32009D0767

L 274/36 SLUŽBENI LIST EUROPSKE UNIJE 20.10.2009.

ODLUKA KOMISIJE

od 16. listopada 2009.

o utvrđivanju mjera kojima se olakšava uporaba postupaka elektroničkim putem preko „jedinstvenih kontaktnih točaka" u skladu s Direktivom 2006/123/EZ Europskog parlamenta i Vijeća o uslugama na unutarnjem tržištu

(priopćena pod brojem dokumenta C(2009) 7806)

(Tekst značajan za EGP)

(2009/767/EZ)

KOMISIJA EUROPSKIH ZAJEDNICA,

uzimajući u obzir Ugovor o osnivanju Europske zajednice,

uzimajući u obzir Direktivu 2006/123/EZ Europskog parlamenta i Vijeća o uslugama na unutarnjem tržištu [1], a posebno njezin članak 8. stavak 3.,

budući da:

(1) Obveze administrativnog pojednostavnjenja koje državama članicama propisuje poglavlje II. Direktive 2006/123/EZ, posebno članci 5. i 8. tog poglavlja, uključuje obvezu pojednostavnjenja postupaka i formalnosti koje se primjenjuju na pristup uslužnoj djelatnosti i obavljanje te djelatnosti te obvezu osiguravanja da te postupke i formalnosti mogu jednostavno obavljati pružatelji usluga na daljinu, elektroničkim putem preko „jedinstvenih kontaktnih točaka".

(2) Obavljanje postupaka i formalnosti preko „jedinstvenih kontaktnih točaka" mora biti moguće preko granica između država članica, kako je utvrđeno u članku 8. Direktive 2006/123/EZ.

(3) Za ispunjavanje obveze pojednostavnjenja postupaka i formalnosti i za olakšavanje prekogranične uporabe „jedinstvenih kontaktnih točaka", postupci elektroničkim putem moraju se temeljiti na jednostavnim rješenjima, uključujući uporabu elektroničkih potpisa. U slučajevima ako se, nakon odgovarajuće procjene rizika konkretnih postupaka i formalnosti, smatra da je potrebna visoka razina sigurnosti ili jednakovrijednost s vlastoručnim potpisom, za određene postupke i formalnosti mogu se od pružatelja usluga zahtijevati napredni elektronički potpisi koji se temelje na kvalificiranom certifikatu sa sredstvom za izradu zaštićenog potpisa ili bez tog sredstva.

(4) Okvir Zajednice za e-potpise uspostavljen je u Direktivi 1999/93/EZ Europskog parlamenta i Vijeća od 13. prosinca 1999. o okviru Zajednice za elektroničke potpise [2]. Da bi se olakšala učinkovita prekogranična uporaba naprednih elektroničkih potpisa koji se temelje na kvalificiranom certifikatu, trebalo bi povećati povjerenje u te elektroničke potpise, bez obzira na državu članicu u kojoj potpisnik ili pružatelj usluge certificiranja koji izdaje kvalificirani certifikat ima poslovni nastan. To se može postići tako da informacije, potrebne za potvrđivanje elektroničkih potpisa, budu lakše dostupne u vjerodostojnom obliku, posebno informacije u vezi s pružateljima usluge certificiranja koji se nadziru ili su ovlašteni u državi članici i uslugama koje nude.

(5) Potrebno je osigurati da države članice omoguće javnu dostupnost tih informacija preko zajedničkog obrasca, kako bi se olakšala njihova uporaba i osigurala odgovarajuća razina pojedinosti, koja primatelju omogućuje potvrđivanje elektroničkog potpisa,

DONIJELA JE OVU ODLUKU:

Članak 1.

Uporaba i prihvaćanje elektroničkih potpisa

1. Ako je to opravdano na temelju odgovarajuće procjene uključenog rizika i u skladu s člankom 5. stavcima 1. i 3. Direktive 2006/123/EZ, države članice mogu zahtijevati da pružatelj usluga, za obavljanje određenih postupaka i formalnosti preko jedinstvenih kontaktnih točaka, u skladu s člankom 8. Direktive 2006/123/EZ, koristi napredne elektroničke potpise koji se temelje na kvalificiranom certifikatu, sa sredstvom za izradu zaštićenog potpisa ili bez tog sredstva, kako je određeno i uređeno Direktivom 1999/93/EZ.

2. Države članice prihvaćaju svaki napredni elektronički potpis koji se temelji na kvalificiranom certifikatu, sa sredstvom za izradu zaštićenog potpisa ili bez tog sredstva, za obavljanje postupaka i formalnosti iz stavka 1., ne dovodeći u pitanje mogućnost da države članice ograniče to prihvaćanje na napredne elektroničke potpise, koji se temelje na kvalificiranom certifikatu i izrađeni su pomoću sredstva za izradu zaštićenog potpisa, ako je to u skladu s procjenom rizika iz stavka 1.

[1] SL L 376, 27.12.2006., str. 36.

[2] SL L 13, 19.1.2000., str. 12.

3. Države članice ne uvjetuju prihvaćanje naprednih elektroničkih potpisa, koji se temelje na kvalificiranom certifikatu, sa sredstvom za izradu zaštićenog potpisa ili bez tog sredstva, zahtjevima koji sprečavaju pružatelje usluga da upotrebljavaju postupke elektroničkim putem preko jedinstvenih kontaktnih točaka.

4. Stavak 2. ne sprečava države članice da prihvaćaju elektroničke potpise različite od naprednih elektroničkih potpisa, koji se temelje na kvalificiranom certifikatu, sa sredstvom za izradu zaštićenog potpisa ili bez tog sredstva.

Članak 2.

Uspostava, održavanje i objava pouzdanih popisa

1. Svaka država članica uspostavlja, održava i objavljuje, u skladu s tehničkim specifikacijama iz Priloga, „pouzdani popis" koji sadrži minimalne informacije u vezi s pružateljima usluga certificiranja koji izdaju kvalificirane certifikate javnosti, koje ona nadzire i ovlašćuje.

2. Države članice uspostavljaju i objavljuju najmanje pouzdani popis u čitljivom obliku, u skladu sa specifikacijama iz Priloga.

3. Države članice izvješćuju Komisiju o tijelu odgovornom za uspostavu, održavanje i objavu pouzdanog popisa, o mjestu gdje je pouzdani popis objavljen te o svim njegovim izmjenama.

Članak 3.

Primjena

Ova se Odluka primjenjuje od 28. prosinca 2009.

Članak 4.

Adresati

Ova je Odluka upućena državama članicama.

Sastavljeno u Bruxellesu 16. listopada 2009.

Za Komisiju
Charlie McCREEVY
Član Komisije

PRILOG

TEHNIČKE SPECIFIKACIJE ZA ZAJEDNIČKI OBRAZAC ZA „POUZDANI POPIS NADZIRANIH/OVLAŠTENIH PRUŽATELJA USLUGA CERTIFICIRANJA”

PREDGOVOR

1. **Općenito**

Namjena zajedničkog obrasca za „Pouzdani popis nadziranih/ovlaštenih pružatelja usluga certificiranja” država članica je utvrditi zajednički način na koji svaka država članica pruža informacije o statusu nadzora/akreditacije usluga certificiranja od strane pružatelja usluga certificiranja ([1]) (CSP-a) koje one nadziru/akreditiraju radi usklađenosti s odgovarajućim odredbama Direktive 1999/93/EZ. To uključuje pružanje povijesnih informacija o statusu nadzora/akreditacije nadziranih/akreditiranih usluga certificiranja.

Obvezne informacije na pouzdanom popisu (TL-u) moraju uključivati najnužnije informacije o nadziranim/akreditiranim CSP-ima koji izdaju kvalificirane certifikate (QC-e) ([2]) u skladu s odredbama utvrđenima u Direktivi 1999/93/EZ (članak 3. stavak 3., članak 3. stavak 2. i članak 7. stavak 1. točka (a)), uključujući informacije o QC-ima koji podupiru elektronički potpis i je li potpis izrađen sredstvom za izradu zaštićenog potpisa (SSCD-om) ili bez tog sredstva ([3]).

Dodatne informacije o ostalim nadziranim/akreditiranim CSP-ima koji ne izdaju QC-e, već pružaju usluge vezane uz elektroničke potpise (na primjer CSP-i koji pružaju usluge izdavanja vremenskog žiga i izdaju žetone vremenskog žiga, CSP-ima koji izdaju nekvalificirane certifikate itd.) mogu biti uključene na pouzdani popis na državnoj razini na dobrovoljnoj osnovi.

Te su informacije usmjerene prvenstveno na podupiranje potvrđivanja kvalificiranih elektroničkih potpisa (QES-a) i naprednih elektroničkih potpisa (AdES-a) ([4]) koji se temelje na kvalificiranom certifikatu ([5]) ([6]).

Predloženi zajednički obrazac u skladu je s provedbom koja se temelji na specifikacijama iz ETSI TS-a 102 231 ([7]) koje se upotrebljavaju za naslovljavanje objekta, objave, lokacije, pristupa, autentikacije i povjerenja u takve vrste popisa.

2. **Smjernice za uređivanje unosa na TL-u**

2.1. *TL-i usredotočeni na nadzirane/akreditirane usluge certificiranja*

Odgovarajuće usluge certificiranja i pružatelji usluga certificiranja na jednom popisu

Pouzdani popis država članica definiran je kao „popis statusa nadzora/akreditacije usluga certificiranja od strane pružatelja usluga certificiranja koje nadzire/akreditira referentna država članica za usklađenost s odgovarajućim odredbama Direktive 1999/93/EZ”.

Takav pouzdani popis mora obuhvaćati:

— **sve pružatelje usluga certificiranja**, kako su utvrđeni u članku 2. stavku 11. Direktive 1999/93/EZ, to jest „subjekt ili pravna ili fizička osoba koja izdaje certifikate ili pruža ostale usluge vezane uz elektroničke potpise”;

— **koji su nadzirani/akreditirani** radi usklađenosti s odgovarajućim odredbama utvrđenim u Direktivi 1999/93/EZ.

Pri razmatranju definicija i odredaba utvrđenih u Direktivi 1999/93/EZ, posebno u vezi s odgovarajućim CSP-ima i njihovim sustavima nadzora/dobrovoljne akreditacije, mogu se razlikovati dvije skupine CSP-a, odnosno CSP-i koji izdaju QC-e javnosti (CSP_{QC}), i CSP-i koji ne izdaju QC-e javnosti, već pružaju „ostale (pomoćne) usluge vezane uz elektroničke potpise”:

([1]) Kako je određeno u članku 2. stavku 11. Direktive 1999/93/EZ.
([2]) Kako je određeno u članku 2. stavku 10. Direktive 1999/93/EZ.
([3]) Kako je određeno u članku 2. stavku 6. Direktive 1999/93/EZ.
([4]) Kako je određeno u članku 2. stavku 2. Direktive 1999/93/EZ.
([5]) Za napredni elektronički potpis koji se temelji na kvalificiranom certifikatu upotrebljava se kratica „$AdES_{QC}$” u cijelom dokumentu.
([6]) Postoji niz elektroničkih usluga koje se temelje na jednostavnom AdES-u čija bi prekogranična uporaba također bila olakšana, pod uvjetom da su potporne usluge certificiranje (na primjer izdavanje nekvalificiranih certifikata) dio nadziranih/akreditiranih usluga koje država članica uključuje u dobrovoljni dio informacija u pouzdanom popisu.
([7]) ETSI TS 102 231 - Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust—service status information.

— **CSP-i koji izdaju QC-e:**

— Mora ih nadzirati država članica u kojoj imaju sjedište ili prebivalište (ako imaju sjedište ili prebivalište u državi članici) te također mogu biti akreditirani za usklađenost s odredbama utvrđenima u Direktivi 1999/93/EZ, uključujući sa zahtjevima Priloga I. (zahtjevi za QC-e), i zahtjevima Priloga II. (zahtjevi za CSP-e koji izdaju QC-e). CSP-i koji izdaju QC-e koji su akreditirani u državi članici moraju još uvijek potpadati pod odgovarajući sustav nadzora navedene države članice, osim ako nemaju sjedište ili prebivalište u navedenoj državi članici.

— Primjenljivi sustav „nadzora" (odnosno sustav „dobrovoljne akreditacije") definiran je i mora ispunjavati odgovarajuće zahtjeve Direktive 1999/93/EZ, posebno one iz članka 3. stavka 3., članka 8. stavka 1., članka 11., uvodne izjave 13. (odnosno, članka 2. stavka 13. članka 3. stavka 2., članka 7. stavka 1. točke (a), članka 8. stavka 1., članka 11., uvodnih izjava 4.-(11.-13.)).

— **CSP-i koji ne izdaju QC-e:**

— Oni mogu potpadati pod sustav „dobrovoljne akreditacije" (kako je određen u i u skladu s Direktivom 1999/93/EZ) i/ili pod nacionalno definiranu „priznatu shemu odobrenja" provedenu na nacionalnoj razini za nadzor usklađenosti s odredbama utvrđenima u Direktivi i po mogućnosti s nacionalnim odredbama u vezi s pružanjem usluga certificiranja (u smislu članka 2. stavka 11. Direktive).

— Neki od fizičkih ili binarnih (logičkih) objekata ostvarenih ili izdanih kao posljedica pružanja usluge certificiranja mogu imati pravo na posebnu „kvalifikaciju" na temelju svoje usklađenosti s odredbama i zahtjevima utvrđenim na nacionalnoj razini, ali značenje takve „kvalifikacije" moglo bi biti ograničeno isključivo na nacionalnu razinu.

Pouzdani popis države članice mora pružati najnužnije informacije o nadziranim/akreditiranim CSP-ima koji izdaju kvalificirane certifikate javnosti u skladu s odredbama utvrđenima u Direktivi 1999/93/EZ (članak 3. stavak 3., članak 3. stavak 2. i članak 7. stavak 1. točka (a)), informacije o QC-ima koji podupiru elektronički potpis te je li potpis stvoren sa sredstvom za izradu zaštićenog potpisa ili bez tog sredstva.

Dodatne informacije o ostalim nadziranim/akreditiranim uslugama od strane CSP-a koji ne izdaju QC-e javnosti (na primjer CSP-i koji pružaju usluge izdavanja vremenskog žiga i izdaju žetone vremenskog žiga, CSP-i koji izdaju nekvalificirane certifikate itd.) mogu se uvrstiti na pouzdani popis na nacionalnoj razini na dobrovoljnoj osnovi.

Pouzdani popis ima za cilj:

— uvrstiti na popis i pružiti pouzdane informacije o statusu nadzora/akreditacije usluga certificiranja od strane pružatelja usluga certificiranja, koje nadzire/akreditira država članica odgovorna za pripremu i ažuriranje popisa radi usklađenosti s odgovarajućim odredbama utvrđenima u Direktivi 1999/93/EZ;

— olakšati potvrđivanje elektroničkih potpisa koji se temelje na navedenim nadziranim/akreditiranim uslugama certificiranja od strane navedenih CSP-a.

Jedinstveni skup vrijednosti statusa nadzora/akreditacije

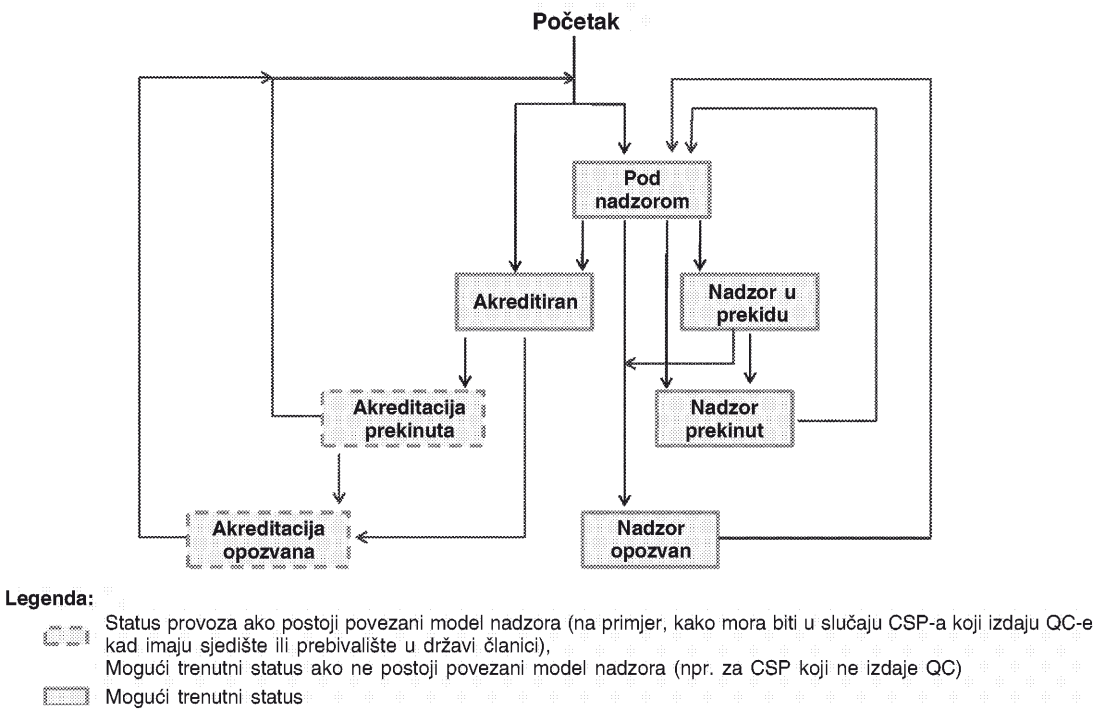
Svaka država članica mora pripremiti i ažurirati jedan jedinstveni TL koji navodi status nadzora i/ili akreditacije onih usluga certificiranja od strane onih CSP-a koje nadzire/akreditira država članica.

