►B ►C1 **ROZHODNUTIE KOMISIE**

zo 16. októbra 2009,

ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu

[oznámené pod číslom K(2009) 7806]

(Text s významom pre EHP)

(2009/767/ES) ◄

(Ú. v. EÚ L 274, 20.10.2009, s. 36)

Zmenené a doplnené:

		Úradný vestník		
		Č.	Strana	Dátum
►M1	Rozhodnutie Komisie 2010/425/EÚ z 28. júla 2010	L 199	30	31.7.2010
►M2	Nariadenie Komisie (EÚ) č. 519/2013 z 21. februára 2013	L 158	74	10.6.2013

Opravené a doplnené:

►C1	Korigendum, Ú. v. EÚ L 299, 14.11.2009, s. 18 (2009/767/ES)
►C2	Korigendum, Ú. v. EÚ L 4, 7.1.2011, s. 6 (2009/767/ES)

▼B
▼C1

ROZHODNUTIE KOMISIE

zo 16. októbra 2009,

ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu

[oznámené pod číslom K(2009) 7806]

(Text s významom pre EHP)

(2009/767/ES)

KOMISIA EURÓPSKYCH SPOLOČENSTIEV,

so zreteľom na Zmluvu o založení Európskeho spoločenstva,

so zreteľom na smernicu Európskeho parlamentu a Rady 2006/123/ES z 12. decembra 2006 o službách na vnútornom trhu ([1]), a najmä na jej článok 8 ods. 3,

keďže:

(1) Povinnosť zjednodušiť administratívne postupy, ktorá sa členským štátom ukladá v kapitole II smernice 2006/123/ES, a najmä v jej článkoch 5 a 8, zahŕňa povinnosť zjednodušiť postupy a formálne náležitosti súvisiace s prístupom k činnostiam v oblasti služieb a ich vykonávaním a povinnosť zabezpečiť, aby tieto postupy a formálne náležitosti mohli poskytovatelia služieb jednoducho vykonať na diaľku a elektronickým spôsobom prostredníctvom „miest jednotného kontaktu“.

(2) Postupy a formálne náležitosti sa musia dať splniť prostredníctvom „miest jednotného kontaktu“ aj cez hranice členských štátov, ako sa ustanovuje v článku 8 smernice 2006/123/ES.

(3) V záujme splnenia povinnosti zjednodušiť administratívne postupy a formálne náležitosti a umožniť cezhraničné využívanie „miest jednotného kontaktu“, by postupy vykonávané pomocou elektronických prostriedkov mali vychádzať z jednoduchých riešení, a to aj pri elektronických podpisoch. V prípadoch, keď sa na základe primeraného posúdenia rizík pri konkrétnych postupoch a formálnych náležitostiach zistí nevyhnutnosť vysokej úrovne bezpečnosti alebo ekvivalentu ručného podpisu, je možné vyžadovať od poskytovateľov služieb pri určitých postupoch a formálnych náležitostiach zdokonalený elektronický podpis založený na kvalifikovanom certifikáte, s bezpečným zariadením na vytvorenie podpisu alebo bez neho.

([1]) Ú. v. EÚ L 376, 27.12.2006, s. 36.

▼C1

(4) Rámec Spoločenstva pre elektronické podpisy sa zriadil smernicou Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy ([1]). S cieľom uľahčiť účinné cezhraničné využívanie zdokonaleného elektronického podpisu založeného na kvalifikovanom certifikáte treba zvýšiť dôveru v tieto elektronické podpisy bez ohľadu na to, v akom členskom štáte má sídlo signatár alebo poskytovateľ certifikačných služieb, ktorý vydáva kvalifikované certifikáty. Táto väčšia dôvera sa dá docieliť jednoduchším sprístupnením informácií potrebných na overovanie elektronických podpisov dôveryhodnou formou, a to predovšetkým informácií týkajúcich sa poskytovateľov certifikačných služieb, ktorí sú pod dohľadom určitého členského štátu alebo sú v ňom akreditovaní, a služieb, ktoré ponúkajú.

(5) Treba zabezpečiť, aby členské štáty tieto informácie sprístupnili verejnosti prostredníctvom spoločného vzoru s cieľom uľahčiť jeho využívanie a zabezpečiť primerané množstvo podrobností, ktoré prijímajúcej strane umožnia overiť elektronický podpis,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Využívanie a akceptovanie elektronických podpisov

1. Členské štáty môžu od poskytovateľa služieb pri spĺňaní určitých postupov a formálnych náležitostí prostredníctvom „miest jednotného kontaktu“ podľa článku 8 smernice 2006/123/ES vyžadovať používanie zdokonaleného elektronického podpisu založeného na kvalifikovanom certifikáte, s bezpečným zariadením na vytvorenie podpisu alebo bez neho, vymedzeného v smernici 1999/93/ES, ak sa jeho využívanie na základe primeraného posúdenia obsiahnutých rizík preukáže ako opodstatnené a v súlade s článkom 5 ods. 1 a ods. 3 smernice 2006/123/ES.

2. Členské štáty na účely splnenia postupov a formálnych náležitostí uvedených v odseku 1 akceptujú všetky zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte, s bezpečným zariadením na vytvorenie podpisu alebo bez neho, pričom nie je dotknutá ich možnosť obmedziť toto akceptovanie na zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte vytvorené bezpečným zariadením na vytvorenie podpisu, ak to je v súlade s posúdením rizík uvedeným v odseku 1.

3. Členské štáty nepodmieňujú akceptovanie zdokonalených elektronických podpisov založených na kvalifikovanom certifikáte, s bezpečným zariadením na vytvorenie podpisu alebo bez neho, požiadavkami, ktoré by bránili poskytovateľom služieb využívať postupy pomocou elektronických prostriedkov prostredníctvom „miest jednotného kontaktu“.

([1]) Ú. v. ES L 13, 19.1.2000, s. 12.

▼C1

4. Odsek 2 nepredstavuje pre členské štáty prekážku akceptovať aj elektronické podpisy iné ako zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte, s bezpečným zariadením na vytvorenie podpisu alebo bez neho.

Článok 2

Zostavenie, vedenie a uverejňovanie zoznamov dôveryhodných informácií

1. Každý členský štát v súlade s technickými špecifikáciami uvedenými v prílohe zostaví, vedie a uverejňuje „zoznam dôveryhodných informácií“ obsahujúci minimálne informácie o poskytovateľoch certifikačných služieb, ktorí vydávajú kvalifikované certifikáty verejnosti a ktorí sú pod dohľadom určitého členského štátu alebo sú v ňom akreditovaní.

▼M1

2. Členské štáty v súlade so špecifikáciami uvedenými v prílohe zostavia a uverejnia zoznam dôveryhodných informácií v podobe čitateľnej ľudským okom, ako aj v strojovo spracovateľnej podobe.

2a. Členské štáty elektronicky podpíšu strojovo spracovateľnú podobu zoznamu dôveryhodných informácií a uverejnia minimálne jeho podobu čitateľnú ľudským okom prostredníctvom bezpečných kanálov, aby sa zaistila jeho autentickosť a celistvosť.

3. Členské štáty oznamujú Komisii tieto informácie:

a) orgán(-y) zodpovedný(-é) za zostavenie, vedenie a uverejňovanie podoby zoznamu dôveryhodných informácií čitateľných ľudským okom alebo jeho strojovo spracovateľnej podoby;

b) lokality, kde je uverejnená podoba zoznamu čitateľného ľudským okom a jeho strojovo spracovateľná podoba;

c) certifikát s verejným kľúčom používaný na zavedenie bezpečného kanála, ktorým sa uverejňuje zoznam dôveryhodných informácií čitateľných ľudským okom, alebo v prípade, že zoznam čitateľný ľudským okom je elektronicky podpísaný, certifikát s verejným kľúčom, ktorý sa použil na jeho podpis;

d) certifikát s verejným kľúčom použitý na elektronický podpis strojovo spracovateľnej podoby zoznamu dôveryhodných informácií;

e) všetky zmeny informácií v písmenách a) až d).

4. Komisia sprístupní všetkým členským štátom informácie uvedené v odseku 3, ktoré oznámili členské štáty, prostredníctvom bezpečného kanála na overenom webovom serveri v podobe čitateľnej ľudským okom, ako aj v podpísanej strojovo spracovateľnej podobe.

▼C1

Článok 3

Uplatňovanie

Toto rozhodnutie sa uplatňuje od 28. decembra 2009.

Článok 4

Adresáti

Toto rozhodnutie je určené členským štátom.

▼C1

PRÍLOHA

TECHNICKÉ ŠPECIFIKÁCIE SPOLOČNÉHO VZORU „ZOZNAMU DÔVERYHODNÝCH POSKYTOVATEĽOV CERTIFIKAČNÝCH SLUŽIEB, KTORÍ PODLIEHAJÚ DOHĽADU/SÚ AKREDITOVANÍ“

PREDHOVOR

1. **Všeobecné**

Účelom spoločného vzoru „Zoznamu dôveryhodných poskytovateľov certifikačných služieb, ktorí podliehajú dohľadu/sú akreditovaní“ členských štátov je určiť spoločný spôsob, akým všetky členské štáty podávajú informácie o štatúte dohľadu nad certifikačnou službou poskytovateľov certifikačných služieb ([1]) (CSP)/štatúte jej akreditácie, pričom dohliadajú na súlad CSP s príslušnými ustanoveniami smernice 1999/93/ES resp. akreditujú ho. Súčasťou postupovaných informácií sú aj historické informácie o štatúte dohľadu nad certifikačnou službou/štatúte akreditácie certifikačnej služby.

Povinné informácie v zozname dôveryhodných poskytovateľov (TL) musia zahŕňať minimálne informácie o CSP, ktorí podliehajú dohľadu/sú akreditovaní a ktorí vydávajú kvalifikované certifikáty (QC) ([2]) v súlade s ustanoveniami v smernici 1999/93/ES [článok 3 ods. 2 a 3 a článok 7 ods. 1 písm. a)] vrátane informácií o QC, ktoré podporujú elektronický podpis, a o tom, či je podpis vytvorený bezpečným zariadením na vytvorenie podpisu (SSCD) ([3]).

Dodatočné informácie o iných CSP, ktorí podliehajú dohľadu/sú akreditovaní, ktorí však nevydávajú QC ale poskytujú služby súvisiace s elektronickým podpisom (napr. CSP, ktorí poskytujú služby časových pečiatok a vydávajú tokeny časových pečiatok, CSP vydávajúci nekvalifikované certifikáty atď.) sa môžu dobrovoľne zahrnúť do zoznamu dôveryhodných poskytovateľov na vnútroštátnej úrovni.

Účelom poskytnutia týchto informácií je v prvom rade podpora overenia kvalifikovaných elektronických podpisov (QES) a zdokonalených elektronických podpisov (AdES) ([4]), ktoré kvalifikovaný certifikát ([5]) ([6]) podporuje.

Navrhovaný spoločný vzor je kompatibilný s implementáciou založenou na špecifikáciách v ETSI TS 102 231 ([7]), ktoré sa používajú na účely zostavenia, uverejnenia, lokalizácie takýchto zoznamov, prístupu k nim, ich autentifikácie a určenia dôveryhodnosti.

([1]) Ako sú vymedzení v článku 2 ods. 11 smernice 1999/93/ES.
([2]) Ako sú vymedzené v článku 2 ods. 10 smernice 1999/93/ES.
([3]) Ako sú vymedzené v článku 2 ods. 6 smernice 1999/93/ES.
([4]) Ako sú vymedzené v článku 2 ods. 2 smernice 1999/93/ES.
([5]) V prípade AdES, ktoré podporuje QC, sa v celom tomto dokumente používa akronym „$AdES_{QC}$“.
([6]) Treba poznamenať, že existuje celý rad elektronických služieb založených na jednoduchých AdES, ktorých cezhraničné využívanie by sa takisto uľahčilo, ak by podporné certifikačné služby (napr. vydávanie nekvalifikovaných certifikátov) boli súčasťou služieb, ktoré sú pod dohľadom/sú akreditované, uvedených členským štátom v dobrovoľnej časti informácií ich zoznamu dôveryhodných poskytovateľov.
([7]) ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

2. **Usmernenia na úpravu údajov v TL**

2.1. *TL zameraný na certifikačné služby pod dohľadom/akreditované certifikačné služby*

Relevantné certifikačné služby a poskytovatelia certifikačných služieb na jednom zozname

Zoznam dôveryhodných poskytovateľov členského štátu sa vymedzuje ako „Zoznam štatútov dohľadu nad certifikačnými službami/akreditácie certifikačných služieb poskytovateľov certifikačných služieb, ktorí sú pod dohľadom uvedeného členského štátu/ktorých uvedený členský štát akreditoval vzhľadom na dodržiavanie príslušných ustanovení smernice 1999/93/ES“.

Takýto zoznam dôveryhodných poskytovateľov musí obsahovať:

— **všetkých poskytovateľov certifikačných služieb**, ako sa vymedzujú v článku 2 ods. 11 smernice 1999/93/ES, teda „subjekt alebo právnická alebo fyzická osoba, ktorá vydáva certifikáty alebo poskytuje iné služby súvisiace s elektronickými podpismi“;

— ktorých súlad s príslušnými ustanoveniami v smernici 1999/93/ES je **pod dohľadom/je akreditovaný**.

Na základe vymedzení pojmov a ustanovení v smernici 1999/93/ES, predovšetkým vzhľadom na príslušných CSP a systémy dohľadu nad nimi/systémy ich dobrovoľnej akreditácie, sa dajú rozlíšiť dva druhy CSP, konkrétne CSP, ktorí vydávajú QC pre verejnosť (CSP_{QC}), a CSP, ktorí nevydávajú QC pre verejnosť, ale poskytujú „iné (doplnkové) služby súvisiace s elektronickými podpismi“:

— **CSP vydávajúci QC:**

  — Členský štát, v ktorom majú sídlo (v prípade, že majú sídlo v členskom štáte), musí nad nimi vykonávať dohľad a prípadne ich akreditovať vzhľadom na súlad s ustanoveniami v smernici 1999/93/ES vrátane požiadaviek uvedených v prílohe I (požiadavky na QC) a v prílohe II (požiadavky na CSP vydávajúce QC). CSP vydávajúce QC, ktoré sú v určitom členskom štáte akreditované, musia v každom prípade spadať pod príslušný systém dohľadu predmetného členského štátu, s výnimkou prípadu, keď nemajú v tomto členskom štáte sídlo.

  — Uplatniteľný systém „dohľadu“ (prípadne systém „dobrovoľnej akreditácie“) je vymedzený a musí spĺňať príslušné požiadavky v smernici 1999/93/ES, predovšetkým požiadavky ustanovené v článku 3 ods. 3, článku 8 ods. 1, článku 11, odôvodnení 13 (prípadne článku 2 ods. 13, článku 3 ods. 2, článku 7 ods. 1 písm. a), článku 8 ods. 1, článku 11, a v odôvodneniach 4 a 11až13).

— **CSP nevydávajúci QC:**

  — Môžu spadať pod systém „dobrovoľnej akreditácie“ (podľa jeho vymedzenia v smernici 1999/93/ES a v súlade s ňou) a/alebo pod vnútroštátne vymedzenú „uznanú schému schvaľovania CSP“ realizovanú na vnútroštátnom základe na účely dohľadu nad súladom s ustanoveniami v smernici a prípadne s vnútroštátnymi ustanoveniami týkajúcimi sa poskytovania certifikačných služieb (v zmysle článku 2 ods. 11 smernice).

  — Niektoré z fyzických alebo binárnych (logických) objektov vygenerovaných alebo vydaných ako výsledok poskytovania certifikačnej služby môžu byť oprávnené na špecifickú „kvalifikáciu“ z dôvodu svojho súladu s vnútroštátnymi ustanoveniami a požiadavkami, ale význam takejto „kvalifikácie“ bude pravdepodobne obmedzený na vnútroštátnu úroveň.

▼C1

Zoznam dôveryhodných poskytovateľov členského štátu musí obsahovať minimálne informácie o CSP pod dohľadom/akreditovaných CSP, ktorí vydávajú kvalifikované certifikáty pre verejnosť v súlade s ustanoveniami v smernici 1999/93/ES [článok 3 ods. 2 a 3 a článok 7 ods. 1 písm. a)] a informácie o QC, ktoré podporujú elektronický podpis, a o tom, či je podpis vytvorený bezpečným zariadením na vytvorenie podpisu.

