve pod drugimi trgovskimi imeni ali v drugih posebnih okvirih in se to odraža v toliko vnosih TSP, kolikor je teh posebnih okvirov, to polje podrobno opredeljuje informacije, povezane s posebnim sklopom storitev, ki so navedene v posameznem vnosu TSP/trgovsko ime.

▼C1

TSP information extensions (klavzula 5.4.5)

To polje je NEOBVEZNO in ga LAHKO, če se uporablja, uporabi upravljavec sheme, v skladu s specifikacijami ETSI TS 102 231 (klavzula 5.4.5), za zagotovitev posebnih informacij, ki se tolmačijo v skladu s pravili specifične sheme.

List of Services

To polje se ZAHTEVA in vsebuje zaporedje, ki opredeljuje vsako od priznanih storitev CSP ter status odobritve (in zgodovino tega statusa) te storitve. Navedena mora biti najmanj ena storitev (tudi če so vse vsebovane informacije pretekle informacije).

Ker se po teh specifikacijah ZAHTEVA hramba preteklih informacij o navedenih storitvah, je TREBA te pretekle informacije hraniti, četudi trenutni status storitve sicer ne zahteva navedbe storitve (npr. storitev je umaknjena). Zato MORA biti z namenom hrambe preteklih informacij CSP vključen, četudi je njegova edina navedena storitev umaknjena.

Service Information

TSP(1) Service(1)

Service type identifier (klavzula 5.5.1)

▼M1

To polje se ZAHTEVA in podrobno opredeljuje identifikator vrste storitve v skladu z vrsto veljavnih specifikacij TSL (tj. „/eSigDir-1999-93-EC-TrustedList/TSLType/generic“).

▼C1

Če je navedena storitev povezana z izdajanjem kvalificiranih potrdil, je naveden URI http://uri.etsi.org/TrstSvc/Svctype/CA/QC (overitelj potrdila, ki izdaja kvalificirana potrdila).

Če je navedena storitev povezana z izdajo žetonov zaupanja varnih storitev, ki niso QC in ne podpirajo izdaje QC, je navedeni URI eden izmed URI, opredeljenih v ETSI 102 231 in navedenih v klavzuli D.2, ki se nanaša na to polje. To velja tudi za tiste žetone zaupanja varnih storitev, ki so nadzorovani/akreditirani zaradi izpolnjevanja nekaterih posebnih kvalifikacij v skladu z nacionalnimi zakonodajami držav članic (npr. t. i. kvalificirani žetoni časovnega žiga v nemščini in madžarščini). Navedeni URI je eden izmed URI, opredeljenih v ETSI 102 231 in navedenih v klavzuli D.2, ki se nanaša na to polje (npr. TSA za nacionalno opredeljene kvalificirane žetone časovnega žiga). Kadar je to primerno, se takšna specifična nacionalna kvalifikacija žetonov zaupanja varnih storitev LAHKO navede v vnosu storitve, v ta namen pa se uporabi razširitev additionalServiceInformation (klavzula 5.8.2) v klavzuli 5.5.9 („Service information extension“).

▼C1

Načeloma za posamezno potrdilo X.509v3 obstaja en vnos (npr. za storitev overjanja vrste CA/QC) v navedenih storitvah overjanja navedenega CSP v zanesljivem seznamu (npr. overitelj potrdila, ki (neposredno) izdaja QC). V nekaterih skrbno predvidenih okoliščinah ter skrbno nadzorovanih in potrjenih pogojih se LAHKO nadzorni organ/akreditacijski organ države članice odloči za uporabo potrdila X.509v3 CA korenske ali višje ravni (tj. overitelja potrdila, ki ne izdaja neposredno QC končnim entitetam, temveč potrjuje hierarhijo CA vse do CA, ki izdajajo QC končnim entitetam) kot „Sdi“ posameznega vnosa na seznam storitev navedenega CSP. Posledice (prednosti in slabosti) uporabe takšnega potrdila X.509v3 korenskega CA ali višjega CA kot vrednosti „Sdi“ vnosov storitev na TL morajo države članice skrbno preučiti in potrditi ([1]). Poleg tega MORAJO države članice pri uporabi te dovoljene izjeme od splošnega načela zagotoviti potrebno dokumentacijo za pospešitev vzpostavitve in potrditve verige overjanja.

Opomba: TSP, kot so strežniki OCSP in izdajatelji CRL, ki so del storitev overjanja CSP_{QC} in predmet uporabe ločenih parov ključev za podpis odzivov OCSP in CRL, se LAHKO navedejo tudi v veljavnem modelu TSL s pomočjo naslednje kombinacije URI:

— vrednost „Service type identifier“ (klavzula 5.5.1):

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

kombinirana z naslednjo vrednostjo „Service information extension“ (klavzula 5.5.9) razširitev additionalServiceInformation (klavzula 5.8.2):

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

Opis: ponudnik statusa potrdila, ki upravlja strežnik OCSP kot del storitve CSP, ki izdaja kvalificirana potrdila.

— vrednost „Service type identifier“ (klavzula 5.5.1):

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

kombinirana z naslednjo vrednostjo „Service information extension“ (klavzula 5.5.9) razširitev additionalServiceInformation (klavzula 5.8.2):

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

Opis: ponudnik statusa potrdila, ki upravlja CRL kot del storitve CSP, ki izdaja kvalificirana potrdila.

