PROVEDBENA ODLUKA KOMISIJE

od 14. listopada 2013.

o izmjeni Odluke 2009/767/EZ s obzirom na izradu, održavanje i objavu pouzdanih popisa pružatelja usluga certificiranja koje nadziru/akreditiraju države članice

(priopćeno pod brojem dokumenta C(2013) 6543)

(Tekst značajan za EGP)

(2013/662/EU)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Direktivu 2006/123/EZ Europskog parlamenta i Vijeća od 12. prosinca 2006. o uslugama na unutarnjem tržištu ([1]), a posebno njezin članak 8. stavak 3.,

budući da:

(1) Odlukom Komisije 2009/767/EZ od 16. listopada 2009. o utvrđivanju mjera za olakšavanje korištenja postupaka elektroničkim sredstvima putem „jedinstvenih kontaktnih točaka" u skladu s Direktivom 2006/123/EZ Europskog parlamenta i Vijeća o uslugama na unutarnjem tržištu ([2]) države članice obvezuju se staviti na raspolaganje informacije potrebne za potvrđivanje naprednih elektroničkih potpisa potkrijepljenih kvalificiranim certifikatom. Te se informacije moraju navoditi na jedinstven način koristeći tzv. „pouzdane popise" koji sadržavaju informacije o pružateljima usluga certificiranja koji izdaju kvalificirane certifikate za javnost u skladu s Direktivom 1999/93/EZ Europskog parlamenta i Vijeća od 13. prosinca 1999. o okviru Zajednice za elektroničke potpise ([3]), a koje nadziru/akreditiraju države članice.

(2) Praktično iskustvo s provedbom Odluke 2009/767/EZ u državama članicama pokazuje da su potrebna određena poboljšanja kako bi se iskoristile sve prednosti pouzdanih popisa. Osim toga, Europski institut za telekomunikacijske norme (ETSI) objavio je nove tehničke specifikacije za pouzdane popise (TS 119 612) koje se temelje na specifikacijama koje su trenutačno obuhvaćene Prilogom Odluci, ali kojima se istodobno uvodi niz poboljšanja postojećih specifikacija.

(3) Odluku 2009/767/EZ trebalo bi stoga izmijeniti kako bi se njome uputilo na tehničke specifikacije ETSI 119 612 i obuhvatile izmjene koje se smatraju potrebnima za poboljšanje i olakšanje provedbe i korištenja pouzdanih popisa.

(4) Odluka bi se trebala primjenjivati od 1. veljače 2014. kako bi se državama članicama omogućilo da obave potrebne tehničke izmjene postojećih pouzdanih popisa.

(5) Mjere predviđene ovom Odlukom u skladu su s mišljenjem Odbora iz Direktive o uslugama,

DONIJELA JE OVU ODLUKU:

Članak 1.

Izmjene Odluke 2009/767/EZ

Odluka 2009/767/EZ mijenja se kako slijedi:

(1) Članak 2. mijenja se kako slijedi:

a) stavci 1., 2. i 2.a zamjenjuju se sljedećima:

„1. Svaka država članica izrađuje, održava i objavljuje ‚pouzdani popis' u skladu s tehničkim specifikacijama utvrđenima u Prilogu, koji barem sadržava informacije o pružateljima usluga certificiranja koji izdaju kvalificirane certifikate za javnost koje ona nadzire/akreditira.

2. Države članice izrađuju i objavljuju pouzdani popis u obliku prilagođenom strojnoj obradi u skladu sa specifikacijama utvrđenima u Prilogu. Ako država članica odluči objaviti pouzdani popis u ljudima čitljivom obliku, on mora biti u skladu sa specifikacijama utvrđenima u Prilogu.

2.a. Države članice elektronički potpisuju svoj pouzdani popis u obliku prilagođenom strojnoj obradi kako bi se osigurala njegova vjerodostojnost i cjelovitost. Ako država članica objavljuje pouzdani popis u ljudima čitljivom obliku, ona će se pobrinuti da taj popis sadržava barem iste podatke kao popis u obliku prilagođenom strojnoj obradi te ga elektronički potpisuje koristeći isti certifikat kao za popis u strojno čitljivom obliku."

([1]) SL L 376, 27.12.2006., str. 36.
([2]) SL L 274, 20.10.2009., str. 36.
([3]) SL L 13, 19.1.2000., str. 12.

b) Umeće se sljedeći stavak 2.b:

„2.b. Države članice osiguravaju da pouzdani popis u obliku prilagođenom strojnoj obradi bude stalno dostupan na lokaciji objave, bez prekida, osim za potrebe održavanja.”

c) Stavak 3. zamjenjuje se sljedećim:

„3. Države članice Komisiji dostavljaju sljedeće informacije:

(a) tijelo ili tijela odgovorna za izradu, održavanje i objavu pouzdanog popisa u obliku prilagođenom strojnoj obradi;

(b) lokacija na kojoj se objavljuje pouzdani popis u obliku prilagođenom strojnoj obradi;

(c) dva ili više certifikata javnog ključa upravitelja sustava s pomakom između rokova valjanosti od najmanje tri mjeseca, koji odgovaraju privatnim ključevima koji se mogu koristiti za elektroničko potpisivanje pouzdanog popisa u obliku prilagođenom strojnoj obradi;

(d) sve promjene informacija iz točaka (a), (b) i (c).”

d) Umeće se sljedeći stavak 3.a:

„3.a. Ako država članica objavi pouzdani popis u ljudima čitljivom obliku, informacije iz stavka 3. dostavljaju se i za popis u ljudima čitljivom obliku.”

(2) Prilog se zamjenjuje Prilogom ovoj Odluci.

Članak 2.

Primjena

Ova se Odluka primjenjuje od 1. veljače 2014.

Članak 3.

Adresati

Ova je Odluka upućena državama članicama.

Sastavljeno u Bruxellesu 14. listopada 2013.

Za Komisiju

Michel BARNIER

Član Komisije

PRILOG

TEHNIČKE SPECIFIKACIJE ZA ZAJEDNIČKI OBRAZAC „POUZDANOG POPISA NADZIRANIH/AKREDITIRANIH PRUŽATELJA USLUGA CERTIFICIRANJA”

OPĆI ZAHTJEVI

1. **Uvod**

Svrha je zajedničkog obrasca „pouzdanog popisa nadziranih/akreditiranih pružatelja usluga certificiranja” država članica utvrditi zajednički način na koji države članice pružaju podatke o statusu nadzora/akreditacije usluga certificiranja koje pružaju pružatelji usluga certificiranja ([1]) koje one nadziru/akreditiraju u svrhu sukladnosti s relevantnim odredbama Direktive 1999/93/EZ. To uključuje pružanje povijesnih podataka o statusu nadzora/akreditacije usluga certificiranja koje se nadziru/akreditiraju.

Ti su podaci ponajprije predviđeni kao podrška potvrđivanju kvalificiranih elektroničkih potpisa i naprednih elektroničkih potpisa ([2]) potkrijepljenih kvalificiranim certifikatom ([3]), ([4]).

Obvezni podaci u pouzdanom popisu kao minimum moraju sadržavati podatke o nadziranim/akreditiranim pružateljima usluga certificiranja koji izdaju kvalificirane certifikate ([5]) u skladu s odredbama utvrđenima u Direktivi 1999/93/EZ (članak 3. stavak 2. i članak 3. stavak 3. te članak 7. stavak 1. točka (a)), uključujući, kad to nije dio kvalificiranih certifikata, podatke o kvalificiranim certifikatima kojima je potkrijepljen elektronički potpis te je li potpis izrađen sigurnim sredstvom za izradu elektroničkog potpisa ([6]).

Dodatni podaci o drugim pružateljima usluga certificiranja koji ne izdaju kvalificirane certifikate nego pružaju usluge koje se odnose na elektroničke potpise (npr. pružatelj usluga certificiranja koji pruža usluge vremenskog označivanja i izdaje tokene vremenskih oznaka, pružatelj usluga certificiranja koji izdaje nekvalificirane certifikate itd.) mogu se uključiti u pouzdani popis na nacionalnoj razini na dobrovoljnoj osnovi, pod uvjetom da se akreditiraju/nadziru slično kao i pružatelji usluga certificiranja koji izdaju kvalificirane certifikate ili da su odobreni prema nekom drugom nacionalnom programu odobrenja. Nacionalni programi odobrenja u nekim se državama članicama mogu razlikovati od programa nadzora ili dobrovoljne akreditacije primijenjenih na pružatelje usluga certificiranja koji izdaju kvalificirane certifikate u pogledu primjenjivih zahtjeva i/ili nadležne organizacije. Izrazi „akreditiran” i/ili „nadziran” u ovim specifikacijama obuhvaćaju i nacionalne programe odobrenja, a države članice u svojim pouzdanim popisima pružaju dodatne podatke o prirodi svakog nacionalnog programa, uključujući objašnjenja u pogledu mogućih razlika u odnosu na programe akreditacije/nadzora primijenjene na pružatelje usluga certificiranja koji izdaju kvalificirane certifikate.

Zajednički obrazac oslanja se na ETSI TS 119 612 v1.1.1. ([7]) (dalje u tekstu: ETSI TS 119 612) koji se bavi izradom, objavljivanjem, lokacijom, pristupom, utvrđivanjem autentičnosti i cjelovitošću takvih popisa.

