VYKONÁVACIE ROZHODNUTIE KOMISIE

zo 14. októbra 2013,

ktorým sa mení rozhodnutie 2009/767/ES, pokiaľ ide o zostavovanie, vedenie a uverejňovanie zoznamov dôveryhodných informácií o poskytovateľoch certifikačných služieb, ktorí podliehajú dohľadu členského štátu alebo sú v ňom akreditovaní

[oznámené pod číslom C(2013) 6543]

(Text s významom pre EHP)

(2013/662/EÚ)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

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) Na základe rozhodnutia Komisie 2009/767/ES 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 [2], sú členské štáty povinné sprístupniť informácie, ktoré sú potrebné na overenie zdokonaleného elektronického podpisu podporovaného kvalifikovaným certifikátom. Tieto informácie musia byť stanovené jednotne s použitím tzv. „zoznamov dôveryhodných informácií“, ktoré obsahujú informácie o poskytovateľoch certifikačných služieb, ktorí vydávajú kvalifikované certifikáty verejnosti v súlade so smernicou Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy [3] a ktorí podliehajú dohľadu členských štátov alebo sú v nich akreditovaní.

(2) Z praktických skúseností s vykonávaním rozhodnutia 2009/767/ES členskými štátmi vyplynulo, že na dosiahnutie maximálnych prínosov zo zoznamov dôveryhodných informácií sú potrebné niektoré zlepšenia. Navyše Európsky inštitút pre telekomunikačné normy (ETSI) zverejnil nové technické špecifikácie týkajúce sa zoznamov dôveryhodných informácií (TS 119 612), ktoré vychádzajú zo špecifikácií v súčasnosti zahrnutých do prílohy k rozhodnutiu, ktoré však zároveň prinášajú niekoľko zlepšení existujúcich špecifikácií.

(3) Rozhodnutie 2009/767/ES by sa preto malo zmeniť, aby odkazovalo na technické špecifikácie ETSI 119 612 a aby zahŕňalo zmeny potrebné na zlepšenie a uľahčenie uplatňovania a používania zoznamov dôveryhodných informácií.

(4) S cieľom umožniť členským štátom vykonať požadované technické zmeny v ich súčasných zoznamoch dôveryhodných informácií je vhodné, aby sa toto rozhodnutie uplatňovalo od 1. februára 2014.

(5) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru zriadeného na základe smernice o službách,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Zmeny rozhodnutia 2009/767/ES

Rozhodnutie 2009/767/ES sa mení takto:

1. Článok 2 sa mení takto:

a) odseky 1, 2 a 2a sa nahrádzajú takto:

„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.

2. Členské štáty v súlade so špecifikáciami uvedenými v prílohe zostavia a uverejnia zoznam dôveryhodných informácií v strojovo spracovateľnej podobe. Ak sa členský štát rozhodne uverejniť zoznam dôveryhodných informácií v podobe čitateľnej ľudským okom, táto podoba musí byť v súlade so špecifikáciami stanovenými v prílohe.

2a. Členské štáty elektronicky podpíšu strojovo spracovateľnú podobu svojho zoznamu dôveryhodných informácií, aby sa zaistila jeho autentickosť a celistvosť. Ak členský štát uverejní zoznam dôveryhodných informácií v podobe čitateľnej ľudským okom, zaistí, aby táto forma zoznamu dôveryhodných informácií obsahovala rovnaké údaje ako strojovo spracovateľná podoba a elektronicky ju podpíše s rovnakým certifikátom, aký sa použil na strojovo spracovateľnú podobu.“;

[1] Ú. v. EÚ L 376, 27.12.2006, s. 36.
[2] Ú. v. EÚ L 274, 20.10.2009, s. 36.
[3] Ú. v. ES L 13, 19.1.2000, s. 12.

b) vkladá sa tento odsek 2b:

„2b. Členské štáty zaistia, aby strojovo spracovateľná podoba zoznamu dôveryhodných informácií bola prístupná v lokalite, kde bola uverejnená, a to vždy a bez prerušenia s výnimkou prípadov údržby.“;

c) odsek 3 sa nahrádza takto:

„3. Členské štáty oznamujú Komisii tieto informácie:

a) orgán alebo orgány zodpovedné za zostavovanie, vedenie a uverejňovanie strojovo spracovateľnej podoby zoznamu dôveryhodných informácií;

b) lokalitu, kde je uverejnená strojovo spracovateľná podoba zoznamu dôveryhodných informácií;

c) dva alebo viac certifikátov s verejným kľúčom prevádzkovateľa schémy s dobou platnosti posunutou aspoň o 3 mesiace, ktoré zodpovedajú súkromným kľúčom, ktoré sa môžu používať na elektronické podpísanie strojovo spracovateľnej podoby zoznamu dôveryhodných informácií;

d) všetky zmeny informácií v písmenách a), b) a c).“;

d) vkladá sa tento odsek 3a:

„3a. Ak členský štát uverejní zoznam dôveryhodných informácií v podobe čitateľnej ľudským okom, informácie uvedené v odseku 3 sa oznámia aj v prípade podoby čitateľnej ľudským okom.“

2. Príloha sa nahrádza prílohou k tomuto rozhodnutiu.

Článok 2

Uplatňovanie

Toto rozhodnutie sa uplatňuje od 1. februára 2014.

Článok 3

Adresáti

Toto rozhodnutie je určené členským štátom.

V Bruseli 14. októbra 2013

Za Komisiu

Michel BARNIER

člen Komisie

PRÍLOHA

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

VŠEOBECNÉ POŽIADAVKY

1. **Úvod**

Účelom spoločného vzoru „Zoznamu dôveryhodných informácií o poskytovateľoch certifikačných služieb, ktorí podliehajú dohľadu/sú akreditovaní“ pre členské štáty je určiť spoločný spôsob, akým každý členský štát podáva informácie o štatúte dohľadu nad certifikačnými službami/akreditácie certifikačných služieb poskytovaných poskytovateľmi certifikačných služieb ([1]) (Certification Service Providers, ďalej len „CSP“), ktorí podliehajú ich dohľadu/sú nimi akreditovaní, pokiaľ ide o súlad s príslušnými ustanoveniami smernice 1999/93/ES. Súčasťou postupovaných informácií sú aj historické informácie o štatúte dohľadu nad certifikačnými službami/štatúte akreditácie certifikačných služieb.

Účelom poskytnutia týchto informácií je v prvom rade podpora overenia kvalifikovaných elektronických podpisov (Qualified Electronic Signatures, ďalej len „QES“) a zdokonalených elektronických podpisov (Advanced Electronic Signatures, ďalej len „AdES“) ([2]) podporovaných kvalifikovaným certifikátom ([3]) ([4]).

Povinné informácie v zozname dôveryhodných informácií o poskytovateľoch musia zahŕňať minimálne informácie o CSP, ktorí podliehajú dohľadu/sú akreditovaní a ktorí vydávajú kvalifikované certifikáty (Qualified Certificates, ďalej len „QC“) ([5]) v súlade s ustanoveniami smernice 1999/93/ES [článok 3 ods. 2 a 3 a článok 7 ods. 1 písm. a)], ak to nie je súčasťou QC vrátane informácií o QC, ktoré podporujú elektronický podpis, a o tom, či je podpis vytvorený bezpečným zariadením na vytvorenie podpisu SSCD (Secure Signature Creation Device, ďalej len „SSCD“) ([6]).

Dodatočné informácie o iných CSP, ktorí však nevydávajú QC, ale poskytujú služby súvisiace s elektronickým podpisom (napríklad CSP, ktorí poskytujú služby časových pečiatok a vydávajú tokeny časových pečiatok, CSP vydávajúci nekvalifikované certifikáty atď.) sa môžu dobrovoľne zahrnúť do zoznamu dôveryhodných informácií o poskytovateľoch na vnútroštátnej úrovni za predpokladu, že sú akreditovaní/podliehajú dohľadu podobným spôsobom, ako CSP, ktorí vydávajú QC, alebo sa môžu schváliť na základe odlišnej vnútroštátnej schémy schvaľovania. Vnútroštátna schéma schvaľovania sa môže v niektorých štátoch odlišovať od dohľadu alebo dobrovoľných akreditačných schém uplatniteľných na CSP, ktoré vydávajú QC vzhľadom na uplatniteľné požiadavky a/alebo zodpovednú organizáciu. Pojmy „akreditovaní“ a/alebo „podliehajúci dohľadu“ v súčasných špecifikáciách takisto zahŕňajú vnútroštátne schémy schvaľovania, ale dodatočné informácie o povahe akýchkoľvek vnútroštátnych schém poskytnú členské štáty vo svojom zozname dôveryhodných informácií o poskytovateľoch vrátane objasnenia možných rozdielov oproti schémam akreditácie/dohľadu uplatňovaným na CSP, ktorí vydávajú QC.