Činjenica da se usluga trenutačno ili nadzire ili akreditira dio je njezinog trenutačnog statusa. Pored toga, status nadzora ili akreditacije može biti „u tijeku", „u prekidu", „prekinut", ili čak „opozvan". Kroz njezin vijek trajanja ista usluga certificiranja može prijeći sa statusa nadzora u status akreditacije i obrnuto ([1]).

Sljedeća slika 1. opisuje očekivani tijek, samo za jednu uslugu certificiranja, između mogućih statusa nadzora/akreditacije:

([1]) Na primjer, pružatelj usluga certificiranja sa sjedištem ili prebivalištem u državi članici koja pruža uslugu certificiranja i kojeg na početku nadzire država članica (nadzorno tijelo), može se, nakon određenog vremena, odlučiti za dobrovoljnu akreditaciju trenutačno nadzirane usluge certificiranja. Suprotno, pružatelj usluga certificiranja u drugoj državi članici može odlučiti da ne prekine obavljati akreditiranu uslugu certificiranja, već da status akreditacije zamijeni statusom nadzora, na primjer iz poslovnih i/ili gospodarskih razloga.

Očekivani tijek statusa nadzora/akreditacije samo za jednu uslugu CSP-a



Slika 1.

Pružatelj usluge certificiranja koji izdaje QC-e mora biti nadziran (ako ima sjedište ili prebivalište u državi članici) i može biti dobrovoljno akreditiran. Vrijednost statusa takve usluge, kad se nalazi na pouzdanom popisu, može imati bilo koju od gore prikazanih vrijednosti statusa kao „trenutnu vrijednost statusa". Međutim, treba napomenuti da „akreditacija prekinuta" i „akreditacija opozvana" moraju obje biti vrijednosti „statusa provoza" samo u slučaju usluga CSP_{QC} sa sjedištem ili prebivalištem u državi članici jer se takve usluge moraju nadzirati prema zadanoj vrijednosti (čak i ako nisu ili više nisu akreditirane).

Zahtijeva se da države članice koje su uspostavile ili uspostavljaju nacionalno definiranu „priznatu shemu odobrenja" provedenu na nacionalnoj razini za nadzor usklađenosti usluga od strane CSP-a koji ne izdaju QC-e s odredbama utvrđenima u Direktivi 1999/93/EZ te s mogućim nacionalnim odredbama u vezi s pružanjem usluga certificiranja (u smislu članka 2. stavka 11. Direktive) razvrstaju takve sheme odobravanja u sljedeće dvije kategorije:

— „dobrovoljna akreditacija" kako je definirana i uređena u Direktivi 1999/93/EZ (članak 2. stavak 13., članak 3. stavak 2., članak 7. stavak 1. točka (a), članak 8. stavak 1., članak 11., uvodne izjave 4.-(11.-13.));

— „nadzor" kako se zahtijeva u Direktivi 1999/93/EZ i provodi nacionalnim odredbama i zahtjevima u skladu s nacionalnim zakonima.

U skladu s tim, pružatelj usluge certificiranja koji izdaje QC-e može se nadzirati ili dobrovoljno akreditirati. Vrijednost statusa takve usluge kada se nalazi na pouzdanom popisu može imati bilo koju od gore prikazanih vrijednosti statusa kao svoju „trenutačnu vrijednost statusa" (vidjeti sliku 1.).

Pouzdani popis mora sadržavati informacije o osnovnoj shemi (shemama) nadzora/akreditacije, posebno:

— Informacije o sustavu nadzora koji se primjenjuje na svaki CSP_{QC};

— Informacije, kad je primjenljivo, o nacionalnoj shemi „dobrovoljne akreditacije" za svaki CSP_{QC};

— Informacije, kad je primjenljivo, o sustavu nadzora koji se primjenjuje na svaki CSP koji ne izdaje QC-e;

— Informacije, kad je primjenljivo, o nacionalnoj shemi „dobrovoljne akreditacije" koja se primjenjuje na svaki CSP koji ne izdaje QC-e.

Zadnja dva niza informacija od ključne su važnosti za to da stranke ocijene razinu kakvoće i sigurnosti takvih sustava nadzora/akreditacije koji se na nacionalnoj razini primjenjuju na CSP-e koji ne izdaju QC-e. Ako je u TL-u pružena informacija o statusu nadzora/akreditacije u vezi s uslugama od strane CSP-a koji ne izdaju QC-e, gore navedeni nizovi informacija na razini TL-a pružaju se pomoću „Scheme information URI" (klauzula 5.3.7 – informacije pružaju države članice), „Scheme type/community/rules" (klauzula 5.3.9 – uporabom teksta zajedničkog svim državama članicama i

neobveznih posebnih informacija koje pruža država članica) i „TSL policy/legal notice" (klauzula 5.3.11 – tekst zajednički svim državama članicama upućivanjem na Direktivu 1999/93/EZ, zajedno s mogućnošću za svaku državu članicu da doda tekst/upućivanja specifična za državu članicu). Dodatne informacije o „kvalifikaciji" određene na razini nacionalnih sustava nadzora/akreditacije za CSP-e koji ne izdaju QC-e mogu se pružiti na razini usluge kad je primjenljivo i kada se zahtijeva (na primjer za razlikovanje između nekoliko razina kakvoće/sigurnosti) uporabom proširenja „additionalServiceInformation" (klauzula 5.8.2) kao dijela „Service information extension" (klauzula 5.5.9). Dodatne informacije o odgovarajućim tehničkim specifikacijama navedene su u detaljnim specifikacijama u poglavlju I.

Unatoč činjenici da različita tijela država članica mogu biti nadležna za nadzor i akreditaciju usluga certificiranja u navedenoj državi članici, očekuje se da se upotrebljava samo jedan unos za jednu uslugu certificiranja (utvrđenu njezinom „Service digital identity" prema ETSI TS-u 102 231 [1]) i da se status nadzora/akreditacije ažurira u skladu s tim. Značenje gore prikazanih statusa opisano je u povezanoj klauzuli 5.5.4 detaljnih tehničkih specifikacija u poglavlju I.

2.2. *Unosi u TL čiji je cilj olakšavanje potvrđivanja QES-a i $AdES_{QC}$-a*

Najvažniji dio stvaranja TL-a je uspostava obveznog dijela TL-a, odnosno „popisa usluga" po CSP-u koji izdaje QC-e, kako bi se pravilno odrazilo točno stanje izdavanja svakog takvog pružatelja usluge certificiranja koji izdaje QC te kako bi se osiguralo da su informacije pružene u svakom takvom unosu dostatne da olakšaju potvrđivanje QES-a i $AdES_{QC}$-a (kada su kombinirane sa sadržajem QC-a krajnjeg subjekta koji izdaje CSP sukladno usluzi certificiranja navedenoj u tom unosu).

Ako nema zaista interoperabilnog i prekograničnog profila za QC, zahtijevane informacije mogle bi uključivati druge informacije koje nisu informacije „Service digital identity" pojedinačnog (Root) CA-a, posebno informacije koje utvrđuju status QC-a izdanog certifikata te jesu li podržani potpisi stvoreni sa SSCD-om ili bez njega. Tijelo u državi članici koje je imenovano za uspostavu, uređivanje i održavanje TL-a (to jest, rukovatelj sheme po ETSI TS-u 102 231) mora stoga uzeti u obzir trenutni profil i sadržaj certifikata u svakom izdanom QC-u, po CSP_{QC}-ima obuhvaćenima TL-om.

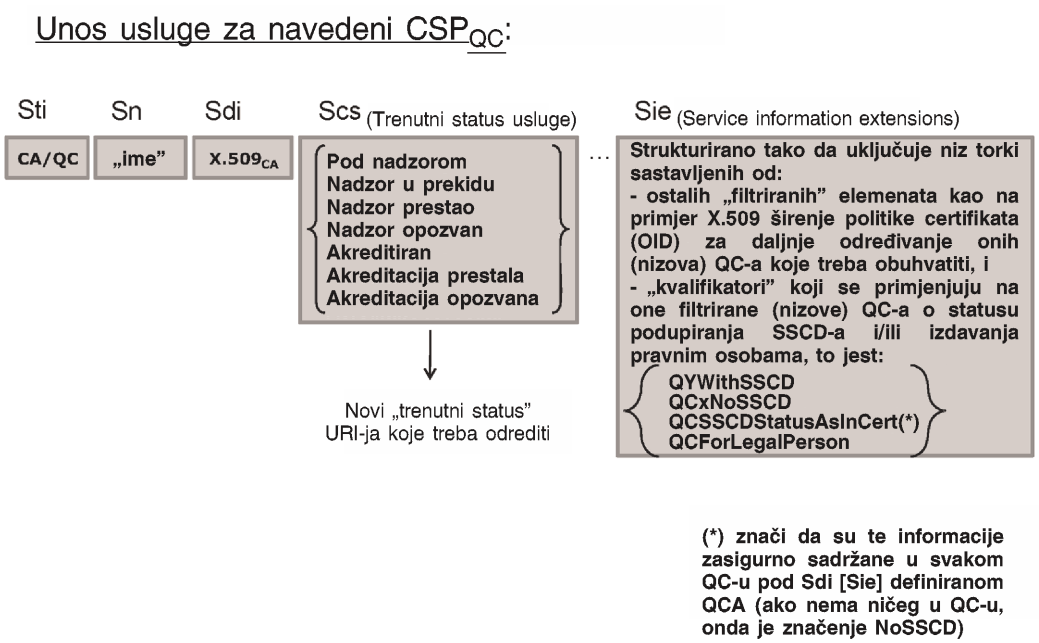
Idealno bi bilo kad bi svaki izdani QC uključivao izjavu QcCompliance [2] određenu od strane ETSI-ja ako se tvrdi da je to QC i ako bi uključivao izjavu QcSSCD određenu od strane ETSI-ja ako se tvrdi da je SSCD podupire za stvaranje e-potpisa, i/ili da svaki izdani QC uključuje jedan od identifikatora objekta (OID-a) politike certifikata QCP/QCP + određen u ETSI TS-u 101 456 [3]. Uporaba od strane CSP-a koji izdaju QC-e različitih standarda kao referenci, široki stupanj tumačenja navedenih standarda, kao i nedostatak svijesti o postajanju i prednosti nekih normativnih tehničkih specifikacija ili standarda dovela je do razlika u stvarnom sadržaju trenutačno izdanih QC-a (na primjer, uporaba il neuporaba izjava QC određenih od strane ETSI-ja) i zbog toga sprečavaju stranke primateljice da se jednostavno oslone na certifikat potpisnika (i povezani lanac/put) da bi ocijenile, barem u strojno čitljivom obliku, tvrdi li se da je certifikat koji podupire e-potpis QC ili ne, te je li povezan sa SSCD-om putem kojeg je e-potpis stvoren.

Ispunjavanje polja „Service type identifer" (Sti), „Service name" (Sn), i „Service digital identity" (Sdi) [4] s informacijama navedenim u polju „Service information extensions" (Sie) omogućuje predloženom zajedničkom obrascu TL-a da u cijelosti odredi posebnu vrstu kvalificiranog certifikata koji je izdao na popisu naveden pružatelj usluga certificiranja koji izdaje QC-e te da pruži informacije o činjenici da ga SSCD podupire ili ne (ako takvih informacija nema u izdanom QC-u). S tim je unosom naravno povezan poseban podatak o „Service current status" (Scs). To je prikazano u donjoj slici 2.

Navođenje usluge samo navodom „Sdi" (Root) CA značilo bi da je osigurano (od strane CSP-a koji izdaje QC-e, ali također i od strane nadzornog/akreditacijskog tijela zaduženog za nadzor/akreditaciju ovog CSP-a) da svaki certifikat krajnjeg subjekta izdan prema tom (Root) CA-u (hijerarhija) sadrži dovoljno informacija određenih od strane ETSI-ja, koje je moguće strojno obraditi, da se ocijeni je li to QC ili nije, te podupire li ih SSCD ili ne. U slučaju, na primjer, da potonja tvrdnja nije točna (na primjer, QC ne sadrži standardizirane navode od strane ETSI-ja, koje je moguće strojno obraditi, o tome podupire li ih SSCD), potom navođenjem samo „Sdi" tog (Root) CA-a, može se samo pretpostaviti da QC-e izdane sukladno toj (Root) CA hijerarhiji ne podupire ni jedan SSCD. Da bi se ti QC-i smatrali podržanim od strane SSCD-a, za navođenje te činjenice treba upotrijebiti „Sie" (to također znači da to jamči CSP koji izdaje QC-e i koji nadzire/akreditira nadzorno, odnosno akreditacijsko tijelo).

[1] ETSI TS 102 231 - Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information
[2] Vidjeti ETSI TS 101 862 - Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.
[3] ETSI TS 101 456 — Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
[4] To jest, najmanje certifikat X.509 v3 izdavatelja QCA-a ili višega CA u putu ovjeravanja.

Opća načela — Pravila uređivanja — CSP_{QC} unosi (navedene usluge)



Slika 2.

Unos usluge za navedeni CSP koji izdaje QC-e u TL-u provedenom u obliku TSL-a

Sadašnje tehničke specifikacije za zajednički obrazac TL omogućuju uporabu kombinacije pet glavnih dijelova informacija u unosu usluge:

— „Service type identifier" (Sti), na primjer utvrđuje CA koji izdaje QC-e (CA/QC),

— „Service name" (Sn),

— podatak „Service digital identity" (Sdi) utvrđuje navedenu uslugu, na primjer certifikat X.509v3 (najmanje) za CA koji izdaje QC-e,

— za usluge CA/QC, neobvezne informacije „Service information extensions" (Sie) koje omogućuju uključivanje niza jedne ili više torki, pri čemu svaka torka nudi:

  — mjerila koja se koriste za dodatno utvrđivanje (filtar) sukladno „Sdi" utvrđenoj usluzi certificiranja točno te usluge (to jest, niz kvalificiranih certifikata) za koju se zahtijevaju/su pružene dodatne informacije u vezi s navodom potpore SSCD-a (i/ili izdavanje pravnoj osobi); i

  — povezane informacije (kvalifikatori) o tome podupire li SSCD ovaj nadalje utvrđeni niz usluga kvalificiranih certifikata ili ne, ili jesu li povezane informacije dio QC-a po standardiziranom obliku koji je moguće strojno obraditi, i/ili informacije u vezi s činjenicom da su takvi QC-i izdani pravnim osobama (u načelu se smatra da se izdaju samo fizičkim osobama);

— informacije o „trenutnom statusu" za ovaj unos usluge koje pružaju informacije:

  — o tome je li to nadzirana ili akreditirana usluga, i

  — o samom statusu nadzora/akreditacije.

2.3. *Smjernice za uređivanje i uporabu unosa usluga CSP_{QC}*

Opće smjernice za uređivanje su:

1. Ako je osigurano (jamstvo koje pruža CSP_{QC} i nadzire/akreditira nadzorno tijelo (SB)/akreditacijsko tijelo (AB)) da, za navedenu uslugu utvrđenu putem „Sdi-ja", svaki QC koji podupire SSCD sadrži od strane ETSI-ja određenu izjavu QcCompliance i izjavu QcSSCD i/ili identifikator objekta (OID) QCP +, onda je uporaba odgovarajućeg „Sdi-ja" dostatna i polje „Sie" može se upotrijebiti kao opcija i ne mora sadržavati informacije o potpori SSCD-u.

2. Ako je osigurano (jamstvo koje pruža CSP_{QC} i nadzire/akreditira SB/AB) da, za navedenu uslugu utvrđenu putem „Sdi-ja”, svaki QC koji ne podupire SSCD sadrži ili izjavu QcCompliance i/ili QCP OID, i takva je da se smatra da ne sadrži izjave QcSSCD ili QCP + OID, onda je uporaba odgovarajućeg „Sdi-ja” dostatna i polje „Sie” može se upotrijebiti kao opcija i ne mora sadržavati informacije o potpori SSCD-u (što znači da ga SSCD ne podupire).

3. Ako je osigurano (jamstvo koje pruža CSP_{QC} i nadzire/akreditira SB/AB) da, za navedenu uslugu utvrđenu putem „Sdi-ja”, svaki QC sadrži izjavu QcCompliance, i neke od navedenih QC-a trebaju podupirati SSCD-i, a neke ne (na primjer, to se može razlikovati prema različitim OID politikama certifikata, specifičnim za CSP ili pomoću drugih informacija specifičnih za CSP u QC-u, izravno ili neizravno, strojno obradivi ili ne), ali ne sadrži NI izjavu QcSSCD NITI ETSI QCP(+) OID, onda uporaba odgovarajućeg „Sdi-ja” može biti nedostatna I polje Sie mora se upotrijebiti da označava izričite informacije o potpori SSCD-u, zajedno s mogućim proširenjem informacija da se utvrdi obuhvaćeni niz certifikata. To bi moglo zahtijevati uključivanje različitih „vrijednosti informacija o potpori SSCD-u” za isti „Sdi” pri uporabi polja „Sie”.