— vrednost „Service type identifier“ (klavzula 5.5.1):

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

([1]) Zaradi uporabe potrdila X.509v3 korenskega CA kot vrednosti „Sdi“ za navedeno storitev bo moral upravljavec sheme upoštevati celoten sklop storitev overjanja pod takšnim korenskim CA kot celoto v zvezi s „statusom nadzora/akreditacije“. Vsaka sprememba statusa, ki se zahteva od enega CA po navedeni korenski hierarhiji, bo npr. zahtevala prevzem te spremembe statusa v celotni hierarhiji.

▼C1

kombinirana z naslednjo vrednostjo „Service information extension“ (klavzula 5.5.9) razširitev additionalServiceInformation (klavzula 5.8.2):

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

Opis: overitelj korenskih potrdil, od katerega je mogoče vzpostaviti verigo overjanja do overitelja potrdil, ki izdaja kvalificirana potrdila.

— vrednost „Service type identifier“ (klavzula 5.5.1):

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

kombinirana z naslednjo vrednostjo „Service information extension“ (klavzula 5.5.9) razširitev additionalServiceInformation (klavzula 5.8.2):

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

Opis: storitev časovnega žigosanja kot del storitve overitelja, ki izdaja kvalificirana potrdila, ki izdajajo TST, ki jih je mogoče uporabiti v postopku potrjevanja kvalificiranega podpisa za zagotovitev in razširitev veljavnosti podpisa, ko je QC preklican ali mu je potekla veljavnost.

Service name (klavzula 5.5.2)

To polje se zahteva in podrobno opredeljuje ime, pod katerim CSP, opredeljen v „TSP name“(klavzula 5.4.1), zagotavlja storitev, opredeljeno v „Service type identifier“ (klavzula 5.5.1). Polje je zaporedje večjezičnih nizov črk (v angleščini kot obveznem jeziku in po možnosti v enem ali več nacionalnih jezikih).

Service digital identity (klavzula 5.5.3)

To polje se ZAHTEVA in podrobno opredeljuje najmanj eno navedbo digitalnega identifikatorja, edinstvenega za storitev, katere vrsta je opredeljena v „Service type identifier“ (klavzula 5.5.1), s katerim je mogoče storitev nedvoumno opredeliti.

V teh specifikacijah je digitalni identifikator, ki se uporablja v tem polju, zadevno potrdilo X.509v3, ki predstavlja javni ključ (ključe), ki ga (jih) CSP uporablja za zagotavljanje storitve, katere vrsta je opredeljena v „Service type identifier“ (klavzula 5.5.1) (tj. ključ, ki ga uporablja korenski CA/QC, ključ, ki se uporablja za podpisovanje potrdil ([1]) ali izdajo žetonov časovnega žiga, podpisovanje CRL ali podpisovanje odzivov OCSP). To povezano potrdilo X.509v3 se uporablja kot minimalen zahtevan digitalni identifikator (ker predstavlja javni ključ (ključe), ki ga (jih) CSP uporablja za zagotavljanje navedenih storitev). LAHKO se uporabijo tudi dodatni identifikatorji, vendar se MORAJO vsi nanašati na isto identiteto (tj. na povezano potrdilo X.509v3):

([1]) To je lahko potrdilo CA, ki izdaja potrdila končnim entitetam (npr. CA/PKC, CA/QC) ali potrdilo zaupanja vrednega overitelja korenskih potrdil, od katerega je mogoče najti pot do kvalificiranih potrdil končne entitete. To informacijo („Service digital identity“) bo morda treba dopolniti s „Service information extensions“) (klavzula 5.5.9), odvisno od tega, ali je te informacije in informacije, ki so navedene v vsakem potrdilu končne entitete, izdanem po tem zaupanja vrednem overitelju korenskih potrdil, mogoče uporabiti za nedvoumno določitev ustreznih lastnosti katerega koli kvalificiranega potrdila.

▼C1

(a) razločevalno ime (DN) potrdila, ki ga je mogoče uporabiti za potrjevanje elektronskih podpisov za storitve CSP, opredeljene v „Service type identifier“ (klavzula 5.5.1);

(b) povezan identifikator javnega ključa (tj. X.509v3 identifikator imetnikovega ključa ali vrednost SKI);

(c) povezan javni ključ.

Načeloma digitalni identifikator (tj. povezano potrdilo x.509v3) v zanesljivem seznamu NI prisoten več kot enkrat, tj. za vsako potrdilo x.509v3 obstaja samo en vnos za storitev overjanja pod navedenimi storitvami overjanja navedenega CSP v zanesljivem seznamu. Nasprotno pa se eno potrdilo x.509v3 uporablja v enem vnosu storitve kot vrednost „Sdi“.

Opomba 1: Edini primer, ko zgoraj navedenega načela ni dovoljeno uporabiti, je stanje, ko se eno potrdilo X.509v3 uporablja za izdajo različnih vrst žetonov varnih storitev, za katere veljajo različne sheme nadzora/akreditacije, na primer CSP eno potrdilo X.509v3 na eni strani uporablja za izdajo QC pod ustreznim sistemom nadzora, na drugi strani pa za izdajo nekvalificiranih potrdil pod drugim statusom nadzora/akreditacije. V tem primeru se uporabita dva vnosa z različnima vrednostma „Sti“ (npr. v zadevnem primeru CA/QC oziroma CA/PKC), z enako vrednostjo „Sdi“ (povezano potrdilo X.509v3).