Dodatočné informácie o iných službách CSP, ktorí podliehajú dohľadu/sú akreditovaní, ale nevydávajú QC pre verejnosť (napr. CSP, ktorí poskytujú služby časových pečiatok, vydávajú tokeny časových pečiatok, CSP vydávajúci nekvalifikované certifikáty atď.) sa môžu dobrovoľne zahrnúť do zoznamu dôveryhodných poskytovateľov na vnútroštátnej úrovni.

Účelom zoznamu dôveryhodných poskytovateľov je:

— zhromažďovať a poskytovať spoľahlivé informácie o štatúte dohľadu nad certifikačnou službou poskytovateľov certifikačných služieb/štatúte jej akreditácie, pričom poskytovatelia certifikačných služieb sú pod dohľadom členského štátu/sú akreditovaní v členskom štáte zodpovednom za zostavenie a vedenie zoznamu o súlade s príslušnými ustanoveniami v smernici 1999/93/ES,

— uľahčovať overovanie elektronických podpisov podporovaných certifikačnými službami pod dohľadom/akreditovanými certifikačnými službami, ktoré poskytujú CSP na zozname.

Jeden súbor hodnôt štatútu dohľadu/akreditácie

V každom členskom štáte sa musí zostaviť a viesť jeden TL s údajmi o štatúte dohľadu nad certifikačnou službou a/alebo štatúte akreditácie certifikačnej služby, ktorú poskytujú tí CSP, ktorí sú pod dohľadom daného členského štátu/sú v ňom akreditovaní.

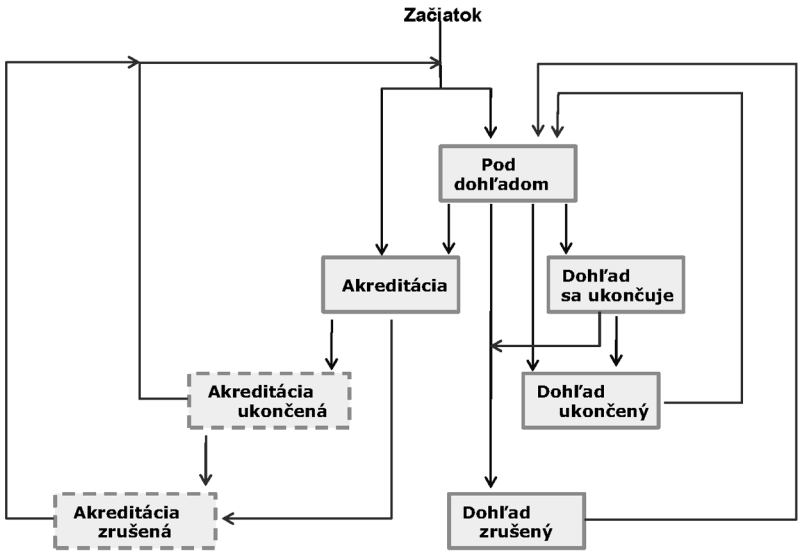
Skutočnosť, že služba je práve pod dohľadom alebo je akreditovaná, je súčasťou jej aktuálneho štatútu. Okrem toho môže byť štatút dohľadu nad ňou alebo štatút jej akreditácie „prebiehajúci“, „ukončuje sa“, „ukončený“ alebo aj „zrušený“. Certifikačná služba môže počas svojho fungovania postúpiť od štatútu pod dohľadom na štatút akreditácie a naopak ([1]).

Na obrázku 1 je opísaný očakávaný vývoj jednej certifikačnej služby medzi možnými štatútmi dohľadu/akreditácie:

([1]) Napr. poskytovateľ certifikačnej služby so sídlom v jednom členskom štáte, ktorý poskytuje certifikačnú službu, ktorá je najprv pod dohľadom členského štátu (dozorného orgánu), sa môže po určitom čase rozhodnúť pre dobrovoľnú akreditáciu certifikačnej služby, ktorá je v tom momente pod dohľadom. Podobne poskytovateľ certifikačnej služby v inom členskom štáte sa môže rozhodnúť nepozastaviť akreditovanú certifikačnú službu, ale zmeniť jej štatút zo štatútu akreditácie na štatút pod dohľadom, napríklad z obchodných a/alebo hospodárskych dôvodov.

▼C1

Očakávané zmeny štatútu dohľadu/akreditácie pri službe CSP



Legenda:

Prechodný štatút, ak existuje pridružený model dohľadu (napr. ako musí byť v prípade CSP vydávajúceho QC ak máso sídlo v členskom štáte),
Možný aktuálny štatút v prípade, ak neexistuje pridružený model dohľadu (napr. pri CSP nevydávajúcich QC)

Možný aktuálny štatút

Obrázok 1

Certifikačná služba, ktorá vydáva QC, musí byť pod dohľadom (ak má sídlo v určitom členskom štáte) a môže byť dobrovoľne akreditovaná. Hodnota „aktuálneho štatútu“ takejto služby uvedenej v zozname dôveryhodných poskytovateľov môže byť ktorákoľvek z uvedených. Tu treba však poznamenať, že štatúty „akreditácia ukončená“ a „akreditácia zrušená“ musia byť hodnotami „prechodného štatútu“ iba pri službách CSPQC zriadených v členskom štáte, pretože takéto služby musia byť pod dohľadom automaticky (aj vtedy, keď už nie sú alebo nikdy neboli akreditované).

Členské štáty, ktoré zriaďujú alebo zriadili vnútroštátne vymedzenú „uznanú schému schvaľovania CSP“ realizovanú na vnútroštátnom základe na účely dohľadu nad súladom služieb, ktoré poskytujú CSP nevydávajúci QC, s ustanoveniami v smernici 1999/93/ES a prípadne s vnútroštátnymi ustanoveniami týkajúcimi sa poskytovania certifikačných služieb (v zmysle článku 2 ods. 11 smernice), sú povinné zatriediť takéto schémy schvaľovania do týchto dvoch kategórií:

— „dobrovoľná akreditácia“, ako sa vymedzuje a reguluje smernicou 1999/93/ES (článok 2 ods. 13, článok 3 ods. 2, článok 7 ods. 1 písm. a), článok 8 ods. 1, článok 11, odôvodnenia 4 a 11 až 13),

— „dohľad“, ako sa vyžaduje v smernici 1999/93/ES a implementuje vnútroštátnymi ustanoveniami a požiadavkami v súlade s vnútroštátnymi právnymi predpismi.

▼C1

Podľa tohto zatriedenia môže byť certifikačná služba, ktorá nevydáva QC, buď pod dohľadom, alebo dobrovoľne akreditovaná. „Hodnota aktuálneho štatútu“ takejto služby môže pri zázname do zoznamu dôveryhodných poskytovateľov byť ktorákoľvek z uvedených (pozri obrázok 1).

Zoznam dôveryhodných poskytovateľov musí obsahovať informácie o základných schémach dohľadu/akreditácie, predovšetkým:

— informácie o systéme dohľadu, ktorý sa vzťahuje na všetky CSP_{QC},

— v prípade potreby informácie o vnútroštátnej schéme „dobrovoľnej akreditácie“, ktorá sa vzťahuje všetky CSPQC,

— v prípade potreby informácie o systéme dohľadu, ktorý sa vzťahuje na všetkých CSP nevydávajúcich QC,

— v prípade potreby informácie o vnútroštátnej schéme „dobrovoľnej akreditácie“, ktorá sa vzťahuje na všetkých CSP nevydávajúcich QC.

Posledné dva súbory informácií sú mimoriadne dôležité pre spoliehajúce sa strany na posúdenie kvality a stupňa bezpečnosti týchto systémov dohľadu/akreditácie, ktoré sa vzťahujú na vnútroštátnej úrovni na CSP nevydávajúcich QC. Keď sa na TL uvádzajú informácie o štatúte dohľadu/akreditácie pri službách poskytovaných CSP nevydávajúcimi QS, uvedený súbor informácií sa na úrovni TL vyjadrí pomocou „Scheme information URI“ (odsek 5.3.7 – informácie, ktoré poskytujú členské štáty), „Scheme type/community/rules“ (odsek 5.3.9 – pomocou textu spoločného pre všetky členské štáty a dobrovoľných konkrétnych informácií, ktoré poskytne členský štát) a „TSL policy/legal notice“ (odsek 5.3.11 – text spoločný pre všetky členské štáty odvolávajúci sa na smernicu 1999/93/ES, spolu s možnosťou doplniť texty/referencie špecifické pre daný členský štát). Dodatočné „kvalifikačné“ informácie vymedzené na úrovni vnútroštátneho systému dohľadu/akreditácie pre CSP nevydávajúcich QC sa môžu poskytnúť na úrovni služby, ak sú potrebné a vyžiadané (napr. na rozlíšenie medzi viacerými úrovňami kvality/bezpečnosti), pomocou rozšírenia „additionalServiceInformation“ (odsek 5.8.2) ako súčasť „Service information extension“ (odsek 5.5.9). Ďalšie informácie o zodpovedajúcich technických špecifikáciách sa uvádzajú v podrobných špecifikáciách v kapitole I.

Napriek tomu, že za dohľad nad certifikačnými službami a ich akreditáciu môžu v jednom členskom štáte byť zodpovedné rôzne orgány tohto členského štátu, očakáva sa, že jedna certifikačná služba bude mať len jeden záznam (identifikovaný podľa „Service digital identity“ v rámci ETSI TS 102 231 ([1])) a že štatút dohľadu nad ním/štatút jeho akreditácie sa bude zodpovedajúcim spôsobom aktualizovať. Význam zobrazených štatútov je opísaný v príslušnom odseku 5.5.4 podrobných technických špecifikácií v kapitole I.

2.2. *Záznamy v TL zamerané na uľahčenie overenia QES a $AdES_{QC}$*

Rozhodujúcou časťou zostavovania TL je vytvorenie povinnej časti TL, teda „zoznamu služieb“ za CSP vydávajúcich QC s cieľom správne vystihnúť presnú situáciu každej takejto služby vydávajúcej QC a zabezpečiť, aby informácie poskytnuté v každom zázname boli dostatočné na umožnenie overenia QES a AdESQC (keď sa skombinujú s obsahom QC konečného subjektu, ktorý vydal CSP v rámci certifikačnej služby uvedenej v tomto zázname).

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

▼C1

Keďže neexistuje skutočne interoperabilný a cezhraničný profil QC, požadované informácie môžu zahŕňať iné údaje ako „digitálnu totožnosť služby“ jednej (koreňovej) CA, predovšetkým údaje o štatúte QC vydaného certifikátu a údaje o tom, či sú podporované podpisy vytvorené pomocou SSCD. Orgán v členskom štáte, ktorý je zodpovedný za zostavenie, úpravu a vedenie TL (t. j. prevádzkovateľ schémy – „Scheme operator“ podľa ETSI TS 102 231) musí preto zohľadniť aktuálny profil a obsah certifikátu v každom vydanom QC, za každý CSP_{QC} uvedený v TL.

V ideálnom prípade by každý vydaný QC mal obsahovať vyhlásenie QcCompliance statement ([1]) vymedzené na základe ETSI, keď sa vyhlasuje, že ide o QC, a mal by obsahovať vyhlásenie QcSSCD vymedzené na základe ETSI, keď sa vyhlasuje, že je podporovaný SSCD na vytváranie elektronických podpisov a/alebo že každý vydaný QC obsahuje jeden z identifikátorov politiky certifikátov QCP/QCP + Object Identifiers (OIDs) vymedzených v ETSI TS 101 456 ([2]). Skutočnosť, že CSP vydávajúci QC využívajú ako referenciu rozličné normy, široká škála výkladu týchto noriem, ako aj nedostatočná informovanosť o existencii a prednosti určitých normatívnych technických špecifikácií alebo noriem majú za následok rozdiely v obsahu v súčasnosti vydávaných QC (napr. používanie alebo nepoužívanie QcStatements vymedzených podľa ETSI), v dôsledku čoho sa prijímajúca strana nemôže jednoducho spoľahnúť na certifikát signatára (a súvisiaci certifikačný reťazec/proces) pri posúdení, aspoň strojom čitateľným spôsobom, či certifikát podporujúci elektronický podpis sa vyhlasuje za QC, alebo nie, a či súvisí s SSCD, pomocou ktorého sa elektronický podpis vytvoril.

Doplnením informácií uvedených v poli „Service information extensions“ („Sie“) do polí „Service type identifier“ („Sti“), „Service name“ („Sn“), and „Service digital identity“ („Sdi“) ([3]) sa v navrhovanom spoločnom vzore TL umožňuje jasne určiť konkrétny typ kvalifikovaného certifikátu vydaného certifikačnou službou CSP vydávajúcou QC uvedenou na zozname a poskytnúť informácie o tom, či je podporovaný SSCD alebo nie (v prípade, že táto informácia chýba vo vydanom QC). Konkrétna informácia o „Service current status“ („Scs“) je samozrejme úzko spojená s týmto záznamom, ako je znázornené na obrázku 2.

Zapísanie služby iba prostredníctvom údaju „Sdi“ (koreňovej) CA by znamenalo, že je zaručené (zo strany CSP vydávajúceho QC ale takisto zo strany dozorného/akreditačného orgánu zodpovedného za akreditáciu tohto CSP/dohľad nad ním), že certifikát konečného subjektu vydaný v rámci tejto (koreňovej) CA (hierarchie) obsahuje informácie vymedzené v ETSI a strojovo spracovateľné, ktoré sú dostatočné na posúdenie toho, či ide o QC a či je podporovaný SSCD. Napríklad v opačnom prípade (teda že v QC nie je strojovo spracovateľný údaj podľa noriem v ETSI o tom, či je QC podporovaný SSCD), potom sa na základe údaju „Sdi“ predmetnej (koreňovej) CA dá usúdiť len to, že vydaný QC podľa tejto (koreňovej) hierarchie CA nie je podporovaný žiadnym SSCD. Na to, aby sa QC mohol považovať za QC podporovaný SSCD, by sa mal uviesť údaj „Sie“ (ktorým sa takisto uvádza, že ho zaručuje CSP vydávajúci QC, ako aj že podlieha dohľadu dozorného alebo akreditačného orgánu resp. že ho takýto orgán akreditoval).

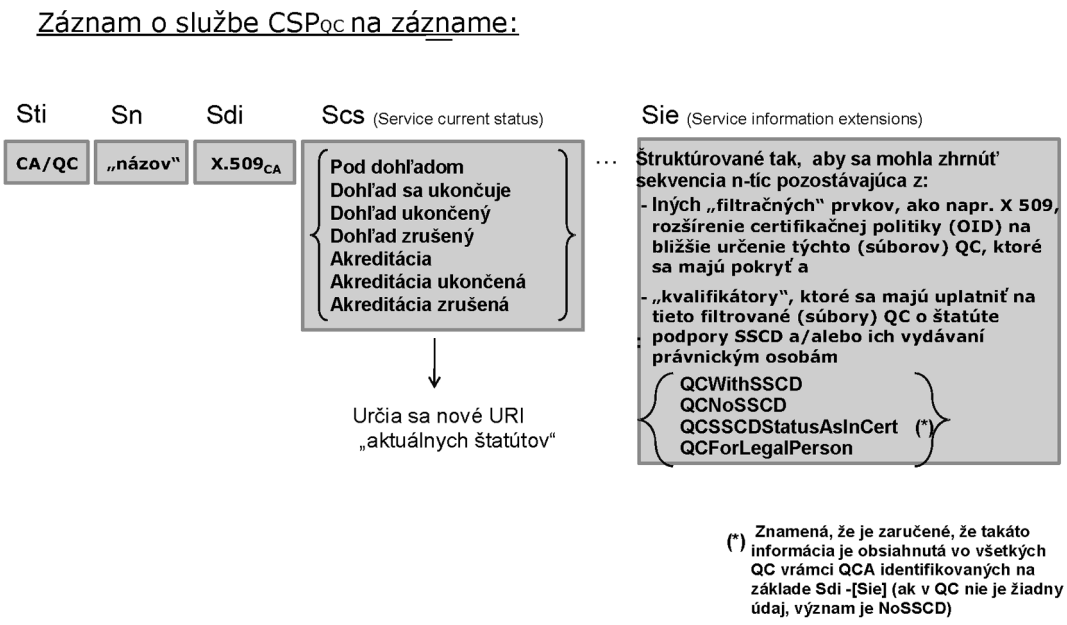
([1]) Pozri ETSI TS 101 862 – Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.

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

([3]) Minimálne teda certifikát X.509 v3 vydávajúcej QCA alebo CA vyššej úrovne v certifikačnom procese.