4. Ako je osigurano (jamstvo koje pruža CSP_{QC} i nadzire/akreditira SB/AB) da, za navedenu uslugu utvrđenu putem „Sdi-ja”, svaki QC sadrži izjavu QcCompliance, QCP OID, izjavu QcSSCD ili QCP + OID, ali je osigurano da se neki od navedenih certifikata krajnjih subjekata izdanih sukladno ovom „Sdi-ju” smatraju QC-ima i/ili podržanim od strane SSCD-a, a neki ne (na primjer, to se može razlikovati prema različitim OID politikama certifikata, specifičnim za CSPQC ili pomoću drugih informacija specifičnih za CSPQC u QC-u, izravno ili neizravno, strojno obradivi ili ne), onda uporaba odgovarajućeg Sdi-ja neće biti dostatna I polje Sie se mora upotrijebiti da označava izričite informacije o potpori SSCD-u. To bi moglo zahtijevati uključivanje različitih „vrijednosti informacija o potpori SSCD-u” za isti „Sdi” pri uporabi polja „Sie”.

Kao opće zadano načelo, za navedeni CSP na pouzdanom popisu mora biti jedan unos usluge za jedan certifikat X.509v3 za vrstu usluge certificiranja, to jest, certifikacijsko tijelo koje (izravno) izdaje QC-e. U nekim pomno predviđenim okolnostima i pomno kontroliranim uvjetima, nadzorno tijelo/akreditacijsko tijelo države članice može se odlučiti za uporabu certifikata X.509v3 Root ili Upper Level CA (to jest, certifikacijsko tijelo koje ne izdaje QC-e izravno krajnjem subjektu, već potvrđuje hijerarhiju CA-a sve do CA-a koji izdaju QC-e krajnjim subjektima) kao Sdi jednog unosa na popis usluga navedenog CSP-a. Posljedice (prednosti i nedostaci) uporabe takvog CA-a X.509v3 Root ili Upper Level CA-a kao vrijednosti unosa usluga na TL-u moraju biti pomno razmotrene i potvrđene od strane država članica. Nadalje, prilikom uporabe odobrene iznimke od zadanog načela, država članica mora osigurati potrebnu dokumentaciju za olakšavanje uspostave i potvrde puta certificiranja.

Kako bi se ilustrirale opće smjernice uređivanja, može se dati sljedeći primjer: U kontekstu CSP_{QC}-a koji koristi jedan Root CA prema kojem nekoliko CA-a izdaje kvalificirane ili nekvalificirane certifikate, ali za koji QC-i sadrže samo izjavu QcCompliance i ne navode jesu li podržani od strane SSCD-a ili ne, navođenje Root CA-a „Sdi” samo bi značilo, prema gore objašnjenim pravilima, da svaki QC izdan sukladno toj Root hijerarhiji CA NIJE podržan od strane SSCD-a. Ako SSCD stvarno podržava navedene QC-e, izričito se preporučuje da se koristi izjava QcSSCD u QC-ima koji će se izdati u budućnosti. U međuvremenu (dok ne istekne valjanost zadnjeg QC-a koji ne sadrži ove informacije), TSL bi trebao koristiti polje Sie i povezano proširenje kvalifikacija, na primjer filtriranje certifikata pomoću posebnih OID-a koje određuje CSP_{QC} koje može potencijalno koristiti CSP_{QC} za razlikovanje različitih vrsta QC-a (neke podupire SSCD, a neke ne) i uključujući izričite „informacije o potpori SSCD-a” u vezi s onim filtriranim certifikatima kroz uporabu „kvalifikatora”.

Opće smjernice za uporabu za aplikacije, usluge ili proizvode za elektroničko potpisivanje, koji se oslanjaju na provedbu TSL pouzdanog popisa sukladno sadašnjim tehničkim specifikacijama, su kako slijedi:

Unos „CA/QC”„Sti” (slično tome unos CA/QC koji je nadalje kvalificiran kao Root CA/QC kroz uporabu „Sie” proširenja additionalServiceInformation)

— označava da su od strane „Sdi-ja” utvrđenog CA-a (slično tome u hijerarhiji CA počevši od Root CA koji utvrđuje „Sdi”), svi izdani certifikati krajnjim subjektima QC-i **pod uvjetom** da j ekao takav naveden u certifikatu uporabom odgovarajućih QcStatement (to jest, QcC, QcSSCD) i/ili QCP(+) OID-a koje određuje ETSI (a to osigurava nadzorno/akreditacijsko tijelo, vidjeti gornje „opće smjernice za uređivanje”).

Napomena: ako nisu prisutne „Sie" „kvalifikacijske informacije" ili ako certifikat krajnjeg subjekta za koji se tvrdi da je QC nije „nadalje utvrđen" povezanim unosom „Sie", onda su „strojno obradive" informacije koje se mogu naći u QC-u nadzirane/akreditirane da budu točne. To znači da je uporaba (ili neuporaba) odgovarajuće QcStatement (to jest, QcC, QcSSCD) i/ili QCP(+) OID-i koje određuje ETSI osigurana u skladu s podacima koje navodi CSP_{QC}.

— **i AKO** je prisutna informacija „Sie"„kvalifikacija", onda se pored gornjeg pravila tumačenja zadane uporabe uzimaju u obzir oni certifikati koji su utvrđeni kroz uporabu tog unosa „Sie"„kvalifikacija", koji je sastavljen po načelu niza „filtara" koji nadalje utvrđuju skup certifikata i pružaju neke dodatne informacije o „potpori SSCD-a" i/ili „pravnoj osobi kao subjektu" (na primjer oni certifikati koji sadrže poseban OID u proširenju politike certifikata, i/ili imaju poseban uzorak „uporabe ključa", i/ili su filtrirani kroz uporabu posebne vrijednosti koja se pojavljuje u određenom polju ili proširenju certifikata itd.), i to u skladu sa sljedećim nizom „kvalifikatora", koji nadoknađuju nedostatak informacija u odgovarajućem QC-u, to jest,:

— navod potpore SSCD-a:

— vrijednost kvalifikatora „QCWithSSCD" znači „QC koji podupire SSCD", ili

— vrijednost kvalifikatora „QCNoSSCD" znači „QC koji ne podupire SSCD", ili

— vrijednost kvalifikatora „QCSSCDStatusAsInCert" znači da su informacije o potpori SSCD-a zasigurno sadržane u QC-u pod pruženim informacijama „Sdi" - „Sie" u tom unosu CA/QC;

I/ILI

— navod izdavanja pravnoj osobi:

— vrijednost kvalifikatora „QCForLegalPerson" znači „certifikat izdan pravnoj osobi".

2.4. *Usluge koje podupiru „CA/QC", ali nisu dio „CA/QC"„Sdi"*

Također treba obuhvatiti slučajeve u kojima su odazivi CRL-a OCSP-a potpisani ključevima različitim od ključeva CA-a koji izdaju QC-e („CA/QC"). To se može obuhvatiti popisom navedenih usluga kao takvih u provedbi TSL-a pouzdanog popisa (to jest, sa „Service type identifier" koji je nadalje kvalificiran proširenjem „additionalServiceInformation"koje odražava OCSP ili uslugu CRL kao dio pružanja QC-a, na primjer s vrstom usluge „OCSP/QC" ili „CRL/QC") jer se navedene usluge mogu smatrati dijelom nadziranih/akreditiranih „kvalificiranih" usluga povezanih s pružanjem usluga certificiranja QC-a. Naravno, poslužitelje OCSP-a ili izdavatelje CRL-a čije certifikate potpisuju CA-i po hijerarhiji navedene usluge CA/QC treba smatrati „valjanima" i u skladu s vrijednošću statusa navedene usluge CA/QC.

Slična se odredba može primjenjivati na usluge certificiranja koje izdaju nekvalificirane certifikate (vrsta usluge „CA/PKC") uporabom zadanih vrsta usluga ETSI TS 102 231 OCSP i CRL.

Treba primijetiti da provedba TSL-a pouzdanog popisa MORA uključivati usluge opoziva kada se povezane informacije ne nalaze u polju AIA konačnih certifikata ili kada ih nije potpisao CA koji je jedan od navedenih CA-a.

2.5. *Kretanje prema interoperabilnom profilu QC-a*

U pravilu, mora se pokušati pojasniti (smanjiti) što je više moguće broj unosa usluga (različiti „Sdi-ji"). To se međutim mora ujednačiti pravilnom identifikacijom onih usluga koje su povezane s izdavanjem QC-a i pružanjem pouzdanih informacija o tome podržava li SSCD navedene QC-e ili ne ako tih informacija nema u izdanom QC-u.

Idealno bi bila da uporaba polja „Sie" i proširenja „kvalifikacija" bude (strogo) ograničena na one posebne slučajeve koje treba riješiti na taj način jer bi QC-i trebali sadržavati dovoljno informacija u vezi s navedenim kvalificiranim statusom i navedenom potporom ili nepotporom SSCD-a.

Države članice bi trebale, što je više moguće, provesti usvajanje i uporabu interoperabilnih profila QC-a.

3. **Struktura zajedničkog obrasca za pouzdani popis**

Predloženi zajednički obrazac za pouzdani popis država članica bit će strukturiran u sljedeće kategorije informacija:

1. Informacije o pouzdanom popisu i shema njegovog izdavanja;

2. Niz polja s nedvosmislenim identifikacijskim informacijama o svakom nadziranom/akreditiranom CSP-u pod shemom (taj niz nije obvezan, to jest, ako se ne upotrebljava, popis će se smatrati praznim, što znači da ni jedan CSP nije nadziran ili akreditiran u povezanoj državi članici u kontekstu područja primjene pouzdanog popisa);

3. Za svaki navedeni CSP, niz polja s nedvosmislenim identifikacijskim informacijama o nadziranoj/akreditiranoj usluzi certificiranja koju pruža CSP (taj niz mora imati najmanje jedan unos);

4. Za svaku navedenu nadziranu/akreditiranu uslugu certificiranja, identifikaciju trenutačnog statusa usluge i povijest tog statusa.

U kontekstu CSP-a koji izdaje QC-e, nedvosmislena identifikacija nadzirane/akreditirane usluge certificiranja koja se navodi na popisu mora uzeti u obzir one situacije u kojima u kvalificiranom certifikatu nema dovoljno raspoloživih informacija o njegovom „kvalificiranom" statusu, njegovoj potencijalnoj potpori od strane SSCD-a, a posebno kako bi se nosio s dodatnom činjenicom da većina (komercijalnih) CSP-a upotrebljava samo jedan kvalificirani CA za izdavanje nekoliko vrsta certifikata konačnim subjektima, kvalificiranih i nekvalificiranih.

Broj unosa na popisu po priznatom CSP-i mogao bi se smanjiti ako postoji jedna ili nekoliko usluga viših CA-a, na primjer u kontekstu komercijalne hijerarhije CA-a od Root CA-a pa sve do CA- izdavatelja. Međutim, čak i u tim slučajevima mora se održati i osigurati načelo osiguranja nedvosmislene veze između usluga certificiranja CSP_{QC} i niza certifikata namijenjenih utvrđivanju kao QC-i.

1. *Informacije o pouzdanom popisu i shemi njegovog izdavanja*

Sljedeće informacije su dio kategorije:

— oznaka pouzdanog popisa koja olakšava utvrđivanje pouzdanog popisa za vrijeme elektroničkih pretraga te također da potvrdi svoje namjene kad je u jasno čitljivom obliku,

— format i identifikator inačice pouzdanog popisa,

— redni broj pouzdanog popisa (ili broj izdavanja),

— **informacije o vrsti** pouzdanog popisa (na primjer, za utvrđivanje činjenice da ovaj pouzdani popis pruža informacije o status nadzora/akreditacije usluga certificiranja od strane CSP-a koje nadzire/akreditira referentna država članica za usklađenost s odredbama utvrđenima u Direktivi 1999/93/EZ),

— informacije o vlasniku pouzdanog popisa (na primjer, ime, adresa, kontaktne informacije itd. tijela države članice zaduženog za uspostavu, sigurnosnu objavu i održavanje pouzdani popis),

— informacije o osnovnoj shemi (shemama) nadzora/akreditacije s kojom (kojima) je pouzdani popis povezan, uključujući, ali ne ograničavajući se na:

  — zemlju u kojoj se primjenjuje,

  — informacije o ili upućivanje na lokaciju na kojoj se mogu naći informacije o shemi (shemama) (model sheme, pravila, mjerila, primjenljiva zajednica, vrsta itd.),

  — razdoblje zadržavanja (povijesnih) informacija,

— obavijest o politici i/ili pravna obavijest, obveze, odgovornosti pouzdanog popisa,

— datum i vrijeme izdavanja i sljedeće predviđeno ažuriranje pouzdanog popisa.

2. *Nedvosmislene identifikacijske informacije o svakom CSP-u priznatom od strane sheme*

Ovaj niz informacija uključuje barem sljedeće:

— ime organizacije CSP-a kako se upotrebljava u formalnim pravnim registrima (to može uključivati UID organizacije CSP-a prema praksama država članica),

— adresu i kontaktne informacije CSP-a,

— dodatne informacije o CSP-u, uključene izravno ili upućivanjem na lokaciju s koje se takve informacije mogu preuzeti.

3. *Za svaki navedeni CSP, niz polja s nedvosmislenom identifikacijom usluge certificiranja koju pruža CSP i nadzirana/akreditirana je u kontekstu Direktive 1999/93/EZ*

Taj skup informacija za svaku uslugu certificiranja navedenog CSP-a uključuje najmanje sljedeće:

— identifikator vrste usluge certificiranja (na primjer, identifikator koji označava da je nadzirana/akreditirana usluga certificiranja od strane CSP-a certifikacijsko tijelo koje izdaje QC-e),

— (trgovački) naziv ove usluge certificiranja,

— nedvosmisleni jedinstveni identifikator usluge certificiranja,

— dodatne informacije o usluzi certificiranja (na primjer, uključene izravno ili uključene upućivanjem na lokaciju s koje se takve informacije mogu preuzeti, informacije o pristupu u vezi s uslugom),

— za usluge CA/QC-a, neobvezan niz torki informacija, pri čemu svaka torka pruža,

i. mjerila, u okviru prema „Sdi-ju" utvrđene usluge certificiranja, za daljnje utvrđivanje (filter) usluge (to jest, niz kvalificiranih certifikata) za koje se zahtijevaju/pružaju dodatne informacije u vezi s navodom potpore SSCD-a (i/ili izdavanje pravnoj osobi); i

ii. povezane „kvalifikatore" koji pružaju informacije o tome podržava li SSCD niz kvalificiranih certifikata iz te nadalje utvrđene usluge ili ne podržava, i/ili informacije o tome jesu li takvi QC-i izdani pravnoj osobi (u načelu se smatra da se izdaju samo fizičkim osobama).

4. *Za svaku navedenu uslugu certificiranja, identifikaciju trenutačnog statusa usluge i povijest tog statusa*

Ovaj niz informacija uključuje najmanje sljedeće:

— identifikator trenutačnog statusa,

— datum i vrijem početka trenutačnog statusa,

— povijesne informacije o ovom statusu.

4. **Definicije i kratice**

Za potrebe ovog dokumenta primjenjuju se sljedeće definicije i akronimi:

Izraz	Akronim	Definicija
Pružatelj usluga certificiranja	CSP	Kako je određeno u članku 2. stavku 11. Direktive 1999/93/EZ
Certifikacijsko tijelo	CA	CA je CSP i može upotrebljavati nekoliko privatnih tehničkih ključeva za potpisivanje, od kojih svaki ima povezani certifikat, radi izdavanja certifikat krajnjim subjektima. CA je tijelo kojemu jedan ili više korisnika povjeruje stvaranje i dodjeljivanje certifikata. Po izboru, certifikacijsko tijelo može stvoriti ključeve korisnika [ETSI TS 102 042]. Smatra se da je CA utvrđen informacijama o identifikaciji koje su navedene u polju Izdavatelj certifikata CA vezane uz (certificiranje) javnog ključa povezanog s privatnim ključem CA-a za potpisivanje i koji CA stvarno koristi za izdavanje certifikata subjektima. CA može imati nekoliko ključeva za potpisivanje. Svaki ključ CA-a za potpisivanje is jedinstveno je utvrđen jedinstvenim identifikatorom kao dijelom polja Authority Key Identifier u certifikatu CA-a.
Certifikacijsko tijelo koje izdaje kvalificirane certifikate	CA/QC	CA koji ispunjava zahtjeve utvrđene u Prilogu II. Direktivi 1999/93/EZ i izdaje kvalificirane certifikate koji ispunjavaju zahtjeve utvrđene u Prilogu I. Direktivi 1999/93/EZ.
Certifikat	Certifikat	Kako je određeno u članku 2.9 Direktive 1999/93/EZ
Kvalificirani certifikat	QC	Kako je određeno u članku 2. stavku 10. Direktive 1999/93/EZ
Potpisnik	Potpisnik	Kako je određeno u članku 2. stavku 3. Direktive 1999/93/EZ

Izraz	Akronim	Definicija
Nadzor	Nadzor	Nadzor se upotrebljava u smislu Direktive 1999/93/EZ (članak 3. stavak 3.). Direktiva zahtijeva od država članica da uspostavi odgovarajući sustav koji omogućuje nadzor CSP-a koji imaju sjedište ili prebivalište njihovom državnom području i izdaju kvalificirane certifikate javnosti, osiguravajući nadzor usklađenosti s odredbama iz Direktive.
Dobrovoljna akreditacija	Akreditacija	Kako je određeno u članku 2. stavku 13. Direktive 1999/93/EZ
Pouzdani popis	TL	Označava popis koji navodi status nadzora/akreditacije usluge certificiranja od strane pružatelja usluga certificiranja koje nadzire/akreditira referentna država članica za usklađenost s odredbama utvrđenima u Direktivi 1999/93/EZ.
Popis statusa pouzdanih usluga	TSL	Oblik potpisanog popisa koji se upotrebljava kao podloga za predstavljanje informacija o statusu pouzdane usluge prema specifikacijama iz ETSI TS 102 231.
Pouzdana usluga		Usluga koja povećava pouzdanje i vjeru u elektroničke transakcije (obično, ali ne nužno koristeći kriptografske tehnike ili uključujući povjerljivo gradivo) (ETSI TS 102 231).
Pružatelj pouzdane usluge	TSP	Tijelo koje upravlja s jednom ili više (elektroničkih) pouzdanih usluga (taj se izraz koristi sa širom primjenom kao CSP).
Žeton pouzdanih usluga	TrST	Fizički ili binarni (logički) objekt stvoren ili izdan kao rezultat uporabe pouzdane usluge. Primjeri binarnih TrST-a su certifikati, CRL-i, žetoni vremenskog žiga i odzivi OCSP-a.
Kvalificirani elektronički potpis	QES	AdES koji podupire QC i koji je stvoren sa SSCD-om kako je određeno u članku 2. Direktive 1999/93/EZ.
Napredni elektronički potpis	AdES	Kako je određeno u članku 2. stavku 2. Direktive 1999/93/EZ.
Napredni elektronički potpis koji podupire kvalificirani certifikat	AdESQC	Znači elektronički potpis koji ispunjava zahtjeve AdES-a i koji podupire QC kako je određeno u članku 2. Direktive 1999/93/EZ.
Sredstvo za izradu zaštićenog potpisa	SSCD	Kako je određeno u članku 2. stavku 6. Direktive 1999/93/EZ.