2. **Struktura zajedničkog obrasca pouzdanog popisa**

Zajednički obrazac pouzdanog popisa države članice prema ETSI TS 119 612 sadržava sljedeće kategorije podataka:

1. Oznaka pouzdanog popisa koja olakšava identifikaciju popisa tijekom elektroničkih pretraga;

2. Podaci o pouzdanom popisu i programu njegova izdavanja;

3. Niz polja koja sadržavaju jasne identifikacijske podatke o svakom nadziranom/akreditiranom pružatelju usluga certificiranja prema programu (taj niz nije obvezan, odnosno kad se ne upotrebljava smatrat će se da popis nema sadržaja, odnosno da u pridruženoj državi članici ne postoji nijedan nadzirani niti akreditirani pružatelj usluga certificiranja za potrebe pouzdanog popisa);

4. Za svakog pružatelja usluga certificiranja uvrštenog u pouzdani popis pojedinosti o njegovim specifičnim uslugama povjerbe, čiji je trenutačni status zabilježen u pouzdanom popisu, navedene su kao niz polja u kojima su jasno utvrđene nadzirane/akreditirane usluge certificiranja koje pruža pružatelj usluga certificiranja i njihov trenutačni status (taj niz mora sadržavati barem jedan unos);

([1]) Kako je definirano u članku 2. stavku 11. Direktive 1999/93/EZ
([2]) Kako je definirano u članku 2. stavku 2. Direktive 1999/93/EZ
([3]) Za napredne elektroničke potpise koji su potkrijepljeni kvalificiranim certifikatom u cijelom se dokumentu koristi kratica „$AdES_{QC}$”.
([4]) Valja napomenuti da postoje brojne elektroničke usluge utemeljene na jednostavnom naprednom elektroničkom potpisu, čija bi prekogranična uporaba također bila olakšana pod uvjetom da su pomoćne usluge certificiranja (npr. izdavanje nekvalificiranih certifikata) dio nadziranih/akreditiranih usluga koje država članica obuhvaća u dijelu pouzdanog popisa koji se odnosi na dobrovoljne podatke države članice.
([5]) Kako je definirano u članku 2. stavku 10. Direktive 1999/93/EZ
([6]) Kako je definirano u članku 2. stavku 6. Direktive 1999/93/EZ
([7]) ETSI TS 119 612 v1. 1. 1. (2013-06) – Elektronički potpisi i infrastrukture (ESI); Pouzdani popisi.

5. Za svaku uslugu certificiranja koja se nadzire/akreditira, podatak o povijesti statusa, kad je primjenjivo;

6. Potpis stavljen na pouzdani popis.

U kontekstu pružatelja usluga certificiranja koji izdaju kvalificirane certifikate, strukturom pouzdanog popisa, a posebice dijelom s podacima o uslugama (kao u gore navedenoj točki 4.), omogućuje se dopuna ekstenzije podataka o uslugama kako bi se time, u slučajevima u kojima u kvalificiranom certifikatu nisu dostatni (strojno obradivi) podaci o njegovu „kvalificiranom" statusu, kompenzirala moguća podrška sigurnog sredstva za izradu elektroničkog potpisa, a posebno suočilo s dodatnom činjenicom da većina (komercijalnih) pružatelja usluga certificiranja koristi jedno certifikacijsko tijelo za izdavanje nekoliko različitih vrsta certifikata za krajnje korisnike, kako kvalificiranih tako i nekvalificiranih.

U kontekstu usluga (certifikacijskog tijela) generiranja certifikata, broj unosa usluga na popisu pružatelja usluga certificiranja može se smanjiti kad unutar infrastrukture javnog ključa (PKI) pružatelja usluge certificiranja postoji jedna ili nekoliko usluga certifikacijskih tijela više razine (npr. u kontekstu hijerarhije certifikacijskog tijela od izvornog certifikacijskog tijela do certifikacijskih tijela koja izdaju certifikate), tako da se na popis uvrste usluge certifikacijskih tijela više razine, a ne usluge certifikacijskih tijela koja izdaju certifikate za krajnje korisnike (npr. navodeći na popisu samo izvorno certifikacijsko tijelo pružatelja usluga certificiranja). Međutim, u tim se slučajevima podatak o statusu primjenjuje na cijelu hijerarhiju usluga certifikacijskih tijela koja se nalazi ispod usluge uvrštene na popis te se mora očuvati i omogućiti načelo omogućavanja jasne veze između usluge certificiranja pružatelja usluge certificiranja koji izdaje kvalificirane certifikate i skupine certifikata namijenjenih da budu prepoznati kao kvalificirani certifikati.

2.1. *Opis podataka u svakoj kategoriji*

1. Oznaka pouzdanog popisa

2. Podaci o pouzdanom popisu i programu njegova izdavanja

Ovom kategorijom obuhvaćeni su sljedeći podaci:

— **identifikator inačice formata** pouzdanog popisa;

— **redni broj ili broj inačice** pouzdanog popisa;

— **vrsta podatka** na pouzdanom popisu (npr. za identifikaciju činjenice da se tim pouzdanim popisom pružaju podaci o statusu nadzora/akreditacije usluga certificiranja pružatelja usluga certificiranja koje referentna država članica nadzire/akreditira kako bi bila u skladu s odredbama utvrđenima Direktivom 1999/93/EZ);

— podaci o upravitelju (vlasniku) sustava pouzdanog popisa (npr. ime, adresa, kontakt podaci itd. tijela države članice zaduženog za utvrđivanje, sigurno objavljivanje i održavanje pouzdanog popisa);

— **podaci o temeljnom programu/programima nadzora/akreditacije** s kojima je pouzdani popis povezan, uključujući, ali ne ograničavajući se na:

  — zemlju u kojoj se primjenjuje,

  — podatak o mjestu ili upućivanje na mjesto gdje se podatak o programu/programima može naći (model programa, pravila, kriteriji, zajednica na koju se primjenjuje, vrsta itd.),

  — razdoblje čuvanja (povijesnih) podataka.

— **opća pravila i/ili pravna obavijest, obveze, odgovornosti** u pouzdanom popisu;

— **datum i vrijeme izdavanja** pouzdanog popisa;

— **sljedeće planirano ažuriranje** pouzdanog popisa.

3. Jasna identifikacija podataka o svim pružateljima usluga certificiranja koji se nadziru/akreditiraju na temelju programa

Ovom skupinom podataka obuhvaćeno je barem sljedeće:

— naziv pružatelja usluga certificiranja upisanog u službenim pravnim evidencijama (uključujući jedinstveni identifikacijski broj pružatelja usluga certificiranja u skladu s praksom države članice);

— adresu i kontaktne podatke pružatelja usluga certificiranja;

— dodatne podatke o pružatelju usluga certificiranja koji su uključeni izravno ili upućivanjem na mjesto gdje se mogu preuzeti.

4. Za svakog pružatelja usluga certificiranja uvrštenog na popis, niz polja koji obuhvaća jasnu identifikaciju usluge certificiranja koju pruža pružatelj usluga certificiranja i koja se nadzire/akreditira u kontekstu Direktive 1999/93/EZ

Tom skupinom podataka obuhvaćeno je barem sljedeće za svaku uslugu certificiranja pružatelja usluga certificiranja uvrštenog na popis:

— identifikator vrste usluge: identifikator vrste usluge certificiranja (npr. identifikator kojim se označava da je nadzirana/akreditirana usluga certificiranja pružatelja usluga certificiranja certifikacijsko tijelo koje izdaje kvalificirane certifikate);

— (trgovačko) ime usluge: (trgovačko) ime te usluge certificiranja;

— digitalni identitet usluge: jasan jedinstveni identifikator usluge certificiranja;

— trenutačni status usluge: identifikator trenutačnog stanja usluge,

— datum i vrijeme početka trenutačnog statusa

— ekstenzija podataka o usluzi, kad je primjenjivo: dodatni podaci o usluzi (npr. uključeni izravno ili upućivanjem na mjesto na kojem se mogu preuzeti): podaci u vezi s definicijom usluge koje pruža upravitelj sustava, pristupni podaci u vezi s uslugom, podaci u vezi s definicijom usluge koje pruža pružatelj usluge certificiranja i ekstenzije podataka o usluzi. Primjerice za usluge certifikacijskih tijela koja izdaju kvalificirane certifikate, neobvezan niz n-torki informacija, a svakom se n-torkom navode:

  — kriteriji upotrijebljeni za daljnju identifikaciju (filtriranje) unutar utvrđene usluge povjerbe koji preciziraju skupinu izlaznih odrednica usluge (npr. skupinu (kvalificiranih) certifikata) za koju su potrebni/pruženi dodatni podaci povezani s njezinim statusom, naznakama podrške sigurnog sredstva za izradu elektroničkog potpisa i/ili izdavanjem pravnoj osobi; i

  — pripadajući 'kvalifikatori' s kojima se pružaju podaci o tome identificira li skupina izlaznih odrednica certifikate kao kvalificirane, odnosno jesu li utvrđeni kvalificirani certifikati te usluge potkrijepljeni sigurnim sredstvom za izradu potpisa, odnosno podaci o tome jesu li takvi kvalificirani certifikati izdani pravnoj osobi (prema zadanim postavkama treba ih se smatrati izdanima fizičkim osobama).

5. Za svaku uslugu certificiranja navedenu na popisu, povijesne podatke o njezinu statusu.

6. Potpis koji se u svrhu utvrđivanja autentičnosti izračunava od svih polja pouzdanog popisa, izuzev same vrijednosti potpisa.

3. **Smjernice za uređivanje unosa na pouzdanom popisu**

3.1. *Podaci o statusu nadziranih/akreditiranih usluga certificiranja i njihovih pružatelja na jednom popisu*

Pouzdani popis države članice znači "Popis statusa nadzora/akreditacije usluga certificiranja pružatelja usluga certificiranja koje nadzire/akreditira referentna država članica radi udovoljavanja odgovarajućim odredbama Direktive 1999/93/EZ".

Takav pouzdani popis jedini je instrument koji relevantna država članica rabi za pružanje podataka o statusu nadzora/akreditacije usluga certificiranja i njihovih pružatelja:

— **svih pružatelja usluga certificiranja**, kako je utvrđeno člankom 2. stavkom 11. Direktive 1999/93/EZ, odnosno „subjekt odnosno pravna ili fizička osoba koja izdaje certifikate ili pruža druge usluge koje se odnose na elektroničke potpise";

— **koji se nadziru/akreditiraju** radi udovoljavanja odgovarajućim odredbama utvrđenima Direktivom 1999/93/EZ.

Pri razmatranju definicija i odredaba utvrđenih Direktivom 1999/93/EZ, posebice u pogledu relevantnih pružatelja usluga certificiranja i njihovih sustava nadzora/dragovoljne akreditacije, razlikujemo dvije skupine pružatelja usluga certificiranja: pružatelje usluga certificiranja koji izdaju kvalificirane certifikate za javnost i pružatelje usluga certificiranja koji ne izdaju kvalificirane certifikate za javnost nego pružaju „druge (pomoćne) usluge povezane s elektroničkim potpisima":

— **Pružatelji usluga certificiranja koji izdaju kvalificirane certifikate**:

  — Mora ih nadzirati država članica u kojoj imaju poslovni nastan (ako imaju poslovni nastan u državi članici), a može ih se i akreditirati, radi udovoljavanja odredbama utvrđenima Direktivom 1999/93/EZ, uključujući zahtjeve iz Priloga I. (Zahtjevi za kvalificirane certifikate) i zahtjeve iz Priloga II. (Zahtjevi za pružatelje usluga certificiranja koji izdaju kvalificirane certifikate). Pružatelji usluga certificiranja koji izdaju kvalificirane certifikate, a akreditirani su u državi članici i dalje moraju biti uključeni u odgovarajući sustav nadzora te države članice, osim ako nemaju poslovni nastan u toj državi članici.