Izvajanja so odvisna od ASN.1 ali XML in so skladna s specifikacijami ETSI TS 102 231 (za ASN.1 glej Prilogo A k ETSI TS 102 231, za XML pa Prilogo B k ETSI TS 102 231).

Opomba 2: Ko je treba navesti dodatne informacije o „kvalifikaciji“ v zvezi z vnosom identificirane storitve, upravljavec sheme, kadar je to primerno, upošteva uporabo razširitve „additionalServiceInformation“ (klavzula 5.8.2) polja „Service information extension“ (klavzula 5.5.9), v skladu z namenom zagotavljanja takšnih dodatnih informacij o „kvalifikaciji“. Poleg tega lahko upravljavec sheme uporabi klavzulo 5.5.6 („Scheme service definition URI“).

Service current status (klavzula 5.5.4)

To polje se ZAHTEVA in podrobno opredeljuje identifikator statusa storitve s pomočjo enega izmed naslednjih URI:

▼C2

— **Under Supervision (Pod nadzorom)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision),

— **Supervision of Service in Cessation (Nadzor storitve se ukinja)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation),

— **Supervision Ceased (Nadzor ukinjen)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased),

— **Supervision Revoked (Nadzor preklican)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked),

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

— **Accreditation Ceased (Akreditacija ukinjena)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased),

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

▼C1

Zgornji statusi se v okviru teh specifikacij zanesljivega seznama tolmačijo, kot sledi:

— ***Pod nadzorom:*** Storitev, opredeljena v „Service digital identity“ (klavzula 5.5.3), ki jo zagotavlja overitelj (CSP), opredeljen v „TSP name“ (klavzula 5.4.1), je trenutno pod nadzorom, zaradi skladnosti z določbami iz Direktive 1999/93/ES, s strani države članice, opredeljene v „Scheme territory“ (klavzula 5.3.10), v kateri ima CSP sedež.

▼M1

— ***Nadzor storitve se ukinja:*** Storitev, opredeljena v „Service digital identity“ (klavzula 5.5.3), ki jo zagotavlja overitelj (CSP), opredeljen v „TSP name“ (klavzula 5.4.1), je trenutno v fazi ukinjanja, vendar je še vedno nadzorovana, dokler se nadzor ne ukine ali prekliče. Če odgovornost za zagotavljanje te faze ukinjanja prevzame druga pravna oseba, ki ni opredeljena v „TSP name“, se identifikacija te nove ali alternativne pravne osebe (alternativni CSP) navede v „Scheme service definition URI“ (klavzula 5.5.6) in „TakenOverBy“ (klavzula L.3.2) vnosa storitve.

▼C1

— ***Nadzor ukinjen:*** Veljavnost ocene nadzora je potekla, ne da bi bila storitev, opredeljena v „Service digital identity“ (klavzula 5.5.3), ponovno ocenjena. Storitev trenutno ni pod nadzorom od datuma veljavnega statusa, saj se šteje, da se je storitev prenehala izvajati.

— ***Nadzor preklican:*** Storitev CSP in sam CSP sta bila nadzorovana in skladnost z določbami iz Direktive 1999/93/ES ni bila več zagotovljena, kar je ugotovila država članica, opredeljena v „Scheme territory“ (klavzula 5.3.10), v kateri ima CSP sedež. V skladu s tem je bilo zahtevano, da se storitev preneha izvajati, in jo je iz zgornjih razlogov treba obravnavati kot ukinjeno.

Opomba 1: Vrednost statusa „Nadzor preklican“ je lahko dokončen status, tudi če je CSP popolnoma prenehal delovati; v tem primeru ni potrebe po uporabi statusa „Nadzor storitve se ukinja“ ali „Nadzor ukinjen“. Dejansko je edini način, kako spremeniti status „Nadzor preklican“, ta, da CSP začne upoštevati določbe iz Direktive 1999/93/ES v skladu z ustreznim sistemom nadzora, ki velja v državi članici, imetnici TL, in da ponovno pridobi status „Pod nadzorom“. Status „Nadzor storitve se ukinja“ ali „Nadzor ukinjen“ se doseže samo, ko CSP neposredno preneha s povezanimi storitvami pod nadzorom, in ne, ko je bil nadzor preklican.

— ***Akreditiran:*** Oceno akreditacije je izvedel akreditacijski organ v imenu države članice, opredeljene v „Scheme territory“ (klavzula 5.3.10), storitev, opredeljena v „Service digital identity“ (klavzula 5.5.3), ki jo zagotavlja CSP ([1]), opredeljen v „TSP name“ (klavzula 5.4.1), pa je skladna z določbami iz Direktive 1999/93/ES.

([1]) Ta akreditiran CSP ima lahko sedež v drugi državi članici, ki ni opredeljena v „Scheme territory“ pri izvajanju TSL zanesljivega seznama, ali v tretji državi (glej člen 7.1(a) Direktive 1999/93/ES).