POGLAVLJE I.

DETALJNE SPECIFIKACIJE ZA ZAJEDNIČKI OBRAZAC ZA „POUZDANI POPIS NADZIRANIH/OVLAŠTENIH PRUŽATELJA USLUGE CERTIFICIRANJA”

U sljedećem dijelu dokumenta ključne riječi „MORA”, „NE SMIJE”, „ZAHTIJEVA”, „TREBA”, „NE TREBA”, „PREPORUČUJE SE”, „MOŽE”, i „NEOBVEZNO” tumače se kako je opisano u RFC-u 2119 ([1]).

Ove specifikacije temelje se na specifikacijama i zahtjevima navedenim u ETSI TS-u 102 231 v3.1.1 (2009-06). Ako u ovim specifikacijama nije naveden ni jedan poseban zahtjev, zahtjevi iz ETSI TS-a 102 231 primjenjuju se u cijelosti. Ako su u ovim specifikacijama navedeni posebni zahtjevi, oni prevladavaju nad odgovarajućim zahtjevima iz ETSI TS-a 102 231 dok se nadopunjuju specifikacijama za format utvrđenim u ETSI TS-u 102 231. U slučaju odstupanja između ovih specifikacija i specifikacija iz ETSI TS-a 102 231, ove specifikacije su normative.

Jezična potpora provodi se i pruža barem na engleskom (EN), a po mogućnosti dodatno na jednom ili više nacionalnih jezika.

Navod datuma i vremena sukladan je klauzuli 5.1.4 ETSI TS-a 102 231.

Uporaba URI-ja sukladna je klauzuli 5.1.5 ETSI TS-a 102 231.

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

Informacije o shemi izdavanja pouzdanog popisa

Tag

TSL tag (klauzula 5.2.1)

Ovo se polje ZAHTIJEVA i sukladno je klauzuli 5.2.1 ETSI TS-a 102 231.

U kontekstu provedbe XML-a, ETSI je stavio na raspolaganje xsd datoteku koja je pružena u trenutnom stanju u Prilogu 1.

Scheme Information

TSL version identifier (klauzula 5.3.1)

Ovo se polje ZAHTIJEVA i postavljeno je na „3” (cijeli broj).

TSL sequence number (klauzula 5.3.2)

Ovo se polje ZAHTIJEVA. Ono točno navodi redni broj TSL-a. Počinje se od „1” pri prvom izdavanju TSL-a, vrijednost tog cijelog broja povećava se za 1 pri svakom sljedećem izdavanju TSL-a. Ne vraća se na „1” kad se gornji „TSL version identifier” povećava.

TSL type (klauzula 5.3.3)

Ovo se polje ZAHTIJEVA i točno navodi vrstu TSL-a. Postavlja se na http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLtype/generic (Generično).

Napomena: Za sukladnost s klauzulom 5.3.3 ETSI TS-a 102 231 i za navođenje posebne vrste TSL-a pri upućivanju na postojanje ovih specifikacija koje uređuju uspostavu provedbe TSL-a pouzdanog popisa država članica ([1]) te omogućavanje parseru da odredi koji se oblik svakog od sljedećih polja ([2]) može očekivati, gdje ta polja imaju posebna (ili alternativna) značenja s obzirom na vrstu predstavljenog TSL-a (u ovom slučaju to je pouzdani popis države članice), gore navedeni URI registrira se i opisuje kako slijedi:

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

Opis: Provedba TSL-a popisa statusa nadzora/akreditacije usluga certificiranja od strane pružatelja usluga certificiranja koje nadzire/akreditira referentna država članica vlasnica provedba TSL-a za usklađenost s odgovarajućim odredbama utvrđenim u Direktivi 1999/93/EZ, putem postupka izravnog nadzora (bilo dobrovoljnog ili regulatornog).

Scheme operator name (klauzula 5.3.4)

Ovo se polje ZAHTIJEVA. Ono točno navodi naziv tijela države članice zaduženog za uspostavu, objavu i održavanje nacionalnog pouzdanog popisa. Točno navodi službeni naziv pod kojim djeluje povezani pravni subjekt ili opunomoćeni subjekt (na primjer za vladine administrativne agencije) povezna s ovim tijelom. To MORA biti naziv koji se upotrebljava u službenoj pravnoj registraciji ili autorizaciji i na koji trebaju biti naslovljene sve službene obavijesti. Polje je slijed višejezičnih nizova slova i provodi se na engleskom (EN) kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika.

Napomena: Država MOŽE imati odvojena nadzorna i akreditacijska tijela te čak i dodatna tijela za bilo koje operativne povezane djelatnosti. Na svakoj je državi članici da imenuje upravitelja sheme provedbe TSL-a pouzdanog popisa države članice. Očekuje se da nadzorno tijelo, akreditacijsko tijelo i upravitelje sheme (kad su to odvojena tijela) imaju svaki svoju odgovornost i obvezu.

([1]) To jest, „popis statusa nadzora/akreditacije usluga certificiranja pružatelja usluga certificiranja, koje nadzire/akreditira referentna država članica radi usklađenosti s odgovarajućim odredbama utvrđenim u Direktivi 1999/93/EZ” (ukratko „pouzdani popis”).

([2]) Označava polja točno navedena u ETSI TS-u 102 231 - Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information i koja su „profilirana” ovim specifikacijama za određivanje uspostave pouzdanog popisa države članice.

Svaka situacija u kojoj je nekoliko tijela odgovorno za nadzor, akreditaciju ili operativne aspekte dosljedno se odražava i identificira u informacijama o shemi kao dijelu TL-a, uključujući informacije specifične za shemu, naveden u „Scheme information URI" (klauzula 5.3.7).

Od imenovanog upravitelja sheme (klauzula 5.3.4) se očekuje da potpiše TSL.

Scheme operator address (klauzula 5.3.5)

Ovo se polje ZAHTIJEVA. Ono točno navodi adresu pravnog subjekta ili ovlaštene organizacije utvrđene u polju „Scheme operator name" (klauzula 5.3.4) i za poštanske i za elektroničke komunikacije. Uključuje i „PostalAddress" (to jest, ulicu, mjesto, (država ili provincija), (poštanski broj) i oznaku zemlje ISO 3166-1 alpha-2) sukladno klauzuli 5.3.5.1; te „ElectronicAddress" (to jest, e-pošta i/ili internetska stranica URI) sukladno klauzuli 5.3.5.2.

Scheme name (klauzula 5.3.6)

Ovo se polje ZAHTIJEVA i točno navodi naziv pod kojim shema djeluje. Naziv je slijed višejezičnih nizova slova (na engleskom kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika) i određeno je kako slijedi:

— Engleska inačica je niz slova strukturiranih kako slijedi:

CC:EN_naziv_vrijednost

gdje je:

— „CC" = oznaka zemlje ISO 3166-1 alpha-2 koja se upotrebljava u polju „Scheme territory" (klauzula 5.3.10);

— ":" = upotrebljava se kao separator;

— „EN_name_value" = „Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Scheme Operator Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC".

— Inačica na nacionalnom jeziku države članice je niz slova strukturiran kako slijedi:

CC:name_value

gdje je:

— „CC" = oznaka zemlje ISO 3166-1 alpha-2 koja se upotrebljava u polju „Scheme territory" (klauzula 5.3.10);

— ":" = upotrebljava se kao separator;

— „name_value" = Službeni prijevod gornje EN_name_value na nacionalni jezik: „Popis statusa nadzora/akreditacije usluga certificiranja od strane pružatelja usluga certificiranja, koje referentna država članica upravitelja sheme nadzire/akreditira radi usklađenosti s odgovarajućim odredbama utvrđenim u Direktivi 1999/93/EZ".

Naziv sheme mora nedvojbeno po imenu utvrđivati shemu navedenu u polju Scheme information URI, te također osigurati da se, ako upravitelj sheme upravlja s više od jednom shemom, svakoj od njih da različit naziv.

Države članice i upravitelji sheme osiguravaju da se, ako država članica ili upravitelj sheme upravlja sa više od jednom shemom, svakoj od njih da različit naziv.

Scheme information URI (klauzula 5.3.7)

Ovo se polje ZAHTIJEVA i točno navodi URI(je) s kojih korisnici (ovisne stranke) mogu dobiti informacije specifične za shemu (na engleskom kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika). Polje je slijed višejezičnih pokazivača (na engleskom kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika). Referentni URI(-ji) MORAJU osigurati put do informacija koje opisuju „odgovarajuće informacije o shemi".

Odgovarajuće informacije o shemi uključuju najmanje:

— Opće uvodne informacije koje su zajedničke svim državama članicama u vezi s opsegom i kontekstom pouzdanog popisa, te s osnovnim shemama nadzora/akreditacije. Zajednički tekst koji se upotrebljava je kako slijedi:

„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 o 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 o 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 osnovnim shemama nadzora/akreditacije, posebno ([1]):

— Informacije o sustavu nadzora koji se primjenjuje na svaki CSP_{QC};

— Informacije, kad je primjenljivo, o nacionalnoj dobrovoljnoj shemi akreditacije koja se primjenjuje na svaki CSP_{QC};

— Informacije, kad je primjenljivo, o sustavu nadzora koji se primjenjuje na svaki CSP koji ne izdaje QC-e;

— Informacije, kad je primjenljivo, o nacionalnoj dobrovoljnoj shemi akreditacije koja se primjenjuje na svaki CSP koji ne izdaje QC-e;

— Te posebne informacije za svaku gore navedenu osnovnu shemu uključuju najmanje:

— Opći opis;

— Informacije o postupku koje upotrebljava nadzorno/akreditacijsko tijelo za nadziranje/akreditiranje CSP-a i CSP-i koji su nadzirani/akreditirani;

— Informacije o mjerila po kojima su CSP-i nadzirani/akreditirani.

— Posebne informacije, kad je primjenljivo, o posebnim kvalifikacijama nekih fizičkih ili binarnih (logičkih) objekata stvorenih ili izdanih kao posljedica pružanja usluge certificiranja mogu imati pravo na posebnu kvalifikaciju na temelju njihove usklađenost s odredbama i zahtjevima utvrđenim na nacionalnoj razini, uključujući značenje takve kvalifikacije te povezane nacionalne odredbe i zahtjeve.

([1]) Zadnja dva skupa informacija od ključne su važnosti za to da ovisne stranke ocijene razinu kakvoće i sigurnosti takvih sustava nadzora/akreditacije. Ti skupovi informacija pružaju se na razini TL-a kroz uporabu trenutne „Scheme information URI" (klauzula 5.3.7 — informacije pruža država članica), „Scheme type/community/rules" (klauzula 5.3.9 — kroz uporabu teksta zajedničkog svim državama članicama) i „TSL policy/legal notice" (klauzula 5.3.11 — tekst zajednički svim državama članicama upućivanjem na Direktivu 1999/93/EZ, zajedno s mogućnošću za svaku državu članicu da doda tekst/upućivanja specifična za svaku državu članicu). Dodatne informacije o nacionalnim sustavima nadzora/akreditacije za CSP-e koji ne izdaju QC-e mogu se pružiti na razini usluge kad je primjenljivo i potrebno (na primjer za razlikovanje između nekoliko razina kakvoće/sigurnosti) kroz uporabu „Scheme service definition URI" (klauzula 5.5.6).

Dodatne specifične informacije države članice o shemi MOGU se dodatno pružiti na dobrovoljnoj osnovi. To uključuje:

— Informacije o mjerilima i pravilima koja se upotrebljavaju za odabir nadzornika/revizora i za određivanje kako su CSP-i nadzirani (kontrolirani)/akreditirani (revidirani),

— Ostale kontaktne i opće informacije koje se primjenjuju na djelovanje sheme.

Status determination approach (klauzula 5.3.8)

Ovo se polje ZAHTIJEVA i točno navodi identifikator pristupa za određivanje statusa. Upotrebljava se sljedeći posebni URI, registriran i opisan kako slijedi:

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

Opis: Status navedenih usluga određuje upravitelj sheme ili netko u njegovo ime prema odgovarajućem sustavu za referentnu državu članicu koji omogućuje „nadzor" (i, kad je primjenljivo, „dobrovoljnu akreditaciju") pružatelja usluga certificiranja koji imaju sjedište ili prebivalište na njezinom državnom području (ili imaju sjedište ili prebivalište u trećoj zemlji u slučaju „dobrovoljne akreditacije") i izdaju kvalificirane certifikate javnosti u skladu s člankom 3. stavkom 3. (odnosno člankom 3. stavkom 2. ili člankom 7. stavkom 1. točkom (a)) Direktive 1999/93/EZ, i, kad je primjenljivo, koji omogućuju"nadzor"/„dobrovoljnu akreditaciju" pružatelja usluga certificiranja koji ne izdaju kvalificirane certifikate, sukladno nacionalno određenim i uspostavljenim „priznatim shemama odobrenja" provedenim na nacionalnoj osnovi za nadzor usklađenosti usluga koje pružaju CSP-i koji ne izdaju QC-e s odredbama utvrđenima u Direktivi 1999/93/EZ i po mogućnosti proširenim nacionalnim odredbama u vezi s pružanjem takvih usluga certificiranja.

Scheme type/community/rules (klauzula 5.3.9)

Ovo se polje ZAHTIJEVA i sadrži najmanje sljedeće registrirane URI-je:

— URI koji je zajednički svim pouzdanim popisima država članica koji pokazuju na opisni tekst koji se primjenjuje na sve TL-e:

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

— Kojim je označeno sudjelovanje sheme države članice (utvrđene putem „TSL type" (klauzula 5.3,3) i „Scheme name" (klauzula 5.3.6)) u shemi shema (to jest, pokazivači popisa TSL-a na sve države članice koje objavljuju i održavaju pouzdani popis u obliku TSL-a);

— Gdje korisnici mogu dobiti politiku/pravila po kojima se ocjenjuju usluge uvrštene na popis i s kojima se može odrediti vrsta TSL-a (vidjeti klauzulu 5.3.3);

— Gdje korisnici mogu dobiti opis o tome kako upotrebljavati i tumačiti sadržaj provedbe TSL-ovog pouzdanog popisa. Ta pravila o uporabi zajednička su svim pouzdanim popisima država članica bez obzira na vrstu navedene usluge ili sustav(e) nadzora/akreditacije.

Opisni tekst:

„**Participation in a scheme**

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

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

Policy/rules for the assessment of the listed services

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3,2 and Art. 7.1(a)), including information o Qualified Certificate (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) 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' o 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)

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 o 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 o fields, description and meaning for the TSL implementation of the Member States' Trusted Lists."

— URI specifičan za svaki pouzdani popis države članice koji pokazuju na opisni tekst koji se primjenjuje na ovaj TL države članice:

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

gdje je CC = oznaka zemlje ISO 3166-1 alpha-2 koja se upotrebljava u polju „Scheme territory" (klauzula 5.3.10)

— Gdje korisnici mogu dobiti posebnu politiku/pravila referentne države članice su skladu s kojima se usluge uvrštene na popis ocjenjuju u skladu s odgovarajućim sustavom nadzora i dobrovoljnim shemama akreditacije.

— Gdje korisnici mogu dobiti opis specifičan za referentnu državu članicu o tome kako upotrijebiti i tumačiti sadržaj provedbe TSL-a pouzdanog popisa u vezi s uslugama certificiranja koje nisu povezane s izdavanjem QC-a. To se može upotrijebiti za navođenje moguće rascjepkanosti u nacionalnim sustavima nadzora/akreditacije povezanim s CSP-ima koji ne izdaju QC-e i za način kako se u tu svrhu upotrebljava „Scheme service definition URI" (klauzula 5.5.6) i polje „Service information extension".