▼C1

Všeobecné zásady — Pravidlá úpravy údajov CSP_{QC} (služby na zozname)



Obrázok 2:

Záznam o službe CSP vydávajúceho QC v TL implementovanom vo formáte TSL

Podľa týchto technických špecifikácií spoločného vzoru TL je možné využiť kombináciu piatich hlavných častí informácie v zázname o službe:

— „Service type identifier“ („Sti“), na základe ktorého sa napríklad identifikuje CA vydávajúca QC („CA/QC“),

— „Service name“ („Sn“),

— informácia o „Service digital identity“ („Sdi“), na základe ktorej sa služba v zozname identifikuje, teda (minimálne) certifikát X.509v3 vydaný CA vydávajúcou QC,

— v prípade služieb CA/QC dobrovoľná informácia „Service information extensions“ („Sie“), na základe ktorej je možné zaradiť sekvenciu jednej alebo viacero n-tíc, pričom každá n-tica poskytuje:

  — kritériá na bližšiu identifikáciu (vytriedenie) v certifikačnej službe identifikovanej na základe „Sdi“ tej konkrétnej služby (teda súboru kvalifikovaných certifikátov), pri ktorej sa požadujú/poskytujú dodatočné informácie o podpore SSCD (a/alebo ich vydaní právnickej osobe) a

  — súvisiace informácie („kvalifikátory“) o tom, či je tento bližšie určený súbor kvalifikovaných certifikátov podporovaný SSCD alebo nie, a či sú tieto súvisiace informácie súčasťou QC v normalizovanej strojovo spracovateľnej forme a/alebo informácie o tom, že takéto QC sa vydávajú právnickým osobám (automaticky sa predpokladá, že sa vydávajú len fyzickým osobám),

▼C1

— informácia o „aktuálnom štatúte“ záznamu o predmetnej službe, ktorá poskytuje informácie o tom:

— či ide o službu pod dohľadom alebo akreditovanú službu a

— samotnom štatúte dohľadu/akreditácie.

2.3. *Usmernenia o úprave a využívaní údajov o službe CSP_{QC}*

Všeobecné usmernenia o úprave údajov:

1. Ak je zaručené [záruka zo strany CSP_{QC} a dohľad/akreditácia zo strany dozorného orgánu (SB)/akreditačného orgánu (AB)], že v prípade služby na zozname identifikovanej na základe „Sdi“ všetky QC podporované SSCD obsahujú vyhlásenie QcCompliance statement vymedzené na základe ETSI a vyhlásenie QcSSCD a/alebo QCP + Object Identifier (OID), v takom prípade je príslušný údaj „Sdi“ postačujúci a pole „Sie“ je dobrovoľné a nemusí obsahovať informáciu o podpore SSCD.

2. Ak je zaručené (záruka zo strany CSP_{QC} a dohľad/akreditácia zo strany SB/AB), že v prípade služby na zozname identifikovanej na základe „Sdi“ všetky QC nepodporované SSCD obsahujú buď vyhlásenie QcCompliance statement a/alebo QCP OID a je to druh QC, ktorý nemá obsahovať vyhlásenie QcSSCD alebo QCP + OID, v takom prípade je príslušný údaj „Sdi“ postačujúci a pole „Sie“ je dobrovoľné a nemusí obsahovať informáciu o podpore SSCD (čo znamená, že nie je podporovaný SSCD).

3. Ak je zaručené (záruka zo strany CSP_{QC} a dohľad/akreditácia zo strany SB/AB), že v prípade služby na zozname identifikovanej na základe „Sdi“ všetky QC obsahujú vyhlásenie QcCompliance statement a niektoré z týchto QC majú byť podporované SSCD a niektoré nie (čo môže byť napr. diferencované rozličnými CSP specific Certificate Policy OIDs alebo prostredníctvom iných informácií špecifických pre CSP v QC, priamo alebo nepriamo, strojovo spracovateľne alebo nie), ale QC neobsahuje ANI vyhlásenie QcSSCD ANI ETSI QCP(+) OID, v takom prípade príslušný údaj „Sdi“ nemusí byť postačujúci A v poli „Sie“ sa musí jednoznačne uviesť podpora SSCD spolu s možným rozšírením informácie s cieľom identifikovať pokrytý súbor certifikátov. Na tento účel bude pravdepodobne potrebné uviesť pri vypĺňaní poľa „Sie“ pri tom istom „Sdi“ rozličné „hodnoty informácie o podpore SSCD“.

4. Ak je zaručené (záruka zo strany CSP_{QC} a dohľad/akreditácia zo strany SB/AB), že v prípade služby na zozname identifikovanej na základe „Sdi“ určitý QC neobsahuje vyhlásenie QcCompliance statement, QCP OID, vyhlásenie QcSSCD ani QCP + OID, ale je zaručené, že niektoré z týchto certifikátov konečného subjektu vydané v rámci tohto „Sdi“ majú byť QC a/alebo podporované SSCD a niektoré nie (čo môže byť napr. diferencované rozličnými Certificate Policy OID špecifickými pre CSP_{QC} alebo prostredníctvom iných informácií špecifických pre CSP_{QC} v QC, priamo alebo nepriamo, strojovo spracovateľne alebo nie), v takom prípade príslušný údaj „Sdi“ nebude postačujúci A v poli „Sie“ sa musí jednoznačne uviesť informácia o podpore SSCD. Na tento účel bude pravdepodobne potrebné uviesť pri vypĺňaní poľa „Sie“ pri tom istom „Sdi“ rozličné „hodnoty informácie o podpore SSCD“.

▼C1

Všeobecnou automatickou zásadou je, že pri každom CSP na zozname dôveryhodných poskytovateľov musí byť za každý certifikát X.509v3 pre certifikačnú službu CA/QC, teda certifikačnú autoritu (priamo) vydávajúcu QC, jeden záznam o službe. Za určitých opatrne zvážených okolností a pri citlivo riadených podmienkach sa dozorný/akreditačný orgán členského štátu môže rozhodnúť použiť certifikát X.509v3 koreňovej CA alebo CA vyššieho stupňa (teda certifikačnej autority, ktorá nevydáva priamo QC konečného subjektu, ale ktorá certifikuje hierarchiu CA až po CA, ktoré priamo vydávajú QC konečného subjektu) ako „Sdi“ jedného záznamu v zozname služieb CSP na zozname dôveryhodných poskytovateľov. Dôsledky (výhody a nevýhody) použitia X.509v3 koreňovej CA alebo CA vyššej úrovne ako hodnoty „Sdi“ údajov o službách v TL musia členské štáty dôkladne zvážiť a schváliť. Okrem toho, ak sa členské štáty rozhodnú využiť túto povolenú výnimku z automatickej zásady, musia poskytnúť potrebnú dokumentáciu, aby sa uľahčilo vytváranie certifikačného procesu a overovanie.

Na ilustráciu všeobecných usmernení o úprave údajov môže poslúžiť tento príklad: V prípade CSP_{QC}, ktorý využíva jednu koreňovú CA, ktorej podlieha niekoľko CA vydávajúcich QC a iné certifikáty ako QC, pričom jeho QC obsahujú len vyhlásenie QcCompliance statement, ale žiadny údaj o tom, či sú podporované SSCD, by uvedenie „Sdi“ koreňovej CA znamenalo len, že podľa pravidiel vysvetlených v predchádzajúcej časti ani jeden QC vydaný v tejto hierarchii koreňovej CA NIE je podporovaný SSCD. Ak sú tieto QC však v skutočnosti podporované SSCD, dôrazne sa odporúča v QC vydaných v budúcnosti využiť vyhlásenie QcSSCD. Medzičasom (kým neuplynie platnosť posledného QC bez tejto informácie) by TSL mal využiť pole „Sie“ a súvisiace rozšírenie „Qualifications“, napr. vytriediť certifikáty pomocou konkrétnych OID vymedzených CSP_{QC}, ktoré CSP_{QC} môžu potenciálne využívať na rozlišovanie medzi rozličnými typmi QC (niektoré podporované SSCD a niektoré nie) a v ktorých je jednoznačne uvedená „informácia o podpore SSCD“ vzhľadom na certifikáty vytriedené pomocou „kvalifikátorov“.

Usmernenia o všeobecnom využívaní aplikácií, služieb a produktov elektronických podpisov, ktoré sú založené na TSL implementácii zoznamu dôveryhodných poskytovateľov podľa týchto technických špecifikácií, sú takéto:

Záznam „CA/QC“„Sti“ (a podobne aj záznam CA/QC bližšie určený ako „koreňová CA/QC“ pomocou rozšírenia „Sie“ additionalServiceInformation):

— znamená, že všetky certifikáty konečného subjektu, ktoré vydala CA identifikovaná na základe „Sdi“ (podobne v rámci hierarchie CA počnúc koreňovou CA identifikovanou na základe „Sdi“), sú QC **za predpokladu**, že sa tak uvádza na samotnom certifikáte prostredníctvom vhodných QcStatements (teda QcC, QcSSCD) a/alebo QCP(+) OID vymedzených na základe ETSI (čo zaručuje dozorný/akreditačný orgán – pozri „Všeobecné usmernenia o úprave údajov“).

Poznámka: ak nie je poskytnutý údaj „Sie“„Qualification“ alebo ak certifikát konečného subjektu, ktorý má byť QC, nie je „bližšie identifikovaný“ prostredníctvom príslušného záznamu „Sie“, v takom prípade „strojovo spracovateľná“ informácia v QC sa pod dohľadom považuje za správnu/sa akredituje ako správna. To znamená, že je zaručené, že použitie (alebo nepoužitie) vhodného QcStatement (teda QcC, QcSSCD) a/alebo QCP(+) OID vymedzeného na základe ETSI je v súlade s vyhláseniami CSP_{QC},

▼C1

— **aAK** sú informácie „Sie“„Qualification“ uvedené, potom dodatočne k uvedenému automatickému pravidlu výkladu použitia sa predmetné certifikáty identifikované pomocou záznamov „Sie“„Qualification“, ktoré sú zostavené na princípe sekvencie „filtrov“ bližšie identifikujúcich súbor certifikátov a poskytujúcich dodatočné informácie o „podpore SSCD“ a/alebo „právnickej osobe ako subjekte“ (napríklad certifikáty, ktoré obsahujú konkrétny OID v rozšírení Certificate Policy a/alebo majú špecifické modely „používania kľúčov“ a alebo sú filtrované pomocou špecifickej hodnoty, ktorá je uvedená v jednom konkrétnom poli alebo rozšírení certifikátu atď.) majú posudzovať podľa nasledovného súboru „kvalifikátorov“, čím sa vykompenzuje nedostatok informácií v zodpovedajúcom QC, teda:

— údaj o podpore SSCD,

  — hodnota kvalifikátora „QCWithSSCD“ znamená „QC podporovaný SSCD“ alebo

  — hodnota kvalifikátora „QCNoSSCD“ znamená „QC nepodporovaný SSCD“ alebo

  — hodnota kvalifikátora „QCSSCDStatusAsInCert“ znamená, že je zaručené, že informácie o podpore SSCD sú obsiahnuté vo všetkých QC, na ktoré sa vzťahujú informácie „Sdi“ – „Sie“ uvedené v tomto zázname CA/QC

A/ALEBO

— údaj o vydaní právnickej osobe:

  — hodnota kvalifikátora „QCForLegalPerson“ znamená „certifikát vydaný právnickej osobe“.

2.4. *Služby podporujúce „CA/QC“, ktoré ale nie sú súčasťou „CA/QC“„Sdi“*

Zahrnúť by sa mali aj prípady, keď CRL a OCSP odpovede sú podpísané inými kľúčmi ako kľúčom od CA vydávajúcej QC („CA/QC“). Dosiahnuť sa to môže tak, že tieto služby sa ako také uvedú v TSL implementácii TL (t. j. pomocou „Service type identifier“ bližšie určeného rozšírením „additionalServiceInformation“, ktorý odráža skutočnosť, že OCSP alebo služba CRL je súčasťou poskytovania QC, teda sa napr. určí ako „OCSP/QC“ alebo „CRL/QC“), keďže tieto služby sa môžu považovať za súčasť „kvalifikovaných“ služieb pod dohľadom/akreditovaných „kvalifikovaných“ služieb súvisiacich s poskytovaním certifikačných služieb QC. Samozrejme, respondery OCSP alebo vydavatelia CRL, ktorých certifikáty podpísali CA v rámci hierarchie služby CA/QC na zozname, sa považujú za „platné“ a v súlade s hodnotou štatútu služby CA/QC na zozname.

Podobné ustanovenie sa môže vzťahovať na certifikačné služby vydávajúce nekvalifikované certifikáty (typu služby „CA/PKC“), ktoré automaticky využívajú ETSI TS 102 231 OCSP a typy služby CRL.

Treba poznamenať, že TSL implementácia TL MUSÍ zahŕňať zrušovaciu službu, keď sa súvisiace informácie nenachádzajú v poli AIA konečného certifikátu alebo keď ich nepodpísala CA, ktorá sa nenachádza na zozname CA.

2.5. *Úsilie o interoperabilný profil QC*

Všeobecne platí, že sa treba usilovať o čo najväčšie možné zjednodušenie (redukovanie) počtu záznamov služieb (rozličné „Sdi“). Pritom sa však musí zabezpečiť správna identifikácia tých služieb, ktoré súvisia s vydávaním QC a poskytovaním dôveryhodných informácií o tom, či dotknuté QC sú podporované SSCD alebo nie, v prípade, keď táto informácia na vydanom QC chýba.

▼C1

V ideálnom prípade by využitie poľa „Sie“ a rozšírenia „Qualification“ malo byť (prísne) obmedzené na tie konkrétne prípady, ktoré sa týmto spôsobom vyriešia, pretože QC by mali obsahovať dostatočné informácie o deklarovanom kvalifikovanom štatúte a deklarovanej podpore SSCD alebo jej neexistencii.

Členské štáty by mali v čo najväčšej možnej miere presadzovať prijatie a využívanie interoperabilných profilov QC.

3. **Štruktúra spoločného vzoru zoznamu dôveryhodných poskytovateľov**

Navrhovaný spoločný vzor zoznamu dôveryhodných poskytovateľov členských štátov bude rozdelený na tieto kategórie informácií:

1. informácie o zozname dôveryhodných poskytovateľov a schéme jeho vydávania;

2. sekvencia polí s jednoznačnými informáciami na identifikáciu o každom CSP pod dohľadom/akreditovanom CSP v rámci schémy (táto sekvencia je dobrovoľná, t. j., ak sa nepoužije, vychádza sa z predpokladu, že zoznam je prázdny, a teda že v predmetnom členskom štáte v súvislosti s rozsahom zoznamu dôveryhodných poskytovateľov nie je pod dohľadom/nie je akreditovaný ani jeden CSP);

3. za každý CSP na zozname sekvencia polí s jednoznačnými informáciami na identifikáciu certifikačnej služby poskytovanej CSP, ktorá je pod dohľadom/je akreditovaná (táto sekvencia musí mať minimálne jeden záznam);

4. za každú certifikačnú službu pod dohľadom/akreditovanú certifikačnú službu na zozname označenie aktuálneho štatútu služby a históriu tohto štatútu.

V súvislosti s CSP vydávajúcimi QC sa pri jednoznačnej identifikácii certifikačnej služby pod dohľadom/akreditovanej certifikačnej služby, ktorá sa má doplniť na zoznam, musia zohľadniť situácie, keď v kvalifikovanom certifikáte nie sú dostatočné informácie o jeho „kvalifikovanom“ štatúte, jeho možnej podpore SSCD a predovšetkým informácie na riešenie dodatočnej skutočnosti, že väčšina (komerčných) CSP používa jedinú vydávajúcu kvalifikovanú CA na vydávanie viacerých typov certifikátov konečného subjektu, a to tak kvalifikovaných, ako aj nekvalifikovaných.

Počet záznamov na zozname za každý uznaný CSP sa môže zredukovať v prípade, keď existuje jedna alebo viac služieb CA vyššej úrovne, napr. pri komerčnej hierarchii CA od koreňovej CA po vydávajúce CA. Avšak aj v týchto prípadoch sa musí zachovať a zaručiť zásada zabezpečenia jednoznačného prepojenia medzi certifikačnou službou CSP_{QC} a súborom certifikátov, ktoré sa majú identifikovať ako QC.