— Sustav „nadzora“ (odnosno sustav „dragovoljne akreditacije“) koji se primjenjuje utvrđen je i mora udovoljiti odgovarajućim zahtjevima iz Direktive 1999/93/EZ, posebice onima utvrđenima člankom 3. stavkom 3., člankom 8. stavkom 1., člankom 11., uvodnom odredbom (13.) (odnosno člankom 2. stavkom 13., člankom 3. stavkom 2., člankom 7. stavkom 1.(a), člankom 8. stavkom 1., člankom 11., uvodnim odredbama (4.), (11.), (12.) i (13.)).

— **Pružatelji usluga certificiranja koji ne izdaju kvalificirane certifikate**:

— Mogu biti uključeni u sustav „dragovoljne akreditacije“ (kako je utvrđeno Direktivom 1999/93/EZ i u skladu s njom) i/ili u nacionalno utvrđen „priznat program odobrenja” proveden na nacionalnoj osnovi za nadzor nad udovoljavanjem odredbama utvrđenima tom Direktivom i, ako je moguće, nacionalnim odredbama o pružanju usluga certificiranja (u smislu članka 2. stavka 11. Direktive 1999/93/EZ).

— Neki fizički ili binarni (logički) objekti generirani ili izdani kao posljedica pružanja usluge certificiranja mogu imati pravo na specifičnu „kvalifikaciju” na osnovu svoje sukladnosti s odredbama i zahtjevima utvrđenima na nacionalnoj razini, ali značenje takve „kvalifikacije” vjerojatno je ograničeno isključivo na nacionalnu razinu.

Svaka država članica mora uspostaviti i održavati samo jedan pouzdani popis za naznačavanje statusa nadzora i/ili akreditacije usluga certificiranja koje pružaju pružatelji usluga certificiranja koje nadzire/akreditira država članica. U pouzdani potpis uključeni su barem oni pružatelji usluga certificiranja koji izdaju kvalificirane certifikate. U pouzdanom popisu može biti naznačen i status drugih usluga certificiranja koje se nadziru ili akreditiraju prema nacionalno utvrđenom programu odobrenja.

3.2. *Pojedinačna skupina vrijednosti statusa nadzora/akreditacije*

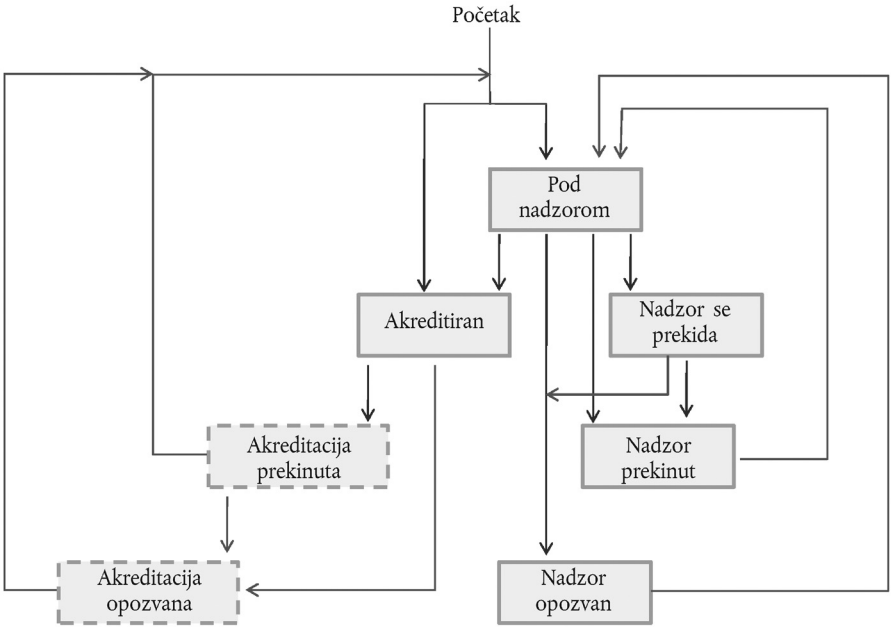
Činjenica da se usluga trenutačno „nadzire” ili „akreditira” na prikazana je na pouzdanom popisu kao vrijednost njezina trenutačnog statusa. Usto, status nadzora ili akreditacije može biti pozitivan („pod nadzorom”, „akreditirana”, „nadzor obustavljen”), prekinut („nadzor prekinut”, „akreditacija prekinuta”) ili čak opozvan („nadzor opozvan”, „akreditacija opozvana”) i postavljen na odgovarajuću vrijednost. Tijekom svog životnog vijeka, ista usluga certificiranja može prelaziti iz statusa nadzora u status akreditacije i obrnuto [1].

Slika 1. opisuje očekivani tijek usluge certificiranja između mogućih statusa nadzora/akreditacije:

[1] Npr. pružatelj usluga certificiranja s poslovnim nastanom u državi članici koji pruža uslugu certificiranja koju država članica (nadzorno tijelo) isprva nadzire nakon nekog vremena, može odlučiti prijeći na dragovoljnu akreditaciju za trenutačno nadziranu uslugu certificiranja. Obratno, pružatelj usluga certificiranja u drugoj državi članici može odlučiti ne prekinuti akreditiranu uslugu certificiranja i premjestiti je iz statusa akreditacije u status nadzora, npr. iz poslovnih i/ili gospodarskih razloga.

Slika 1.

Očekivani tijek statusa nadzora/akreditacije jedne usluge pružatelja usluga certificiranja



Legend:

Prijelazni status kad postoji pripadajući nadzorni model (npr. za pružatelja usluga certificiranja koji izdaje kvalificirane certifikate, a koji se akreditira i nadzire u državi članici u kojoj ima poslovni nastan),
Moguć trenutačni status kad ne postoji pripadajući nadzorni model (npr. za pružatelja usluga certificiranja koji se akreditira u državi članici u kojoj nema poslovni nastan)

Moguć trenutačni status

Pružatelj usluge certificiranja koji izdaje kvalificirane certifikate s poslovnim nastanom u državi članici mora biti nadziran (od strane države članice u kojoj ima poslovni nastan) i može biti dragovoljno akreditiran. Vrijednost statusa takve usluge, kad je uvrštena na pouzdani popis, mora imati jednu od gore prikazanih vrijednosti kao „trenutačnu vrijednost statusa", u skladu sa svojim stvarnim statusom, i mora se mijenjati, kad je primjenjivo, prema gore prikazanom tijeku statusa. Međutim, obje vrijednosti „akreditacija istekla " i „akreditacija opozvana" moraju biti vrijednosti „prijelaznog statusa" kad se odgovarajuća usluga pružatelja usluga certificiranja koji izdaje kvalificirane certifikate nalazi na pouzdanom popisu države članice u kojoj pružatelj ima poslovni nastan, jer se takva usluga prema zadanim postavkama mora nadzirati (čak i ako nije akreditiran ili ako više nije akreditiran); kad je odgovarajuća usluga uvrštena na popis (akreditirana) u državi članici u kojoj pružatelj nema poslovni nastan, te vrijednosti mogu biti konačne vrijednosti.

Države članice koje utvrđuju ili su utvrdile nacionalno utvrđen "priznat program/priznate programe odobrenja" proveden/ provedene na nacionalnoj osnovi za nadzor sukladnosti usluga pružatelja usluga certificiranja koji **ne** izdaju kvalificirane certifikate s odredbama utvrđenima Direktivom 1999/93/EZ i mogućim nacionalnim odredbama o pružanju usluga certificiranja (u smislu članka 2. stavka 11. Direktive 1999/93/EZ), takav program/takve programe odobrenja moraju svrstati u sljedeće dvije kategorije:

— „dragovoljna akreditacija" kako je utvrđeno i uređeno Direktivom 1999/93/EZ (članak 2. stavak 13., članak 3. stavak 2., članak 7. stavak 1.(a), članak 8. stavak 1., članak 11., uvodne napomene (4.), (11.), (12.) i (13.));

— „nadzor"' prema zahtjevima Direktive 1999/93/EZ proveden nacionalnim odredbama i zahtjevima u skladu s nacionalnim zakonima.

U skladu s tim, pružatelj usluga certificiranja koji ne izdaje kvalificirane certifikate može biti nadziran ili dragovoljno akreditiran. Vrijednost statusa takve usluge uvrštene na pouzdani popis mora imati jednu od gore prikazanih vrijednosti statusa kao svoju "trenutačnu vrijednost statusa" (vidi sliku 1.), u skladu sa svojim stvarnim statusom i mora se razvijati, kad je primjenjivo, prema gore prikazanom tijeku statusa.

Pouzdani popis mora sadržavati podatke o temeljnom programu/ temeljnim programima nadzora/akreditacije, a posebice:

— podatak o sustavu nadzora koji se primjenjuje na svakog pružatelja usluga certificiranja koji izdaje kvalificirane certifikate;

— podatak, kad je primjenjivo, o nacionalnom programu „dragovoljne akreditacije“ koji se primjenjuje na svakog pružatelja usluga certificiranja koji izdaje kvalificirane certifikate;

— podatak, kad je primjenjivo, o sustavu nadzora koji se primjenjuje na svakog pružatelja usluga certificiranja koji ne izdaje kvalificirane certifikate;

— podatak, kad je primjenjivo, o nacionalnom programu „dragovoljne akreditacije“ koji se primjenjuje na svakog pružatelja usluga certificiranja koji ne izdaje kvalificirane certifikate;

Posljednje su dvije skupine podataka relevantnim stranama od ključne važnosti za ocjenjivanje razine kakvoće i sigurnosti sustava nadzora/akreditacije koji se na nacionalnoj razini primjenjuju na pružatelje usluga certificiranja koji ne izdaju kvalificirane certifikate. Kad se na pouzdanom popisu nalazi podatak o statusu nadzora/akreditacije u pogledu usluga pružatelja usluga certificiranja koji ne izdaju kvalificirane certifikate, gore spomenute skupine podataka na razini pouzdanog popisa nude se korištenjem polja „Podaci o programu URI“ (točka 5.3.7. – podatke daju države članice), polja „Vrsta programa/zajednica/pravila” (točka 5.3.9. – korištenjem teksta zajedničkog svim državama članicama te neobveznih specifičnih podataka koje pruža svaka država članica) i polja „Opća pravila/pravne obavijesti“ (točka 5.3.11. – tekst zajednički svim državama članicama iz Direktive 1999/93/EZ, uz mogućnost svake države članice da doda specifičan tekst/upute za državu članicu).