Države članice MOGU odrediti dodatne URI-je iz gore navedenog URI-ja specifičnog za državu članicu URI (to jest, URI-je određene iz tog hijerarhijskog specifičnog URI-ja).

Scheme territory (klauzula 5.3.10)

U kontekstu tih specifikacija, ovo se polje ZAHTIJEVA i točno navodi zemlju u kojoj je shema uspostavljena (oznaka zemlje ISO 3166-1 alpha-2).

TSL policy/legal notice (klauzula 5.3.11)

U kontekstu tih specifikacija, ovo se polje ZAHTIJEVA i točno navodi politiku sheme ili daje obavijest u vezi s pravnim statusom sheme ili pravnim zahtjevima koje je shema ispunila za jurisdikciju u kojoj je shema uspostavljena i/ili sva ograničenja i uvjete pod kojima se TL održava i objavljuje.

To je višejezični niz slova (običan tekst) sastavljen od dva dijela:

— prvog obveznog dijela, zajedničkog svim pouzdanim popisima država članica (na engleskom kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika), koji navodi da je primjenljivi pravni okvir Direktiva 1999/93/EZ i njezina odgovarajuća provedba u zakonodavstvu država članica, navedene u polju „Scheme Territory".

Engleska inačica zajedničkog teksta:

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

Tekst na hrvatskom jeziku:

„Primjenljivi pravni okvir za sadašnju provedbu TSL-a pouzdanog popisa nadziranih/ovlaštenih pružatelja usluga certificiranja za [naziv odgovarajuće države članice] je Direktiva 1999/93/EZ Europskog parlamenta i Vijeća od 13. prosinca 1999. o okviru Zajednice za elektroničke potpise i njezina provedba u zakonodavstvu [naziv odgovarajuće države članice."

— drugog obveznog dijela, specifičnog za svaki TL (na engleskom kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika) koji navodi upućivanja na posebne primjenljive nacionalne pravne okvire (na primjer, posebno ako se odnose na nacionalne sheme nadzora/akreditacije za CSP-e koji ne izdaju QC-e).

Historical information period (klauzula 5.3.12)

Ovo se polje ZAHTIJEVA i točno navodi razdoblje (cijeli broj) tijekom kojeg su povijesne informacije u TSL-u pružene. Ta vrijednost izražena cijelim brojem navodi se brojem dana i u kontekstu tih specifikacija. Vrijednost je veća od ili jednaka 3 653 (to jest, znači da provedba TSL-a pouzdanog popisa država članica MORA sadržavati povijesne informacije najmanje deset godina). Veće vrijednosti trebaju voditi računa o pravnim zahtjevima za zadržavanje podataka u državi članici, navedenim u „Scheme Territory" (klauzula 5.3.10).

Pointers to other TSLs (klauzula 5.3.13)

U kontekstu tih specifikacija, ovo se polje ZAHTIJEVA i uključuje, ako je to na raspolaganju, pokazivač na ETSI TS 102 231 odgovarajućeg obrasca popisa veza (pokazivača) koji sastavlja EZ prema svim provedbama TSL-a pouzdanih popisa država članica. Specifikacije iz ETSI TS-a 102 231, klauzula 5.3.13 primjenjuju se dok se daje ovlast za uporabu neobveznog digitalnog identiteta, koji predstavlja izdavatelja TSL-a na kojeg je ukazano, oblikovanu kako je utvrđeno u klauzuli 5.5.3.

Napomena: Dok se čeka na provedbu od strane EZ-a sastavljenog popisa veza do provedbe TSL-a pouzdanih popisa država članica, koja je u skladu s ETSI TS-om 102 231, ovo se polje NE UPOTREBLJAVA.

List issue date and time (klauzula 5.3.14)

Ovo se polje ZAHTIJEVA i točno navodi datum i vrijeme (UTC izražen kao Zulu) kada je TSL izdan uporabom vrijednosti datuma i vremena kako je utvrđeno u ETSI TS-u 102 231, klauzula 5.1.4.

Next update (klauzula 5.3.15)

Ovo se polje ZAHTIJEVA i točno navodi zadnji datum i vrijeme (UTC izražen kao Zulu) do kojeg će sljedeći TSL biti izdan ili ništavan što znači da je TSL zatvoren (uporabom vrijednosti datuma i vremena kako je utvrđeno u ETSI TS-u 102 231, klauzula 5.1.4).

U slučaju da nema privremenih promjena statusa nekog od TSP-a ili usluge obuhvaćene shemom, TSL MORA biti ponovno izdan do isteka valjanosti zadnjeg izdanog TSL-a.

U kontekstu tih specifikacija, razlika između datuma i vremena „Next update"i „List issue date and time" NE prelazi **šest (6)** mjeseci.

Distribution points (klauzula 5.3.16)

Ovo je polje NEOBVEZNO. Ako se upotrebljava točno navodi lokacije gdje je objavljena trenutačna provedba TSL-a pouzdanog popisa i gdje se mogu naći ažuriranja trenutačnog TSL-a. Ako je utvrđeno više distribucijskih točaka sve MORAJU pružati jednake preslike trenutačnog TSL-a ili njegove ažurirane inačice. Kada se upotrebljava, ovo polje se oblikuje kao puni slijed nizova, od kojih je svaki u skladu s RFC-om 3986 ([1]).

Scheme extensions (klauzula 5.3.17)

Ovo je polje NEOBVEZNO i ne upotrebljava se u kontekstu ove specifikacije.

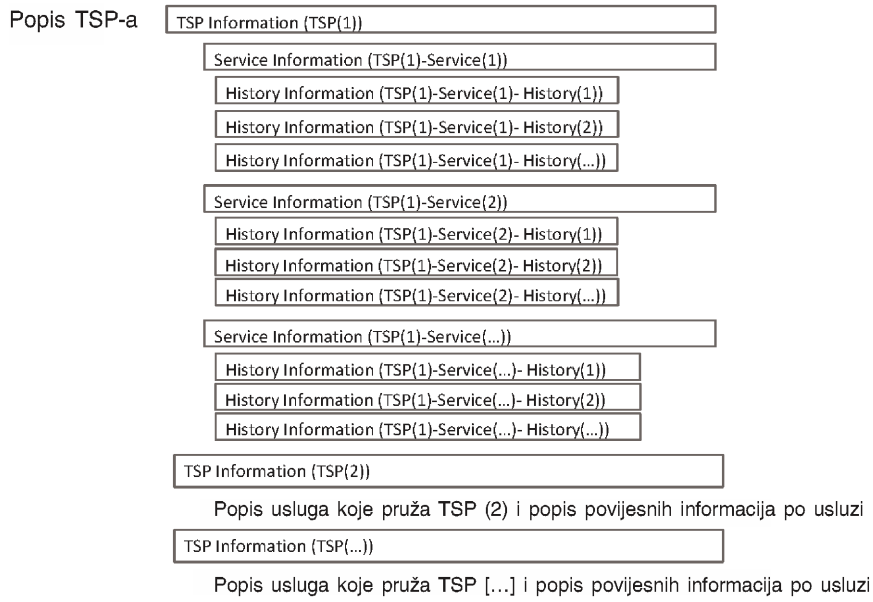
List of Trust Service Providers

Ovo je polje NEOBVEZNO.

Ako se CSP-i u državi članici nadziru/akreditiraju ili su bili nadzirani/akreditirani u kontekstu sheme, ovo polje se ne upotrebljava. Dogovoreno je, međutim, da čak ako država članica nema CSP-a koje nadzire ili akreditira shema, države članice provode TSL bez uporabe tog polja. Ako na popisu nema nijednog CSP-a to znači da nema CSP-a koji su nadzirani/akreditirani u zemlji navedenoj u „Scheme Territory".

Ako se jedna ili više usluga CSP-a nadzire/akreditira ili je bila nadzirana/akreditirana od strane sheme, onda polje sadrži slijed koji utvrđuje svakog CSP-a koji pruža jednu ili više takvih nadziranih/akreditiranih usluga, s detaljima o status nadzora/akreditacije i povijesti statusa svake usluge CSP-a (TSP = CSP na donjoj slici).

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



Popis TSP-a je organiziran kako je prikazano na gornjoj slici. Za svaki TSP postoji niz polja s informacijama o TSP-u („TSP Information”), čemu slijedi popis usluga. Za svaku takvu navedenu uslugu postoji niz polja s informacijama o usluzi („Service Information”) i niz polja o povijesti statusa odobrenja usluge („Service approval history”).

TSP Information

TSP(1)

TSP name (klauzula 5.4.1)

Ovo se polje ZAHTIJEVA i točno navodi naziv **pravnog subjekta** odgovornog za usluge CSP-a koje se nadziru ili akreditiraju ili su bile nadzirane ili akreditirane prema shemi. To je slijed višejezičnih nizova slova (na engleskom kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika). Taj naziv MORA biti naziv koji se upotrebljava u službenim pravnim registrima i na koji će biti naslovljene sve službene obavijesti.

TSP trade name (klauzula 5.4.2)

Ovo je polje NEOBVEZNO i, ako se upotrebljava, točno navodi alternativni naziv pod kojim se CSP identificira u posebnom kontekstu pružanja onih usluga koje se mogu naći u ovom TSL-u pod unosom „TSP name” (klauzula 5.4.1).

Napomena: Ako jedan pravni subjekt CSP-a pruža usluge pod različitim trgovačkim nazivima ili u različitim posebnim kontekstima, moglo bi biti onoliko unosa CSP-a koliko je takvih posebnih konteksta (na primjer unosi naziv/trgovački naziv). Alternativa je navesti svaki CSP (pravni subjekt) samo jednom i pružiti informacije o kontekstu specifičnom za uslugu. Na upravitelju sheme države članice je da s CSP-ima raspravi i dogovori najpogodniji pristup.

TSP address (klauzula 5.4.3)

Ovo se polje ZAHTIJEVA i točno navodi adresu pravnog subjekta ili ovlaštene organizacije utvrđene u polju „TSP name” (klauzula 5.4.1) i za poštanske i za elektroničke komunikacije. Uključuje i „PostalAddress” (to jest, ulicu, mjesto, (država ili provincija), (poštanski broj) i oznaku države ISO 3166-1 alpha-2) sukladno klauzuli 5.3.5.1; te „ElectronicAddress” (to jest, e-pošta i/ili internetska stranica URI) sukladno klauzuli 5.3.5.2.

TSP information URI (klauzula 5.4.4)

Ovo se polje ZAHTIJEVA i točno navodi URI(je) s kojih korisnici (ovisne stranke) mogu dobiti informacije specifične za CSP. Polje je slijed višejezičnih pokazivača (na engleskom kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika). Referentni URI(-i) MORAJU osigurati put do informacija koje opisuju opće uvjete CSP-a, njegove prakse, pravna pitanja, njegovu politiku zaštite potrošača i ostale generičke informacije koje se primjenjuju na sve ili usluge navedenu u unosu CSP-a u TSL.

Napomena: Ako jedan pravni subjekt CSP-a pruža usluge pod različitim trgovačkim nazivima ili u različitim posebnim kontekstima i to se odražava na toliko unosa TSP-a koliko je tih specifičnih konteksta, ovo polje točno navodi informacije vezane uz poseban skup usluga navedenih u unosu TSP/trgovački naziv.

TSP information extensions (klauzula 5.4.5)

Ovo je polje NEOBVEZNO i, ako se upotrebljava, MOŽE ga upotrebljavati upravitelj sheme, u skladu sa specifikacijama ETSI TS 102 231 (klauzula 5.4.5), da pruži posebne informacije, koje se tumače u skladu s pravilima specifične sheme.

List of Services

Ovo se polje ZAHTIJEVA i sadrži slijed koji utvrđuje svaku priznatu uslugu CSP-a te status odobrenja (i povijest tog statusa) navedene usluge. Mora biti navedena najmanje jedna usluga (čak i ako su sve sadržane informacije u cijelosti povijesne).

Kako se prema ovim specifikacijama ZAHTIJEVA zadržavanje povijesnih informacija o navedenim uslugama, te se povijesne informacije MORAJU zadržati čak i ako trenutačni status usluge ne bi obično zahtijevao da bude navedena (na primjer, usluga je povučena). Zato CSP MORA biti uključen čak i ako je njegova jedina navedena usluga u takvom stanju, kako bi se sačuvala povijest.

Service Information

TSP(1) Service(1)

Service type identifier (klauzula 5.5.1)

Ovo se polje ZAHTIJEVA i točno navodi identifikator vrste usluge u skladu s vrstom važećih specifikacija TSL-a (to jest, „/eSigDir-1999-93-EC-TrustedList/TSLtype/generic").

Ako je navedena usluga povezana s izdavanjem kvalificiranih certifikata, navedeni URI je http://uri.etsi.org/TrstSvc/Svctype/CA/QC (certifikacijsko tijelo koje izdaje kvalificirane certifikate).

Ako je navedena usluga povezana s izdavanjem žetona pouzdane usluge koji nisu QC-i i ne podupiru izdavanje QC-a, navedeni URI je jedan od URI-ja određenih u ETSI-ju 102 231 i navedenih u klauzuli D.2 koja se odnosi na ovo polje. To se primjenjuje čak i na one žetone pouzdane usluge koji su nadzirani/akreditirani radi ispunjavanja nekih posebnih kvalifikacija u skladu s nacionalnim zakonodavstvom država članica (na primjer, takozvani kvalificirani žetoni vremenskog žiga na njemačkom ili mađarskom), navedeni URI je jedan od URI-ja određenih u ETSI-ju 102 231 i navedenih u klauzuli D.2 koja se odnosi na ovo polje (na primjer, TSA za nacionalno određene kvalificirane žetone vremenskog žiga). Kad je primjenljivo, takva specifična nacionalna kvalifikacija žetona pouzdane usluge MOŽE se navesti u unosu usluge, a u tu se svrhu upotrebljava proširenje additionalServiceInformation (klauzula 5,8.2) i klauzula 5.5.9 (Service information extension).

Kao opće zadano načelo, za navedeni CSP na pouzdanom popisu postoji jedan unos za jedan certifikat X.509v3 (na primjer, za vrstu usluge certificiranja CA/QC) pod navedenim uslugama certificiranja od strane navedenog CSP-a na pouzdanom popisu (na primjer, certifikacijsko tijelo koje (izravno) izdaje QC-e). U nekim pomno predviđenim okolnostima i pomno kontroliranim i potvrđenim uvjetima, nadzorno tijelo/akreditacijsko tijelo države članice MOŽE se odlučiti za uporabu certifikata X.509v3 Root ili Upper Level CA (na primjer, certifikacijsko tijelo koje ne izdaje QC-e izravno krajnjem subjektu, već potvrđuje hijerarhiju CA-a sve do CA-a koji izdaju QC-e krajnjim subjektima) kao Sdi jednog unosa na popis usluga navedenog CSP-a. Posljedice (prednosti i nedostaci) uporabe takvog CA-a X.509v3 Root ili Upper Level CA-a kao vrijednosti unosa usluga na TL-u moraju biti pomno razmotrene i potvrđene od strane država članica [1]. Nadalje, prilikom uporabe odobrene iznimke od zadanog načela, države članice MORAJU osigurati potrebnu dokumentaciju za olakšavanje uspostave i potvrde puta certificiranja.

[1] Uporaba certifikata RootCA X.509v3 kao vrijednosti „Sdi-a" za navedenu uslugu, prisilit će upravitelja sheme da uzme u obzir čitavi skup usluga certificiranja pod takvim Root CA-om kao cjelinu u vezi sa „statusom nadzora/akreditacije". Na primjer, svaka promjena statusa koja se zahtijeva od jednog CA-a prema navedenoj root hijerarhiji, prisilit će čitavu hijerarhiju da preuzme tu promjenu statusa.

Napomena: TSP-i kao što su poslužitelji OCSP-a i izdavatelji CRL-a koji su dio usluge certificiranja CSP_{QC} i predmet uporabe odvojenih parova ključeva za potpisivanje odaziva OCSP-a i CRL-a MOGU biti navedeni na ovom obrascu TSL-a uporabom sljedeće kombinacije URI-ja:

— vrijednost „Service type identifier" (klauzula 5.5.1):

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

kombinirana sa sljedećom vrijednošću „Service information extension" (klauzula 5.5.9) additionalServiceInformation extension (klauzula 5.8.2):

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

Opis: pružatelj statusa certifikata koji upravlja poslužiteljem OCSP kao dio usluge koju pruža CSP koji izdaje kvalificirane certifikate,

— vrijednost „Service type identifier" (klauzula 5.5.1):

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

kombinirana sa sljedećom vrijednošću „Service information extension" (klauzula 5.5.9) additionalServiceInformation extension (klauzula 5.8.2):

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

Opis: pružatelj statusa certifikata koji upravlja CRL-om kao dio usluge koju pruža CSP koji izdaje kvalificirane certifikate,

— vrijednost „Service type identifier" (klauzula 5.5.1):

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

kombinirana sa sljedećom vrijednošću „Service information extension" (klauzula 5.5.9) additionalServiceInformation extension (klauzula 5.8.2):

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

Opis: Root certifikacijsko tijelo od kojeg je moguće uspostaviti put certificiranja do certifikacijskog tijela koje izdaje kvalificirane certifikate,

— vrijednost „Service type identifier" (klauzula 5.5.1):

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

kombinirana sa sljedećom vrijednošću „Service information extension" (klauzula 5.5.9) additionalServiceInformation extension (klauzula 5.8.2):

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

Opis: usluga vremenskog žiga kao dio usluge pružatelja usluga certificiranja koji izdaje kvalificirane certifikate koji izdaju TST-e koji se mogu upotrebljavati u postupku potvrđivanja kvalificiranog potpisa za utvrđivanje i proširenje valjanosti potpisa ako je QC is opozvan ili je istekao.