1. *Informácie o zozname dôveryhodných poskytovateľov a schéme jeho vydávania*

Súčasťou tejto kategórie sú tieto informácie:

— **tag** identifikáciu zoznamu dôveryhodných poskytovateľov pri elektronickom vyhľadávaní a na potvrdenie jeho účelu vo forme čitateľnej ľudským okom,

— **formát a identifikátor verzie formátu** zoznamu dôveryhodných poskytovateľov,

— **sériové číslo (alebo číslo vydania)** zoznamu dôveryhodných poskytovateľov,

— **informácie o type** zoznamu dôveryhodných poskytovateľov (napr. na identifikáciu skutočnosti, že predmetný zoznam dôveryhodných poskytovateľov uvádza informácie o štatúte dohľadu nad certifikačnými službami/akreditácie certifikačných služieb poskytovaných CSP, ktorí sú pod dohľadom uvedeného členského štátu/sú ním akreditovaní vzhľadom na súlad s ustanoveniami v smernici 1999/93/ES),

▼C1

— **informácie o majiteľovi** zoznamu dôveryhodných poskytovateľov (napr. meno, adresa, kontaktné informácie atď. orgánu členského štátu zodpovedného za zostavenie, bezpečné uverejnenie a vedenie zoznamu dôveryhodných poskytovateľov),

— **informácie o schémach, ktoré sú základom dohľadu/akreditácie** a s ktorými zoznam dôveryhodných poskytovateľov súvisí, vrátane, ale nie výlučne:

  — krajiny, na ktorú sa zoznam vzťahuje,

  — informácie o lokalitách, kde sa informácie o schéme nachádzajú (model schémy, pravidlá, kritériá, príslušná komunita, typ, atď.), alebo odkazy na ne,

  — lehota uchovávania (historických) informácií,

— **politika a/alebo právne upozornenie, ručenie, oblasti zodpovednosti** zoznamu dôveryhodných poskytovateľov;

— **dátum a čas vydania** zoznamu dôveryhodných poskytovateľov **a jeho nasledujúca plánovaná aktualizácia**.

2. *Jednoznačné informácie na identifikáciu každého CSP uznaného v schéme*

Tento súbor informácií obsahuje minimálne:

— názov organizácie CSP v podobe, v akej sa použil pri formálnej zákonnej registrácii (môže zahŕňať UID organizácie CSP podľa praktík príslušného členského štátu),

— adresa a kontaktné informácie CSP,

— dodatočné informácie o CSP, buď uvedené priamo, alebo pomocou odkazu na lokalitu, odkiaľ sa takéto informácie dajú stiahnuť.

3. *Za každý CSP na zozname sekvencia polí s jednoznačnými informáciami na identifikáciu certifikačnej služby poskytovanej CSP, ktorá je pod dohľadom/je akreditovaná v súvislosti so smernicou 1999/93/ES*

Tento súbor informácií obsahuje minimálne tieto údaje za každú certifikačnú službu poskytovanú CSP na zozname:

— identifikátor typu certifikačnej služby (napr. identifikátor, na základe ktorého sa určuje, že certifikačná služba, ktorú poskytuje CSP a ktorá je pod dohľadom/je akreditovaná, je certifikačná autorita vydávajúca QC),

— (obchodný) názov certifikačnej služby,

— jednoznačný jedinečný identifikátor certifikačnej služby,

— dodatočné informácie o certifikačnej službe (buď uvedené priamo, alebo pomocou odkazu na lokalitu, odkiaľ sa takéto informácie dajú stiahnuť, informácie o prístupe k službe),

— v prípade služieb CA/QC dobrovoľná sekvencia n-tíc s informáciami, pričom každá n-tica poskytuje:

  i) kritériá na bližšiu identifikáciu (vytriedenie) v certifikačnej službe identifikovanej na základe „Sdi“ tej konkrétnej služby (teda súboru kvalifikovaných certifikátov), v prípade ktorej sa požadujú/poskytujú dodatočné informácie týkajúce sa údaju o podpore SSCD (a/alebo vydaní právnickej osobe), a

  ii) súvisiace „kvalifikátory“ poskytujúce informácie o tom, či tento súbor kvalifikovaných certifikátov z tejto bližšie určenej služby je podporovaný SSCD, alebo nie, a/alebo informácie o tom, či sa takéto QC vydávajú právnickým osobám (automaticky sa predpokladá, že sa vydávajú len fyzickým osobám).

▼C1

4. *Za každú certifikačnú službu na zozname označenie aktuálneho štatútu služby a históriu tohto štatútu*

Tento súbor informácií obsahuje minimálne:

— identifikátor aktuálneho štatútu,

— dátum a čas, odkedy aktuálny štatút začal platiť,

— historické informácie o tomto štatúte.

4. **Vymedzenie pojmov a skratky**

Na účely tohto dokumentu sa uplatňujú nasledujúce vymedzenia pojmov a akronymy:

Pojem	Akronym	Vymedzenie pojmov
Poskytovateľ certifikačných služieb	CSP	Ako je vymedzené v článku 2 ods. 11 smernice 1999/93/ES.
Certifikačná autorita	CA	CA je CSP, ktorá môže používať súkromné podpisové kľúče viacerých technických CA, pričom každý kľúč má súvisiaci certifikát, na účely vydávania certifikátov konečného subjektu. CA je orgán, ktorému jeden alebo viacero používateľov zverilo úlohu vytvárať a prideľovať certifikáty. Takisto môže dobrovoľne vytvárať kľúče používateľov [ETSI TS 102 042]. CA sa identifikuje na základe identifikačných informácií uvedených v poli Issuer (vystavujúca autorita) na certifikáte CA, ktoré sa týkajú verejného kľúča (certifikujúcich ho) súvisiaceho so súkromným podpisovým kľúčom CA a ktoré CA používa na vydávanie certifikátov subjektom. CA môže mať niekoľko podpisových kľúčov. Každý podpisový kľúč CA je jedinečne identifikovaný jedinečným identifikátorom ako súčasťou poľa Authority Key Identifier v certifikáte CA.
Certifikačná autorita vydávajúca kvalifikované certifikáty	CA/QC	CA, ktorá spĺňa požiadavky ustanovené v prílohe II k smernici 1999/93/ES a vydáva kvalifikované certifikáty, ktoré spĺňajú požiadavky ustanovené v prílohe I k smernici 1999/93/ES.
Certifikát	Certifikát	Ako je vymedzené v článku 2 ods. 9 smernice 1999/93/ES.
Kvalifikovaný certifikát	QC	Ako je vymedzené v článku 2 ods. 10 smernice 1999/93/ES.
Signatár	Signatár	Ako je vymedzené v článku 2 ods. 3 smernice 1999/93/ES.
Dohľad	Dohľad	Pojem „dohľad“ sa používa v zmysle smernice 1999/93/ES (článok 3 ods. 3). V smernici sa vyžaduje, aby členské štáty zriadili primeraný systém, ktorý umožní dohľad nad CSP so sídlom na ich území vydávajúcimi kvalifikované certifikáty verejnosti a ktorý zabezpečí dohľad nad spĺňaním ustanovení smernice.
Dobrovoľná akreditácia	Akreditácia	Ako je vymedzené v článku 2 ods. 13 smernice 1999/93/ES.
Zoznam dôveryhodných poskytovateľov	TL	Označuje zoznam štatútov dohľadu nad certifikačnými službami/akreditácie certifikačných služieb poskytovateľov certifikačných služieb, ktorí sú pod dohľadom dotknutého členského štátu/ktorých členský štát akreditoval vzhľadom na dodržiavanie ustanovení smernice 1999/93/ES.

▼C1

Pojem	Akronym	Vymedzenie pojmov
Zoznam štatútov dôveryhodnej služby	TSL	Forma podpísaného zoznamu používaná ako základ prezentácie informácií o štatúte dôveryhodnej služby podľa špecifikácií v ETSI TS 102 231.
Dôveryhodná služba		Služba, ktorá zvyšuje dôveru voči elektronickým transakciám (bežne, ale nie nevyhnutne pomocou kryptografických techník alebo dôverného materiálu) (ETSI TS 102 231).
Poskytovateľ dôveryhodných služieb	TSP	Orgán, ktorý prevádzkuje jednu alebo viac (elektronických) dôveryhodných služieb (tento pojem sa používa v širšom zmysle ako CSP).
Token dôveryhodných služieb	TrST	Fyzický alebo binárny (logický) objekt vygenerovaný alebo vydaný v dôsledku využitia dôveryhodnej služby. Príkladom binárnych TrST sú certifikáty, CRL, tokeny časových pečiatok a odpovede OCSP.
Kvalifikovaný elektronický podpis	QES	AdES, ktorý je podporovaný QC a ktorý je vytvorený SSCD, ako je vymedzené v článku 2 smernice 1999/93/ES.
Zdokonalený elektronický podpis	AdES	Ako je vymedzené v článku 2 ods. 2 smernice 1999/93/ES.
Zdokonalený elektronický podpis podporovaný kvalifikovaným certifikátom	$AdES_{QC}$	Ide o elektronický podpis, ktorý spĺňa požiadavky na AdES a je podporovaný QC, ako je vymedzené v článku 2 smernice 1999/93/ES.
Bezpečné zariadenie na vytvorenie podpisu	SSCD	Ako je vymedzené v článku 2 ods. 6 smernice 1999/93/ES.

KAPITOLA I

PODROBNÉ ŠPECIFIKÁCIE SPOLOČNÉHO VZORU „ZOZNAMU DÔVERYHODNÝCH POSKYTOVATEĽOV CERTIFIKAČNÝCH SLUŽIEB, KTORÍ PODLIEHAJÚ DOHĽADU/SÚ AKREDITOVANÍ“

V tejto časti dokumentu sa kľúčové slová „MUSÍ“, „NESMIE“, „POVINNÉ“, „MALO BY“, „NEMALO BY“, „ODPORÚČA SA“, „MÔŽE“, a „VOLITEĽNÉ“ a OZNAMOVACÍ SPÔSOB a PRÍTOMNÝ ČAS pri slovesách veľkými písmenami, ktoré sú obsiahnuté v tomto dokumente, majú vykladať v súlade s opisom uvedeným v RFC2119 ([1]).

►M1 Tieto špecifikácie sú založené na špecifikáciách a požiadavkách uvedených v ETSI TS 102 231 v.3.1.2. Ak sa v týchto špecifikáciách neuvádza žiadna osobitná požiadavka, UPLATŇUJÚ SA požiadavky v ETSI TS 102 231 v.3.1.2 v celom rozsahu. ◄ Ak sa v týchto špecifikáciách uvádzajú osobitné požiadavky MAJÚ prednosť pred zodpovedajúcimi požiadavkami v ETSI TS 102 231, pričom ich dopĺňajú špecifikácie formátu v ETSI TS 102 231. V prípade rozdielov medzi týmito špecifikáciami a špecifikáciami v ETSI TS 102 231 SÚ normatívnymi špecifikáciami tieto špecifikácie.

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

▼C1

Jazyková podpora SA IMPLEMENTUJE a POSKYTUJE minimálne v anglickom jazyku (EN) a potenciálne v jednom alebo viacerých dodatočných národných jazykoch.

Údaj o dátume a čase JE v súlade s odsekom 5.1.4 ETSI TS 102 231.

Používanie URI JE v súlade s odsekom 5.1.5 ETSI TS 102 231.

Informácie o schéme vydávania zoznamu dôveryhodných poskytovateľov

Tag

TSL tag (odsek 5.2.1)

Toto pole je POVINNÉ a JE v súlade s odsekom 5.2.1 ETSI TS 102 231.

▼M1

_____

▼C1

Scheme Information

TSL version identifier (odsek 5.3.1)

Toto pole je POVINNÉ a STANOVUJE sa na hodnotu „3“ (celé číslo).

TSL sequence number (odsek 5.3.2)

▼M1

Toto pole je POVINNÉ a URČUJE číslo sekvencie TSL. Počiatočná hodnota pri prvom vydaní TSL je „1“, pričom táto hodnota celého čísla SA ZVYŠUJE pri každom následnom vydaní TSL. NENASTAVUJE SA späť na „1“, keď sa hodnota uvedeného „TSL version identifier“ zvýši.

▼C1

TSL type (odsek 5.3.3)

▼M1

Toto pole je POVINNÉ a konkretizuje typ TSL. STANOVUJE SA na adrese: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic).

▼C1

Poznámka: Na účely splnenia ETSI TS 102 231 odsek 5.3.3 a na uvedenie špecifického typu TSL pri odkaze na existenciu týchto špecifikácií, ktoré upravujú zavedenie TSL implementácie Zoznamu dôveryhodných poskytovateľov ([1]) členských štátov a aby sa parseru povolilo určiť, aká forma ktoréhokoľvek z nasledujúcich polí ([2]) sa dá očakávať, v prípadoch, keď tieto polia majú osobitné (alebo alternatívne) významy podľa typu reprezentovaného TSL (v tomto prípade ide o Zoznam ČŠ dôveryhodných poskytovateľov), sa ZAREGISTRUJE a OPISUJE uvedené URI takto:

([1]) Teda „Zoznam štatútov dohľadu nad certifikačnými službami/akreditácie certifikačných služieb poskytovateľov certifikačných služieb, ktorí sú pod dohľadom dotknutého členského štátu/ktorých členský štát akreditoval vzhľadom na dodržiavanie príslušných ustanovení smernice 1999/93/ES“ (skrátene „Zoznam dôveryhodných poskytovateľov“).

([2]) Teda polia špecifikované v ETSI TS 102 231 – Elektronické podpisy a infraštruktúry (Electronic Signatures and Infrastructures – ESI): Provision of harmonized Trust-service status information a „profilované“ v súčasných špecifikáciách tak, aby stanovovali v členských štátoch zostavenie Zoznamu dôveryhodných poskytovateľov.

▼M1

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

▼C1

Opis: TSL implementácia zoznamu štatútov dohľadu nad certifikačnou službou poskytovateľov certifikačných služieb/štatútov jej akreditácie, pričom poskytovatelia certifikačných služieb sú pod dohľadom referenčného členského štátu/sú akreditovaní v referenčnom členskom štáte, ktorý je prostredníctvom priameho dohľadu (dobrovoľného alebo na základe právneho predpisu) zodpovedný za spĺňanie príslušných ustanovení v smernici 1999/93/ES.

Scheme operator name (odsek 5.3.4)

Toto pole je POVINNÉ. ŠPECIFIKUJE sa v ňom názov orgánu členského štátu zodpovedného za zostavenie, uverejňovanie a vedenie vnútroštátneho zoznamu dôveryhodných poskytovateľov. ŠPECIFIKUJE formálny názov, pod ktorým pridružený právny subjekt alebo subjekt, ktorému sa udelil mandát (napr. v prípade vládnych administratívnych agentúr), pridružený k uvedenému orgánu, pôsobí. MUSÍ to byť názov, ktorý sa použil pri formálnej právnej registrácii alebo schválení a na ktorý treba adresovať všetku formálnu komunikáciu. JE to sekvencia viacjazyčných reťazcov znakov a IMPLEMENTUJE sa v angličtine (EN) ako povinnom jazyku a prípadne v jednom alebo viacerých národných jazykoch.

Poznámka: Krajiny MÔŽU mať oddelené dozorné a akreditačné orgány, ako aj dodatočné orgány zodpovedné za akékoľvek operatívne súvisiace činnosti. ►M1 Určenie prevádzkovateľa schémy (scheme operator) TSL implementácie TL členských štátov spadá do kompetencie členských štátov. ◄ Vychádza sa z predpokladu, že dozorný orgán, akreditačný orgán a prevádzkovateľ schémy (v prípade, že ide o rozličné orgány) budú všetky mať svoje vlastné úlohy a oblasti, za ktoré budú zodpovedné.

Všetky situácie, keď za dohľad, akreditáciu alebo operačné aspekty sú zodpovedné viaceré orgány, sa neprestajne ZVAŽUJÚ a ako také IDENTIFIKUJÚ v Scheme information ako súčasti TL vrátane informácií špecifických pre danú schému uvedených pomocou „Scheme information URI“ (odsek 5.3.7).

▼M1

Vymenovaný prevádzkovateľ schémy (scheme operator) (odsek 5.3.4) je subjekt, ktorý podpíše TSL.

▼C1

Scheme operator address (odsek 5.3.5)

Toto pole je POVINNÉ. ŠPECIFIKUJE adresu právneho subjektu alebo organizácie, ktorej sa udelil mandát, identifikovanej v poli „Scheme operator name“ (odsek 5.3.4) na účely poštovej a elektronickej komunikácie. OBSAHUJE „PostalAddress“ (ulicu, lokalitu [štát alebo región]], [poštové smerovacie číslo] a kód krajiny podľa ISO 3166-1 alpha-2) v súlade s odsekom 5.3.5.1, ako aj „ElectronicAddress“ (t. j. e-mail: a/alebo webovú stránku URI) v súlade s odsekom 5.3.5.2.