Spoločný vzor vychádza z normy ETSI TS 119 612 v1.1.1 ([7]) (ďalej sa uvádza ako „ETSI TS 119 612“), v ktorej sa stanovuje vytvorenie, uverejnenie, lokalita, prístup, autentickosť a celistvosť takýchto zoznamov.

2. **Štruktúra spoločného vzoru zoznamu dôveryhodných informácií o poskytovateľoch**

Spoločný vzor zoznamu dôveryhodných informácií o poskytovateľoch členských štátov sa podľa ETSI TS 119 612 skladá z týchto kategórií informácií:

1. tagu zoznamu dôveryhodných informácií o poskytovateľoch uľahčujúceho identifikáciu pri elektronickom vyhľadávaní;

2. informácií o zozname dôveryhodných informácií o poskytovateľoch a schéme jeho vydávania;

3. sekvencie polí obsahujúcich jednoznačné informácie na identifikáciu o každom CSP, ktorý podlieha dohľadu/je akreditovaný v rámci schémy (táto sekvencia je dobrovoľná, t. j. ak sa nepoužije, vychádza sa z predpokladu, že zoznam nemá žiadny obsah, a teda že v pridruženom členskom štáte nepodlieha dohľadu/nie je akreditovaný ani jeden CSP na účely zoznamu dôveryhodných informácií o poskytovateľoch);

4. za každý CSP na zozname sa podrobnosti jeho špecifických dôveryhodných služieb, ktorých aktuálny štatút je zaznamenaný v zozname dôveryhodných informácií o poskytovateľoch, poskytujú ako sekvencia polí na jednoznačnú identifikáciu certifikačných služieb, ktoré podliehajú dohľadu/sú akreditované a poskytovaných CSP a ich aktuálny štatút (táto sekvencia musí mať aspoň jeden vstup);

([1]) Ako sú vymedzené v článku 2 ods. 11 smernice 1999/93/ES.
([2]) Ako sú vymedzené v článku 2 ods. 2 smernice 1999/93/ES.
([3]) V prípade AdES, ktoré podporuje QC, sa v celom tomto dokumente používa akronym „$AdES_{QC}$“.
([4]) Treba poznamenať, že existuje celý rad elektronických služieb založených na jednoduchých AdES, ktorých cezhraničné využívanie by sa takisto uľahčilo, ak by podporné certifikačné služby (napríklad vydávanie nekvalifikovaných certifikátov) boli súčasťou služieb, ktoré podliehajú dohľadu/sú akreditované uvedeným členským štátom v dobrovoľnej časti informácií ich zoznamu dôveryhodných informácií o poskytovateľoch.
([5]) Ako sú vymedzené v článku 2 ods. 10 smernice 1999/93/ES.
([6]) Ako sú vymedzené v článku 2 ods. 6 smernice 1999/93/ES.
([7]) ETSI TS 102 778-06 v1.1.1 (2013-06) – Elektronické podpisy a infraštruktúry (Electronic Signatures and Infrastructures – ESI): Zoznamy dôveryhodných informácií o poskytovateľoch.

5. za každú certifikačnú službu na zozname, ktorá podlieha dohľadu/je akreditovaná, podľa potreby informácie o histórii tohto štatútu;

6. podpis použitý na zozname dôveryhodných informácií o poskytovateľoch.

V súvislosti s CSP vydávajúcimi QC štruktúra zoznamu dôveryhodných informácií o poskytovateľoch, a najmä zložka služobných informácií (podľa bodu 4) umožňuje kompenzáciu doplňujúcich informácií v rozšíreniach služobných informácií v tých situáciách, keď v kvalifikovanom certifikáte nie sú dostatočné informácie o jeho „kvalifikovanom" štatúte, jeho možnej podpore zo strany SSCD a predovšetkým informácie na riešenie dodatočnej skutočnosti, že väčšina (komerčných) CSP používa jedinú vydávajúcu certifikačnú autoritu (Certification Authority, ďalej len „CA") na vydávanie viacerých typov certifikátov konečného subjektu, a to tak kvalifikovaných, ako aj nekvalifikovaných.

V kontexte služieb vydávania certifikátov (CA) sa počet údajov o službách v zozname CSP môže znížiť, ak jedna alebo niekoľko služieb CA vyššej úrovne existuje v rámci PKI CSP (napríklad v rámci hierarchie CA od koreňovej CA smerom dolu k niekoľkým vydávajúcim CA) uvedením takýchto služieb CA vyššej úrovne, a nie služieb CA vydávajúcich certifikáty konečného subjektu (napríklad uvedením iba koreňovej CA CSP). V týchto prípadoch sa však informácia o stave uplatňuje na celú hierarchiu služieb CA v rámci služby na zozname a musí sa dodržiavať a zabezpečovať zásada zabezpečenia jednoznačného prepojenia medzi certifikačnou službou CSP_{QC} a súborom certifikátov, ktoré sa majú identifikovať ako QC.