S e r v i c e n a m e (klauzula 5.5.2)

Ovo se polje ZAHTIJEVA i točno navodi naziv pod kojim CSP utvrđen u „TSP name" (klauzula 5.4.1) pruža uslugu utvrđenu u „Service type identifier" (klauzula 5.5.1). Polje je slijed višejezičnih nizova slova (na engleskom kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika).

S e r v i c e d i g i t a l i d e n t i t y (klauzula 5.5.3)

Ovo se polje ZAHTIJEVA i točno navodi najmanje jedan opis digitalnog identifikatora jedinstvenog za uslugu čija je vrsta utvrđena u „Service type identifier" (klauzula 5.5.1) s kojom se usluga može nedvosmisleno utvrditi.

U ovim specifikacijama digitalni identifikator koji se upotrebljava u ovom polju je odgovarajući certifikat X.509v3 koji predstavlja javni ključ (javne ključeve) koje CSP upotrebljava za pružanje usluge čija je vrsta utvrđena u „Service type identifier" (klauzula 5.5.1) (to jest, ključ koji upotrebljava Root CA/QC, ključ koji se upotrebljava za potpisivanje certifikata ([1]), ili alternativno za izdavanje žetona vremenskog žiga, potpisivanje CRL-a ili potpisivanje odziva OCSP-a). Taj povezani certifikat X.509v3 SHALL upotrebljava se kao minimalno zahtijevan digitalni identifikator (koji predstavlja javni ključ (javne ključeve) koje CSP upotrebljava za pružanje navedene usluge). MOGU se upotrebljavati dodatni identifikatori kako slijedi, ali svi se MORAJU odnositi na isti identitet (to jest, povezani certifikat X.509v3):

(a) razlikovni naziv (DN) certifikata koji se može upotrebljavati za potvrđivanje elektroničkih potpis za usluge CSP-a utvrđene u „Service type identifier" (klauzula 5.5.1);

(b) povezani identifikator javnog ključa (to jest, X.509v3 identifikator ključa subjekta ili vrijednost SKI);

(c) povezani javni ključ.

Kao opće zadano načelo, digitalni identifikator (to jest, povezani certifikat X.509v3) ne smije biti prisutan na pouzdanom popisu više od jedanput, to jest, za svaki certifikat X.509v3 postoji samo jedan unos za uslugu certificiranja pod navedenim uslugama certificiranja navedenog CSP-a na pouzdanom popisu. Suprotno, jedan certifikat X.509v3 upotrebljava se u jednom unosu usluge kao vrijednost „Sdi".

Napomena (1): Jedini slučaj na koji se gornje opće zadano načelo ne može primijeniti je situacija u kojoj se jedan certifikat X.509v3 upotrebljava pri izdavanju različitih vrsta žetona pouzdanih usluga za koje se primjenjuju različite sheme nadzora/akreditacije, na primjer, s jedne strane CSP upotrebljava jedan certifikat X.509v3pri izdavanju QC-a pod odgovarajućim sustavom nadzora, a s druge strane pri izdavanju nekvalificiranih certifikata pod različitim statusom nadzora/akreditacije. U ovom slučaju i primjeru bi se upotrebljavala dva unosa s različitom vrijednošću „Sti" (na primjer CA/QC i CA/PKC u navedenom primjeru) i s istom vrijednošću „Sdi" (povezani certifikat X.509v3).

Provedbe ovise o ASN.1 ili XML-u i sukladne su specifikacijama ETSI TS 102 231 (za ASN.1 vidjeti Prilog A ETSI TS-u 102 231, a za XML vidjeti Prilog B ETSI TS-u 102 231).

Napomena (2): Kada treba pružiti dodatne informacije o „kvalifikaciji" u vezi s unosom identificirane usluge, onda, prema potrebi, upravitelj sheme uzima u obzir uporabu proširenja „additionalServiceInformation" (klauzula 5.8.2) polja „Service information extension" (klauzula 5.5.9) u skladu s namjenom pružanja takvih dodatnih informacija o „kvalifikaciji". Pored toga, upravitelj sheme može upotrebljavati klauzulu 5.5.6 (Scheme service definition URI).

Service current status (klauzula 5.5.4)

Ovo se polje ZAHTIJEVA i točno navodi identifikator statusa usluge putem jednog od sljedećih URI-ja:

— **Pod nadzorom** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undernadzor);

— **Nadzor usluge u prekidu** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/nadzorincessation);

— **Nadzor prekinut** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/nadzorceased);

— **Nadzor opozvan** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/nadzorrevoked);

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

— **Akreditacija prekinuta** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/akreditacijaceased);

— **Akreditacija opozvana** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/akreditacijarevoked).

Gornji statusi se u kontekstu ovih specifikacija pouzdanog popisa tumače kako slijedi:

— ***Pod nadzorom:*** Usluga utvrđena u „Service digital identity" (klauzula 5.5.3) koju pruža pružatelj usluga certificiranja (CSP) utvrđen u „TSP name" (klauzula 5.4.1) trenutačno je pod nadzorom, radi usklađenosti s odredbama utvrđenim u Direktivi 1999/93/EZ, od strane države članice utvrđene u „Scheme territory" (klauzula 5.3.10) u kojoj CSP ima sjedište ili prebivalište.

([1]) To može biti certifikat CA koji izdaje certifikate krajnjim subjektima (na primjer CA/PKC, CA/QC) ili certifikat pouzdanog root CA-a od kojeg je moguće naći put do kvalificiranih certifikata krajnjih subjekata. Ovisno o tome mogu li se ove informacije i informacije koje su navedene u svakodnevnom certifikatu krajnjeg subjekta, izdanom prema tom pouzdanom root-u upotrijebiti za nedvosmisleno određivanje odgovarajućih značajki svakog kvalificiranog certifikata, ove informacije (Service digital identity) možda treba dopuniti podacima „Service information extensions" (vidjeti klauzulu 5.5.9).

— ***Nadzor usluge u prekidu:*** Usluga utvrđena u „Service digital identity” (klauzula 5.5.3) koju pruža CSP utvrđen u „TSP name” (klauzula 5.4.1) i trenutačno je u fazi prekida, ali je još uvijek nadzirana dok se nadzor ne prekine ili opozove. Ako je različita pravna osobe od one utvrđene u „TSP name” preuzela odgovornost za osiguranje ove faze prekida, identifikacija te nove ili zamjenske pravne osobe (zamjenski CSP) navodi se u klauzuli 5.5.6 unosa usluge.

— ***Nadzor prekinut:*** Valjanost ocjene nadzora istekla je bez da je usluga utvrđena u „Service digital identity” (klauzula 5.5.3) ponovno ocijenjena. Usluga trenutačno nije pod nadzorom od datuma trenutačnog statusa jer se smatra da je usluga prestala djelovati.

— ***Nadzor opozvan:*** Nakon što je prethodno nadzirana, usluga CSP-a i po mogućnosti sam CSP nije ispunio odredbe utvrđene u Direktivi 1999/93/EZ, kako je odredila država članica utvrđena u „Scheme territory” (klauzula 5.3.10) u kojoj CSP ima sjedište ili prebivalište. U skladu s tim, od usluge se zahtijeva da prekine s djelovanje, i mora se smatrati prekinutom iz gore navedenog razloga.

Napomena (1): Vrijednost statusa „Nadzor opozvan” može biti konačni status, čak i ako CSP tada u potpunosti prekine svoju aktivnost; u tom slučaju nema potrebe prijeći na status „Nadzor usluge u prekidu” ili „Nadzor prekinut”. Zapravo, jedini način da se promijeni status „Nadzor opozvan” je taj da CSP počne poštovati odredbe utvrđene u Direktivi 1999/93/EZ u skladu s odgovarajućim sustavom nadzora važećim u državi članica koja posjeduje TL, te ponovnim dobivanjem statusa „Pod nadzorom”. Status „Nadzor usluge u prekidu” ili „Nadzor prekinut” događa se samo kada CSP izravno prekine svoje povezane uslugama pod nadzorom, a ne kada je nadzor opozvan.

— ***Akreditiran:*** Ocjenu akreditacije izvršilo je akreditacijsko tijelo u ime države članice utvrđene u „Scheme territory” (klauzula 5.3.10), a usluga utvrđena u „Service digital identity” (klauzula 5.5.3) koju pruža CSP ([1]) utvrđen u „TSP name” (klauzula 5.4.1) u skladu je s odredbama utvrđenim u Direktivi 1999/93/EZ.

Napomena (2): Kada se upotrebljava u kontekstu CSP-a koji izdaje QC-e, kojima ima sjedište ili prebivalište na „Scheme territory” (klauzula 5.3.10), sljedeća dva statusa „Akreditacija opozvana” i „Akreditacija prekinuta” MORAJU se smatrati „tranzitnim statusima” i NE SMIJU se upotrebljavati kao vrijednost za „Service current status” jer, ako se upotrebljavaju, MORA im odmah slijediti u „Service approval history information” ili u „Service current status” status „Pod nadzorom”, čemu može slijediti neki drugi status nadzora određen gore i prikazan na slici 1. Kada se upotrebljava u kontekstu CSP-a koji ne izdaje QC-e ako postoji samo jedna povezana „dobrovoljna shema akreditacije” bez povezane sheme nadzora ili u kontekstu CSP-a koji izdaje QC-e ako CSP nema sjedište ili prebivalište na „Scheme territory” (klauzula 5.3.10) (na primjer u trećoj zemlji), navedeni statusi „Akreditacija opozvana” i „Akreditacija prekinuta” MOGU se upotrebljavati kao vrijednost za „Service current status”:

— ***Akreditacija prekinuta:*** Valjanost ocjene akreditacije istekla je bez da je usluga utvrđena u „Service digital identity” (klauzula 5.5.3) ponovno ocijenjena.

— ***Akreditacija opozvana:*** Nakon što je prethodno utvrđeno da je sukladna mjerilima sheme, usluga utvrđena u „Service digital identity” (klauzula 5.5.3) koju pružaju pružatelji usluga certificiranja (CSP-i) utvrđeni u „TSP name” (klauzula 5.4.1) i po mogućnosti sam CSP nisu ispunili odredbe utvrđene u Direktivi 1999/93/EZ.

Napomena (3): Potpuno isti status vrijednosti mora se upotrebljavati za CSP-e koji izdaju QC-e i za CSP-i koji ne izdaju QC-e (na primjer pružatelji usluga vremenskog žiga koji izdaju TST-e, CSP-i koji izdaju nekvalificirane certifikate itd.). „Service Type identifier” (klauzula 5.5.1) se upotrebljava za razlikovanje između primjenljivih sustava nadzora/akreditacije.

Napomena (4): Dodatne informacije vezane uz status o „kvalifikaciji” određene na razini nacionalnih sustava nadzora/akreditacije za CSP-e koji ne izdaju QC-e MOGU se pružiti na razini usluge kad je primjenljivo i potrebno (na primjer za razlikovanje između nekoliko razina kakvoće/sigurnosti). Upravitelji sheme upotrebljavaju proširenje „additionalServiceInformation” (klauzula 5.8.2) polja „Service information extension” (klauzula 5.5.9) u skladu s namjenom pružanja takvih dodatnih informacija o „kvalifikaciji”. Pored toga, upravitelj sheme može upotrebljavati klauzulu 5.5.6 („Scheme service definition URI”).

Current status starting date and time (klauzula 5.5.5)

Ovo se polje ZAHTIJEVA i točno navodi datum i vrijeme kada je trenutni status odobrenja stupio na snagu (vrijednost datuma i vremena kako je određeno u ETSI TS-u 102 231, klauzula 5.1.4).

Scheme service definition URI (klauzula 5.5.6)

Ovo je polje NEOBVEZNO, a ako se upotrebljava točno navodi URI(-e) s kojih ovisne stranke mogu dobiti informacije specifične za uslugu koju pruža upravitelj sheme kao slijed višejezičnih pokazivača (na engleskom kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika).

([1]) Tako akreditiran CSP može imati sjedište ili prebivalište u drugoj državi članici one utvrđene u „Scheme territory” pri provedbi TSL-a TL-a ili u trećoj zemlji (vidjeti članak 7. stavak 1. točku (a) Direktive 1999/93/EZ).

Ako se upotrebljavaju, referentni URI(ji) MORAJU osigurati put do informacija koje opisuju uslugu kako je utvrđeno shemom. To posebno MOŽE uključivati kad je primjenljivo:

(a) URI koji navodi identitet zamjenskog CSP-a u slučaju nadzora usluge u prekidu za koju je uključen zamjenski CSP (vidjeti „Service current status" — klauzula 5.5.4);

(b) URI koji vode ka dokumentima koji pružaju dodatne informacije vezane uz uporabu nekih nacionalno određenih posebnih kvalifikacija za usluge osiguranja nadziranih/akreditiranih žetona pouzdane usluge u skladu s uporabom polja „Service information extension" (klauzula 5.5.9) s proširenjem „additionalServiceInformation" kako je određeno u klauzuli 5.8.2.

Service supply points (klauzula 5.5.7)

Ovo je polje NEOBVEZNO, a ako se upotrebljava točno navodi URI(je) s kojih ovisne stranke mogu pristupiti usluzi pomoću slijeda niza slova čija sintaksa MORA biti sukladna MUST RFC-u 3986.

TSP service definition URI (klauzula 5.5.8)

Ovo je polje NEOBVEZNO, a ako se upotrebljava točno navodi URI(je) s kojih ovisne stranke mogu dobiti informacije specifične za uslugu koju pruža TSP kao slijed višejezičnih pokazivača (na engleskom kao službenom jeziku i po mogućnosti na jednom ili više nacionalnih jezika). Referentni URI(ji) MORAJU osigurati put do informacija koje opisuju uslugu kako je utvrđeno od strane TSP-a.

Service information extensions (klauzula 5.5.9)

U kontekstu ovih specifikacija, ovo je polje NEOBVEZNO, ali se upotrebljava kada informacije pružene u „Service digital identity" (klauzula 5.5.3) nisu dostatne da nedvosmisleno utvrde kvalificirane certifikate izdane tom uslugom i/ili informacije navedene u povezanim kvalificiranim certifikatima ne dopuštaju strojno obrađene definicije činjenica o tome je li QC poduprt SSCD-om ([1]).

U kontekstu ovih specifikacija, ako se njegova uporaba ZAHTIJEVA, na primjer za usluge CA/QC, upotrebljava se neobvezno polje „Service information extensions" (Sie) koje je strukturirano kao slijed jedne ili više torki, u skladu s proširenjem „kvalifikacije" određenim u Prilogu L.3.1 ETSI TS-u 102 231, a svaka torka pruža:

— (filtre) Informacije koje se koriste za daljnje utvrđivanje prema „Sdi-ju" utvrđenoj usluzi certificiranja one usluge (to jest, niz kvalificiranih certifikata) za koje se zahtijevaju/pružaju dodatne informacije u vezi s prisutnošću ili odsutnošću podrške SSCD-a (i/ili izdavanje pravnoj osobi); i

— povezane informacije (kvalifikatore) o tome podržava li SSCD ovaj nadalje utvrđeni niz usluga kvalificiranih certifikata ili ne (ako je ova informacija „QCSSCDStatusAsInCert", to znači da su te povezane informacije dio QC-a u strojno obradivom obliku standardiziranom od strane ETSI-ja ([2])), i/ili informacije u vezi s činjenicom da se takvi QC-i izdaju pravnoj osobi (u načelu se smatra da se izdaju samo fizičkim osobama).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): znači da je osigurano od strane CSP-a i kontrolirano (model nadzora) ili revidirano (model akreditacije) od strane države članice (njezinog nadzornog tijela ili akreditacijskog tijela) da svaki QC izdan u okviru usluge (QCA), utvrđen u „Service digital identity" (klauzula 5.5.3) i nadalje utvrđen gornjim (filtri) informacijama koje se upotrebljavaju za daljnje utvrđivanje prema „Sdi-ju" utvrđene usluge certificiranja onog niza kvalificiranih certifikata za koji se te dodatne informacije zahtijevaju u vezi s prisutnošću ili odsutnošću potpore SSCD-a podupire SSCD (to jest, da je privatni ključ koji je povezan s javnim ključem u certifikatu pohranjen u sredstvu za izradu zaštićenog potpisa u skladu s Prilogom III. Direktivi 1999/93/EZ);

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD): znači da je osigurano od strane CSP-a i kontrolirano (model nadzora) ili revidirano (model akreditacije) od strane države članice (njezinog nadzornog tijela ili akreditacijskog tijela) da svaki QC izdan u okviru usluge (RootCA/QC ili CA/QC), utvrđen u „Service digital identity" (klauzula 5.5.3) i nadalje utvrđen gornjim (filtri) informacijama koje se upotrebljavaju za daljnje utvrđivanje prema „Sdi-ju" utvrđene usluge certificiranja onog niza kvalificiranih certifikata za koji se te dodatne informacije zahtijevaju u vezi s prisutnošću ili odsutnošću potpore SSCD-a podupire SSCD ne podupire SSCD (to jest, da je privatni ključ koji je povezan s javnim ključem u certifikatu pohranjen u sredstvu za izradu zaštićenog potpisa u skladu s Prilogom III. Direktivi 1999/93/EZ]).