Scheme name (odsek 5.3.6)

Toto pole je POVINNÉ a špecifikuje názov prevádzkovanej schémy. JE to sekvencia viacjazyčných reťazcov znakov (v EN ako povinnom jazyku a prípadne v jednom alebo viacerých národných jazykoch), podľa tohto vymedzenia:

▼C1

— EN verzia JE reťazec znakov s takouto štruktúrou:

CC:EN_name_value

pričom

— „CC“ = kód krajiny podľa ISO 3166-1 alpha-2 použitý v poli „Scheme territory“ (odsek 5.3.10),

— „:“ = sa používa na oddeľovanie polí,

▼M1

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

▼C1

— Verzia v národnom jazyku ktoréhokoľvek členského štátu JE reťazec znakov s takouto štruktúrou:

CC:name_value

pričom

— „CC“ = kód krajiny podľa ISO 3166-1 alpha-2 použitý v poli „Scheme territory“ (odsek 5.3.10,)

— „:“ = sa používa na oddeľovanie polí,

— „name_value“ = oficiálny preklad uvedeného „EN_name_value“ do národného jazyka.

Názov schémy je povinný na účely jednoznačnej identifikácie podľa názvu schémy, na ktorú sa odkazuje prostredníctvom „Scheme information URI“ a takisto na zabezpečenie toho, že v prípade, ak prevádzkovateľ schémy prevádzkuje viaceré schémy, každá schéma má jasne odlíšiteľný názov.

Členské štáty a prevádzkovatelia schémy ZABEZPEČUJÚ, aby v prípade, ak členské štáty alebo prevádzkovateľ schémy prevádzkujú viac ako jednu schému, každá schéma mala jasne odlíšiteľný názov.

Scheme information URI (odsek 5.3.7)

Toto pole je POVINNÉ a ŠPECIFIKUJE URI, na ktorých používatelia (spoliehajúce sa strany) môžu získať špecifické informácie o schéme (pričom EN je povinný jazyk s prípadne jedným alebo viacerými národnými jazykmi). JE to sekvencia viacjazyčných ukazovateľov (v EN ako povinnom jazyku a prípadne v jednom alebo viacerých národných jazykoch). Uvedené URI, na ktoré sa odkazuje, MUSIA zabezpečovať prístup k informáciám o „primeraných informáciách o schéme“.

„Primerané informácie o schéme“ ZAHŔŇAJÚ minimálne:

— Všeobecné úvodné informácie, spoločné pre všetky členské štáty, o rozsahu a súvislostiach zoznamu dôveryhodných poskytovateľov a schémach dohľadu/akreditačných schémach, na ktorých sú založené. Znenie spoločného textu, ktorý sa má použiť:

▼C1

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

The Trusted List aims at:

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

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

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3,2 and Art. 7.1(a)), including information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable ‚supervision' system (respectively ‚voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3,3, Art. 8,1, Art. 11 (respectively, Art.2.13, Art. 3,2, Art 7.1(a), Art. 8,1, Art. 11)

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

— Konkrétne informácie o základných schémach dohľadu/akreditačných schémach, predovšetkým ([1]):

— informácie o systéme dohľadu, ktorý sa vzťahuje na všetky CSP_{QC};

([1]) Posledné dva súbory informácií sú mimoriadne dôležité pre spoliehajúce sa strany na posúdenie kvality a stupňa bezpečnosti týchto systémov dohľadu/akreditácie. Tieto súbory informácií sa uvádzajú na úrovni TL pomocou súčasných „Scheme information URI“ (odsek 5.3.7 – informácie, ktoré poskytujú členské štáty), „Scheme type/community/rules“ (odsek 5.3.9 – pomocou textu spoločného pre všetky členské štáty) a „TSL policy/legal notice“ (odsek 5.3.11 – text spoločný pre všetky členské štáty odvolávajúci sa na smernicu 1999/93/ES, spolu s možnosťou doplniť texty/referencie špecifické pre daný členský štát). Dodatočné informácie o vnútroštátnych systémoch dohľadu/akreditácie pre CSP, ktorí nevydávajú QC, sa môžu, v prípade potreby a ak sa o to požiada, poskytovať na úrovni služby (napr. na účely odlíšenia viacerých úrovní kvality/bezpečnosti) pomocou „Scheme service definition URI“ (odsek 5.5.6).

▼C1

— v prípade potreby informácie o vnútroštátnej schéme dobrovoľnej akreditácie, ktorá sa vzťahuje na všetky CSP_{QC};

— v prípade potreby, informácie o systéme dohľadu, ktorý sa vzťahuje na všetky CSP nevydávajúce QC,

— v prípade potreby informácie o vnútroštátnej schéme dobrovoľnej akreditácie, ktorá sa vzťahuje na všetky CSP nevydávajúce QC.

— Tieto konkrétne informácie ZAHŔŇAJÚ pri každej uvedenej základnej schéme minimálne:

— všeobecný opis,

— informácie o postupe dozorného orgánu/akreditačného orgánu pri vykonávaní dohľadu nad CSP/akreditácii CSP a o postupe CSP pri dohľade, ktorému podlieha/pri akreditácii;

— informácie o kritériách, podľa ktorých sa vykonáva dohľad nad CSP/podľa ktorých sú CSP akreditované.

— V prípade potreby konkrétne informácie o špecifických „kvalifikáciách“, na ktoré môžu niektoré z fyzických alebo binárnych (logických) objektov vygenerované alebo vydané v dôsledku poskytovania certifikačnej služby byť oprávnené na základe svojho súladu s ustanoveniami a požiadavkami platnými na vnútroštátnej úrovni vrátane významu takejto „kvalifikácie“ a pridružených vnútroštátnych ustanovení a požiadaviek.

Dodatočne sa MÔŽU poskytnúť dodatočné špecifické informácie členských štátov o schéme. Takéto informácie ZAHŔŇAJÚ:

— informácie o kritériách a pravidlách uplatnených pri výbere osôb vykonávajúcich dozor/audítorov a pri vymedzení spôsobu, akým nad CSP vykonávajú dohľad (spôsob ich kontroly)/spôsobu, akým ich akreditujú (spôsob vykonávania auditu),

— iné kontaktné a všeobecné informácie, ktoré sa týkajú prevádzkovania schémy.

Status determination approach (odsek 5.3.8)

Toto pole je POVINNÉ a ŠPECIFIKUJE identifikátor koncepcie určovania štatútu. POUŽÍVA sa tento URI tak, ako sa tu registruje a opisuje:

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

Opis: Štatút služieb na zozname v príslušnom členskom štáte určuje prevádzkovateľ schémy alebo sa určuje v jeho mene v rámci vhodného systému, ktorý umožňuje „dohľad“ nad poskytovateľmi certifikačných služieb (a prípadne ich „dobrovoľnú akreditáciu“), ktorí majú sídlo na jeho území (alebo v tretej krajine v prípade „dobrovoľnej akreditácie)“ a vydávajú kvalifikované certifikáty pre verejnosť v súlade s článkom 3 ods. 3 [prípadne článkom 3 ods. 2 alebo článkom 7 ods. 1 písm. a)] smernice 1999/93/ES, a v prípade potreby umožňuje „dohľad“ nad poskytovateľmi certifikačných služieb, ktorí nevydávajú kvalifikované certifikáty/ich „dobrovoľnú akreditáciu“ podľa vnútroštátne vymedzených a zriadených „uznaných schém schvaľovania CSP“ vnútroštátne implementovaných na účely dohľadu nad tým, či služby, ktoré CSP nevydávajúce QC poskytujú, spĺňajú ustanovenia v smernici 1999/93/ES potenciálne rozšírené o vnútroštátne ustanovenia o poskytovaní takýchto certifikačných služieb.

▼C1

Scheme type/community/rules (odsek 5.3.9)

Toto pole je POVINNÉ a OBSAHUJE minimálne tieto registrované URI:

— URI spoločný pre všetky zoznamy dôveryhodných poskytovateľov členských štátov, ktorý odkazuje na opisný text, ktorý JE uplatniteľný na všetky TL

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

— ktorým sa označuje účasť schémy členského štátu (identifikovanej pomocou „TSL type“ [odsek 5.3.3) and „Scheme name“ (odsek 5.3.6)] na schéme schém (teda TSL so zoznamom ukazovateľov na všetky členské štáty, ktoré uverejňujú a vedú TL vo forme TSL),

— kde používatelia majú prístup k politikám/pravidlám, na základe ktorých sa služby na zozname POSUDZUJÚ a dá sa určiť typ TSL (pozri odsek 5.3.3),

— kde používatelia majú prístup k opisu ako využívať a vykladať obsah TSL implementácie zoznamu dôveryhodných poskytovateľov. Tieto pravidlá používania SÚ spoločné pre všetky zoznamy dôveryhodných poskytovateľov členských štátov, bez ohľadu na typ služby na zozname a systémy dohľadu/akreditácie.

Opisný text:

„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. decembra 1999 on a Community framework for electronic signatures.

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

Policy/rules for the assessment of the listed services

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3,2 and Art. 7.1(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

▼C1

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable ‚supervision' system (respectively ‚voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3,3, Art. 8,1, Art. 11 (respectively, Art.2.13, Art. 3,2, Art 7.1(a), Art. 8,1, Art. 11).

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

CSPs not issuing QCs but providing ancillary services, may fall under a ‚voluntary accreditation' system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined ‚recognised approval scheme' implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Art. 2,11 of the Directive). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific ‚qualification' on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a ‚qualification' is likely to be limited solely to the national level.

Interpretation of the TSL implementation of the Trusted List

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

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

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

▼C1

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

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

— to indicate the nature of the SSCD support:

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

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

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

AND/OR

— to indicate issuance to Legal Person:

— ‚QCForLegalPerson' qualifier value meaning ‚Certificate issued to a Legal Person'

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

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

▼C1

— Špecifický URI pre zoznam dôveryhodných poskytovateľov každého členského štátu, ktorý je odkazom na opisný text, ktorý JE uplatniteľný na TL tohto členského štátu:

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

pričom „CC“ = kód krajiny podľa ISO 3166-1 alpha-2 použitý v poli „Scheme territory“ (odsek 5.3.10):

— kde používatelia majú prístup k osobitným politikám/pravidlám dotknutého členského štátu, podľa ktorých sa služby na zozname POSUDZUJÚ v súlade s vhodným systémom dohľadu a schémami dobrovoľnej akreditácie členského štátu,

— kde používatelia majú prístup k osobitnému opisu členského štátu ako používať a vykladať obsah TSL implementácie zoznamu dôveryhodných poskytovateľov vzhľadom na certifikačné služby, ktoré nesúvisia s vydávaním QC. Tento opis sa môže použiť na znázornenie možnej nesúrodosti vnútroštátnych systémov dohľadu/akreditácie súvisiacich s CSP, ktorí nevydávajú QC, a toho, ako sa na tento účel používajú polia „Scheme service definition URI“ (odsek 5.5.6) a „Service information extension“.

Členské štáty MÔŽU vymedziť dodatočné URI k uvedenému URI špecifickému pre daný členský štát (teda URI vymedzené na základe tohto hierarchického špecifického URI).

Scheme territory (odsek 5.3.10)

V súvislosti s týmito špecifikáciami je toto pole POVINNÉ a ŠPECIFIKUJE krajinu, v ktorej je schéma zriadená (kód krajiny podľa ISO 3166-1 alpha-2).

TSL policy/legal notice (odsek 5.3.11)

V súvislosti s týmito špecifikáciami je toto pole POVINNÉ a ŠPECIFIKUJE politiku schémy alebo sa v ňom uvádza právny štatút schémy alebo právne požiadavky, ktoré schéma spĺňa, na území, pod ktorého právomoc spadá, a/alebo obmedzenia a podmienky, za ktorých sa TL vedie a uverejňuje.

JE to viacjazyčný reťazec znakov (vo formáte „plain text“) pozostávajúci z dvoch častí:

— Prvej, povinnej časti, spoločnej pre TL všetkých členských štátov (v EN ako povinnom jazyku a prípadne v jednom alebo viacerých národných jazykoch), v ktorom sa uvádza, že platným právnym rámcom je smernica 1999/93/ES a jej zodpovedajúca implementácia v právnych predpisoch členských štátoch sa uvedie v poli „Scheme Territory“.

Anglická verzia spoločného znenia:

„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. decembra 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.“

▼C1

Znenie v národnom jazyku (národných jazykoch) členského štátu: [úradný preklad (preklady) uvedeného anglického znenia].

— Druhej, dobrovoľnej časti, špecifickej pre každý TL (v EN ako povinnom jazyku a prípadne v jednom alebo viacerých národných jazykoch) s odkazmi na osobitné uplatniteľné vnútroštátne právne rámce (napr. predovšetkým vtedy, ak sa týkajú vnútroštátnych schém dohľadu/akreditácie CSP, ktorí nevydávajú QC).

Historical information period (odsek 5.3.12)

Toto pole je POVINNÉ a ŠPECIFIKUJE dobu (celým číslom), počas ktorej sa v TSL poskytujú historické informácie. Táto hodnota vyjadrená pomocou celého čísla označuje počet dní a v súvislosti s týmito špecifikáciami JE väčšia alebo SA ROVNÁ 3 653 (čo znamená, že TSL implementácia TL členských štátov MUSÍ obsahovať historické informácie za minimálne desať rokov). Pri väčších hodnotách by sa náležitým spôsobom mali zohľadniť právne požiadavky na uchovávanie údajov v členskom štáte uvedenom v „Scheme Territory“ (odsek 5.3.10)

Pointers to other TSLs (odsek 5.3.13)

V súvislosti s týmito špecifikáciami je toto pole POVINNÉ a ZAHŔŇA ukazovateľa, ak je taký k dispozícii, na zoznam liniek (ukazovateľov) na všetky TSL implementácie zoznamov dôveryhodných poskytovateľov členských štátov, ktorý zostavila EK a je v podobe zodpovedajúcej ETSI TS 102 231. Špecifikácie ETSI TS 102 231, odsek 5.3.13 sa uplatňujú, pričom je povinné použitie voliteľnej digitálnej totožnosti, ktorá predstavuje vydavateľa TSL, na ktorého sa odkazuje, vo formáte podľa odseku 5.5.3.

Poznámka: Toto pole sa NEPOUŽÍVA, pokiaľ sa čaká na implementáciu zoznamu liniek k TSL implementácii TL jednotlivých členských štátov, ktorý zostavila EK, podľa ETSI TS 102 231.

List issue date and time (odsek 5.3.14)

Toto pole je POVINNÉ a ŠPECIFIKUJE dátum a čas (UTC vyjadrený ako Zulu), keď sa TSL vydal pomocou hodnoty dátum-čas, ako je špecifikované v ETSI TS 102 231 odsek 51.4.

Next update (odsek 5.3.15)

Toto pole je POVINNÉ a ŠPECIFIKUJE najneskorší dátum a čas (UTC vyjadrený ako Zulu), keď sa vydá nasledujúci TSL alebo JE prázdne, čo znamená, že TSL sa uzatvoril (pomocou hodnoty dátum-čas, ako je špecifikované v ETSI TS 102 231, odsek 5.1.4).

Ak sa pri TSP alebo akejkoľvek službe patriacej do schémy priebežne štatút nezmení, MUSÍ sa po uplynutí platnosti posledne vydaného TSL vydať nový TSL.

V súvislosti s týmito špecifikáciami rozdiel medzi dátumom a časom „Next update“ a „List issue date and time“ NEPRESAHUJE šesť (6) mesiacov.

▼C1

Distribution points (odsek 5.3.16)

Toto pole je VOLITEĽNÉ. Ak sa použije, ŠPECIFIKUJE lokality, kde je uverejnená aktuálna TSL implementácia TL a kde možno nájsť aktualizácie platnej TSL. Ak sú špecifikované viaceré distribučné miesta, všetky MUSIA poskytovať identické kópie platného TSL alebo jeho aktualizovanej verzie. Ak sa toto pole používa, formátuje sa ako neprázdna sekvencia reťazcov, pričom všetky musia byť v súlade s RFC 3986 ([1]).

Scheme extensions (odsek 5.3.17)

Toto pole je VOLITEĽNÉ a v súvislosti s týmito špecifikáciami sa nepoužíva.

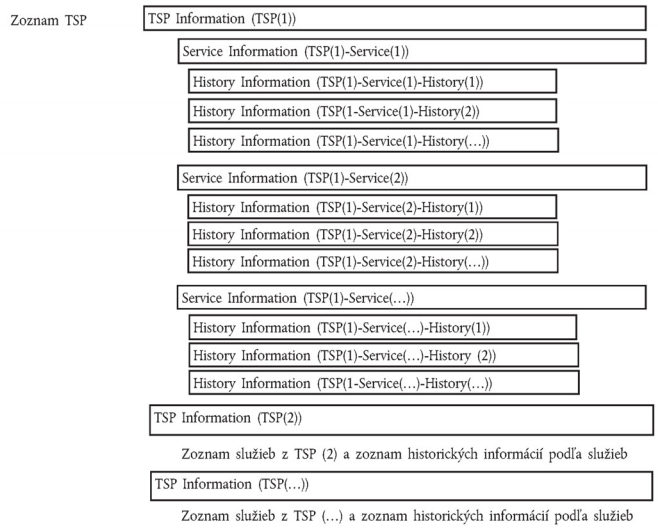
List of Trust Service Providers

Toto pole je VOLITEĽNÉ.