Dodatni podaci povezani s “kvalifikacijom” utvrđeni na razini nacionalnih sustava nadzora/akreditacije za pružatelje usluga certificiranja koji ne izdaju kvalificirane certifikate, mogu se pružiti na razini usluge kad je to primjenjivo i kad se to zahtijeva (npr. za razlikovanje različitih razina kakvoće/sigurnosnih razina) korištenjem polja “Ekstenzija dodatnih podataka o usluzi” (additionalServiceInformation Extension) (točka 5.5.9.4.) kao dio polja “Ekstenzije podataka o usluzi” (točka 5.5.9.). Daljnji podaci povezani s odgovarajućim tehničkim specifikacijaama potanko su izneseni u tehničkim specifikacijama u Poglavlju I.

Unatoč tome što za nadzor i akreditacija usluga certificiranja u državi članici mogu biti zadužena zasebna tijela, očekuje se da se za jednu uslugu certificiranja mora koristiti samo jedan unos i da status nadzora/akreditacije te usluge mora biti ažuriran sukladno tome.

3.3. *Podaci na pouzdanom popisu namijenjeni olakšavanju potvrđivanja kvalificiranog elektroničkog potpisa i naprednog elektroničkog potpisa potkrijepljenog kvalificiranim certifikatom*

Najvažniji je dio izrade pouzdanog popisa utvrđivanje obveznog dijela pouzdanog popisa, odnosno „Popisa usluga” pružatelja usluga certificiranja koji izdaje kvalificirane certifikate, kako bi se ispravno prikazala točna situacija svake usluge certificiranja kojom se izdaju kvalificirani certifikati te kako bi se omogućilo da su podaci navedeni u svakom unosu dostatni da omoguće potvrđivanje kvalificiranog elektroničkog potpisa i naprednog elektroničkog potpisa potkrijepljenog kvalificiranim certifikatom (kad su združeni sa sadržajem kvalificiranog certifikata za krajnje korisnike koji izdaje pružatelj usluga certificiranja prema usluzi certificiranja navedenoj na popisu pod tim unosom).

Potrebni podaci mogu sadržavati i druge podatke osim „Digitalnog identiteta usluge” jednog (izvornog) certifikacijskog tijela, a posebice podatke kojima se utvrđuje status kvalificiranih certifikata koje izdaje takvo certifikacijsko tijelo, kao i podatak o tome jesu li potpisi potkrijepljeni kvalificiranim certifikatima izrađeni sigurnim sredstvom za izradu potpisa. Tijelo koje je država članica imenovala za izradu, uređivanje i održavanje pouzdanog popisa mora zato uzeti u obzir trenutačni profil i sadržaj certifikata u svakom izdanom kvalificiranom certifikatu prema usluzi pružatelja usluga certificiranja koji izdaje kvalificirane certifikate obuhvaćenoj pouzdanim popisom.

U najboljem slučaju, svaki izdani kvalificirani certifikat trebao bi sadržavati izjavu o sukladnosti kvalificiranog certifikata (QcCompliance) ([1]) koju je utvrdio ETSI kad se tvrdi da je certifikat kvalificiran i izjavu o sigurnom sredstvu za izradu potpisa za kvalificirane certifikate (QcSSCD) koju je utvrdio ETSI kad se tvrdi da je pri generiranju elektroničkih potpisa podržan sigurnim sredstvom za izradu potpisa, i/ili da svaki izdani kvalificirani certifikat sadržava Opća pravila kvalificiranog certifikata (QCP), odnosno Opća pravila kvalificiranog certifikata (QCP)+ identifikatore objekta općih pravila certifikata (QCP/QCP+ certificate policy Object Identifiers (OIDs)) utvrđene normom ETSI EN 319 411-2 ([2]). Primjena drugih normi kao smjernica od strane pružatelja usluga certificiranja koji izdaju kvalificirane certifikate, široka tumačenja tih normi, kao i neupoznatost s postojanjem i prioritetom pojedinih normativnih tehničkih specifikacija ili normi, za posljedicu ima razlike u stvarnom sadržaju trenutačno izdanih kvalificiranih certifikata (npr. uporaba odnosno neuporaba Izjava o kvalificiranim certifikatima koje je utvrdio ETSI) pa zato sprečavaju stranke koje primaju certifikate da se jednostavno oslone na potpisnikov certifikat (i s njim povezan certifikacijski lanac/stazu) za ocjenjivanje, barem na strojno čitljiv način, je li certifikat kojim je potkrijepljen elektronički potpis kvalificirani certifikat ili ne te je li povezan sa sigurnim sredstvom za izradu potpisa kojim je elektronički potpis izrađen.

([1]) Za definiciju takve izjave vidi ETSI EN 319 412-5 Elektronički potpisi i infrastrukture (ESI) – Profili za pružatelje usluga povjerbe koji izdaju certifikate – 5. dio: Ekstenzije za profile kvalificiranih certifikata).

([2]) ETSI EN 319 411-2 – Elektronički potpisi i infrastrukture (ESI) – Opća pravila i sigurnosni zahtjevi za pružatelje usluga povjerbe koji izdaju certifikate – 2. dio: Zahtjevi za opća pravila za certifikacijska tijela koja izdaju kvalificirane certifikate.

Popunjavanje polja „Identifikator vrste usluge“ („Sti“), „Naziv usluge“ („Sn“) i „Digitalni identitet usluge“ („Sdi”) u unosu o usluzi na pouzdanom popisu s podacima iz polja „Ekstenzije podataka o usluzi“ („Sie“) omogućuje potpuno određivanje specifične vrste kvalificiranog certifikata izdanog od strane pružatelja usluga certificiranja koji izdaje kvalificirane certifikate i pruža podatak je li certifikat podržan sigurnim sredstvom za izradu potpisa (kad izdani kvalificirani certifikat ne sadržava taj podatak). S tim poljem povezani su specifični podaci iz polja „Trenutačni status usluge“ („Scs“). To je prikazano na slici 2. u nastavku.

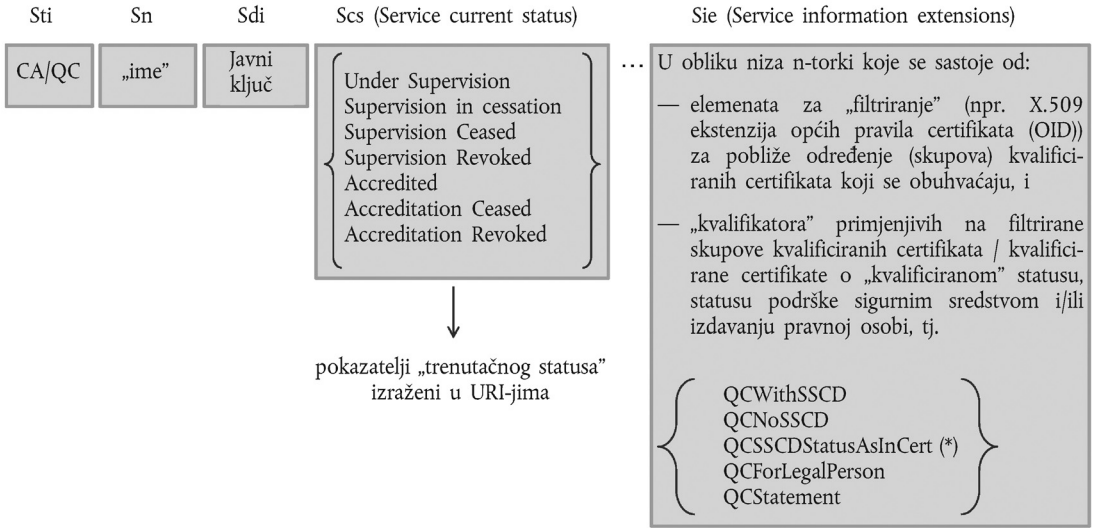
Unošenje usluge na popis pružanjem samo „Digitalnog identiteta usluge“ („Sdi”) (izvornog) certifikacijskog tijela, značilo bi da je omogućeno (od strane pružatelja usluga certificiranja koji izdaju kvalificirane certifikate, ali i od strane tijela za nadzor/akreditaciju zaduženog za nadzor/akreditaciju tog pružatelja usluga certificiranja) da bilo koji certifikat za krajnje korisnike izdan pod tim (izvornim) certifikacijskim tijelom (hijerarhija) sadržava dovoljno strojno obradivih podataka koje je utvrdio ETSI da u kvalificiranom certifikatu nema strojno obradive naznake utvrđene u okviru ETSI normi o tome je li certifikat podržan sigurnim sredstvom za izradu potpisa), a uvrštavanjem na popis samo „Digitalnog identiteta usluge“ (“Sdi”) tog (izvornog) certifikacijskog tijela može se pretpostaviti samo da kvalificirani certifikati izdani pod hijerarhijom tog (izvornog) certifikacijskog tijela nisu podržani ni jednim sigurnim sredstvom za izradu potpisa. Kako bi se naznačilo da se ti kvalificirani certifikati moraju smatrati podržanima sigurnim sredstvom za izradu potpisa, treba koristiti polje „Ekstenzije podataka o usluzi“ („Sie“) (što ujedno označava da za taj podatak jamči pružatelj usluga certificiranja koji izdaje kvalificirane certifikate kojeg nadzire/akreditira nadzorno tijelo odnosno tijelo za akreditaciju).

Slika 2.