▼C1

Opomba 2: V okviru CSP, ki izdaja QC in ima sedež na „Scheme territory“ (klavzula 5.3.10), se MORATA statusa „Akreditacija preklicana“ in „Akreditacija ukinjena“ obravnavati kot „tranzitna statusa“ in se NE SMETA uporabljati kot vrednost za „Service current status“, saj jima MORA v „Service approval history information“ ali v „Service current status“ nemudoma slediti, če se uporabljata, status „Pod nadzorom“, lahko pa sledi tudi drug status nadzora, opredeljen zgoraj in prikazan v sliki 1. Pri uporabi v okviru CSP, ki ne izdaja QC, če obstaja samo povezana prostovoljna shema akreditacije brez povezane sheme nadzora, ali v okviru CSP, ki izdajajo QC, pri čemer CSP nima sedeža na „Scheme territory“ (klavzula 5.3.10) (npr. ima sedež v tretji državi), se statusa „Akreditacija preklicana“ in „Akreditacija ukinjena“ LAHKO uporabita kot vrednost za „Service current status“.

— ***Akreditacija ukinjena:*** Veljavnost ocene akreditacije je potekla, ne da bi bila storitev, opredeljena v „Service digital identity“ (klavzula 5.5.3), ponovno ocenjena.

— ***Akreditacija preklicana:*** Potem ko je bilo predhodno ugotovljeno, da je skladna z merili sheme, storitev, opredeljena v „Service digital identity“ (klavzula 5.5.3), ki jo zagotavlja overitelj (CSP), opredeljen v „TSP name“ (klavzula 5.4.1), in po možnosti tudi sam CSP nista več izpolnjevala določil iz Direktive 1999/93/ES.

Opomba 3: Za CSP, ki izdajajo QC, in za CSP, ki ne izdajajo QC (npr. ponudniki storitev časovnega žigosanja, ki izdajajo TST, CSP, ki izdajajo nekvalificirana potrdila, itd.), je treba uporabiti iste vrednosti statusa. „Service Type identifier“ (klavzula 5.5.1) se uporabi za razlikovanje med veljavnimi sistemi nadzora/akreditacije.

Opomba 4: Na ravni storitve, kadar je to primerno in potrebno (npr. za razlikovanje med več ravnmi kakovosti/varnosti), se LAHKO navedejo dodatne, s statusom povezane informacije o „kvalifikaciji“, opredeljene na ravni nacionalnih sistemov nadzora/akreditacije za CSP, ki ne izdajajo QC. Upravljavci shem uporabijo razširitev „additionalServiceInformation“ (klavzula 5.8.2) polja „Service information extension“ (klavzula 5.5.9), v skladu z namenom zagotavljanja takšnih dodatnih informacij o „kvalifikaciji“. Poleg tega lahko upravljavec sheme uporabi klavzulo 5.5.6 („Scheme service definition URI“).

Current status starting date and time (klavzula 5.5.5)

To polje se ZAHTEVA in podrobno opredeljuje datum in čas, ko je trenutni status odobritve postal veljaven (vrednost datuma in časa, kot je opredeljena v ETSI TS 102 231, klavzula 5.1.4).

Scheme service definition URI (klavzula 5.5.6)

To polje je NEOBVEZNO. Če se uporabi, podrobno opredeljuje URI, kjer lahko odvisne stranke pridobijo za storitev specifične informacije, ki jih zagotovi upravljavec sheme kot zaporedje večjezičnih kazalcev (v angleščini kot obveznem jeziku in po možnosti v enem ali več nacionalnih jezikih).

Če se uporabijo referenčni URI, MORAJO zagotavljati pot do informacij, ki opisujejo storitev, kot je opredeljeno s shemo. To LAHKO, kadar je to primerno, vključuje zlasti:

(a) URI, ki navajajo identiteto alternativnega CSP v primeru nadzora storitve, ki se ukinja, pri katerem je alternativni CSP udeležen (glej „Service current status“ – klavzula 5.5.4);

▼C1

(b) URI, ki vodijo do dokumentov z dodatnimi informacijami v zvezi z uporabo nekaterih nacionalno opredeljenih posebnih kvalifikacij za storitve zagotavljanja nadzorovanih/akreditiranih žetonov varnih storitev v skladu z uporabo polja „Service information extension“ (klavzula 5.5.9) z razširitvijo „additionalServiceInformation“, kot je opredeljeno v klavzuli 5.8.2).

Service supply points (klavzula 5.5.7)

To polje je NEOBVEZNO. Če se uporablja, podrobno opredeljuje URI, kjer lahko odvisne stranke dostopajo do storitve s pomočjo zaporedja nizov črk, katerih sintaksa MORA biti skladna z RFC 3986.

TSP service definition URI (klavzula 5.5.8)

To polje je NEOBVEZNO. Če se uporabi, podrobno opredeljuje URI, kjer lahko odvisne stranke pridobijo za storitev specifične informacije, ki jih zagotovi TSP kot zaporedje večjezičnih kazalcev (v angleščini kot obveznem jeziku in po možnosti v enem ali več nacionalnih jezikih). Referenčni URI MORAJO zagotavljati pot do informacij, ki opisujejo storitev, kot je opredeljena s strani TSP.

Service information extensions (klavzula 5.5.9)

V okviru teh specifikacij je to polje NEOBVEZNO, vendar se uporabi, če informacije, navedene v „Service digital identity“ (klavzula 5.5.3), ne zadostujejo za nedvoumno določitev kvalificiranih potrdil, izdanih s to storitvijo, in/ali če informacije, navedene v povezanih kvalificiranih potrdilih, ne omogočajo strojno obdelane opredelitve dejstev o tem, ali je QC podprt s SSCD ([1]).