2.1. *Opis informácií v každej kategórii*

1. Tag zoznamu dôveryhodných informácií o poskytovateľoch

2. Informácie o zozname dôveryhodných informácií o poskytovateľoch a schéme jeho vydávania

Súčasťou tejto kategórie sú tieto informácie:

— **formát a identifikátor verzie** zoznamu dôveryhodných informácií o poskytovateľoch,

— **sériové číslo (alebo číslo vydania)** zoznamu dôveryhodných informácií o poskytovateľoch,

— **informácie o type** zoznamu dôveryhodných informácií o poskytovateľoch (napríklad na identifikáciu skutočnosti, že predmetný zoznam dôveryhodných informácií o poskytovateľoch obsahuje informácie o štatúte dohľadu nad certifikačnými službami/štatúte akreditácie certifikačných služieb poskytovaných CSP, ktorí podliehajú dohľadu členského štátu, na ktorý sa odkazuje/sú v ňom akreditovaní z hľadiska dosiahnutia súladu s ustanoveniami v smernici 1999/93/ES),

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

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

  — krajina, na ktorú sa zoznam vzťahuje,

  — informácie o lokalitách, v ktorých sa informácie o schéme(-ach) 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 informácií o poskytovateľoch,

— **dátum a čas** vydania zoznamu dôveryhodných informácií o poskytovateľoch,

— **budúca plánovaná aktualizácia** zoznamu dôveryhodných informácií o poskytovateľoch.

3. Jednoznačné informácie na identifikáciu každého CSP podliehajúceho dohľadu/akreditovaného v schéme

Tento súbor informácií obsahuje minimálne:

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

— adresu a kontaktné informácie CSP,

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

4. Za každý CSP na zozname sekvencia polí s jednoznačnými informáciami na identifikáciu certifikačnej služby poskytovanej CSP, ktorá podlieha dohľadu/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 služby: identifikátor typu certifikačnej služby (napríklad identifikátor, na základe ktorého sa určuje, že certifikačná služba, ktorú poskytuje CSP a ktorá podlieha dohľadu/je akreditovaná, je certifikačná autorita vydávajúca QC),

— názov služby (obchodu): (obchodný) názov tejto certifikačnej služby,

— digitálna identita služby: jednoznačný jedinečný identifikátor certifikačnej služby,

— aktuálny štatút služby: identifikátor aktuálneho stavu služby,

— dátum a čas, odkedy aktuálny štatút začal platiť,

— podľa potreby rozšírenie informácií o službe: dodatočné informácie o službe (buď uvedené priamo, alebo pomocou odkazu na lokalitu, odkiaľ sa takéto informácie dajú stiahnuť, informácie o prístupe k službe): informácie o vymedzení služby poskytované prevádzkovateľom schémy, informácie o prístupe v súvislosti so službou, informácie o vymedzení služby poskytované CSP a rozšírenie informácií o službe. V prípade služieb CA/QC dobrovoľná sekvencia s n-tíc informáciami, pričom každá n-tica poskytuje

  — kritériá na bližšiu identifikáciu (vytriedenie) v rámci identifikovanej dôveryhodnej služby, ktoré spresňujú súbor výstupov služby (teda súboru kvalifikovaných certifikátov), v prípade ktorej sa požadujú/poskytujú dodatočné informácie o jej štatúte, údaje o podpore SSCD (a/alebo vydaní právnickej osobe), ako aj

  — súvisiace „kvalifikátory“ poskytujúce informácie o tom, či tento súbor výstupov služby identifikuje certifikáty považované za kvalifikované a/alebo či sú identifikované kvalifikované certifikáty z tejto služby podporované SSCD, alebo nie, a/alebo informácie o tom, či sa takéto QC vydávajú právnickým osobám (automaticky sa predpokladá, že sa vydávajú len fyzickým osobám).

5. Za každú certifikačnú službu na zozname historické informácie o jej štatúte.

6. Podpis vytvorený na autentifikačné účely cez všetky polia TL s výnimkou hodnoty samotného podpisu.

3. **Usmernenia na úpravu údajov v zozname dôveryhodných informácií o poskytovateľoch**

3.1. *Informácie o štatúte certifikačných služieb, ktoré podliehajú dohľadu/sú akreditované, a o ich poskytovateľoch v jednom zozname*

Zoznam dôveryhodných informácií o poskytovateľoch členského štátu predstavuje „Zoznam štatútov dohľadu nad certifikačnými službami/akreditácie certifikačných služieb poskytovateľov certifikačných služieb, ktorí podliehajú dohľadu uvedeného členského štátu alebo sú v ňom akreditovaní vzhľadom na dodržiavanie príslušných ustanovení smernice 1999/93/ES“.