Unos o usluzi za uvrštenog pružatelja usluga certificiranja koji izdaje kvalificirane certifikate na pouzdanom popisu

Opća načela – Pravila uređivanja – unosi za CSP_{QC} (usluge uvrštene na popis)

Unos o usluzi za CSP_{QC} uvrštenog na popis:



(*) znači da su ti podaci sadržani u svakom kvalificiranom certifikatu pod Sdi-[Sie] određenog CA/QC (ako nisu u kvalificiranom certifikatu, znači nema sigurnog sredstva za izradu potpisa)

Ove tehničke specifikacije za zajednički obrazac pouzdanog popisa omogućuju uporabu kombinacije pet osnovnih dijelova podataka u unosu o usluzi:

— „Identifikator vrste usluge“ („Sti“), npr. kojim se identificira certifikacijsko tijelo koje izdaje kvalificirane certifikate („CA/QC”);

— „Ime usluge“ („Sn“);

— „Digitalni identitet usluge“ (“Sdi”), podatak kojim se identificira usluga uvrštena na popis, npr. (barem) javni ključ certifikacijskog tijela koje izdaje kvalificirane certifikate;

— za usluge certifikacijskog tijela koje izdaje kvalificirane certifikate, neobvezni podaci u polju „Ekstenzija podataka o usluzi“ („Sie“) koji omogućuju uključivanje nekoliko stavki podataka povezanih sa specifičnim uslugama u pogledu opoziva isteklih certifikata, dodatnih obilježja kvalificiranog certifikata, preuzimanja pružatelja usluga certificiranja od strane drugog pružatelja usluga certificiranja te drugih dodatnih podataka o usluzi. Primjerice, dodatna obilježja kvalificiranih certifikata predstavljena su nizom jedne ili nekoliko n-torki, a svakom se n-torkom navode:

  — kriteriji koji se koriste za daljnju identifikaciju (filtriranje) usluge certificiranja utvrđene podacima u polju „Digitalni identitet usluge“ koji preciziraju skupinu kvalificiranih certifikata za koju su potrebni/pruženi dodatni podaci povezani s naznakom statusa „kvalifikacije“, podrške sigurnog sredstva za izradu potpisa i/ili izdavanja pravnoj osobi; i

  — pripadajuće podatke („kvalifikatori“) o tome hoće li se taj skup kvalificiranih certifikata smatrati „kvalificiranim“, je li podržan sigurnim sredstvom za izradu potpisa i jesu li pripadajući podaci dio kvalificiranog certifikata prema normiziranom strojno obradivom obliku, odnosno podatke u vezi s činjenicom da su takvi kvalificirani certifikati izdani pravnim osobama (prema zadanim postavkama treba ih se smatrati izdanima samo fizičkim osobama).

— podaci o „trenutačnom statusu“ unosa o usluzi koji pružaju podatak:

  — o tome je li riječ o usluzi koja se nadzire ili o usluzi koja se akreditira, te

  — samom statusu nadzora/akreditacije.

3.4. *Smjernice za uređivanje i uporabu unosa o usluzi pružatelja usluga certificiranja koji izdaju kvalificirane certifikate*

Opće smjernice za uređivanje su:

1. Kada je za uslugu uvrštenu na popis i utvrđenu prema „Digitalnom identitetu usluge” („Sdi”) omogućeno (jamstvo pruža pružatelj usluga certificiranja koji izdaje kvalificirane certifikate, a nadzire/akreditira ga nadzorno tijelo/tijelo za akreditaciju) da svaki kvalificirani certifikat koji nije podržan sigurnim sredstvom za izradu potpisa sadržava Izjavu o sukladnosti kvalificiranog certifikata (QcCompliance statement) utvrđenu u okviru ETSI normi i da sadržava Izjavu o sigurnom sredstvu za izradu potpisa za kvalificirane certifikate i/ili identifikatora objekta Općih pravila kvalificiranog certifikata+ (QCP+ Object Identifier (OID)), tada je korištenje odgovarajućeg „Digitalnog identiteta usluge“ („Sdi“) dovoljno, a uporaba polja „Ekstenzija podataka o usluzi“ („Sie“) je neobvezna i ne mora sadržavati podatak povezan s podrškom sigurnog sredstva za izradu potpisa.

2. Kada je za uslugu uvrštenu na popis i utvrđenu prema „Digitalnom identitetu usluge” („Sdi”) omogućeno (jamstvo pruža pružatelj usluga certificiranja koji izdaje kvalificirane certifikate, a nadzire/akreditira ga nadzorno tijelo/tijelo za akreditaciju) da svaki kvalificirani certifikat koji nije podržan sigurnim sredstvom za izradu potpisa sadržava Izjavu o sukladnosti kvalificiranog certifikata i/ili identifikatora objekta Općih pravila kvalificiranog certifikata+ (QCP OID) te da ne sadržava Izjavu o sigurnom sredstvu za izradu potpisa za kvalificirane certifikate ili identifikator objekta Općih pravila kvalificiranog certifikata+ (QCP+ OID), tada je korištenje odgovarajućeg „Digitalnog identiteta usluge” („Sdi”) dovoljno, a korištenje polja „Ekstenzija podataka o usluzi” („Sie”) je neobvezno i ne mora sadržavati podatak u vezi podrške sigurnog sredstva za izradu potpisa (što znači da nije podržan sigurnim sredstvom za izradu potpisa).

3. Kada je za uslugu navedenu na popisu i utvrđenu prema “Digitalnom identitetu usluge” (“Sdi”) omogućeno (jamstvo daje pružatelj usluga certificiranja koji izdaje kvalificirane certifikate, a nadzire/akreditira ga nadzorno tijelo/tijelo za akreditaciju) da svaki kvalificirani certifikat koji nije podržan sigurnim sredstvom za izradu potpisa sadržava Izjavu o sukladnosti kvalificiranog certifikata te da su neki od tih kvalificiranih certifikata predodređeni da budu podržani sigurnim sredstvom za izradu potpisa, a neki ne (to se, primjerice, može razlikovati različitim specifičnim identifikatorima objekta općih pravila certifikata pružatelja usluga certificiranja (CSP specific Certificate Policy OIDs) ili nekim drugim specifičnim podacima pružatelja usluga certificiranja koje kvalificirani certifikat sadržava, izravno ili neizravno, strojno obradivo ili ne), ali da certifikat koji je podržan sigurnim sredstvom za izradu potpisa NE sadržava Izjavu o sigurnom sredstvu za izradu potpisa za kvalificirane certifikate NITI NE sadržava identifikator objekta Općih pravila kvalificiranog certifikata+ u okviru ETSI normi (ETSI QCP(+) OID), tada uporaba odgovarajućeg „Digitalnog identiteta usluge“ („Sdi“) možda neće biti dostatna, A korištenje polja „Ekstenzija podataka o usluzi“ („Sie”) je obvezno zbog jasnog naznačavanja podatka o tome je li certifikat podržan sigurnim sredstvom za izradu potpisa, kao i moguće ekstenzije podataka zbog identifikacije obuhvaćene skupine certifikata. To će najvjerojatnije, pri korištenju polja „Ekstenzija podataka o usluzi“ („Sie”), zahtijevati uključivanje različitih „vrijednosti podataka u vezi podrške sigurnog sredstva za izradu potpisa” za isti „Digitalni identitet usluge” („Sdi”).

4. Kada je za uslugu uvrštenu na popis i utvrđenu prema „Digitalnom identitetu usluge” („Sdi”) omogućeno (jamstvo daje pružatelj usluga certificiranja koji izdaje kvalificirane certifikate, a nadzire/akreditira ga nadzorno tijelo/tijelo za akreditaciju) da svaki kvalificirani certifikat ne sadržava Izjavu o sukladnosti kvalificiranog certifikata, identifikator objekta općih pravila kvalificiranog certifikata (QCP OID), Izjavu o sigurnom sredstvu za izradu potpisa za kvalificirane certifikate ni identifikator objekta Općih pravila kvalificiranog certifikata+ (QCP+ OID), ali je omogućeno da neki od certifikata za krajnje korisnike izdani prema tom „Digitalnom identitetu usluge” (“Sdi”) budu predodređeni da budu kvalificirani certifikati i/ili podržani sigurnim sredstvima za izradu potpisa, a neki ne (to se, primjerice može razlikovati različitim specifičnim identifikatorima objekta općih pravila certifikata pružatelja usluga certificiranja ili nekim drugim specifičnim podacima pružatelja usluga certificiranja koje kvalificirani certifikat sadržava, izravno ili neizravno, strojno obradivo ili ne), tada korištenje odgovarajućeg „Digitalnog identiteta usluge“ („Sdi”) neće biti dovoljno, a korištenje polja „Ekstenzija podataka o usluzi” („Sie”) je obvezno zbog jasnog naznačavanja podataka o kvalifikaciji certifikata. To će najvjerojatnije, pri korištenju polja „Ekstenzije podataka o usluzi” („Sie”) zahtijevati uključivanje različitih „vrijednosti podataka u pogledu podrške sigurnog sredstva za izradu potpisa” za isti „Digitalni identitet usluge” („Sdi”).