([1]) Vidjeti odjeljak 2.2. ovog dokumenta.
([2]) To se odnosi na odgovarajuću kombinaciju prema ETSI-ju određene izjave QcCompliance, izjave QcSSCD [ETSI TS 101 862] ili QCP/QCP + prema ETSI-ju određen OID [ETSI TS 101 456].

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): znači da je osigurano od strane CSP-a i kontrolirano (model nadzora) ili revidirano (model akreditacije) od strane države članice (njezinog nadzornog tijela ili akreditacijskog tijela) da svaki QC izdan u okviru usluge (CA/QC), utvrđen u „Service digital identity" (klauzula 5.5.3) i nadalje utvrđen gornjim (filtri) informacijama koje se upotrebljavaju za daljnje utvrđivanje prema „Sdi-ju" utvrđene usluge certificiranja onog niza kvalificiranih certifikata za koji se te dodatne informacije zahtijevaju u vezi s prisutnošću ili odsutnošću potpore SSCD-a sadrži strojno obradive informacije koje označavaju je li QC poduprt SSCD-om;

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): znači da je osigurano od strane CSP-a i kontrolirano (model nadzora) ili revidirano (model akreditacije) od strane države članice (njezinog nadzornog tijela ili akreditacijskog tijela) da svaki QC izdan u okviru usluge (QCA), utvrđen u „Service digital identity" (klauzula 5.5.3) i nadalje utvrđen gornjim (filtri) informacijama koje se upotrebljavaju za daljnje utvrđivanje prema „Sdi-ju" utvrđene usluge certificiranja onog niza kvalificiranih certifikata za koji se te dodatne informacije zahtijevaju u vezi s izdavanjem pravnoj osobi, izdan pravnoj osobi.

Ti se kvalifikatori upotrebljavaju samo kao proširenje, ako je vrsta usluge http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Ovo polje je specifično za provedbu (ASN.1 or XML) i MORA ispunjavati specifikacije iz Priloga L.3.1 ETSI TS-u 102 231.

U kontekstu provedbe XML-a, specifičan sadržaj takvih dodatnih informacija mora biti kodiran pomoću datoteke iz poglavlja 3.

Service Approval History

Ovo je polje NEOBVEZNO, ali MORA biti prisutno ako „Historical information period" (klauzula 5.3.12) nije ništavno. Zato, u kontekstu ovih specifikacija, shema MORA zadržati povijesne informacije. Ako povijesne informacije namjeravaju zadržati, ali usluga nema povijesti prije trenutačnog statusa (to jest, to jest upravitelj sheme nije zadržao prvi zabilježeni status ili povijesnu informaciju) ovo polje ostaje prazno. U protivnom, za svaku promjenu trenutačnog statusa usluge TSP koja se dogodila u razdoblju povijesnih informacija kako je utvrđeno u ETSI TS-u 102 231, klauzula 5.3.12, informacije o prethodnom statusu odobrenja pružaju se po opadajućem redoslijedu datuma i vremena promjene statusa s (to jest, datum i vrijeme kada je sljedeći status odobrenja stupio na snagu).

To je slijed povijesnih informacije kako je određeno u nastavku.

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

Service type identifier (klauzula 5.6.1)

Ovo se polje ZAHTIJEVA i točno navodi identifikator vrste usluge, s oblikom i značenjem koje se upotrebljava u „TSP Service Information — Service type identifier" (klauzula 5.5.1).

Service name (klauzula 5.6.2)

Ovo se polje ZAHTIJEVA i točno navodi naziv pod kojim je CSP pružio uslugu utvrđenu u „TSP Service Information — Service type identifier" (klauzula 5.5.1), s oblikom i značenjem koje se upotrebljava u „TSP Service Information — Service name" (klauzula 5.5.2). Ova klauzula ne zahtijeva da naziv bude isti kao onaj utvrđen u klauzuli 5.5.2. Promjena naziva MOŽE biti jedna od okolnosti koje zahtijevaju novi status.

Service digital identity (klauzula 5.6.3)

Ovo se polje ZAHTIJEVA i točno navodi najmanje jedan opis digitalnog identifikatora jedinstvenog za uslugu utvrđenu u „TSP Service Information - Service digital identity" (klauzula 5.5.3) u istom obliku i s istim značenjem.

Service previous status (klauzula 5.6.4)

Ovo se polje ZAHTIJEVA i točno navodi identifikator prethodnog statusa usluge, s oblikom i značenjem koje se upotrebljava u „TSP Service Information - Service current status" (klauzula 5.5.4).

Previous status starting date and time (klauzula 5.6.5)

Ovo se polje ZAHTIJEVA i točno navodi datum i vrijeme kada je prethodni predmetni status stupio na snagu, s oblikom i značenjem koje se upotrebljava u „TSP Service Information - Service current status starting date and time" (klauzula 5.5.5).

Service information extensions (klauzula 5.6.6)

Ovo je polje NEOBVEZNO i MOGU ga upotrebljavati upravitelji sheme za pružanje posebnih informacija povezanih s uslugom, s oblikom i značenjem koje se upotrebljava u „TSP Service Information — Service Information extensions" (klauzula 5.5.9).

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

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

…

TSP(1) Service(2)

Isto za TSP(1) Service 2 (kako je primjenljivo)

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

…

TSP(2) Informacije

Isto za TSP 2 (kako je primjenljivo)

Isto za TSP 2 Service 1

Isto za TSP 2 Service 1 History 1

…

Signed TSL

TSL, pripremljen prema ovim specifikacijama, TREBA ([1]) potpisati sa „Scheme operator name" (klauzula 5.3.4) da bi se osigurala njegova autentičnost i integritet.

Preporučuje se da je oblik potpisa CAdES BES/EPES za ASN.1 provedbe, a XAdES BES/EPES kako je utvrđeno u specifikacijama ETSI TS-a 101 903 za provedbe XML-a ([2]). Talva provedbe elektroničkog potpisa ispunjavaju zahtjeve kako je navedeno u Prilogu A odnosno B ETSI TS-u 102 231.

Dodatni opći zahtjevi u vezi s potpisom navedeni su u sljedećim odjeljcima.

Scheme identification (klauzula 5.7.2)

Ovo se polje ZAHTIJEVA i točno navodi upućivanje koje dodjeljuje upravitelj sheme koje jedinstveno utvrđuje shemu opisanu u ovim specifikacijama i uspostavljenom TSL-u, te MORA biti uključena u izračun potpisa. Očekuje se da to bude niz slova ili niz bitova.

U kontekstu ovih specifikacija dodijeljeno upućivanje je ulančavanje „TSL type" (klauzula 5.3.3), „Scheme name" (klauzula 5.3.6) i vrijednosti proširenja identifikatora ključa subjekta certifikata koji upotrebljava upravitelj sheme za elektroničko potpisivanje TSL-a.

Signature algorithm identifier (klauzula 5.7.3)

Ovo se polje ZAHTIJEVA i točno navodi kriptografski algoritam koji je upotrijebljen za stvaranje potpisa. Ovisno o upotrijebljenom algoritmu, ovo polje MOŽE zahtijevati dodatne parametre. Ovo polje MORA biti uključeno u izračun potpisa.

([1]) Dok se provedba njihovog TL-a koji su u cijelosti sukladni ETSI TS-u 102 231, i zato elektronički potpisani, može smatrati idealnim ciljem za sve države članice, kako bi se jamčio doista interoperabilan, online i strojno obradiv okvir za olakšavanje potvrđivanja i prekogranične uporabe QES-a i $AdES_{QC}$-a, državama članicama omogućuje se da iz praktičnih razloga provode intermedijarne oblike svojih TL-a u skladu s ovim tehničkim specifikacijama, pod uvjetom da osiguraju širenje navedenih intermedijarnih oblika TL-a putem sigurnih kanala.

([2]) Obvezno je zaštititi upravitelja sheme koji potpisuje certifikat s potpisom izrađenim na jedan od načina koje utvrđuje ETSI TS 101 733 odnosno ETSI TS 101 903.

Signature value (klauzula 5.7.4)

Ovo se polje ZAHTIJEVA i sadrži stvarnu vrijednost digitalnog potpisa. Sva polja TSL-a (osim same vrijednosti potpisa) MORAJU biti uključena u izračun potpisa.

TSL extensions (klauzula 5.8)

Proširenje **expiredCertsRevocationInfo** (klauzula 5.8.1)

Ovo proširenje je NEOBVEZNO. Ako se upotrebljava, MORA biti sukladno specifikacijama ETSI TS-a 102 231, klauzula 5.8.1.

Proširenje **additionalServiceInformation** (klauzula 5.8.2)

Ovo se NEOBVEZNO proširenje MORA, ako se upotrebljava, upotrijebiti samo na razini usluge i samo u polju određenom u klauzuli 5.5.9 („Service information extension"). Upotrebljava se za pružanje dodatnih informacija o usluzi. To je slijed jedne ili više torki, pri čemu svaka torka navodi:

(a) URI koji utvrđuje dodatne informacije, na primjer:

— URI koji označava neke nacionalno određene posebne kvalifikacije za usluge osiguranja nadziranih/akreditiranih žetona pouzdane usluge, na primjer

— posebnu razinu rascjepkanosti sigurnosti/kakvoće u vezi s nacionalnom shemom nadzora/akreditacije za CSP-e koji ne izdaju QC-e (na primjer RGS */**/*** na FR, poseban status „nadzora" utvrđen nacionalnim zakonodavstvom za posebne CSP-e koji izdaju QC-e na DE), vidjeti Napomenu (4) „Service current status" — klauzula 5.5.4,

— ili poseban status za osiguranje nadziranih/akreditiranih žetona pouzdane usluge (na primjer nacionalno određen „kvalificirani TST" kao na DE ili HU),

— ili značenje posebnog identifikatora politike prisutnog u certifikatu X.509v3 iz polja „Sdi",

— ili registrirani URI kako je utvrđen u „Service type identifier", klauzula 5.5.1, kako bi se dodatno utvrdilo sudjelovanje usluge koju utvrđuje „Sti" kao sastavnog dijela usluge pružatelja usluga certificiranja koji izdaje QC (na primjer, OCSP-QC, CRL-QC, i RootCA-QC);

(b) neobvezni niz koji sadrži vrijednost informacija o usluzi, sa značenjem utvrđenim u shemi (na primjer *, ** ili ***);

(c) sve neobvezne dodatne informacije pružene u obliku specifičnom za shemu.

Dereferenciranje URI-ja TREBALO bi voditi do jasno čitljivih dokumenata koji sadrže sve detalje potrebne za razumijevanje proširenja, a posebno za objašnjavanje značenja navedenih URI-ja, utvrđivanjem moguće vrijednosti za informacije o usluzi i značenjem svake vrijednost.

Qualifications Extension (klauzula L.3.1)

Opis: Ovo je polje NEOBVEZNO, ali se upotrebljava ako se njegova upotreba ZAHTIJEVA, na primjer za usluge RootCA/QC ili CA/QC, i ako

— informacije pružene u „Service digital identity" nisu dostatne za nedvosmisleno utvrđivanje kvalificiranih certifikata izdanih tom uslugom,

— informacije naveden u povezanim kvalificiranim certifikatima ne dopuštaju strojno obradivu identifikaciju činjenica o tome je li QC podržan od SSCD-a ili ne,

Ako se upotrebljava, ovo proširenje razine usluge MORA se upotrebljavati samo u polju utvrđenom u „Service information extension" (klauzula 5.5.9).

Oblik: Puni slijed jednog ili više elemenata kvalifikacije (klauzula L.3.1.2), kako je utvrđeno u Prilogu L.3 ETSI TS-u 102 231.

POGLAVLJE II.