Tento zoznam dôveryhodných informácií o poskytovateľoch je jediný nástroj, ktorý má používať príslušný členský štát na poskytovanie informácií o štatúte dohľadu nad certifikačnými službami/akreditácie certifikačných služieb a ich poskytovateľov:

— **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“,

— **ktorí podliehajú dohľadu/sú akreditovaní**, pokiaľ ide o súlad s príslušnými ustanoveniami smernice 1999/93/ES.

Na základe vymedzení pojmov a ustanovení v smernici 1999/93/ES, predovšetkým vzhľadom na príslušných CSP a systémy dohľadu nad nimi/systémy 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), nad nimi musí vykonávať dohľad a prípadne môžu byť akreditovaní, pokiaľ ide o súlad s ustanoveniami smernice 1999/93/ES vrátane požiadaviek uvedených v prílohe I (požiadavky na QC) a v prílohe II (požiadavky na CSP vydávajúcich QC). CSP vydávajúci QC, ktorí sú akreditovaní v členskom štáte, musia patriť do príslušného systému dohľadu daného členského štátu okrem prípadu, keď nie sú usadení v danom členskom štáte.

— Platný systém „dohľadu“ (prípadne systém „dobrovoľnej akreditácie“) je vymedzený a musí spĺňať príslušné požiadavky v smernici 1999/93/ES, predovšetkým požiadavky stanovené 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, 11, 12 a 13).

— **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“ realizovanú na vnútroštátnom základe na účely dohľadu nad súladom s ustanoveniami uvedenej smernice a prípadne s vnútroštátnymi ustanoveniami týkajúcimi sa poskytovania certifikačných služieb (v zmysle článku 2 ods. 11 smernice 1999/93/ES).

— 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 len vnútroštátnu úroveň.

V každom členskom štáte sa musí zostaviť a viesť jeden zoznam dôveryhodných informácií o poskytovateľoch s údajmi o štatúte dohľadu nad certifikačnými službami a/alebo štatúte akreditácie tých certifikačných služieb, ktoré poskytujú tí CSP, ktorí sú pod dohľadom daného členského štátu/sú v ňom akreditovaní. Zoznam dôveryhodných informácií o poskytovateľoch zahŕňa aspoň tých CSP, ktorí vydávajú QC. V zozname dôveryhodných informácií o poskytovateľoch sa môže takisto uvádzať štatút iných certifikačných služieb podliehajúcich dohľadu alebo akreditovaných v rámci vnútroštátne vymedzenej schémy schvaľovania.