Če je njegova uporaba ZAHTEVANA, npr. za storitve CA/QC, se v okviru teh specifikacij uporabi neobvezno polje „Service information extensions“ („Sie“), ki je strukturirano kot zaporedje ene ali več terk, v skladu z razširitvijo „kvalifikacije“, opredeljeno v ETSI TS 102 231, Priloga L.3.1. Vsaka terka zagotavlja:

— (filtre) informacije za nadaljnjo opredelitev, po „Sdi“ opredeljeni storitvi overjanja, tiste storitve (tj. niz kvalificiranih potrdil), za katero se zahtevajo/zagotovijo dodatne informacije v zvezi z navedbo prisotnosti ali odsotnosti podpore SSCD (in/ali izdajo pravni osebi), in

— povezane informacije („kvalifikatorje“) o tem, ali je ta nadalje opredeljeni niz kvalificiranih potrdil podprt s SSCD (če je ta informacija „QCSSCDStatusAsInCert“, to pomeni, da je ta povezana informacija del QC v s strani ETSI standardizirani obliki, ki jo je mogoče strojno obdelati ([2]), in/ali informacije v zvezi z dejstvom, da se takšna QC izdajo pravnim osebam (načeloma se šteje, da se izdajo samo fizičnim osebam).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD) pomeni, da je zagotovljeno s strani CSP in nadzorovano (model nadzora) ali revidirano (model akreditacije) s strani države članice (nadzornega organa oziroma akreditacijskega organa), da so QC, izdani v okviru storitve (QCA), opredeljeni v „Service digital identity“ (klavzula 5.5.3) in nadalje opredeljeni z zgornjimi (filtri) informacijami, ki se uporabljajo za opredelitev, po „Sdi“ opredeljeni storitvi overjanja, tistega niza kvalificiranih potrdil, za katerega se te dodatne informacije zahtevajo v zvezi s prisotnostjo ali odsotnostjo podpore SSCD, **PODPRTI** s SSCD (tj. da je zasebni ključ, povezan z javnim ključem v potrdilu, shranjen v napravi za varno tvorjenje podpisa, v skladu s Prilogo III k Direktivi 1999/93/ES),

([1]) Glej oddelek 2.2 tega dokumenta.

([2]) To se nanaša na ustrezno kombinacijo v ETSI opredeljene izjave QcCompliance, izjave QcSSCD (ETSI TS 101 862) ali QCP/QCP+ v ETSI opredeljene OID (ETSI TS 101 456).

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD) pomeni, da je zagotovljeno s strani CSP in nadzorovano (model nadzora) ali revidirano (model akreditacije) s strani države članice (nadzornega organa oziroma akreditacijskega organa), da QC, izdani po storitvi (korenski CA/QC ali CA/QC), opredeljeni v „Service digital identity“ (klavzula 5.5.3) in nadalje opredeljeni z zgornjimi (filtri) informacijami, ki se uporabljajo za opredelitev, po „Sdi“ opredeljeni storitvi overjanja, tistega niza kvalificiranih potrdil, za katerega se te dodatne informacije zahtevajo v zvezi s prisotnostjo ali odsotnostjo podpore SSCD, **NISO PODPRTI** s SSCD (tj. da zasebni ključ, povezan z javnim ključem v potrdilu, **ni** shranjen v napravi za varno tvorjenje podpisa, v skladu s Prilogo III k Direktivi 1999/93/ES),

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert) pomeni, da je zagotovljeno s strani CSP in nadzorovano (model nadzora) ali revidirano (model akreditacije) s strani države članice (nadzornega organa oziroma akreditacijskega organa), da QC, izdani po storitvi (CA/QC), opredeljeni v „Service digital identity“ (klavzula 5.5.3) in nadalje opredeljeni z zgornjimi (filtri) informacijami, ki se uporabljajo za opredelitev, po „Sdi“ opredeljeni storitvi overjanja, tistega niza kvalificiranih potrdil, za katerega se te dodatne informacije zahtevajo v zvezi s prisotnostjo ali odsotnostjo podpore SSCD, VSEBUJEJO informacije, ki jih je mogoče strojno obdelati in ki navajajo, ali je QC podprt s SSCD,

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson) pomeni, da je zagotovljeno s strani CSP in nadzorovano (model nadzora) ali revidirano (model akreditacije) s strani države članice (nadzornega organa oziroma akreditacijskega organa), da so QC, izdani po storitvi (QCA), opredeljeni v „Service digital identity“ (klavzula 5.5.3) in nadalje opredeljeni z zgornjimi (filtri) informacijami, ki se uporabljajo za opredelitev, po „Sdi“ opredeljeni storitvi overjanja, tistega niza kvalificiranih potrdil, za katerega se te dodatne informacije zahtevajo v zvezi z izdajo pravni osebi, dejansko **IZDANI** pravni osebi.

Ti kvalifikatorji se uporabljajo samo kot razširitev, če je vrsta storitve http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

To polje je specifično za izvajanje (ASN.1 ali XML) in MORA izpolnjevati specifikacije iz Priloge L.3.1 k ETSI TS 102 231.

▼M1

V okviru izvajanja XML mora biti specifična vsebina teh dodatnih informacij kodirana s pomočjo datotek xsd iz Priloge C k ETSI TS 102 231.