V prípade, že sa v dotknutom členskom štáte v rámci schémy nevykonával dohľad nad žiadnymi CSP/žiadne CSP neakreditovali, toto pole SA VYNECHÁVA. Dohodlo sa však, že aj v prípade, ak členský štát v rámci schémy nad žiadnym CSP nevykonáva dohľad/žiadny CSP neakreditoval, IMPLEMENTUJE TSL a toto pole je vynechané. Absencia CSP na zozname ZNAMENÁ, že v krajine určenej v „Scheme Territory“ sa nevykonáva dohľad na žiadnym CSP/sa žiadny CSP neakreditoval.

Ak sa v rámci schémy vykonáva alebo vykonával dohľad nad jedným alebo viacerými CSP/jeden alebo viaceré CSP sú alebo boli akreditované, potom pole OBSAHUJE sekvenciu identifikujúcu každý CSP poskytujúci jednu alebo viac služieb, nad ktorými sa vykonáva dohľad/ktoré sú akreditované, spolu s podrobnosťami o štatúte dohľadu/akreditácie a historického štatútu služieb CSP (TSP = CSP v nasledujúcom obrázku).

▼C2



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

▼C1

Zoznam TSP je zorganizovaný tak, ako je znázornené v uvedenom obrázku. Pre každý TSP existuje sekvencia polí s informáciami o TSP („TSP Information“), za ktorou nasleduje zoznam služieb. Pre každú takúto službu na zozname existuje sekvencia polí s informáciami o službe („Service Information“) a sekvencia polí o histórii schvaľovania štatútu služby („Service approval history“).

TSP Information

TSP(1)

TSP name (odsek 5.4.1)

Toto pole je POVINNÉ a ŠPECIFIKUJE názov **právneho subjektu** zodpovedného za služby CSP, ktoré sú alebo boli v rámci tejto schémy pod dohľadom/sú alebo boli akreditované. Je to sekvencia viacjazyčných reťazcov znakov (v EN ako povinnom jazyku a prípadne v jednom alebo viacerých národných jazykoch). MUSÍ to byť názov, ktorý sa použil na formálne zákonné registrácie a na ktorý sa adresuje všetka formálna komunikácia.

TSP trade name (odsek 5.4.2)

Toto pole je VOLITEĽNÉ a ak je zahrnuté, ŠPECIFIKUJE alternatívny názov, pomocou ktorého sa CSP sám identifikuje v konkrétnej situácii poskytovania tých služieb, ktoré sú uvedené v tomto TSL v jeho zázname „TSP name“ (odsek 5.4.1).

Poznámka: V prípadoch, keď jeden právny subjekt CSP poskytuje služby pod rozličnými obchodnými názvami alebo v rozličných konkrétnych situáciách, môže byť toľko záznamov CSP, koľko je konkrétnych situácií (teda záznamy o názvoch/obchodných názvoch). Inou možnosťou je zapísať každý CSP (právny subjekt) iba raz a uviesť informácie o službe v konkrétnych situáciách. Za prediskutovanie tejto otázky a určenie najlepšieho prístupu v spolupráci s CSP je zodpovedný prevádzkovateľ schémy členského štátu.

TSP address (odsek 5.4.3)

Toto pole je povinné a ŠPECIFIKUJE adresu právneho subjektu alebo organizácie, ktorej sa udelil mandát, identifikovanej v poli „TSP name“ (odsek 5.4.1) na účely poštovej i elektronickej komunikácie. OBSAHUJE „PostalAddress“ (teda ulicu, lokalitu [štát alebo región], [PSČ] a kód krajiny podľa ISO 3166-1 alpha-2) v súlade s odsekom 5.3.5.1 a „ElectronicAddress“ (teda e-mail: a/alebo webovú stránku URI) v súlade s odsekom 5.3.5.2.

TSP information URI (odsek 5.4.4)

Toto pole je POVINNÉ a ŠPECIFIKUJE URI, na ktorých používatelia (teda spoliehajúce sa strany) môžu získať konkrétne informácie o CSP. JE to sekvencia viacjazyčných ukazovateľov (v EN ako povinnom jazyku a prípadne v jednom alebo viacerých národných jazykoch). Uvedené URI MUSIA zabezpečovať prístup k informáciám o všeobecných podmienkach CSP, jeho praktikách, právnych otázkach a stratégiách starostlivosti o zákazníka a k iným generickým informáciám, ktoré sa týkajú všetkých jeho služieb uvedených v zázname CSP v TSL.

Poznámka: V prípadoch, keď jeden právny subjekt CSP poskytuje služby pod rozličnými obchodnými názvami alebo v rozličných konkrétnych situáciách, a táto skutočnosť sa odrazila v takom istom počte záznamov TSP ako je počet konkrétnych situácií, ŠPECIFIKUJÚ sa v tomto poli informácie týkajúce sa konkrétneho súboru služieb na zozname v rámci konkrétneho záznamu TSP/TraderName.

▼C1

TSP information extensions (odsek 5.4.5)

Toto pole je VOLITEĽNÉ a, ak je zahrnuté, MÔŽE ho použiť prevádzkovateľ schémy v súlade so špecifikáciami ETSI TS 102 231 (odsek 5.4.5) na poskytnutie osobitných informácií, ktoré sa vyložia podľa pravidiel predmetnej schémy.

List of Services

Toto pole je POVINNÉ a OBSAHUJE sekvenciu identifikujúcu každú z uznaných služieb CSP a štatút schvaľovania (a históriu tohto štatútu) dotknutej služby. Musí sa uviesť minimálne jedna služba (aj vtedy, ak má informácia výlučne historický charakter).

Keďže uchovávanie historických informácií o službách na zozname je podľa týchto špecifikácií POVINNÉ, MUSIA sa tieto historické informácie uchovávať aj vtedy, ak by si platný štatút služby za normálnych okolností nevyžadoval ich uvedenie na zozname (napr. ak sa služba zrušila). Preto CSP MUSÍ byť zahrnutý aj vtedy, keď jeho jediná služba na zozname má len taký štatút, aby sa uchovali záznamy o jej histórii.

Service Information

TSP(1) Service(1)

Service type identifier (odsek 5.5.1)

▼M1

Toto pole je POVINNÉ a ŠPECIFIKUJE identifikátor typu služby podľa typu týchto špecifikácií TSL (teda „/eSigDir-1999-93-EC-TrustedList/TSLType/generic“).

▼C1

Keď služba na zozname súvisí s vydávaním kvalifikovaných certifikátov, uvedeným URI JE http://uri.etsi.org/TrstSvc/Svctype/CA/QC (certifikačná autorita vydávajúca kvalifikované certifikáty).

Keď služba na zozname súvisí s vydávaním tokenov dôveryhodnej služby, ktoré nie sú QC a nepodporujú vydávanie QC, uvedeným URI JE jeden z URI vymedzených v ETSI 102 231 a nachádzajúci sa na zozname v odseku D.2, ktorá sa týka tohto poľa. Toto SA UPLATŇUJE aj v prípade tých tokenov dôveryhodnej služby, ktoré sú pod dohľadom/sú akreditované vzhľadom na dodržiavanie konkrétnych kvalifikácií podľa vnútroštátnych právnych predpisov členských štátov (napr. tzv. kvalifikovaný token časovej pečiatky v DE alebo HU), uvedeným URI JE jeden z URI vymedzených v ETSI 102 231 a nachádzajúci sa na zozname v odseku D.2, ktorý sa týka tohto poľa (teda TSA pre vnútroštátne vymedzené kvalifikované tokeny časovej pečiatky). V prípade potreby sa tieto osobitné vnútroštátne kvalifikácie tokenov dôveryhodnej služby MÔŽU uviesť v zázname o službe a na tento účel SA POUŽÍVA rozšírenie additionalServiceInformation (odsek 5.8.2) v odseku 5.5.9 („Service information extension“).

▼C1

Všeobecnou automatickou zásadou je, že pri certifikačných službách na zozname služieb poskytovaných CSP na zozname dôveryhodných poskytovateľov (teda certifikačná autorita (priamo) vydávajúca QC) JE za každý certifikát X.509v3 (napr. typ certifikačnej služby CA/QC) jeden záznam. V určitých opatrne zvážených okolnostiach a pozorne riadených a schválených podmienkach sa dozorný/akreditačný orgán členského štátu MÔŽE rozhodnúť použiť certifikát X.509v3 koreňovej CA alebo CA vyššieho stupňa (teda certifikačnej autority, ktorá nevydáva priamo QC konečného subjektu, ale ktorá certifikuje hierarchiu CA až po CA, ktoré priamo vydávajú QC konečného subjektu) ako „Sdi“ jedného záznamu v zozname služieb CSP na zozname dôveryhodných poskytovateľov. Dôsledky (výhody a nevýhody) použitia certifikátu X.509v3 koreňovej CA alebo CA vyššej úrovne ako hodnoty „Sdi“ údajov o službách v TL musia členské štáty dôkladne zvážiť a schváliť ([1]). Okrem toho, ak sa členské štáty rozhodnú využiť takúto povolenú výnimku z automatickej zásady, MUSIA poskytnúť potrebnú dokumentáciu, aby sa uľahčilo vytváranie a overovanie certifikačnej cesty.

Poznámka: TSP ako respondery OCSP alebo vydavatelia CRL, ktorí sú súčasťou certifikačných služieb CSP_{QC} a používajú dva odlišné páry kľúčov na podpisovanie odpovedí OCSP a CRL sa MÔŽU takisto uviesť v platnom vzore TSL pomocou týchto kombinácií URI:

— Hodnota „Service type identifier“ („Sti“) (odsek 5.5.1):

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

v kombinácii s touto hodnotou „Service information extension“ (odsek 5.5.9) rozšírenia additionalServiceInformation (odsek 58.2):

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

Opis: poskytovateľ štatútu certifikátu prevádzkujúci OCSP server ako súčasť služby poskytovanej CSP vydávajúcim kvalifikované certifikáty.

— Hodnota „Service type identifier“ („Sti“) (odsek 5.5.1):

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

v kombinácii s touto hodnotou „Service information extension“ (odsek 5.5.9) rozšírenia additionalServiceInformation (odsek 5.8.2):

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

Opis: poskytovateľ štatútu certifikátu prevádzkujúci CRL ako súčasť služby poskytovanej CSP vydávajúcim kvalifikované certifikáty.

— Hodnota „Service type identifier“ („Sti“) (odsek 5.5.1):

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

([1]) Použitie certifikátu X.509v3 koreňovej CA ako hodnoty „Sdi“ pre službu na zozname bude pohnútkou pre prevádzkovateľa schémy posúdiť celý súbor certifikačných služieb v rámci takejto koreňovej CA ako celku vzhľadom na „štatút dohľadu/akreditácie“. To znamená, že akákoľvek zmena štatútu požadovaná jedinou CA v rámci uvedenej koreňovej hierarchie prinúti celú hierarchiu prebrať túto zmenu štatútu.

▼C1

v kombinácii s touto hodnotou „Service information extension“ (odsek 5.5.9) rozšírenie additionalServiceInformation (odsek 5.8.2):

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

Opis: Koreňová certifikačná autorita, od ktorej možno určiť priebeh certifikačnej cesty až po certifikačnú autoritu vydávajúcu kvalifikované certifikáty.

— Hodnota „Service type identifier“ („Sti“) (odsek 5.5.1):

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

v kombinácii s touto hodnotou „Service information extension“ (odsek 5.5.9) rozšírenia additionalServiceInformation (odsek 5.8.2):

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

Opis: služba časovej pečiatky ako súčasť služby poskytovateľa certifikačnej služby vydávajúceho kvalifikované certifikáty, ktoré vydávajú TST, ktoré sa môžu použiť pri overovaní kvalifikovaného podpisu na určenie a predĺženie platnosti podpisu v prípadoch, keď je QC zrušený alebo uplynula jeho platnosť.

Service name (odsek 5.5.2)

Toto pole je POVINNÉ a ŠPECIFIKUJE názov, pod ktorým CSP identifikovaný v „TSP name“ (odsek 5.4.1) poskytuje služby identifikované v „Service type identifier“ (odsek 5.5.1). JE to sekvencia viacjazyčných reťazcov znakov (v EN ako povinnom jazyku a prípadne v jednom alebo viacerých národných jazykoch).

Service digital identity (odsek 5.5.3)

Toto pole je POVINNÉ a ŠPECIFIKUJE minimálne jedno znázornenie digitálneho identifikátora jedinečného pre službu, ktorej typ sa určil v „Service type indentifier“ (odsek 5.5.1), na základe ktorého možno službu jednoznačne identifikovať.

V týchto špecifikáciách JE digitálnym identifikátorom použitým v tomto poli príslušný certifikát X.509v3, ktorý predstavuje verejné kľúče, ktoré CSP využíva na poskytovanie služieb, ktorých typ je určený v „Service type identifier“ (odsek 5.5.1) (teda kľúč, ktorý používa koreňová CA/QC, kľúč používaný na podpisovanie certifikátov [1]) alebo vydávanie tokenov časovej pečiatky alebo podpisovanie CRL alebo odpovedí OCSP). Tento príslušný certifikát X.509v3 SA POUŽÍVA ako minimálny vyžadovaný digitálny identifikátor (pretože predstavuje verejné kľúče, ktoré CSP používajú na poskytovanie služby na zozname). Dodatočné identifikátory sa MÔŽU použiť, ako sa uvádza ďalej, pričom sa ale MUSIA vzťahovať na tú istú identitu (teda príslušný certifikát X.509v3):

[1] Môže to byť certifikát CA vydávajúcej certifikáty konečného subjektu (napr. CA/PKC, CA/QC) **alebo** certifikát dôveryhodnej koreňovej CA, od ktorej možno určiť priebeh certifikačného procesu až po kvalifikované certifikáty konečného subjektu. V závislosti od toho, či sa tieto informácie a informácie v každom certifikáte konečného subjektu vydané touto dôveryhodnou koreňovou CA môžu použiť na jednoznačné určenie primeraných charakteristík akéhokoľvek kvalifikovaného certifikátu, alebo nie, môže byť potrebné doplniť tieto informácie („Service digital identity“) údajmi zo „Service information extensions“ (pozri odsek 55.9).

▼C1

a) názov DN („Distinguished name“ – DN) certifikátu, ktorý sa môže použiť na overovanie elektronických podpisov služby CSP špecifikovanej v „Service type identifier“ (odsek 5.5.1);

b) príslušný identifikátor verejného kľúča (teda X.509v3 SubjectKeyIdentifier alebo hodnota SKI);

c) príslušný verejný kľúč.

Všeobecnou automatickou zásadou je, že digitálny identifikátor (t. j. príslušný certifikát X.509v3) sa na zozname dôveryhodných poskytovateľov NENACHÁDZA viac ako jedenkrát, teda za jeden certifikát X.509v3 JE vždy jeden záznam pri certifikačnej službe v rámci certifikačných služieb CSP na zozname dôveryhodných poskytovateľov. Naopak, jeden certifikát X.509v3 SA POUŽÍVA v jedinom zázname o službe ako hodnota „Sdi“.

Poznámka 1: Jediný prípad, keď nie je možné postupovať podľa uvedenej všeobecnej automatickej zásady, je situácia, keď sa jeden certifikát X509v3 používa pri vydávaní rozličných typov tokenov dôveryhodnej služby, na ktoré sa vzťahujú rôzne schémy dohľadu/akreditácie, napríklad jeden certifikát X.509v3 používa CSP na jednej strane pri vydávaní QC v rámci vhodného systému dohľadu a na druhej strane pri vydávaní nekvalifikovaných certifikátov s iným štatútom dohľadu/akreditácie. V tomto prípade a príklade by sa použili dva záznamy s rôznymi hodnotami „Sti“ (teda CA/QC, ako aj CA/PKC v uvedenom príklade) a s rovnakou hodnotou „Sdi“ (príslušný certifikát X.509v3).

Implementácie závisia od ASN.1 alebo XML a SÚ v súlade so špecifikáciami ETSI TS 102 231 (v prípade ASN.1 pozri prílohu A ETSI TS 102 231 a v prípade XML pozri prílohu B ETSI TS 102 231).