3.2. *Jeden súbor hodnôt štatútu dohľadu/akreditácie*

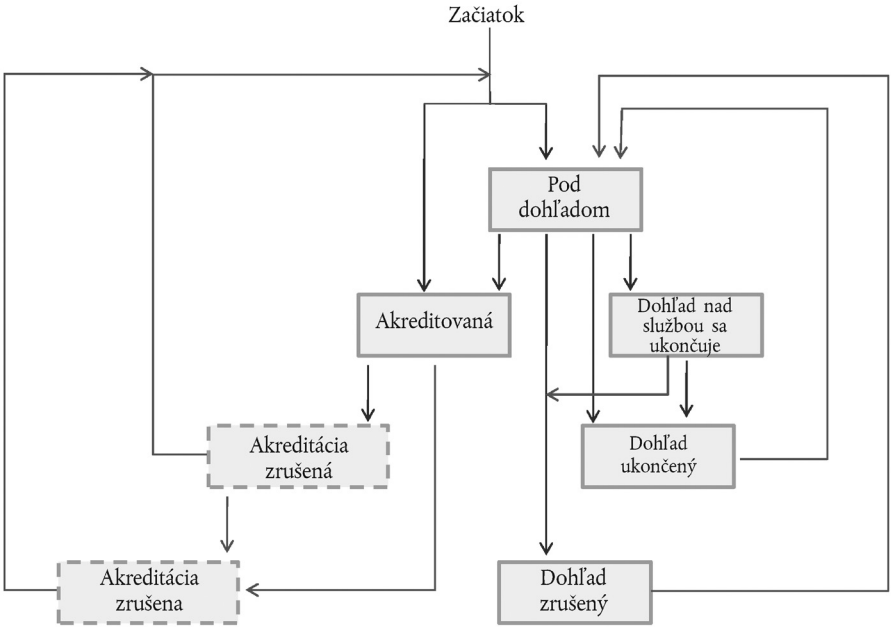
V zozname dôveryhodných informácií o poskytovateľoch je skutočnosť, že služba práve „podlieha dohľadu“ alebo je „akreditovaná“, daná hodnotou jej aktuálneho štatútu. Okrem toho štatút dohľadu alebo akreditácie môže byť kladný („pod dohľadom“, „akreditovaný“, „dohľad nad službou sa ukončuje“), ukončený („dohľad ukončený“, „akreditácia ukončená“) alebo aj zrušený („dohľad zrušený“, „akreditácia zrušená“) a stanovený na zodpovedajúcu hodnotu. Tá istá 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] Napríklad poskytovateľ certifikačnej služby so sídlom v jednom členskom štáte, ktorý poskytuje certifikačnú službu, ktorá je najprv pod dohľadom členského štátu (orgánu dohľadu), sa môže po určitom čase rozhodnúť pre dobrovoľnú akreditáciu certifikačnej služby, ktorá je v danom čase pod dohľadom. Podobne sa poskytovateľ certifikačnej služby v inom členskom štáte môže rozhodnúť nepozastaviť akreditovanú certifikačnú službu, ale zmeniť jej štatút zo štatútu akreditácie na štatút pod dohľadom, napríklad z obchodných a/alebo hospodárskych dôvodov.

Obrázok 1

Očakávaný vývoj štatútu dohľadu/akreditácie v prípade jednej služby CSP



Vysvetlivky:

Prechodný štatút, ak je pridružení model dohľadu (napr. v pripade CSP vydávajúceho QC, ktorý je akreditovaný a nad ktorým sa vykonáva dohľad v členskom štáte, v ktorom má sídlo)
Možný aktálny štatút, ak nie je prirudzený žiadny model dohľadu (napr. v prípade CSP, ktorý) je akreditovaný v členskom štáte, v ktorom nemá sídlo)

Mozny aktualny štatút

V prípade usadenia v členskom štáte musí certifikačná služba vydávajúca QC podliehať dohľadu (členského štátu, v ktorom je usadená) a môže byť dobrovoľne akreditovaná. Hodnota štatútu takejto služby na zozname dôveryhodných informácií o poskytovateľoch musí mať jednu z uvedených hodnôt štatútu ako „hodnotu aktuálneho štatútu“ v súlade s jej aktuálnym štatútom a musí sa podľa potreby zmeniť podľa opísaného vývoja štatútu. Aj „akreditácia ukončená“ aj „akreditácia zrušená“ však musia byť hodnotami „prechodného štatútu“, keď je zodpovedajúca služba CSP_{QC} uvedená na zozname dôveryhodných informácií o poskytovateľoch členského štátu, v ktorom je usadená, pretože takáto služba musí podliehať dohľadu štandardne (aj vtedy, keď už nie je alebo nikdy nebola akreditovaná); keď je zodpovedajúca služba uvedená na zozname (akreditovaná) v inom členskom štáte, ako je ten, v ktorom je usadená, tieto hodnoty môžu byť konečné.

Členské štáty, ktoré zriaďujú alebo zriadili vnútroštátne vymedzenú „uznanú schému (-y) schvaľovania CSP“ realizovanú(-é) na vnútroštátnom základe na účely dohľadu nad súladom služieb, ktoré poskytujú CSP **nevydávajúci** QC, s ustanoveniami smernice 1999/93/ES a prípadne s vnútroštátnymi ustanoveniami týkajúcimi sa poskytovania certifikačných služieb (v zmysle článku 2 ods. 11 uvedenej smernice), musia 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, 11, 12 a 13),

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

Podľa tohto zatriedenia môže byť certifikačná služba, ktorá nevydáva QC, buď pod dohľadom alebo dobrovoľne akreditovaná. Hodnota štatútu takejto služby na zozname dôveryhodných informácií o poskytovateľoch musí mať jednu z uvedených hodnôt štatútu ako „hodnotu aktuálneho štatútu“ (pozri obrázok 1) v súlade s jej aktuálnym štatútom a musí sa podľa potreby zmeniť podľa opísaného vývoja štatútu.