▼C1

Service Approval History

To polje je NEOBVEZNO, vendar MORA biti prisotno, če „Historical information period“ (klavzula 5.3.12) ni ničelno. Zato MORA shema v okviru teh specifikacij hraniti pretekle informacije. Če so pretekle informacije namenjene hrambi, storitev pa nima zgodovine pred trenutnim statusom (tj. prvi evidentirani status ali pa upravljavec sheme ni hranil preteklih informacij), to polje ostane prazno. Za vsako spremembo trenutnega statusa storitve TSP, ki se je zgodila v obdobju preteklih informacij, kot je opredeljeno v ETSI TS 102 231, klavzula 5.3.12, se informacije o predhodnem statusu odobritve navedejo padajoče, po datumu in času spremembe statusa (tj. datum in čas, ko začne veljati naslednji status odobritve).

▼C1

To je zaporedje preteklih informacij, kot je opredeljeno v nadaljevanju.

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

Service type identifier (klavzula 5.6.1)

To polje se ZAHTEVA in podrobno opredeljuje identifikator vrste storitve, z obliko in pomenom, ki se uporabljata v „TSP Service Information – Service type identifier“ (klavzula 5.5.1).

Service name (klavzula 5.6.2)

To polje se ZAHTEVA in podrobno opredeljuje ime, pod katerim je CSP zagotavljal storitev, opredeljeno v „TSP Service Information – Service type identifier“ (klavzula 5.5.1), z obliko in pomenom, ki se uporabljata v „TSP Service Information – Service name“ (klavzula 5.5.2). Ta klavzula ne zahteva, da je ime enako imenu, opredeljenemu v klavzuli 5.5.2. Sprememba imena je LAHKO ena izmed okoliščin, ki zahtevajo nov status.

▼M1

Service digital identity (klavzula 5.6.3)

To polje se ZAHTEVA in podrobno opredeljuje najmanj eno navedbo digitalnega identifikatorja (npr. potrdilo X.509v3), uporabljenega v „TSP Service Information – Service digital identity“ (klavzula 5.5.3), z enako obliko in pomenom, kot je opredeljeno v ETSI TS 102 231, klavzula 5.5.3.

Opomba: Za vrednost potrdila X.509v3, ki se je uporabila za storitev v „Sdi“ klavzuli 5.5.3, je lahko na zanesljivem seznamu samo en vnos storitve za posamezno vrednost „Sti:Sie/additionalServiceInformation“. Informacije o „Sdi“ (klavzula 5.6.3), uporabljene v podatkih o zgodovini statusa odobritve storitve, povezanih z vnosom storitve, in informacije o „Sdi“ (klavzula 5.5.3), uporabljene pri tem vnosu storitve, se MORAJO nanašati na isto vrednost potrdila X.509v3. Kadar se za navedeno storitev spremeni „Sdi“ (tj. zaradi obnovitve ali ponovne izdaje potrdila X.509v3 za npr. CA/PKC ali CA/QC) ali za tako storitev ustvari nov „Sdi“ (četudi z identičnimi vrednostmi za ustrezne „Sti“, „Sn“ in [„„Sie“]), upravljavec sheme MORA ustvariti drug vnos storitve, ki ni enak prejšnjemu.

▼C1

Service previous status (klavzula 5.6.4)

To polje se ZAHTEVA in podrobno opredeljuje identifikator predhodnega statusa storitve, z obliko in pomenom, ki se uporabljata v „TSP Service Information – Service current status“ (klavzula 5.5.4).

Previous status starting date and time (klavzula 5.6.5)

To polje se ZAHTEVA in podrobno opredeljuje datum in čas, ko je zadevni predhodni status začel veljati, z obliko in pomenom, ki se uporabljata v „TSP Service Information – Service current status starting date and time“ (klavzula 5.5.5).

Service information extensions (klavzula 5.6.6)

To polje je NEOBVEZNO in ga LAHKO uporablja upravljavec sheme za navedbo posebnih s storitvijo povezanih informacij, z obliko in pomenom, ki se uporabljata v „TSP Service Information – Service information extensions“ (klavzula 5.5.9).

▼C1

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

Isto za TSP(1) Service(1) History(2) (pred History 1)

…

TSP(1) Service(2)

Isto za TSP(1) Service 2 (kakor se uporablja)

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

…

TSP(2) Information

Isto za TSP 2 (kakor se uporablja)

Isto za TSP 2 Service 1

Isto za TSP 2 Service 1 History 1

…

▼M1

Signed TSL

Berljiva oblika izvajanja TSL zanesljivega seznama, pripravljena po teh specifikacijah in zlasti Poglavju IV, se podpiše s „Scheme operator name“ (klavzula 5.3.4), da se zagotovita njena avtentičnost in celovitost ([1]). Oblika podpisa je PAdES, del 3 (ETSI TS 102 778-3 ([2])), v okviru specifičnega zanesljivega modela, določenega z objavo potrdil, uporabljenih za podpis zanesljivih seznamov, pa je oblika podpisa lahko tudi PadES, del 2 (ETSI TS 102 778-2 ([3])).

Za strojno obdelavo primerna oblika izvajanja TSL zanesljivega seznama, pripravljena po teh specifikacijah, se podpiše s „Scheme operator name“ (klavzula 5.3.4), da se zagotovita njena avtentičnost in celovitost. Za strojno obdelavo primerna oblika izvajanja TSL zanesljivega seznama, pripravljena po teh specifikacijah, ima obliko XML in je skladna s specifikacijami iz prilog B in C k ETSI TS 102 231.