DATOTEKA ETSI XSD U VEZI S ETSI TS 102 231 INAČICA 3

Te se informacije pružaju u njihovim trenutnom stanju. Pojave li se problemi pri uporabi ove xsd datoteke, treba ih prijaviti ETSI-ju koji će ih pokušati otkloniti.

```
<?xml version='1,0' encoding='UTF-8'?>
<!-- edited with XML Spy v4,1 U (http://www.xmlspy.com) by Juan Carlos
Cruellas (UPC Dpt. Arquitectura de Computadors) -->
<!-- ****** NOTICE ******
This version of this document is NOT a formally-approved and issued ETSI
publication.
This document is a Â'work-in-progressÂ' being undertaken by the TC ESI STF
290 and has been revised
to correct identified errors and omissions in the current extant formal
ETSI publication and to
also resolve issues of interpretation raised during implementations based
upon that publication
which are considered to be neither contentious nor to change the
fundamental TSL structure defined
in the original TS 102 231 document and its XSD counterpart.
-->
<xsd:schema targetNamespace='http://uri.etsi.org/02231/v2#"
xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
xmlns:xsd='http://www.w3.org/2001/XMLSchema'
xmlns:ds='http://www.w3.org/2000/09/xmldsig#"
xmlns:tsl='http://uri.etsi.org/02231/v2#" elementFormDefault='qualified'
attributeFormDefault='unqualified'>
        <!-- Imports -->
        <xsd:import namespace='http://www.w3.org/XML/1998/namespace'
schemaLocation='http://www.w3.org/2001/xml.xsd'/>
        <xsd:import namespace='http://www.w3.org/2000/09/xmldsig#"
schemaLocation='http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd'/>
        <!-- Begin auxiliary types -->
        <!--InternationalNamesType-->
        <xsd:complexType name='InternationalNamesType'>
        <xsd:sequence>
        <xsd:element name='Name' type='tsl:MultiLangNormStringType'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name='MultiLangNormStringType'>
        <xsd:simpleContent>
        <xsd:extension base='tsl:NonEmptyNormalizedString'>
        <xsd:attribute ref='xml:lang' use='required'/>
        </xsd:extension>
        </xsd:simpleContent>
        </xsd:complexType>
        <xsd:complexType name='MultiLangStringType'>
        <xsd:simpleContent>
        <xsd:extension base='tsl:NonEmptyString'>
        <xsd:attribute ref='xml:lang' use='required'/>
        </xsd:extension>
        </xsd:simpleContent>
        </xsd:complexType>
        <xsd:simpleType name='NonEmptyString'>
        <xsd:restriction base='xsd:string'>
        <xsd:minLength value='1'/>
        </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name='NonEmptyNormalizedString'>
        <xsd:restriction base='xsd:normalizedString'>
```

```
        <xsd:minLength value='1'/>
        </xsd:restriction>
        </xsd:simpleType>
        <!-- AddressType -->
        <xsd:complexType name='AddressType'>
        <xsd:sequence>
        <xsd:element ref='tsl:PostalAddresses'/>
        <xsd:element ref='tsl:ElectronicAddress'/>
        </xsd:sequence>
        </xsd:complexType>
        <!--PostalAddressList Type-->
        <xsd:element name='PostalAddresses'
type='tsl:PostalAddressListType'/>
        <xsd:complexType name='PostalAddressListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:PostalAddress' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!--PostalAddress Type-->
        <xsd:element name='PostalAddress' type='tsl:PostalAddressType'/>
        <xsd:complexType name='PostalAddressType'>
        <xsd:sequence>
        <xsd:element name='StreetAddress' type='tsl:NonEmptyString'/>
        <xsd:element name='Locality' type='tsl:NonEmptyString'/>
        <xsd:element name='StateOrProvince' type='tsl:NonEmptyString'
minOccurs='0'/>
        <xsd:element name='PostalCode' type='tsl:NonEmptyString'
minOccurs='0'/>
        <xsd:element name='CountryName' type='tsl:NonEmptyString'/>
        </xsd:sequence>
        <xsd:attribute ref='xml:lang' use='required'/>
        </xsd:complexType>
        <!--ElectronicAddressType-->
        <xsd:element name='ElectronicAddress'
type='tsl:ElectronicAddressType'/>
        <xsd:complexType name='ElectronicAddressType'>
        <xsd:sequence>
        <xsd:element name='URI' type='tsl:NonEmptyURIType'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- Types for extensions in TSL -->
        <xsd:complexType name='AnyType' mixed='true'>
        <xsd:sequence minOccurs='0' maxOccurs='unbounded'>
        <xsd:any processContents='lax'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:element name='Extension' type='tsl:ExtensionType'/>
        <xsd:complexType name='ExtensionType'>
        <xsd:complexContent>
        <xsd:extension base='tsl:AnyType'>
        <xsd:attribute name='Critical' type='xsd:boolean' use='required'/>
        </xsd:extension>
        </xsd:complexContent>
        </xsd:complexType>
        <xsd:complexType name='ExtensionsListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:Extension' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!--NonEmptyURIType-->
        <xsd:simpleType name='NonEmptyURIType'>
        <xsd:restriction base='xsd:anyURI'>
```

```
        <xsd:minLength value='1'/>
        </xsd:restriction>
        </xsd:simpleType>
        <!--NonEmptyURIType with language indication-->
        <xsd:complexType name='NonEmptyMultiLangURIType'>
        <xsd:simpleContent>
        <xsd:extension base='tsl:NonEmptyURIType'>
        <xsd:attribute ref='xml:lang' use='required'/>
        </xsd:extension>
        </xsd:simpleContent>
        </xsd:complexType>
        <!--List of NonEmptyURIType with language indication-->
        <xsd:complexType name='NonEmptyMultiLangURIListType'>
        <xsd:sequence>
        <xsd:element name='URI' type='tsl:NonEmptyMultiLangURIType'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!--List of NonEmptyURIType-->
        <xsd:complexType name='NonEmptyURIListType'>
        <xsd:sequence>
        <xsd:element name='URI' type='tsl:NonEmptyURIType'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- End auxiliary types -->
        <!-- ROOT Element -->
        <xsd:element name='TrustServiceStatusList'
type='tsl:TrustStatusListType'/>
        <!-- Trust Status List Type Definition -->
        <xsd:complexType name='TrustStatusListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:SchemeInformation'/>
        <xsd:element ref='tsl:TrustServiceProviderList' minOccurs='0'/>
        <xsd:element ref='ds:Signature'/>
        </xsd:sequence>
        <xsd:attribute name='TSLTag' type='tsl:TSLTagType' use='required'/>
        <xsd:attribute name='Id' type='xsd:ID' use='optional'/>
        </xsd:complexType>
        <!-- TSLTagType -->
        <xsd:simpleType name='TSLTagType'>
        <xsd:restriction base='xsd:anyURI'>
        <xsd:enumeration value='http://uri.etsi.org/02231/TSLTag'/>
        </xsd:restriction>
        </xsd:simpleType>
        <!-- TrustServiceProviderListType-->
        <xsd:element name='TrustServiceProviderList'
type='tsl:TrustServiceProviderListType'/>
        <xsd:complexType name='TrustServiceProviderListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:TrustServiceProvider' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- TSL Scheme Information -->
        <xsd:element name='SchemeInformation'
type='tsl:TSLSchemeInformationType'/>
        <xsd:complexType name='TSLSchemeInformationType'>
        <xsd:sequence>
        <xsd:element name='TSLVersionIdentifier' type='xsd:integer'
fixed='3'/>
        <xsd:element name='TSLSequenceNumber' type='xsd:positiveInteger'/>
        <xsd:element name='TSLType' type='tsl:NonEmptyURIType'/>
```

```
        <xsd:element name='SchemeOperatorName'
type='tsl:InternationalNamesType'/>
        <xsd:element name='SchemeOperatorAddress' type='tsl:AddressType'/>
        <xsd:element name='SchemeName' type='tsl:InternationalNamesType'/>
        <xsd:element name='SchemeInformationURI'
type='tsl:NonEmptyMultiLangURIListType'/>
        <xsd:element name='StatusDeterminationApproach'
type='tsl:NonEmptyURIType'/>
        <xsd:element name='SchemeTypeCommunityRules'
type='tsl:NonEmptyURIListType' minOccurs='0'/>
        <xsd:element ref='tsl:SchemeTerritory' minOccurs='0'/>
        <xsd:element ref='tsl:PolicyOrLegalNotice' minOccurs='0'/>
        <xsd:element name='HistoricalInformationPeriod'
type='xsd:nonNegativeInteger'/>
        <xsd:element ref='tsl:PointersToOtherTSL' minOccurs='0'/>
        <xsd:element name='ListIssueDateTime' type='xsd:dateTime'/>
        <xsd:element ref='tsl:NextUpdate'/>
        <xsd:element ref='tsl:DistributionPoints' minOccurs='0'/>
        <xsd:element name='SchemeExtensions' type='tsl:ExtensionsListType'
minOccurs='0'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- SchemeTerritory -->
        <xsd:element name='SchemeTerritory'
type='tsl:SchemeTerritoryType'/>
        <xsd:simpleType name='SchemeTerritoryType'>
        <xsd:restriction base='xsd:string'>
        <xsd:length value='2'/>
        </xsd:restriction>
        </xsd:simpleType>
        <!-- Policy or Legal Notice -->
        <xsd:element name='PolicyOrLegalNotice'
type='tsl:PolicyOrLegalnoticeType'/>
        <xsd:complexType name='PolicyOrLegalnoticeType'>
        <xsd:choice>
        <xsd:element name='TSLPolicy' type='tsl:NonEmptyMultiLangURIType'
maxOccurs='unbounded'/>
        <xsd:element name='TSLLegalNotice' type='tsl:MultiLangStringType'
maxOccurs='unbounded'/>
        </xsd:choice>
        </xsd:complexType>
        <xsd:element name='NextUpdate' type='tsl:NextUpdateType'/>
        <xsd:complexType name='NextUpdateType'>
        <xsd:sequence>
        <xsd:element name='dateTime' type='xsd:dateTime' minOccurs='0'/>
        </xsd:sequence>
        </xsd:complexType>
        <!--OtherTSLPointersType-->
        <xsd:element name='PointersToOtherTSL'
type='tsl:OtherTSLPointersType'/>
        <xsd:complexType name='OtherTSLPointersType'>
        <xsd:sequence>
        <xsd:element ref='tsl:OtherTSLPointer' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:element name='OtherTSLPointer'
type='tsl:OtherTSLPointerType'/>
        <xsd:complexType name='OtherTSLPointerType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceDigitalIdentities' minOccurs='0'/>
        <xsd:element name='TSLLocation' type='tsl:NonEmptyURIType'/>
        <xsd:element ref='tsl:AdditionalInformation'/>
        </xsd:sequence>
```

```
        </xsd:complexType>
        <xsd:element name='ServiceDigitalIdentities'
type='tsl:ServiceDigitalIdentityListType'/>
        <xsd:complexType name='ServiceDigitalIdentityListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceDigitalIdentity'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:element name='AdditionalInformation'
type='tsl:AdditionalInformationType'/>
        <xsd:complexType name='AdditionalInformationType'>
        <xsd:choice maxOccurs='unbounded'>
        <xsd:element name='TextualInformation'
type='tsl:MultiLangStringType'/>
        <xsd:element name='OtherInformation' type='tsl:AnyType'/>
        </xsd:choice>
        </xsd:complexType>
        <!--DistributionPoints element-->
        <xsd:element name='DistributionPoints'
type='tsl:ElectronicAddressType'/>
        <!-- TSPType -->
        <xsd:element name='TrustServiceProvider' type='tsl:TSPType'/>
        <xsd:complexType name='TSPType'>
        <xsd:sequence>
        <xsd:element ref='tsl:TSPInformation'/>
        <xsd:element ref='tsl:TSPServices'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- TSPInformationType -->
        <xsd:element name='TSPInformation' type='tsl:TSPInformationType'/>
        <xsd:complexType name='TSPInformationType'>
        <xsd:sequence>
        <xsd:element name='TSPName' type='tsl:InternationalNamesType'/>
        <xsd:element name='TSPTradeName' type='tsl:InternationalNamesType'
minOccurs='0'/>
        <xsd:element name='TSPAddress' type='tsl:AddressType'/>
        <xsd:element name='TSPInformationURI'
type='tsl:NonEmptyMultiLangURIListType'/>
        <xsd:element name='TSPInformationExtensions'
type='tsl:ExtensionsListType' minOccurs='0'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- TSP Services-->
        <xsd:element name='TSPServices' type='tsl:TSPServicesListType'/>
        <xsd:complexType name='TSPServicesListType'>
        <xsd:sequence>
        <xsd:element ref='tsl:TSPService' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:element name='TSPService' type='tsl:TSPServiceType'/>
        <xsd:complexType name='TSPServiceType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceInformation'/>
        <xsd:element ref='tsl:ServiceHistory' minOccurs='0'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- TSPServiceInformationType -->
        <xsd:element name='ServiceInformation'
type='tsl:TSPServiceInformationType'/>
        <xsd:complexType name='TSPServiceInformationType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceTypeIdentifier'/>
```

```
        <xsd:element name='ServiceName' type='tsl:InternationalNamesType'/>
        <xsd:element ref='tsl:ServiceDigitalIdentity'/>
        <xsd:element ref='tsl:ServiceStatus'/>
        <xsd:element name='StatusStartingTime' type='xsd:dateTime'/>
        <xsd:element name='SchemeServiceDefinitionURI'
type='tsl:NonEmptyMultiLangURIListType' minOccurs='0'/>
        <xsd:element ref='tsl:ServiceSupplyPoints' minOccurs='0'/>
        <xsd:element name='TSPServiceDefinitionURI'
type='tsl:NonEmptyMultiLangURIListType' minOccurs='0'/>
        <xsd:element name='ServiceInformationExtensions'
type='tsl:ExtensionsListType' minOccurs='0'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- Service status -->
        <xsd:element name='ServiceStatus' type='tsl:NonEmptyURIType'/>
        <!-- Type for Service Supply Points -->
        <xsd:element name='ServiceSupplyPoints'
type='tsl:ServiceSupplyPointsType'/>
        <xsd:complexType name='ServiceSupplyPointsType'>
        <xsd:sequence maxOccurs='unbounded'>
        <xsd:element name='ServiceSupplyPoint' type='tsl:NonEmptyURIType'/>
        </xsd:sequence>
        </xsd:complexType>
        <!-- TSPServiceIdentifier -->
        <xsd:element name='ServiceTypeIdentifier'
type='tsl:NonEmptyURIType'/>
        <!-- DigitalIdentityType -->
        <xsd:element name='ServiceDigitalIdentity'
type='tsl:DigitalIdentityListType'/>
        <xsd:complexType name='DigitalIdentityListType'>
        <xsd:sequence>
        <xsd:element name='DigitalId' type='tsl:DigitalIdentityType'
minOccurs='0' maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name='DigitalIdentityType'>
        <xsd:choice>
        <xsd:element name='X509Certificate' type='xsd:base64Binary'/>
        <xsd:element name='X509SubjectName' type='xsd:string'/>
        <xsd:element ref='ds:KeyValue'/>
        <xsd:element name='X509SKI' type='xsd:base64Binary'/>
        <xsd:element name='Other' type='tsl:AnyType'/>
        </xsd:choice>
        </xsd:complexType>
        <!-- ServiceHistory element-->
        <xsd:element name='ServiceHistory' type='tsl:ServiceHistoryType'/>
        <xsd:complexType name='ServiceHistoryType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceHistoryInstance' minOccurs='0'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:element name='ServiceHistoryInstance'
type='tsl:ServiceHistoryInstanceType'/>
        <xsd:complexType name='ServiceHistoryInstanceType'>
        <xsd:sequence>
        <xsd:element ref='tsl:ServiceTypeIdentifier'/>
        <xsd:element name='ServiceName' type='tsl:InternationalNamesType'/>
        <xsd:element ref='tsl:ServiceDigitalIdentity'/>
        <xsd:element ref='tsl:ServiceStatus'/>
        <xsd:element name='StatusStartingTime' type='xsd:dateTime'/>
        <xsd:element name='ServiceInformationExtensions'
type='tsl:ExtensionsListType' minOccurs='0'/>
```

```
        </xsd:sequence>
        </xsd:complexType>
        <!-- Elements and types for Extensions -->
        <!-- Extensions children of tsl:VaExtension-->
        <!-- Element ExpiredCertsRevocationInfo -->
        <xsd:element name='ExpiredCertsRevocationInfo'
type='xsd:dateTime'/>
        <!-- Element additionalServiceInformation -->
        <xsd:element name='AdditionalServiceInformation'
type='tsl:AdditionalServiceInformationType'/>
        <xsd:complexType name='AdditionalServiceInformationType'>
        <xsd:sequence>
        <xsd:element name='URI' type='tsl:NonEmptyMultiLangURIListType'/>
        <xsd:element name='InformationValue' type='xsd:string'
minOccurs='0'/>
        <xsd:element name='OtherInformation' type='tsl:AnyType'/>
        </xsd:sequence>
        </xsd:complexType>
</xsd:schema>
```

POGLAVLJE III.

DATOTEKA XSD U VEZI S KODIRANJEM POLJA „SIE"

Te se informacije pružaju u njihovim trenutačnom stanju.

```
<?xml version='1,0' encoding='UTF-8'?>
<schema targetNamespace='http://uri.etsi.org/TrstSvc/SvcInfoExt/eSigDir-
1999-93-EC-TrustedList/#" xmlns:xsi='http://www.w3.org/2001/XMLSchema-
instance' xmlns:xsd='http://www.w3.org/2001/XMLSchema'
xmlns:xades='http://uri.etsi.org/01903/v1.3.2#"
xmlns:tsl='http://uri.etsi.org/02231/v2#"
xmlns:tns='http://uri.etsi.org/TrstSvc/SvcInfoExt/eSigDir-1999-93-EC-
TrustedList/#" xmlns='http://www.w3.org/2001/XMLSchema'
elementFormDefault='qualified' attributeFormDefault='unqualified'>
        <!--
        <xsd:import namespace='http://uri.etsi.org/02231/v2#"
schemaLocation='./draft_ts102231v030101xsd.xsd'>
</xsd:import>
-->
        <xsd:import namespace='http://uri.etsi.org/01903/v1.3.2#"
schemaLocation='http://uri.etsi.org/01903/v1.3.2/XAdES.xsd'></xsd:import>
        <element name='Qualifications' type='tns:QualificationsType'/>
        <complexType name='QualificationsType'>
        <sequence maxOccurs='unbounded'>
        <element name='QualificationElement'
type='tns:QualificationElementType'/>
        </sequence>
        </complexType>
        <complexType name='QualificationElementType'>
        <sequence>
        <element name='Qualifiers' type='tns:QualifiersType'/>
        <element name='CriteriaList' type='tns:CriteriaListType'/>
        </sequence>
        </complexType>
        <complexType name='CriteriaListType'>
        <sequence>
        <element name='KeyUsage' type='tns:KeyUsageType' minOccurs='0'
```

```
maxOccurs='unbounded'/>
        <element name='PolicySet' type='tns:PoliciesListType' minOccurs='0'
maxOccurs='unbounded'/>
        <element name='otherCriteriaList' type='tsl:AnyType'
minOccurs='0'/>
        </sequence>
        <attribute name='assert'>
        <simpleType>
        <restriction base='xsd:string'>
        <enumeration value='all'/>
        <enumeration value='atLeastOne'/>
        <enumeration value='none'/>
        </restriction>
        </simpleType>
        </attribute>
        </complexType>
        <complexType name='QualifiersType'>
        <sequence maxOccurs='unbounded'>
        <element name='Qualifier' type='tns:QualifierType'/>
        </sequence>
        </complexType>
        <complexType name='QualifierType'>
        <attribute name='uri' type='anyURI'/>
        </complexType>
        <complexType name='PoliciesListType'>
        <sequence maxOccurs='unbounded'>
        <element name='PolicyIdentifier'
type='xades:ObjectIdentifierType'/>
        </sequence>
        </complexType>
        <complexType name='KeyUsageType'>
        <sequence maxOccurs='9'>
        <element name='KeyUsageBit' type='tns:KeyUsageBitType'/>
        </sequence>
        </complexType>
        <complexType name='KeyUsageBitType'>
        <simpleContent>
        <extension base='xsd:boolean'>
        <attribute name='name'>
        <simpleType>
        <restriction base='xsd:string'>
        <enumeration value='digitalSignature'/>
        <enumeration value='nonRepudiation'/>
        <enumeration value='keyEncipherment'/>
        <enumeration value='dataEncipherment'/>
        <enumeration value='keyAgreement'/>
        <enumeration value='keyCertSign'/>
        <enumeration value='crlSign'/>
        <enumeration value='encipherOnly'/>
        <enumeration value='decipherOnly'/>
        </restriction>
        </simpleType>
        </attribute>
        </extension>
        </simpleContent>
        </complexType>
</schema>
```

POGLAVLJE IV.

SPECIFIKACIJE ZA JASNO ČITLJIV OBLIK PROVEDBE TSL-a POUZDANOG POPISA

Jasno čitljiv oblik (HR) provedbe TSL-a pouzdanog popisa MORA biti javno raspoloživ i dostupan elektroničkim putem. TREBA se pružiti u obliku dokumenta Portable Document Format (PDF) u skladu s ISO 32000 koji MORA biti formatiran u skladu s profilom PDF/A (ISO 19005).

Sadržaj jasno čitljivog oblika provedbe TSL-a pouzdanog popisa na temelju PDF/A TREBA biti u skladu sa sljedećim zahtjevima:

— Struktura jasno čitljivog oblika TREBA odražavati logički model opisan u odjeljku 5.1.2 ETSI TS-a 102 231;

— Svako polje TREBA biti prikazano i navoditi:

  — naziv polja (na primjer „Service type identifier”);

  — vrijednost polja (na primjer „CA/QC”);

  — značenje (opis) vrijednosti polja, kad je primjenljivo i posebno kako je predviđeno u Prilogu D ETSI TS-u 102 231 ili u ovim specifikacijama za registrirane URI-je (na primjer „certifikacijsko tijelo koje izdaje certifikate javnog ključa.”);

  — više inačica na prirodnim jezicima kako je predviđeno u provedbi TSL-a pouzdanog popisa, kad je primjenljivo.

— Sljedeća polja i odgovarajuće vrijednosti digitalnih certifikata navedene u polju „Service digital identity” TREBAJU biti prikazani u jasno čitljivom obliku:

  — Inačica,

  — Serijski broj,

  — Algoritam za potpis,

  — Izdavatelj,

  — Vrijedi od,

  — Vrijedi do,

  — Subjekt,

  — Javni ključ,

  — Politike certifikata,

  — Identifikator ključa subjekta,

  — Distribucijske točke CRL-a,

  — Identifikator ključa izdavatelja,

  — Uporaba ključa,

  — Osnovna ograničenja,

  — Algoritam za otisak prsta,

  — Otisak prsta,

— Jasno čitljivi oblik TREBA biti jednostavan za tiskanje,

— Jasno čitljivi oblik MOŽE se elektronički potpisati. Kad je potpisan MORA ga potpisati upravitelj sheme u skladu s istim specifikacijama za potpis kao za provedu TSL-a pouzdanog popisa.