Poznámka 2: Keď treba vzhľadom na záznam identifikovanej služby poskytnúť dodatočné „kvalifikačné“ informácie, prevádzkovateľ schémy v prípade potreby ZVÁŽI použitie rozšírenia „additionalServiceInformation“ (odsek 58.2) poľa „Service information extension“ (odsek 5.5.9) podľa účelu, na ktorý sa takéto dodatočné „kvalifikačné“ informácie poskytujú. Prevádzkovateľ schémy môže takisto dobrovoľne použiť odsek 5.5.6 („Scheme service definition URI“).

Service current status (odsek 5.5.4)

Toto pole je POVINNÉ a ŠPECIFIKUJE identifikátor štatútu služby pomocou jedného z týchto URI:

— ►C2 **Under Supervision (Pod dohľadom)** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision),

— ►C2 **Supervision of Service in Cessation (Dohľad nad službou sa ukončuje)** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation),

— ►C2 **Supervision Ceased (Dohľad ukončený)** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased),

— ►C2 **Supervision Revoked (Dohľad zrušený)** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked),

▼M1

— ►C2 **Accredited (Akreditácia)** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited),

▼C1

— ►C2 **Accreditation Ceased (Akreditácia ukončená)** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased),

— ►C2 **Accreditation Revoked (Akreditácia zrušená)** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

Uvedené štatúty SA VYKLADAJÚ v súvislosti s týmito špecifikáciami zoznamu dôveryhodných poskytovateľov takto:

— ***Pod dohľadom:*** Služba identifikovaná v „Service digital identity“ (odsek 5.5.3), ktorú poskytuje poskytovateľ certifikačnej služby (CSP) identifikovaný v „TSP name“ (odsek 5.4.1), je v súčasnosti pod dohľadom vzhľadom na dodržiavanie ustanovení smernice 1999/93/ES v členskom štáte identifikovanom v „Scheme territory“ (odsek 5.3.10), v ktorom má CSP sídlo.

▼M1

— ***Dohľad nad službou sa ukončuje::*** Dohľad nad službou identifikovanou v „Service digital identity“ (odsek 5.5.3), poskytovanou CSP identifikovaným v „TSP name“ (odsek 5.4.1), sa v súčasnosti ukončuje, pričom služba zostáva pod dohľadom dovtedy, kým sa dohľad neukončí alebo nezruší. V prípade, že zodpovednosť za túto ukončovaciu fázu prebrala iná právnická osoba ako právnická osoba identifikovaná v „TSP name“, identifikácia tejto novej alebo záložnej právnickej osoby (záložný CSP) sa uvedie v „Scheme service definition URI“ (odsek 5.5.6) a v rozšírení „TakenOverBy“ (odsek L.3.2) záznamu o službe.

▼C1

— ***Dohľad ukončený:*** Platnosť posúdenia dohľadu uplynula bez toho, aby sa služba identifikovaná v „Service digital identity“ (odsek 5.5.3) opätovne posúdila. Služba momentálne nie je pod dohľadom od dátumu aktuálneho štatútu, pretože sa usudzuje, že služba ukončila svoje operácie.

— ***Dohľad zrušený:*** Služby CSP a prípadne aj samotný CSP po tom, ako boli v minulosti pod dohľadom, už viac nespĺňajú ustanovenia smernice 1999/93/ES, ako určil členský štát identifikovaný v „Scheme territory“ (odsek 5.3.10), v ktorom má CSP sídlo. Preto sa požadovalo ukončenie operácií služby a služba sa z uvedeného dôvodu musí považovať za ukončenú.

Poznámka 1: Štatút „Dohľad zrušený“ môže byť konečným štatútom, aj ak CSP potom úplne ukončí svoju činnosť; v takom prípade nie je potrebné prejsť na štatút „Dohľad nad službou sa ukončuje“ ani „Dohľad ukončený“. Vskutku jediná možnosť zmeniť štatút „Dohľad zrušený“ je opäť dosiahnuť súlad s ustanoveniami v smernici 1999/93/ES podľa vhodného systému dohľadu platného v členskom štáte, ktorý TL vedie, a znova získať štatút „Pod dohľadom“. Štatúty „Dohľad nad službou sa ukončuje“ alebo „Dohľad ukončený“ sa nadobúdajú iba vtedy, keď CSP priamo ukončí svoje príslušné služby, ktoré sú pod dohľadom, nie v prípade, keď sa dohľad zruší.

— ***Akreditácia:*** Akreditačný orgán vykonal v mene členského štátu identifikovaného v „Scheme territory“ (odsek 5.3.10) posúdenie na účely akreditácie, pričom dospel k zisteniu, že služba identifikovaná v „Service digital identity“ (odsek 5.5.3), ktorú poskytuje CSP ([1]) identifikovaný v „TSP name“ (odsek 5.4.1), je v súlade s ustanoveniami smernice 1999/93/ES.

([1]) Treba poznamenať, že tento akreditovaný CSP môže mať sídlo v inom členskom štáte, ako je členský štát identifikovaný v „Scheme territory“ TSL implementácie TL alebo v tretej krajine (pozri článok 7 ods. 1 písm. a) smernice 1999/93/ES).

▼C1

Poznámka 2: Ak sa štatúty „Akreditácia zrušená“ alebo „Akreditácia ukončená“ použijú pri CSP vydávajúcom QC, ktorý je identifikovaný v „Scheme territory“ (odsek 5.3.10), MUSIA sa považovať za „prechodné štatúty“ a NESMÚ sa použiť ako hodnota pre „Service current status“ („Scs“), pretože ak sa použijú, MUSÍ bezprostredne za nimi v „Service approval history information“ alebo v „Service current status“ („Scs“) nasledovať štatút „Pod dohľadom“, za ktorým môže nasledovať akýkoľvek iný tu vymedzený štatút, ako sa ilustruje na obrázku 1. Ak sa štatúty „Akreditácia zrušená“ alebo „Akreditácia ukončená“ použijú pri CSP nevydávajúcich QC v prípade, keď je zriadená len pridružená schéma „dobrovoľnej akreditácie“ bez pridruženej schémy dohľadu, alebo pri CSP vydávajúcich QC v prípade, keď CSP nie je určený v „Scheme territory“ (odsek 5.3.10) (teda v tretej krajine), MÔŽU sa použiť ako hodnota v „Service current status“ („Scs“):

— ***Akreditácia ukončená:*** Platnosť posúdenia akreditácie uplynula bez toho, aby sa služba identifikovaná v „Service digital identity“ (odsek 55.3) opätovne posúdila.

— ***Akreditácia zrušená:*** Služba identifikovaná v „Service digital identity“ (odsek 55.3), ktorú poskytuje poskytovateľ certifikačných služieb (CSP) identifikovaný v „TSP name“ (odsek 54.1), ktorá v minulosti spĺňala kritériá schémy, rovnako ako prípadne samotný CSP už viac nespĺňajú ustanovenia v smernici 1999/93/ES.

Poznámka 3: Pri CSP vydávajúcich QC a CSP nevydávajúcich QC (napr. poskytovateľoch služieb časových pečiatok vydávajúcich TST, CSP vydávajúcich nekvalifikované certifikáty atď.) sa musia použiť úplne rovnaké hodnoty. Na rozlíšenie uplatniteľných systémov dohľadu/akreditácie sa použije „Service type identifier“ (odsek 5.5.1).

Poznámka 4: Dodatočné „kvalifikačné“ informácie týkajúce sa štatútu, vymedzené na úrovni vnútroštátnych systémov dohľadu/akreditácie pre CSP nevydávajúce QC sa MÔŽU poskytnúť úrovni služby, ak je to vhodné a požadované (napr. na účely odlíšenia viacerých úrovní kvality/bezpečnosti). Prevádzkovatelia schémy POUŽÍVAJÚ rozšírenie „additionalServiceInformation“ (odsek 5.8.2) poľa „Service information extension“ (odsek 5.5.9) podľa účelu poskytovania takýchto dodatočných „kvalifikačných“ informácií. Prevádzkovateľ schémy môže takisto voliteľne použiť odsek 5.5.6 („Scheme service definition URI“).

Current status starting date and time (odsek 5.5.5)

Toto pole je POVINNÉ a ŠPECIFIKUJE dátum a čas, keď začal platiť aktuálny štatút schválenia (hodnota dátumu a času podľa vymedzenia v ETSI TS 102 231 odsek 5.1.4).

Scheme service definition URI (odsek 5.5.6)

Toto pole je VOLITEĽNÉ a, ak je zahrnuté, ŠPECIFIKUJE URI, na ktorých spoliehajúce sa strany môžu získať informácie špecifické pre službu od prevádzkovateľa schémy ako sekvenciu viacjazyčných ukazovateľov (pričom EN je povinný jazyk prípadne s jedným alebo viacerými národnými jazykmi).

Uvedené URI MUSIA, ak sa použijú, zabezpečovať prístup k informáciám o službe, ako sa špecifikuje v schéme. Tieto informácie MÔŽU v prípade potreby zahŕňať:

a) URI ako údaj o totožnosti záložného CSP v prípade ukončovaného dohľadu nad službou, na ktorej sa podieľa záložný CSP (pozri „Service current status“ – odsek 5.5.4);

▼C1

b) URI ako linku na dokumenty s doplňujúcimi informáciami o používaní niektorých vnútroštátne vymedzených špecifických kvalifikácií pre službu poskytovania tokenu dôveryhodnej služby pod dohľadom/akreditovaného token dôveryhodnej služby v súlade s používaním poľa „Service information extension“ (odsek 5.5.9) s rozšírením „additionalServiceInformation“, ako sa vymedzuje v odseku 5.8.2.

Service supply points (odsek 5.5.7)

Toto pole je VOLITEĽNÉ a, ak je zahrnuté, ŠPECIFIKUJE URI na ktorých spoliehajúce sa strany majú prístup k službe prostredníctvom sekvencie reťazcov znakov, ktorých syntax MUSÍ byť v súlade s RFC 3986.

TSP service definition URI (odsek 5.5.8)

Toto pole je VOLITEĽNÉ a, ak je zahrnuté, ŠPECIFIKUJE URI, na ktorých spoliehajúce sa strany môžu získať špecifické informácie o službe poskytnuté TSP ako sekvenciu viacjazyčných ukazovateľov (pričom EN je povinný jazyk prípadne s jedným alebo viacerými národnými jazykmi). Uvedené URI MUSIA zabezpečovať prístup k informáciám o službe, ako sa špecifikuje v TSP.

Service information extensions (odsek 5.5.9)

V súvislosti s týmito špecifikáciami je toto pole VOLITEĽNÉ, ale ZAHRNIE SA, ak informácie uvedené v „Service digital identity“ (odsek 5.5.3) nie sú dostatočné na jednoznačnú identifikáciu kvalifikovaných certifikátov vydaných touto službou a/alebo informácie uvedené v súvisiacich kvalifikovaných certifikátoch neumožňujú strojovo spracovateľnú identifikáciu skutočnosti, či je QC podporovaný SSCD ([1]) alebo nie.

V súvislosti s týmito špecifikáciami sa POUŽÍVA voliteľné informačné pole „Service information extensions“ („Sie“) v prípade, že je POVINNÉ, napr. pre služby CA/QC, a ZOSTAVUJE sa v súlade s rozšírením „Qualifications“ vymedzeným v ETSI TS 102 231 príloha L.3.1 ako sekvencia jednej alebo viacerých n-tíc, pričom každá n-tica poskytuje:

— (filtruje) informácie na bližšiu identifikáciu v certifikačnej službe identifikovanej na základe „Sdi“ tej konkrétnej služby (teda súboru kvalifikovaných certifikátov), v prípade ktorej sa požadujú/poskytujú dodatočné informácie týkajúce sa údaju o podpore SSCD (a/alebo vydaní právnickej osobe) a

— súvisiace informácie („kvalifikátory“) o tom, či tento bližšie určený súbor služieb kvalifikovaných certifikátov je podporovaný SSCD, alebo nie, (keď táto informácia je „QCSSCDStatusAsInCert“, čo znamená, že táto pridružená informácia je súčasťou QC vo forme štandardizovanej podľa ETSI a strojovo spracovateľnej ([2]), a/alebo informácie o tom, či sa takéto QC vydávajú právnickým osobám (automaticky sa predpokladá, že sa vydávajú len fyzickým osobám).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): znamená, že CSP zaručuje a členský štát (respektíve jeho dozorný alebo jeho akreditačný orgán) kontroluje (v prípade modelu dohľadu) alebo audituje (v prípade modelu akreditácie), že QC vydané v rámci služby (QCA) identifikovanej v „Service digital identity“ (odsek 5.5.3) a bližšie určenej uvedenými (filtrami) informáciami použitými na účely bližšieho určenia pomocou certifikačnej služby identifikovanej v „Sdi“ toho súboru kvalifikovaných certifikátov, v prípade ktorých sa požadujú dodatočné informácie o prítomnosti podpory SSCD alebo jej absencii, SÚ podporované SSCD (teda, že súkromný kľúč súvisiaci s verejným kľúčom v certifikáte je uložený v bezpečnom zariadení na vytvorenie podpisu, ktoré zodpovedá prílohe III k smernici 1999/93/ES),

([1]) Pozri oddiel 2.2. tohto dokumentu.

([2]) To znamená primeranú kombináciu QcCompliance statement, QcSSCD statements [ETSI TS 101 862] vymedzených v ETSI alebo a QCP/QCP + OID vymedzeného v ETSI [ETSI TS 101 456].

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD): znamená, že CSP zaručuje a členský štát (respektíve jeho dozorný alebo jeho akreditačný orgán) kontroluje (v prípade modelu dohľadu) alebo audituje (v prípade modelu akreditácie), že QC vydané v rámci služby (koreňová CA/QC alebo CA/QC) identifikovanej v „Service digital identity“ (odsek 5.5.3) a bližšie určenej uvedenými (filtrami) informáciami použitými na účely bližšieho určenia pomocou certifikačnej služby identifikovanej v „Sdi“ toho súboru kvalifikovaných certifikátov, v prípade ktorých sa požadujú dodatočné informácie o prítomnosti podpory SSCD alebo jej absencii, NIE SÚ podporované SSCD (teda, že súkromný kľúč súvisiaci s verejným kľúčom v certifikáte nie je uložený v bezpečnom zariadení na vytvorenie podpisu, ktoré zodpovedá prílohe III k smernici 1999/93/ES),

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert)): znamená, že CSP zaručuje a členský štát (respektíve jeho dozorný alebo jeho akreditačný orgán) kontroluje (v prípade modelu dohľadu) alebo audituje (v prípade modelu akreditácie), že QC vydané v rámci služby (CA/QC) identifikovanej v „Service digital identity“ (odsek 5.5.3) a bližšie určenej uvedenými (filtrami) informáciami použitými na účely bližšieho určenia pomocou certifikačnej služby identifikovanej v „Sdi“ toho súboru kvalifikovaných certifikátov, v prípade ktorých sa požadujú dodatočné informácie o prítomnosti podpory SSCD alebo jej absencii, OBSAHUJÚ strojovo spracovateľné informácie o tom, či QC je podporovaný SSCD alebo nie,

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson):): znamená, že CSP zaručuje a členský štát (respektíve jeho dozorný alebo jeho akreditačný orgán) kontroluje (v prípade modelu dohľadu) alebo audituje (v prípade modelu akreditácie), že QC vydané v rámci služby (QCA) identifikovanej v „Service digital identity“ (odsek 5.5.3) a bližšie určenej uvedenými (filtrami) informáciami použitými na účely bližšieho určenia pomocou certifikačnej služby identifikovanej v „Sdi“ toho súboru kvalifikovaných certifikátov, v prípade ktorých sa požadujú dodatočné informácie o ich vydávaní právnickým osobám, SA VYDÁVAJÚ právnickým osobám.

Tieto kvalifikátory treba používať len ako rozšírenie, ak typ služby je http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Toto pole závisí od implementácie (ASN.1 alebo XML) a MUSÍ spĺňať špecifikácie ustanovené v ETSI TS 102 231, príloha L.3.1.

▼M1

Pri XML implementácii sa špecifický obsah takýchto dodatočných informácií musí kódovať pomocou súborov xsd poskytnutých v prílohe C k ETSI TS 102231.