Oblika podpisa je XAdES BES ali EPES, kot je opredeljeno v specifikacijah ETSI TS 101 903 za izvajanja XML. Tako izvajanje elektronskega podpisa izpolnjuje zahteve iz Priloge B k ETSI TS 102 231 ([4]). Dodatne splošne zahteve v zvezi s tem podpisom so navedene v nadaljevanju.

▼C1

Scheme identification (klavzula 5.7.2)

To polje se ZAHTEVA in podrobno opredeljuje referenco, ki jo dodeli upravljavec sheme, ki enolično opredeli shemo, opisano v teh specifikacijah in vzpostavljenem TSL, in ki MORA biti vključena v izračun podpisa. Pričakuje se, da gre za niz znakov ali bitni niz.

([1]) Kadar berljiva oblika izvajanja TSL zanesljivega seznama ni podpisana, je TREBA njeno avtentičnost in celovitost zagotoviti s primernim komunikacijskim kanalom z enakovredno ravnjo varnosti. Za ta namen se priporoča uporaba TLS (IETF RFC 5246: „Varni protokol TLS (Transport Layer Security), različica 1.2“), država članica pa MORA uporabnikom TSL prstni odtis na potrdilu za kanal TLS zagotoviti prek drugega pasu.

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

([4]) Potrdilo o podpisu upravljavca sheme je treba obvezno zaščititi, in sicer s podpisom, izdelanim na enega izmed načinov, opredeljenih v ETSI TS 101 903, ds:keyInfo pa mora po potrebi vsebovati ustrezno verigo potrdila.

▼M1

Dodeljena referenca v okviru teh specifikacij vsebuje „TSL type“ (klavzula 5.3.3), „Scheme name“ (klavzula 5.3.6) in vrednost razširitve potrdila „identifikator imetnikovega ključa“ („SubjectKeyIdentifier“), ki ga upravljavec sheme uporabi za elektronsko podpisovanje TSL.

▼C1

Signature algorithm identifier (klavzula 5.7.3)

To polje se ZAHTEVA in podrobno opredeljuje kriptografski algoritem, ki je bil uporabljen pri ustvarjanju podpisa. Glede na uporabljen algoritem LAHKO to polje zahteva dodatne parametre. To polje MORA biti vključeno v izračun podpisa.

Signature value (klavzula 5.7.4)

To polje se ZAHTEVA in vsebuje dejansko vrednost digitalnega podpisa. Vsa polja TSL (razen same vrednosti podpisa) MORAJO biti vključena v izračun podpisa.

TSL extensions (klavzula 5.8)

Razširitev **expiredCertsRevocationInfo** (klavzula 5.8.1)

Ta razširitev je NEOBVEZNA. Če se uporabi, MORA biti skladna s specifikacijami ETSI TS 102 231, klavzula 5.8.1.

Razširitev **additionalServiceInformation** (klavzula 5.8.2)

Ta NEOBVEZNA razširitev se MORA, če se uporablja, uporabiti samo na ravni storitve in samo v polju, opredeljenem v klavzuli 5.5.9 („Service information extension“). Z njo zagotovimo dodatne informacije o storitvi. Je zaporedje ene ali več terk, pri čemer vsaka terka navaja:

(a) URI, ki opredeljuje dodatne informacije, npr.

— URI, ki navaja nekatere nacionalno opredeljene posebne kvalifikacije za storitev zagotavljanja nadzorovanih/akreditiranih žetonov varnih storitev, npr.

— posebno raven razdrobljenosti varnosti/kakovosti v zvezi z nacionalno shemo nadzora/akreditacije za CSP, ki ne izdajajo QC (npr. RGS */**/*** v FR, poseben status „nadzora“, določen z nacionalno zakonodajo za posebne CSP, ki izdajajo QC, v DE), glej opombo 4 „Service current status“ – klavzula 5.5.4,

— ali posebni pravni status za zagotavljanje nadzorovanih/akreditiranih žetonov varnih storitev (npr. nacionalno opredeljeni „kvalificirani TST“ kot v DE ali HU),

— ali pomen posebnega identifikatorja politike, prisotnega v potrdilu X.509v3 iz polja „Sdi“,

— ali registriran URI, kot je opredeljen v „Service type identifier“, klavzula 5.5.1, za dodatno opredelitev udeležbe s „Sti“ opredeljene storitve kot sestavnega dela storitve overitelja, ki izdaja QC (npr. OCSP-QC, CRL-QC, in korenski CA-QC);

(b) neobvezni niz, ki vsebuje vrednost informacije o storitvi, s pomenom, opredeljenim v shemi (npr. *, ** ali ***);

(c) vse neobvezne dodatne informacije, zagotovljene v obliki, specifični za shemo.

▼**M1**

Dereferenciranje URI vodi do berljivih informacij (najmanj v angleščini, po možnosti pa v še enem ali več nacionalnih jezikih), ki se štejejo za primerne in zadostne za to, da lahko stranka razširitev razume, in ki zlasti obrazložijo pomen navedenih URI ter opredelijo možne vrednosti za serviceInformation in pomen za vsako vrednost.