Prema općem zadanom načelu, za svakog pružatelja usluga certificiranja koji se nalazi na pouzdanom popisu dopušten je jedan unos usluge po jednom javnom ključu za uslugu certifikacije koju pruža certifikacijsko tijelo koje izdaje kvalificirane certifikate, odnosno po certifikacijskom tijelu (izravno) koje izdaje kvalificirane certifikate. U nekim izvanrednim okolnostima i pomno upravljanim uvjetima, nadzorno tijelo/tijelo za akreditaciju države članice kao „Digitalni identitet usluge“ („Sdi”) jednog unosa s popisa usluga tog pružatelja usluga certificiranja navedenog na popisu, može odlučiti koristiti javni

ključ izvornog certifikacijskog tijela ili certifikacijskog tijela više razine unutar infrastrukture javnog ključa (PKI) pružatelja usluga certificiranja (primjerice, u kontekstu hijerarhije certifikacijskih tijela pružatelja usluga certificiranja, od početnog certifikacijskog tijela do certifikacijskih tijela koja izdaju certifikate) umjesto da navodi sva certifikacijska tijela niže razine koja izdaju certifikate (primjerice, navodeći certifikacijsko tijelo koje ne izdaje kvalificirane certifikate za krajnje korisnike izravno nego certificira hijerarhiju certifikacijskih tijela do certifikacijskih tijela koja izdaju kvalificirane certifikate krajnjim korisnicima). Države članice pri provedbi moraju pomno razmotriti posljedice (prednosti i nedostatke) korištenja takvog jednog javnog ključa izvornog certifikacijskog tijela ili javnog ključa certifikacijskog tijela više razine kao vrijednosti „Digitalnog identiteta usluge“ („Sdi”) kada uvrštavaju usluge na pouzdani potpis. Štoviše, u slučaju primjene te odobrene iznimke zadanog načela, država članica mora pružiti nužnu dokumentaciju kako bi olakšala izgradnju certifikacijske staze i potvrdu valjanosti. Na primjer, u kontekstu pružatelja usluga certificiranja koji izdaju kvalificirane certifikate, korištenje jednog izvornog certifikacijskog tijela pod kojim se nalazi nekoliko certifikacijskih tijela koja izdaju kvalificirane certifikate i certifikacijskih tijela koja ne izdaju kvalificirane certifikate, ali za koje kvalificirani certifikati sadrže samo Izjavu o sukladnosti kvalificiranog certifikata i ne naznačuju je li certifikat podržan sigurnim sredstvom za izradu potpisa, navođenje „Digitalnog identiteta usluge“ („Sdi“) izvornog certifikacijskog tijela, prema gore objašnjenim pravilima, značilo bi samo da sigurno sredstvo za izradu potpisa ne podržava ni jedan kvalificirani certifikat koji je izdan pod tim izvornim certifikacijskim tijelom. Postoje li kvalificirani certifikati koje sigurno sredstvo za izradu potpisa doista podržava, a nema strojno obradivih prikaza koji bi naznačili da oni sadrže takvu podršku, svesrdno se preporučuje da se uz buduće izdane kvalificirane certifikate koristi Izjava o sigurnom sredstvu za izradu potpisa za kvalificirane certifikate. U međuvremenu (dok ne isteke posljednji kvalificirani certifikat koji ne sadržava taj podatak), u pouzdanom popisu treba koristiti polje „Ekstenzija podataka o usluzi” („Sie”) i pripadajuće polje „Ekstenzija kvalifikacija”, primjerice pružajući podatke za filtriranje identifikacijskih skupova certifikata korištenjem specifičnih identifikatora objekata utvrđenih od strane pružatelja usluga certificiranja koji izdaju kvalificirane certifikate, a koje pružatelji usluga certificiranja koji izdaju kvalificirane certifikate mogu koristiti za razlikovanje različitih vrsta kvalificiranih certifikata (neki podržani sigurnim sredstvom za izradu potpisa, a neki ne) te za povezivanje jasnog „podatka povezanog s podrškom sigurnog sredstva za izradu potpisa” s tim utvrđenim (filtriranim) skupovima certifikata korištenjem „Kvalifikatora”.

Opće smjernice za korištenje za aplikacije, usluge ili proizvode s elektroničkim potpisima koji se oslanjaju na pouzdani popis i udovoljavaju ovim tehničkim specifikacijama:

Unos „Certifikacijsko tijelo koje izdaje kvalificirane certifikate” „Identifikator vrste usluge” („CA/QC” “Sti”) (odnosno unos “Certifikacijsko tijelo koje izdaje kvalificirane certifikate” koji se korištenjem polja „Ekstenzija dodatnih podataka o usluzi” (“Sie” additionalServiceInformation Extension) dalje kvalificira kao izvorno certifikacijsko tijelo koje izdaje kvalificirane certifikate)

— označava da su svi certifikati za krajnje korisnike certifikacijskog tijela navedenog u polju „Digitalni identitet usluge” (slično je u hijerarhiji certifikacijskih tijela počevši od izvornog certifikacijskog tijela navedenog u polju „Digitalni identitet usluge”) kvalificirani certifikati, **pod uvjetom** da se u certifikatu tvrdi da je takav zbog korištenja odgovarajuće strojno obradive Izjave o kvalificiranim certifikatima (odnosno Izjave o sukladnosti kvalificiranog certifikata) i/ili identifikatora objekta Općih pravila kvalificiranog certifikata+ (QCP(+) OIDs) utvrđenih u okviru ETSI normi (što omogućuje nadzorno tijelo/tijelo za akreditaciju; vidi gore navedene „Opće smjernice za uređivanje”).

  Napomena: kada u polju „Ekstenzija podataka o usluzi” „Ekstenzija kvalifikacija” („Sie” „Qualifications Extension”) nema podataka ili ako certifikat za krajnjeg korisnika za koji se tvrdi da je kvalificiran nije dalje utvrđen podacima u pripadajućem polju „Ekstenzija podataka o usluzi” „Ekstenzija kvalifikacija”, tada se nadzire/akreditira točnost strojno obradivih podataka iz kvalificiranog certifikata. To znači da je omogućeno da korištenje (ili nekorištenje) odgovarajućih Izjava o kvalificiranim certifikatima (odnosno Izjave o sukladnosti kvalificiranog certifikata i Izjave o sigurnom sredstvu za izradu potpisa za kvalificirane certifikate) i/ili identifikatora objekta Općih pravila kvalificiranog certifikata+ (QCP(+) OIDs) utvrđenih u okviru ETSI normi bude u skladu s onime što tvrdi pružatelj usluga certificiranja koji izdaje kvalificirane certifikate.

— **i KADA** polje „Ekstenzija podataka o usluzi” „Ekstenzija kvalifikacija” („Sie” „Qualifications Extension”) sadržava podatke, tada se uz gore navedeno zadano pravilo tumačenja korištenja ti certifikati utvrđeni korištenjem podatka u polju “Ekstenzija podataka o usluzi” “Ekstenzija kvalifikacija”, ustrojenom prema načelu niza filtara za daljnju identifikaciju skupine certifikata, moraju promatrati u skladu s pripadajućim kvalifikatorima koji nude dodatne podatke u pogledu statusa kvalifikacije certifikata, „Podrške sigurnog sredstva za izradu potpisa“ i/ili „Pravne osobe kao subjekta” (primjerice, certifikati koji u ekstenziji općih pravila certifikata sadrže specifični identifikator objekta i/ili imaju specifičan model „Korištenja ključa“, i/ili su filtrirani korištenjem neke specifične vrijednosti koja se pojavljuje u nekom specifičnom polju certifikata ili ekstenziji itd.). Ti su kvalifikatori dio sljedeće skupine „Kvalifikatora” koji se primjenjuju za nadoknađivanje manjka podataka u sadržaju odgovarajućeg kvalificiranog certifikata i koriste se za:

  — naznaku statusa kvalifikacije certifikata: Izjava o kvalificiranim certifikatima u značenju da je utvrđeni certifikat odnosno utvrđeni certifikati kvalificirani;

    I/ILI

  — naznaku naravi podrške sigurnog sredstva za izradu potpisa

    — „QCWithSSCD” je vrijednost koja označava da je „Kvalificirani certifikat podržan sigurnim sredstvom za izradu potpisa”, ili

    — „QCNoSSCD” je vrijednost koja označava da „Kvalificirani certifikat nije podržan sigurnim sredstvom za izradu potpisa”, ili

    — „QCSSCDStatusAsInCert” je vrijednost koja označava da je omogućeno da svaki kvalificirani certifikat prema podacima u poljima „Digitalni identitet usluge“ - „Ekstenzija podataka o usluzi” („Sdi”-„Sie”) u unosu tog certifikacijskog tijela koje izdaje kvalificirane certifikate sadržava podatak u vezi podrške sigurnog sredstva za izradu potpisa;

    I/ILI

— naznaku izdavanja pravnoj osobi:

— „QCForLegalPerson" je vrijednost koja označava da je „Certifikat izdan pravnoj osobi"

3.5. *Usluge koje podržavaju usluge certifikacijskog tijela koje izdaje kvalificirane certifikate, ali nisu dio "Digitalnog identiteta usluge" certifikacijskog tijela koje izdaje kvalificirane certifikate*

Usluge statusa valjanosti certifikata koje se odnose na kvalificirane certifikate za koje podatak o statusu valjanosti certifikata (npr. odgovori CRL (Popisi opozvanih certifikata) i odgovori OCSP (Protokola za status certifikata)) potpisuje subjekt čiji privatni ključ nije certificiran prema certifikacijskoj stazi koja vodi do certifikacijskog tijela koje izdaje kvalificirane certifikate navedenog na popisu, uključuju uvrštavaju se na pouzdani popis navođenjem tih usluga statusa valjanosti certifikata kao takvih na pouzdani popis (odnosno s vrstom usluge „OCSP/QC", odnosno „CRL/QC"), s obzirom na to da se te usluge mogu smatrati dijelom nadziranih/akreditiranih „kvalificiranih" usluga koje se odnose na pružanje usluga certificiranja kvalificiranih certifikata. Dakako, odgovori OCSP ili izdavatelji CRL certifikata čije certifikate potpisuju certifikacijska tijela prema hijerarhiji navedenih usluga certifikacijskih tijela koja izdaju kvalificirane certifikate, smatrat će se „valjanima" i u skladu s vrijednošću statusa navedene usluge certifikacijskog tijela koje izdaje kvalificirane certifikate.

Slična se odredba može primijeniti na usluge certificiranja koje izdaju nekvalificirane certifikate (vrste usluge "CA/PKC").

U pouzdani popis uključene se usluge statusa valjanosti certifikata kad certifikati za krajnje korisnike na koje se usluge statusa valjanosti certifikata odnose ne sadrže pripadajući podatak o lokaciji za takve usluge.