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

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

— v prípade potreby informácie o vnútroštátnej schéme „dobrovoľnej akreditácie“, ktorá sa vzťahuje na každého CSP_{QC},

— v prípade potreby, informácie o systéme dohľadu, ktorý sa vzťahuje na každého CSP nevydávajúceho QC,

— v prípade potreby informácie o vnútroštátnej schéme „dobrovoľnej akreditácie“, ktorá sa vzťahuje na každého CSP nevydávajúceho 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 zozname dôveryhodných informácií o poskytovateľoch uvádzajú informácie o štatúte dohľadu/akreditácie pri službách poskytovaných CSP nevydávajúcimi QS, uvedené súbory informácií sa na úrovni zoznamu dôveryhodných informácií o poskytovateľoch uvedú pomocou „Scheme information URI“ (odsek 5.3.7 – informácie poskytované členskými štátmi), „Scheme type/community/rules“ (odsek 5.3.9 – prostredníctvom textu spoločného pre všetky členské štáty a dobrovoľných konkrétnych informácií poskytovaných členským štátom) 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 „kvalifikácii“ vymedzené na úrovni vnútroštátneho systému dohľadu/akreditácie pre CSP nevydávajúcich QC sa môžu poskytnúť na úrovni služby, ak sú potrebné a vyžiadané (napríklad na rozlíšenie medzi viacerými úrovňami kvality/bezpečnosti), prostredníctvom použitia rozšírenia „additionalServiceInformation Extension“ (odsek 5.5.9.4) ako súčasť „Service information extensions“ (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 byť v jednom členskom štáte zodpovedné rôzne orgány tohto členského štátu, očakáva sa, že jedna certifikačná služba bude mať len jeden záznam a že štatút dohľadu nad ním/štatút jeho akreditácie sa musí zodpovedajúcim spôsobom aktualizovať.

3.3. *Záznamy v zozname dôveryhodných informácií o poskytovateľoch s cieľom uľahčiť validáciu QES a $AdES_{QC}$*

Rozhodujúcou časťou zostavovania zoznamu dôveryhodných informácií o poskytovateľoch je vytvorenie povinnej časti zoznamu dôveryhodných informácií o poskytovateľoch, teda „zoznamu služieb“ podľa 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 $AdES_{QC}$ (keď sa skombinujú s obsahom QC konečného subjektu, ktorý vydal CSP v rámci certifikačnej služby uvedenej v tomto zázname).

Požadované informácie by mohli zahŕňať iné informácie než „digitálna identita služby“ jednej (koreňovej) CA, najmä informácie identifikujúce štatút QC certifikátov vydaných takouto službou CA, a údaje o tom, či sú podporované podpisy vytvorené pomocou SSCD. Orgán v členskom štáte, ktorý je zodpovedný za zostavenie, úpravu a vedenie zoznamu dôveryhodných informácií o poskytovateľoch musí preto zohľadniť aktuálny profil a obsah certifikátu v každom vydanom QC, za každý CSP_{QC} uvedený v zozname dôveryhodných informácií o poskytovateľoch.

V ideálnom prípade by každý vydaný QC mal obsahovať vyhlásenie QcCompliance ([1]) statement (vyhlásenie o zhode QC) 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 predmetu certifikačnej politiky QCP/QCP + Object Identifiers (OIDs) vymedzených v ETSI EN 319 411-2 ([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 (napríklad 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 posudzovaní, aspoň strojom čitateľným spôsobom, či sa certifikát podporujúci elektronický podpis vyhlasuje za QC, alebo nie, a či súvisí s SSCD, pomocou ktorého sa elektronický podpis vytvoril.

([1]) Pozri ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI): Profily poskytovateľov dôveryhodných služieb vydávajúcich certifikáty; Časť 5: Rozšírenie profilu kvalifikovaného certifikátu na vymedzenie takého vyhlásenia.

([2]) ETSI EN 319 411-2 – Electronic Signatures and Infrastructures (ESI): Politické a bezpečnostné požiadavky na poskytovateľov dôveryhodných služieb vydávajúcich certifikáty; Časť 2: Politické požiadavky na poskytovateľov certifikačných služieb vydávajúcich kvalifikované certifikáty.