Qualifications Extension (klavzula L.3.1)

Opis: To polje je NEOBVEZNO, vendar se uporabi, če se njegova uporaba ZAHTEVA, npr. za storitve korenskega CA/QC ali CA/QC, in če:

— informacije, navedene v „Service digital identity“, ne zadostujejo za nedvoumno opredelitev kvalificiranih potrdil, izdanih s to storitvijo,

— informacij, navedenih v povezanih kvalificiranih potrdilih, ni mogoče strojno obdelati za identifikacijo dejstev o tem, ali so QC podprti s SSCD.

Če se ta razširitev ravni storitve uporabi, MORA biti uporabljena samo v polju, opredeljenem v „Service information extension“ (klavzula 5.5.9) in je skladna s specifikacijami iz Priloge L.3.1 k ETSI TS 102 231.

TakenOverBy Extension (klavzula L.3.2)

Opis: Ta razširitev je NEOBVEZNA, vendar je prisotna, kadar storitev, za katero je prej bil pravno odgovoren overitelj, prevzame drug ponudnik TSP, njen namen pa je uradno dodeliti pravno odgovornost za določeno storitev in programski opremi za preverjanje omogočiti, da uporabniku zagotovi določene pravne informacije. Informacije, zagotovljene s to razširitvijo, so skladne z uporabo klavzule 5.5.6, na katero se nanašajo, in ustrezajo specifikacijam iz Priloge L.3.2 k ETSI TS 102 231.

▼M1

POGLAVJE II

Pri pripravljanju zanesljivih seznamov bodo države članice uporabile:

oznake jezikov z malimi črkami in oznake držav z veliki črkami;

oznake jezikov in držav, kot so navedene v tabeli spodaj;

Kadar se uporablja latinica (z ustrezno oznako jezika), se doda v latinico prečrkovani zapis z ustrezno oznako jezika iz spodnje tabele.

Kratko ime (v izvirnem jeziku)	Kratko ime (v angleščini)	Oznaka države	Oznaka jezika	Opombe	Prerkovanje v latinico
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	Oznaka države, ki jo je priporočila EU	el-Latn
España	Spain	ES	es	tudi katalonšina (ca), baskovšina (eu), galicijšina (gl)	
France	France	FR	fr		
▼M2 Hrvatska	Croatia	HR	hr		
▼M1 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**

Kratko ime (v izvirnem jeziku)	Kratko ime (v angleščini)	Oznaka države	Oznaka jezika	Opombe	Prerkovanje v latinico
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Oznaka države, ki jo je priporočila EU	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Prečrkovanje v latinico: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

_____

▼C1

POGLAVJE IV

SPECIFIKACIJE ZA BERLJIVO OBLIKO IZVAJANJA TSL ZANESLJIVEGA SEZNAMA

Berljiva oblika izvajanja TSL zanesljivega seznama MORA biti javno dostopna in dostopna po elektronski poti. Na voljo mora biti v obliki dokumenta Portable Document Format (PDF), v skladu z ISO 32000, dokument PDF pa MORA biti oblikovan v skladu s profilom PDF/A (ISO 19005).

Vsebina berljive oblike izvajanja TSL zanesljivega seznama na podlagi PDF/A MORA biti skladna z naslednjimi zahtevami:

▼M1

— Naslov berljive oblike zanesljivih seznamov se sestavi kot povezava iz naslednjih elementov:

  — neobvezna slika zastave države članice;

  — prazen prostor;

  — kratko ime države v izvirnih jezikih (kot so navedena v prvem stolpcu tabele v Poglavju II);

  — prazen prostor;

  — „(“;

  — kratko ime države v angleščini (kot so navedena v drugem stolpcu tabele v Poglavju II) v oklepajih;

  — „):“ kot zaklepaj in znak za presledek;

  — prazen prostor;

  — „Trusted List“;

  — neobvezen logo upravitelja sheme države članice.

▼C1

— Struktura berljive oblike MORA odražati logični model, opisan v oddelku 5.1.2 ETSI TS 102 231.

— Vsako polje MORA biti prikazano in navajati:

  — naziv polja (npr. „Service type identifier“),

  — vrednost polja (npr. „CA/QC“),

  — pomen (opis) vrednosti polja, kadar je to primerno in zlasti, kot je navedeno v Prilogi D k ETSI TS 102 231 ali v teh specifikacijah za registrirane URI (npr. „overitelj potrdil, ki izdaja potrdila javnega ključa“),

  — več različic v naravnih jezikih, kot je opredeljeno v izvajanju TSL zanesljivega seznama, kadar je to primerno.

— Naslednja polja in ustrezne vrednosti digitalnih potrdil, navedene v polju „digitalna identiteta storitve“, MORAJO biti prikazani v berljivi obliki:

  — Različica

  — Serijska številka

  — Algoritem za podpis

  — Izdajatelj

  — Velja od

  — Velja do

  — Imetnik

▼C1

— Javni ključ

— Politika, pod katero je bilo izdano potrdilo

— Identifikator imetnikovega ključa

— Distribucijske točke registra preklicanih potrdil

— Identifikator izdajateljevega ključa

— Uporaba ključa

— Osnovne omejitve

— Algoritem za razpoznavni odtis

— Razpoznavni odtis

— Berljiva oblika MORA biti enostavna za tiskanje.

— Berljivo obliko je MOGOČE podpisati elektronsko. Ko je podpisana, jo MORA podpisati upravljavec sheme v skladu z enakimi specifikacijami za podpis, kot veljajo za izvajanje TSL zanesljivega seznama.