▼C1

Service Approval History

Toto pole je VOLITEĽNÉ, ale MUSÍ sa zahrnúť, ak hodnota „Historical information period“ (odsek 5.3.12) je iná ako nula. To znamená, že v súvislosti s týmito špecifikáciami schéma MUSÍ uchovávať historické informácie. V prípade, keď treba historické informácie uchovávať, ale služba nemá históriu pred aktuálnym stavom (t. j. štatút ako prvý záznam alebo historické informácie prevádzkovateľ schémy neuchoval), OSTÁVA toto pole prázdne. V ostatných prípadoch sa pri každej zmene aktuálneho štatútu služby TSP, ktorá sa udiala v období, na ktoré sa historické informácie majú vzťahovať, ako sa špecifikuje v ETSI TS 102 231 odsek 5.3.12, POSKYTUJÚ informácie o predchádzajúcom štatúte schválenia v zostupnom poradí dátumom a časov zmien štatútu (t. j. dátumov a časov, keď nasledujúci štatút schválenia začal platiť).

▼C1

JE to sekvencia historických informácií podľa týchto vymedzení:

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

Service type identifier (odsek 5.6.1)

Toto pole je POVINNÉ a ŠPECIFIKUJE identifikátor typu služby vo formáte a v zmysle použitom v „TSP Service Information – Service type identifier“ (odsek 5.5.1).

Service name (odsek 5.6.2)

Toto pole je POVINNÉ a ŠPECIFIKUJE názov, pod ktorým CSP poskytlo službu identifikovanú v „TSP Service Information – Service type identifier“ (odsek 5.5.1) vo formáte a v zmysle použitom v „TSP Service Information – Service name“ (odsek 5.5.2). V tomto odseku sa nevyžaduje, aby názov bol rovnaký ako názov špecifikovaný v odseku 5.5.2. Zmena názvu MÔŽE byť jednou z okolností, ktoré si vyžadujú nový štatút.

▼M1

Service digital identity (odsek 5.6.3).

Toto pole je POVINNÉ a ŠPECIFIKUJE minimálne jedno znázornenie digitálneho identifikátora (teda certifikátu X.509v3) použitého v „TSP Service Information – Service digital identity“ (odsek 5.5.3) s formátom a významom podľa ETSI TS 102231, odsek 5.5.3.

Poznámka: V prípade hodnoty na certifikáte X.509v3 použitej v Sdi (odsek 5.5.3) služby sa musí pre každú hodnotu „Sti:Sie/additionalServiceInformation“ v zozname dôveryhodných informácií uvádzať iba jediný záznam o službe. Informácie Sdi (odsek 5.6.3) použité v histórii schvaľovania služby (service approval history), súvisiace so záznamom o službe, a informácie Sdi (odsek 5.5.3) použité v tomto zázname o službe SA MUSIA vzťahovať na tú istú hodnotu na certifikáte X.509v3. Zmena Sdi služby v zozname (teda obnova certifikátu X.509v3 alebo jeho nový kľúč napríklad pre CA/PKC alebo CA/QC), alebo vytváranie nového Sdi takejto služby, dokonca aj v prípade použitia rovnakých hodnôt súvisiacich s Sti, Sn a Sie, znamená, že prevádzkovateľ schémy (scheme operator) MUSÍ vytvoriť záznam o službe, ktorý sa odlišuje od predchádzajúceho.

▼C1

Service previous status (odsek 5.6.4)

Toto pole je POVINNÉ a ŠPECIFIKUJE identifikátor predchádzajúceho štatútu služby vo formáte a v zmysle použitom v „TSP Service Information – Service current status“ (odsek 5.5.4).

Previous status starting date and time (odsek 5.6.5)

Toto pole je POVINNÉ a ŠPECIFIKUJE dátum a čas, keď príslušný predchádzajúci štatút začal platiť vo formáte a v zmysle použitom v „TSP Service Information – Service current status starting date and time“ (odsek 5.5.5).

Service information extensions (odsek 5.6.6)

Toto pole je VOLITEĽNÉ a prevádzkovatelia schémy ho MÔŽU využiť na poskytnutie informácií týkajúcich sa služby vo formáte a v zmysle použitom v „TSP Service Information – Service information extensions“ (odsek 5.5.9).

▼C1

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

Idem pre TSP(1) Service(1) History(2) (pred History 1)

…

TSP(1) Service(2)

Idem pre TSP(1) Service 2 (prípadne)

Idem pre TSP 2 Service 1 History 1

…

TSP(2) Information

Idem pre TSP 2 (prípadne)

Idem pre TSP 2 Service 1

Idem pre TSP 2 Service 1 History 1

…

▼M1

Signed TSL

TSL implementácia zoznamu dôveryhodných informácií zriadeného podľa týchto špecifikácií, a najmä podľa kapitoly IV, čitateľná ľudským okom, BY MALA byť podpísaná „Scheme operator name“ (odsek 5.3.4), aby sa zaistila jeho autentickosť a celistvosť ([1]). Formát podpisu BY MAL byť PAdES part 3 (ETSI TS 102 778-3 ([2])), ale v rámci špecifického dôveryhodného modelu zriadeného prostredníctvom uverejnenia certifikátov používaných na podpisovanie zoznamov dôverných informácií to MÔŽE byť PAdES part 2 (ETSI TS 102 778-2 ([3])).

TSL implementácia zoznamu dôveryhodných informácií zriadeného podľa týchto špecifikácií v strojovo spracovateľnej podobe MUSÍ byť podpísaná „Scheme operator name“ (odsek 5.3.4), aby sa zaistila jeho autentickosť a celistvosť. Formát TSL implementácie zoznamu dôveryhodných informácií zriadeného podľa týchto špecifikácií v strojovo spracovateľnej podobe MUSÍ byť XML a MUSÍ spĺňať špecifikácie uvedené v prílohách B a C k ETSI TS 102231.

Formát podpisu MUSÍ byť XAdES BES alebo EPES v súlade so špecifikáciami ETSI TS 101 903 pre XML implementácie. Takáto implementácia elektronického podpisu MUSÍ spĺňať požiadavky prílohy B k ETSI TS 102 231 ([4]). Dodatočné všeobecné požiadavky na podpis sú uvedené v nasledujúcich oddieloch.

▼C1

Scheme identification (odsek 5.7.2)

Toto pole je POVINNÉ a ŠPECIFIKUJE referenciu pridelenú prevádzkovateľom schémy, ktorá jedinečne identifikuje schému opísanú v týchto špecifikáciách a zriadený TSL a MUSÍ byť zahrnutá v kalkulácii podpisu. Táto referencia by mala byť reťazec znakov alebo bitový reťazec.

([1]) V prípade, že TSL implementácia zoznamu dôveryhodných informácií čitateľná ľudským okom nie je podpísaná, jeho autentickosť a celistvosť SA MUSÍ zaručiť prostredníctvom náležitých komunikačných kanálov so zodpovedajúcou úrovňou zabezpečenia. Na tento účel sa odporúča používať TLS [IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2“] a odtlačok certifikátu TLS kanála MUSÍ členský štát sprístupniť TSL používateľom iným kanálom.

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

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

([4]) Podpisový certifikát prevádzkovateľa schémy sa musí chrániť podpisom jedným z dvoch spôsobov špecifikovaných v ETSI TS 101 903 a ds:keyInfo by mal prípadne obsahovať príslušný certifikačný reťazec.

▼M1

Pri týchto špecifikáciách JE pridelenou referenciou „TSL type“ (odsek 5.3.3), „Scheme name“ (odsek 5.3.6) a hodnota rozšírenia SubjectKeyIdentifier certifikátu, ktorý prevádzkovateľ schémy použil na elektronické podpísanie TSL.

▼C1

Signature algorithm identifier (odsek 5.7.3)

Toto pole je POVINNÉ a ŠPECIFIKUJE kryptografický algoritmus, ktorý sa použil na vytvorenie podpisu. V závislosti od použitého algoritmu si toto pole MÔŽE vyžadovať dodatočné parametre. Toto pole MUSÍ byť začlenené v kalkulácii podpisu.

Signature value (odsek 5.7.4)

Toto pole je POVINNÉ a OBSAHUJE skutočnú hodnotu digitálneho podpisu. Všetky polia TSL (s výnimkou samotnej hodnoty podpisu) MUSIA byť zahrnuté v kalkulácii podpisu.

TSL extensions (odsek 5.8)

Rozšírenie **expiredCertsRevocationInfo** (odsek 5.8.1)

Toto rozšírenie je VOLITEĽNÉ. V prípade, ak sa použije, MUSÍ spĺňať špecifikácie v ETSI TS 102 231 odsek 58.1.

Rozšírenie **additionalServiceInformation** (odsek 5.8.2)

Ak sa toto VOLITEĽNÉ rozšírenie použije, MUSÍ sa použiť iba na úrovni služby a iba v poli vymedzenom v odseku 5.5.9 („Service information extension“). Používa sa na poskytnutie dodatočných informácií o službe. Tieto informácie SÚ sekvenciou jednej alebo viacerých n-tíc, pričom v každej z nich sa uvádza:

a) URI identifikujúci dodatočné informácie, napr.:

   — URI označujúci určité vnútroštátne vymedzené špecifické kvalifikácie služby poskytovania tokenu dôveryhodnej služby, ktorá je pod dohľadom/je akreditovaná, napr.:

      — špecifickú bezpečnostnú/kvalitatívnu úroveň nesúrodosti vzhľadom na vnútroštátnu schému dohľadu/akreditácie pre CSP nevydávajúcich QC (napr. RGS */**/*** vo Francúzsku, špecifický štatút „dohľadu“ ustanovený vo vnútroštátnej legislatíve pre špecifických CSP vydávajúcich QC v Nemecku), pozri pozn. 4 k „Service current status“ – odsek 5.5.4,

      — alebo špecifický právny štatút poskytovania tokenov dôveryhodnej služby, ktoré je pod dohľadom/je akreditované (napríklad vnútroštátne vymedzené „kvalifikované TST“ ako v Nemecku alebo Maďarsku),

      — alebo význam špecifického politického identifikátora začleneného v certifikáte X.509v3 uvedeného v poli „Sdi“,

   — alebo registrovaný URI, ako sa špecifikuje v „Service type identifier“, odsek 55.1, na účely bližšieho určenia účasti služby identifikovanej v „Sti“ ako súčasti služby poskytovateľa certifikačnej služby vydávajúceho QC (napr. OCSP-QC, CRL-QC a koreňové CA-QC);

b) dobrovoľný reťazec obsahujúci hodnotu serviceInformation, s významom špecifikovaným v schéme (napr. *, ** alebo ***);

c) akékoľvek dodatočné informácie poskytnuté vo formáte špecifickom pre schému.

▼M1

Údajmi, na ktoré URI odkazujú, BY MALI byť informácie čitateľné ľudským okom (minimálne v anglickom jazyku a prípadne v jednom alebo vo viacerých národných jazykoch), ktoré sa považujú za vhodné a dostatočné pre stranu, ktorá sa na ne spolieha s cieľom pochopiť rozšírenie, a najmä na vysvetlenie významu daných URI, stanovenie prípadných hodnôt pre serviceInformation a vysvetlenie významu každej hodnoty.

Qualifications Extension (odsek L.3.1)

Opis:: Toto pole je VOLITEĽNÉ, ale UVÁDZA SA, keď je jeho použitie POVINNÉ, napr. v prípade koreňových RootCA/QC alebo služieb CA/QC, a keď:

— informácie poskytnuté v „Service digital identity“ nestačia na jednoznačnú identifikáciu kvalifikovaných certifikátov vydaných touto službou,

— informácie uvedené v príslušných kvalifikovaných certifikátoch neumožňujú strojovo spracovateľnú identifikáciu údajov o tom, či je QC podporovaný SSCD, alebo nie.

Toto rozšírenie na úrovni služby sa v prípade jeho použitia MUSÍ použiť len v poli vymedzenom v „Service information extension“ (odsek 5.5.9) a MUSÍ SPĹŇAŤ špecifikácie ustanovené v prílohe L.3.1 k ETSI TS 102 231.

TakenOverBy Extension (odsek L.3.2)

Opis: Toto rozšírenie je VOLITEĽNÉ, ale UVÁDZA SA, keď službu, za ktorú bol predtým zodpovedný CSP, prebral iný TSP, a je určené na formálne uvedenie právnej zodpovednosti za službu a na to, aby overovací softvér mohol používateľovi ukázať niektoré podrobnosti právnej povahy. Informácie poskytnuté prostredníctvom tohto rozšírenia SÚ v súlade so súvisiacim použitím odseku 5.5.6 a SPĹŇAJÚ špecifikácie v prílohe L.3.2 k ETSI TS 102 231.

▼M1

KAPITOLA II

Členské štáty v rámci zostavovania svojich zoznamov dôveryhodných informácií použijú:

kódy jazykov s malými písmenami a kódy krajiny s veľkými písmenami;

kódy jazykov a krajín v súlade s tabuľkou uvedenou nižšie;

keď sa píše latinkou (s príslušným kódom jazyka), pridáva sa transliterácia do latinky a uvedú sa príslušné kódy jazykov uvedené v tejto tabuľke.

Skrátený názov (zdrojový jazyk)	Skrátený názov (angličtina)	Kód krajiny	Kód jazyka	Poznámky	Transliterácia do latinky
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	kód krajiny, ktorý odporúča EÚ	el-Latn
España	Spain	ES	es	aj katalánčina (ca), baskičtina (eu), galícijčina (gl)	
France	France	FR	fr		
▼M2 Hrvatska	Croatia	HR	hr		
▼M1 Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼**M1**

Skrátený názov (zdrojový jazyk)	Skrátený názov (angličtina)	Kód krajiny	Kód jazyka	Poznámky	Transliterácia do latinky
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	kód krajiny, ktorý odporúča EÚ	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Transliterácia do latinky: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

KAPITOLA IV

ŠPECIFIKÁCIE FORMY TSL IMPLEMENTÁCIE ZOZNAMU DÔVERYHODNÝCH POSKYTOVATEĽOV ČITATEĽNEJ ĽUDSKÝM OKOM

Forma TSL implementácie zoznamu dôveryhodných poskytovateľov čitateľná ľudským okom (Human Readable – HR) MUSÍ byť verejne dostupná a prístupná elektronickými prostriedkami. MALA BY byť poskytnutá vo formáte dokumentu PDF podľa ISO 32000, ktorý MUSÍ byť naformátovaný podľa profilu PDF/A (ISO 19005).

Obsah formy HR TSL implementácie zoznamu dôveryhodných poskytovateľov vo formáte PDF/A BY MAL spĺňať tieto požiadavky:

▼M1

— názov podoby zoznamov dôveryhodných informácií čitateľnej ľudským okom sa skladá zo zreťazenia týchto prvkov:

  — nepovinný obrázok vlajky členského štátu,

  — medzera,

  — skrátený názov krajiny v zdrojovom(-ých) jazyku(-och) (v súlade s prvým stĺpcom tabuľky v kapitole II),

  — medzera,

  — „(“,

  — skrátený názov krajiny v angličtine (v súlade s druhým stĺpcom tabuľky v kapitole II) v zátvorke,

  — „): “ako koniec zátvorky a oddeľovací znak,

  — medzera,

  — „Trusted List“,

  — nepovinné logo prevádzkovateľa schémy členského štátu,

▼C1

— štruktúra formy HR BY MALA odrážať logický model opísaný v časti 5.1.2 ETSI TS 102 231,

— každé zahrnuté pole BY MALO byť zobrazené a uvádzať:

  — názov poľa (napr. „Service type identifier“),

  — hodnotu poľa (napr. „QA/QC“),

  — prípadne význam (opis) hodnoty poľa, a predovšetkým ako sa ustanovuje v prílohe D ETSI TS 102 231 alebo v týchto špecifikáciách pre registrované URI (napr. „certifikačná autorita vydávajúca certifikáty s verejným kľúčom“),

  — prípadne viacero verzií v národných jazykoch, ako sa ustanovuje v TSL implementácii zoznamu dôveryhodných poskytovateľov.

— Na forme HR by sa minimálne mali uviesť tieto polia a zodpovedajúce hodnoty digitálnych certifikátov uvedené v poli „Service digital identity“:

  — Verzia

  — Sériové číslo

  — Algoritmus podpisu

  — Vydavateľ

  — Platnosť od

  — Platnosť do

  — Predmet

▼C1

— Verejný kľúč

— Politika certifikátu

— Identifikátor kľúča predmetu

— Distribučné body CRL

— Identifikátor kľúča autority

— Používanie kľúča

— Základné obmedzenia

— Algoritmus odtlačku prsta

— Odtlačok prsta

— Forma HR BY SA MALA ľahko dať vytlačiť.

— Forma HR MÔŽE byť elektronicky podpísaná. Ak je podpísaná, MUSÍ byť podpísaná prevádzkovateľom schémy podľa tých istých špecifikácií podpisu, ako pri TSL implementácii zoznamu dôveryhodných poskytovateľov.