4. **Definicije i kratice**

Za potrebe ovog dokumenta primjenjuju se sljedeće definicije i kratice:

Izraz	Izvorna kratica	Definicija
Pružatelj usluga certificiranja	CSP	Kako je utvrđeno člankom 2. stavkom 11. Direktive 1999/93/EZ.
Certifikacijsko tijelo	CA	1) pružatelj usluga certificiranja koji izrađuje i dodjeljuje certifikate javnog ključa; ili 2) tehnička služba za generiranje certifikata koju pružatelj usluga certificiranja koristi za izradu i dodjeljivanje certifikata javnog ključa. *NAPOMENA*: za dodatno objašnjenje pojma certifikacijsko tijelo vidi točku 4. dokumenta EN 319 411-2 ([1]).
Certifikacijsko tijelo koje izdaje kvalificirane certifikate	CA/QC	Certifikacijsko tijelo koje udovoljava zahtjevima utvrđenim u Prilogu II. Direktive 1999/93/EZ i izdaje kvalificirane certifikate koji udovoljavaju zahtjevima utvrđenima u Prilogu I. Direktive 1999/93/EZ.
Certifikat	Certificate	Kako je utvrđeno člankom 2. stavkom 9. Direktive 1999/93/EZ.
Kvalificirani certifikat	QC	Kako je utvrđeno člankom 2. stavkom 10. Direktive 1999/93/EZ.
Potpisnik	Signatory	Kako je utvrđeno člankom 2. stavkom 3. Direktive 1999/93/EZ.
Nadzor	Supervision	Odnosi se na nadzor predviđen člankom 3. stavkom 3. Direktive 1999/93/EZ. Direktiva 1999/93 od država članica zahtjeva uspostavljanje odgovarajućeg sustava koji dopušta nadzor nad pružateljima usluga certificiranja koji imaju poslovni nastan na njihovim državnim područjima te izdaju kvalificirane certifikate za javnost, omogućujući nadzor nad udovoljavanjem odredbama utvrđenima tom Direktivom.
Dragovoljna akreditacija	Accreditation	Kako je utvrđeno člankom 2. stavkom 13. Direktive 1999/93/EZ.
Pouzdani popis pružatelja usluga certificiranja	TL	Označava popis koji označava status nadzora/akreditacije usluga certificiranja pružatelja usluga certificiranja koje referentna država članica nadzire/akreditira radi udovoljavanja odredbama utvrđenima Direktivom1999/93/EZ.

Izraz	Izvorna kratica	Definicija
Popis statusa usluge povjerbe	TSL	Oblik potpisanog popisa koji se koristi kao osnova za prikaz podatka o statusu usluge povjerbe u skladu sa specifikacijama utvrđenima u ETSI TS 119 612.
Usluga povjerbe		Usluga koja povećava povjerenje u elektroničke transakcije (za koje se obično, ali ne i nužno, koriste kriptografske tehnike ili kojima su obuhvaćeni povjerljivi materijal (ETSI TS 119 612). *NAPOMENA*: ovaj izraz ima širu primjenu od usluge certificiranja koja izdaje certifikate ili pruža druge usluge koje se odnose na elektroničke potpise.
Pružatelj usluga povjerbe	TSP	Tijelo koje upravlja jednom (elektroničkom) uslugom povjerbe ili više njih (izraz ima širu primjenu od pružatelja usluga certificiranja).
Token usluge povjerbe	TrST	Fizički ili binaran (logički) objekt generiran ili izdan kao posljedica korištenja usluge povjerbe. Primjeri binarnih tokena usluga povjerbe su certifikati, popisi opoziva certifikata (CRL), vremenske oznake i odgovori OCSP (Online Certificate Status Protocol).
Kvalificiran elektronički potpis	QES	Napredan elektronički potpis potkrijepljen kvalificiranim certifikatom i izrađen sigurnim sredstvom za izradu potpisa kako je utvrđeno člankom 2. Direktive 1999/93/EZ.
Napredan elektronički potpis	AdES	Kako je utvrđeno člankom 2. stavkom 2. Direktive 1999/93/EZ.
Napredan elektronički potpis podržan kvalificiranim certifikatom	$AdES_{QC}$	Znači elektronički potpis koji udovoljava zahtjevima naprednog elektroničkog potpisa i potkrijepljen je kvalificiranim certifikatom kako je utvrđeno člankom 2. Direktive 1999/93/EZ.
Sigurno sredstvo za izradu potpisa	SSCD	Kako je utvrđeno člankom 2. stavkom 6. Direktive 1999/93/EZ.

([1]) EN 319 411-2: Elektronički potpisi i infrastrukture (ESI); Opća pravila i sigurnosni zahtjevi za pružatelje usluga povjerbe; 2. dio: Zahtjevi za opća pravila za certifikacijska tijela koja izdaju kvalificirane certifikate.

U sljedećim poglavljima ključne riječi istaknute velikim tiskanim slovima „MORA“, „NE SMIJE“, „ZAHTIJEVA SE“, „TREBAO BI“, „NE BI TREBAO“, „PREPORUČUJE SE“, „MOŽE“ i „NEOBVEZAN“ tumače se kako je opisano u RFC 2119 ([1]).

POGLAVLJE I.

DETALJNE SPECIFIKACIJE ZA ZAJEDNIČKI OBRAZAC „POUZDANOG POPISA NADZIRANIH/AKREDITIRANIH PRUŽATELJA USLUGA CERTIFICIRANJA“

Ove specifikacije oslanjaju se na specifikacije i zahtjeve utvrđene normom ETSI TS 119 612 v1.1.1 (dalje u tekstu ETSI TS 119 612).

Kad ne postoje specifični zahtjevi utvrđeni ovim specifikacijama, PRIMJENJUJU SE u potpunosti zahtjevi utvrđeni normom ETSI TS 119 612 točkama 5. i 6. Kad postoje specifični zahtjevi utvrđeni ovim specifikacijama, oni IMAJU PREDNOST nad odgovarajućim zahtjevima iz norme ETSI TS 119 612. U slučaju neslaganja između ovih specifikacija i specifikacija iz norme ETSI TS 119 612, ove specifikacije VRIJEDE kao normativne.

Ime upravitelja sustava (točka 5.3.4.)

Polje je PRISUTNO i UDOVOLJAVA specifikacijama iz norme TS 119 612 točke 5.3.4.

([1]) IETF RFC 2119: „Ključne riječi za uporabu u RFC-ima kojima se označuju razine zahtjeva”.

Država MOŽE imati zasebno nadzorno tijelo i zasebno tijelo za akreditaciju, čak i zasebna dodatna tijela za sve operativne aktivnosti. Svaka država članica sama određuje upravitelja sustava za svoj pouzdani popis. Očekuje se da nadzorno tijelo, tijelo za akreditaciju i upravitelj sustava (u slučaju kad su zasebna tijela) imaju vlastite obveze i odgovornosti.

Svaka situacija u kojoj je nekoliko tijela odgovorno za nadzor, akreditaciju ili operativne aspekte dosljedno se odražava i identificira kao takva u podacima o programu koji su dio pouzdanog popisa, uključujući podatke specifične za program iz polja "Podaci o programu URI" (točka 5.3.7.).

Ime programa (točka 5.3.6.)

Polje je PRISUTNO i UDOVOLJAVA specifikacijama iz norme TS 119 612 točke 5.3.6., gdje se za program koristi sljedeće ime:

"EN_name_value" = „Popis statusa nadzora/akreditacije certificiranih usluga pružatelja usluga certificiranja koje nadzire/akreditira referentna država članica upravitelja sustava radi udovoljavanja relevantnim odredbama utvrđenima Direktivom 1999/93/EZ Europskog parlamenta i Vijeća od 13. prosinca 1999. o okviru Zajednice za elektroničke potpise".

Podaci o programu URI (točka 5.3.7.)

Polje je PRISUTNO i UDOVOLJAVA specifikacijama iz norme TS 119 612 točke 5.3.7., gdje "Odgovarajući podaci o programu" SADRŽE barem:

— Uvodne podatke zajedničke svim državama članicama u pogledu područja primjene i sadržaja pouzdanog popisa te temeljnog/temeljnih programa nadzora/akreditacije. Opći tekst koji se koristi u donjem tekstu s nizom znakova „[*ime relevantne države članice*]# ZAMJENJUJE SE imenom relevantne države članice:

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

The Trusted List aims at:

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

— allowing for a trusted validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including, when this is not part of the QCs, information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including compliance 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 Article 3(3), Article 8.(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 at a national level on a voluntary basis."

— Specifične podatke o temeljnom/temeljnim programu/programima nadzora/akreditacije, posebice ([1]):

  — podatak o sustavu nadzora primijenjenog na svakog pružatelja usluga certificiranja koji izdaje kvalificirane certifikate;

  — podatak, kad je primjenjivo, o nacionalnom programu ‚dragovoljne akreditacije' primjenjivog na svakog pružatelja usluga certificiranja koji izdaje kvalificirane certifikate;

  — podatak, kad je primjenjivo, o sustavu nadzora primjenjivog na svakog pružatelja usluga certificiranja koji ne izdaje kvalificirane certifikate;

  — podatak, kad je primjenjivo, o nacionalnom programu ‚dragovoljne akreditacije' primjenjivog na svakog pružatelja usluga certificiranja koji ne izdaje kvalificirane certifikate;

  Ti specifični podaci za svaki gore navedeni temeljni program SADRŽE barem sljedeće:

  — opći opis;

  — podatke o postupku kojeg se pridržava nadzorno tijelo/tijelo za akreditaciju u provedbi nadzora/akreditacije pružatelja usluga certificiranja i kojeg se pridržavaju pružatelji usluga certificiranja radi nadzora/akreditacije;

  — podatke o kriterijima prema kojima se pružatelji usluga certificiranja nadziru/akreditiraju.

— Specifične podatke, kad je primjenjivo, o specifičnim „kvalifikacijama" koje neki fizički ili binarni (logički) objekti generirani ili izdani kao posljedica pružanja usluge certificiranja mogu imati pravo dobiti na osnovu svoje sukladnosti s odredbama i zahtjevima utvrđenima na nacionalnoj razini, uključujući značenje takve „kvalifikacije" i pripadajućih nacionalnih odredaba i zahtjeva.

Dodatni specifični podaci o programu države članicu MOGU biti ponuđeni na dragovoljnoj osnovi, primjerice:

— podatak o kriterijima i pravilima korištenima za izbor nadzornika/revizora i definiranje načina na koji nadzornici/revizori nadziru/akreditiraju pružatelje usluga certificiranja;

— drugi kontaktni i opći podaci koji se primjenjuju na izvođenje programa.

Vrsta programa/zajednica/pravila (točka 5.3.9.)

Polje je PRISUTNO i UDOVOLJAVA specifikacijama iz norme TS 119 612 točke 5.3.9. te SADRŽAVA barem dva URI-ja:

— URI zajednički svim pouzdanim popisima država članica koji upućuje na opisni tekst koji SE PRIMJENJUJE na svim pouzdanim popisima, i to:

  URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

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

  Policy/rules for the assessment of the listed services

  The Trusted List of a Member State must provide, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

([1]) Posljednje dvije skupine podataka od ključne su važnosti za stranke koje pomoću njih ocjenjuju razinu kakvoće i sigurnosnu razinu sustava nadzora/akreditacije koji se primjenjuju na pružatelje usluga certificiranja koji ne izdaju kvalificirane certifikate. Ti se skupovi podataka na razini pouzdanog popisa nude korištenjem „URI podataka o programu" (točka 5.3.7. – podatke daje država članica), „Vrsta/zajednica/pravila programa" (točka 5.3.9. – korištenjem teksta koji je zajednički svim državama članicama) te „Općih pravila/pravnih obavijesti popisa statusa pouzdane usluge" (točka 5.3.11. – tekst zajednički svim državama članicama koji se odnosi na Direktivu 1999/93/EZ, uz mogućnost svake države članice da doda specifičan tekst/upute za državu članicu). Dodatni podaci u vezi s nacionalnim sustavima nadzora/akreditacije za pružatelje usluga certificiranja koji ne izdaju kvalificirane certifikate mogu biti ponuđeni na razini usluge kad je to primjenjivo i kad se zahtijeva (primjerice za razlikovanje različitih razina kakvoće/sigurnosnih razina) uporabom "URI definicije usluge programa" (točka 5.5.6.).

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 compliance 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 Article 3(3), Article 8)(1), Article 11 (respectively, Article2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 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 Article 2(11) of Directive 1999/93/EC). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific "qualification" on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a "qualification" is likely to be limited solely to the national level.

Interpretation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a Trusted List according to the Annex of Commission Decision [reference to the present Decision] 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 EN 319 412-5 defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or EN 319 411-2 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

Note: if no "Sie" "Qualifications Extension" information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related "Sie" "Qualifications Extension" information, 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. QcCompliance, QcSSCD, etc.) 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" "Qualifications Extension" information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this "Sie" "Qualifications Extension" information, which is constructed on the principle of a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing some additional information regarding the qualified status, the "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 qualified status: "QCStatement" meaning the identified certificate(s) is(are) qualified;

AND/OR

— to indicate the nature of the SSCD support:

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

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

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

AND/OR

— to indicate issuance to Legal Person:

— "QCForLegalPerson" qualifier value meaning "Certificate issued to a Legal Person".

The general interpretation rule for any other "Sti" type entry is that the listed service named according to the "Sn" field value and uniquely identified by the "Sdi" field value has a current supervision/accreditation status according to the "Scs" field value as from the date indicated in the "Current status starting date and time". Specific interpretation rules for any additional information with regard to a listed service (e.g. "Service information extensions" field) may be found, when applicable, in the Member State specific URI as part of the present "Scheme type/community/rules" field.

Please refer to the Technical specifications for a Common Template for the "Trusted List of supervised/accredited Certification Service Providers" in the Annex of Commission Decision 2009/767/EC for further details on the fields, description and meaning for the Member States' Trusted Lists."

— URI specifičan za pouzdani popis svake države članice koji upućuje na opisni tekst koji SE PRIMJENJUJE na pouzdani popis te države članice:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, gdje je CC = ISO 3166-1 ([1]) alpha-2 karakterističan brojčani kôd države iz polja „Državno područje programa" (točka 5.3.10.)

— gdje korisnici mogu dobiti specifična Opća pravila/pravila referentne države članice prema kojima se usluge koje popis sadržava OCJENJUJU u sukladu s odgovarajućim sustavom nadzora i programima dragovoljne akreditacije;

— gdje korisnici mogu dobiti opis specifičan za svaku državu članicu o tome kako koristiti i kako tumačiti sadržaj pouzdanog popisa povezanog s uslugama certificiranja koje se ne odnose na izdavanje kvalificiranih certifikata. To se može koristiti za naznačavanje moguće granularnosti u nacionalnim sustavima nadzora/akreditacije u pogledu pružatelja usluga certificiranja koji ne izdaju kvalificirane certifikate te za naznačavanje kako u tu svrhu koristiti polja „URI definicije usluge programa" (točka 5.5.6.) i „Ekstenzija podataka o usluzi" (točka 5.5.9.).

Država članica MOŽE definirati i koristiti dodatne URI-je iz gore navedenog specifičnog URI-ja države članice (odnosno URI-je utvrđene prema tom hijerarhijski specifičnom URI-ju).

Opća pravila/pravne obavijesti popisa statusa pouzdane usluge (točka 5.3.11)

Polje je PRISUTNO i UDOVOLJAVA specifikacijama iz norme TS 119 612 točke 5.3.11. Polje Opća pravila/pravne obavijesti koje se odnosi na pravni status programa ili pravne zahtjeve kojima program udovoljava prema području ovlasti u kojem je utemeljen i/ili bilo kojim ograničenjima i uvjetima prema kojima se popis održava i objavljuje, višejezičan je niz znakova (običan tekst) sastavljen od dva dijela:

1. Prvi, obvezan dio koji je zajednički pouzdanim popisima svih država članica (s britanskim engleskim jezikom kao obveznim jezikom i moguće jednim ili više nacionalnih jezika) i u kojem se navodi da je pravni okvir koji se primjenjuje Direktiva 1999/93/EZ i njezina odgovarajuća primjena u pravima države članice naznačene u polju „Državno područje programa" ("Scheme Territory").

   Inačica zajedničkog teksta na engleskom jeziku jest:

   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 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.

([1]) ISO 3166-1:2006: „Kodovi za prikaz imena država i njihovih podcjelina – 1. dio: karakteristični brojčani kodovi".

Tekst na nacionalnom jeziku/jezicima država članica: [službeni prijevod/prijevodi gore navedenog teksta na engleskom jeziku].

2. Drugi, neobvezni dio specifičan za svaki pouzdani popis (s britanskim engleskim jezikom kao obveznim jezikom i moguće jednim ili više nacionalnih jezika), koji upućuje na specifične nacionalne pravne okvire koji se primjenjuju (primjerice, posebice kad se odnose na nacionalne programe nadzora/akreditacije za pružatelje usluga certificiranja koji ne izdaju kvalificirane certifikate).

POGLAVLJE II.

KONTINUITET POUZDANOG POPISA

Certifikati koji se prijavljuju Komisiji prema članku 3.(c) ove Odluke IZDAJU SE tako da:

— su između njihovih datuma valjanosti barem tri mjeseca,

— izrađeni su na novim parovima ključeva jer se ni jedan prethodno korišteni par ključeva iznova ne certificira.

U slučaju kompromitacije ili povlačenja JEDNOG od privatnih ključeva koji odgovaraju javnom ključu koji bi se mogao koristiti za potvrđivanje potpisa pouzdanog popisa, koji je prijavljen Komisiji i objavljen na središnjem popisu pokazivača Komisije, države članice:

— PONOVNO IZDAJU, bez odgađanja, novi pouzdani popis potpisan nekompromitiranim privatnim ključem u slučaju da je objavljen pouzdani popis bio potpisan kompromitiranim ili povučenim privatnim ključem;

— odmah PRIJAVLJUJU Komisiji novi popis certifikata javnog ključa koji odgovara privatnim ključevima koji bi se mogli koristiti za potpisivanje pouzdanog popisa.

U slučaju kompromitacije ili povlačenja SVIH privatnih ključeva koji odgovaraju javnim ključevima koji bi se mogli koristiti za potvrđivanje potpisa pouzdanog popisa, koji su prijavljeni Komisiji i objavljeni na središnjem popisu pokazivača Komisije, države članice:

— GENERIRAJU nove parove ključeva koji se mogu koristiti za potpisivanje pouzdanog popisa i odgovarajućih certifikata javnog ključa;

— PONOVNO IZDAJU, bez odgađanja, novi pouzdani popis potpisan s jednim od tih novih privatnih ključeva, čiji odgovarajući javni ključ treba prijaviti;

— odmah PRIJAVLJUJU Komisiji novi popis certifikata javnog ključa koji odgovara privatnim ključevima koji bi se mogli koristiti za potpisivanje pouzdanog popisa.

POGLAVLJE III.

SPECIFIKACIJE ZA POUZDANI POPIS U LJUDIMA ČITLJIVOM OBLIKU

Ako se pouzdani popis izrađuje i objavljuje u ljudima čitljivom obliku, on bi TREBAO biti u obliku dokumenta u PDF formatu u skladu s normom ISO 32000 ([1]) koji MORA biti formatiran u skladu s profilom PDF/A (ISO 19005 ([2])).

Sadržaj tog PDF/A dokumenta pouzdanog popisa u ljudima čitljivom obliku TREBAO bi udovoljavati sljedećim zahtjevima:

— struktura pouzdanog popisa u ljudima čitljivom obliku TREBALA BI odražavati logički model opisan u normi TS 119 612;

— svako polje TREBALO BI biti prikazano i pružati:

  — naslov polja (npr. „Identifikator vrste usluge”);

  — vrijednost polja (npr. „CA/QC”);

  — značenje (opis) vrijednosti polja, kad je primjenjivo (npr. „Certifikacijsko tijelo koje izdaje certifikate javnog ključa.”);

  — više inačica na prirodnim jezicima kako je navedeno u pouzdanom popisu, kad je primjenjivo.

([1]) ISO 32000-1:2008: Upravljanje dokumentima – Format prenosivih dokumenata – 1. dio: PDF 1.7.
([2]) ISO 19005-2:2011: Upravljanje dokumentima – Elektronički format datoteke dokumenta za dugoročno čuvanje – 2. dio: Uporaba ISO 32000-1 (PDF/A-2)

— Sljedeća polja i odgovarajuće vrijednosti digitalnih certifikata prisutne u polju „Digitalni identitet usluge” TREBALI BI barem biti prikazani u ljudima čitljivom obliku:

  — inačica

  — serijski broj

  — algoritam potpisa

  — izdavatelj

  — vrijedi od

  — vrijedi do

  — subjekt

  — javni ključ

  — opća pravila certifikata

  — identifikator ključa subjekta

  — distribucijska točka CRL-a

  — identifikator ključa ovlasti

  — uporaba ključa

  — osnovna ograničenja

  — algoritam otiska prsta

  — otisak prsta

— pouzdani popis u ljudima čitljivom obliku TREBAO BI se lako ispisivati

— pouzdani popis u ljudima čitljivom obliku MORA biti potpisan od strane upravitelja sustava u skladu s Osnovnim profilom potpisa PAdES ([1]).

([1]) ETSI TS 103 172 (ožujak 2012.) – Elektronički potpisi i infrastrukture (ESI) – Osnovni profil PAdES