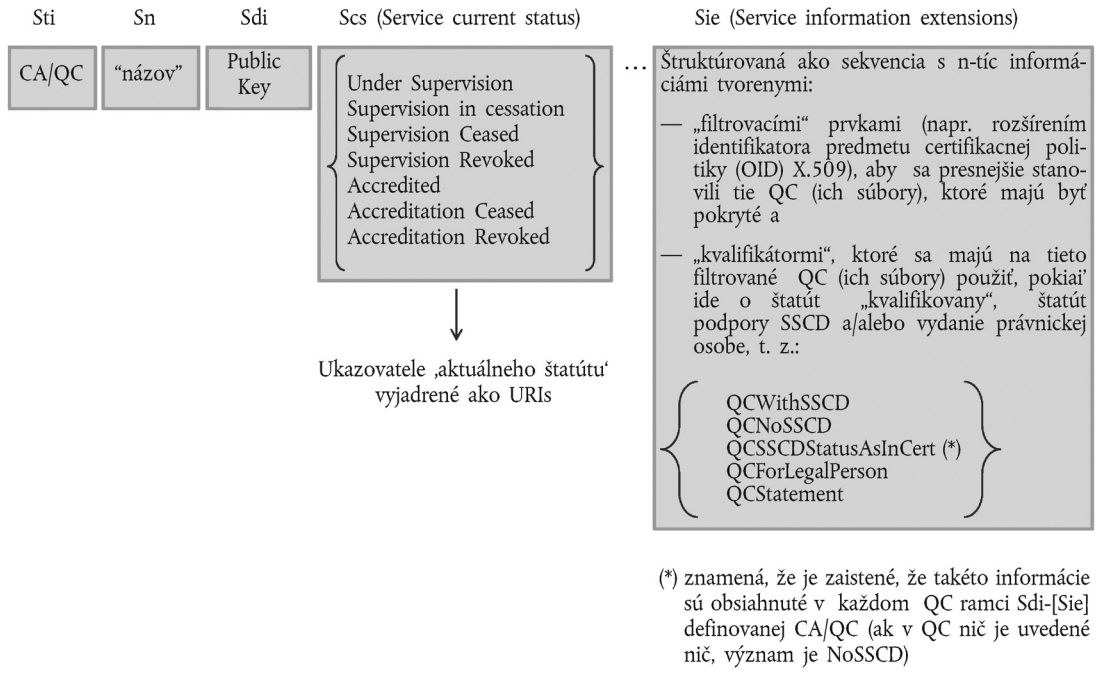
Doplnenie informácií uvedených v poliach „Service type identifier“ („Sti“), „Service name“ („Sn“) a „Service digital identity“ („Sdi“) záznamu o službe v zozname dôveryhodných informácií o poskytovateľoch o informácie poskytnuté v poli „Service information extensions“ („Sie“) umožňuje jasne určiť konkrétny 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). S týmto záznamom súvisí konkrétna informácia „Service current status“ („Scs“ – aktuálny štatút služby), ako je znázornené na obrázku 2.

Zapísanie služby iba prostredníctvom údaja „Sdi“ (koreňovej) CA by znamenalo, že je zaručené (zo strany CSP vydávajúceho QC ale takisto zo strany orgánu dohľadu/akreditačného orgánu zodpovedného za dohľad nad týmto CSP/jeho akreditáciu), 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 alebo nie. V opačnom prípade, napríklad (teda že v QC nie je strojovo spracovateľný údaj podľa noriem v ETSI o tom, či je QC podporovaný SSCD), potom sa na základe údaja „Sdi“ predmetnej (koreňovej) CA dá usúdiť len to, že vydaný QC podľa tejto (koreňovej) hierarchie CA nie je podporovaný žiadnym SSCD. S cieľom uviesť, že tieto QC sa musia považovať za QC podporované SSCD, by sa malo použiť pole „Sie“ (ktorým sa takisto uvádza, že tieto informácie zaručuje CSP vydávajúci QC a podliehajúci dohľadu zo strany orgánu dohľadu alebo akreditačného orgánu alebo akreditovaný takýmto orgánom).

Obrázok 2

Záznam o službe týkajúci sa služby CSP vydávajúceho QC a uvedeného na zozname dôveryhodných informácií o poskytovateľoch

Všeobecné zásady – Pravidlá úpravy – záznamy CSP_{QC} (služby na zozname)



Tieto technické špecifikácie spoločného vzoru zoznamu dôveryhodných informácií o poskytovateľoch umožňujú využiť kombináciu piatich hlavných častí informácie v zázname o službe:

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

— „Service name“ („Sn“ – názov služby),

— informácia o „Service digital identity“ („Sdi“ – digitálna identita služby), na základe ktorej sa služba v zozname identifikuje, teda (minimálne) verejný kľúč CA vydávajúcej QC,

— v prípade služieb CA/QC voliteľná informácia „Service information extension“ („Sie“ – rozšírenie informácie o službe), ktorá umožňuje zaradiť niekoľko položiek informácií týkajúcich sa služby vzťahujúcich sa na štatút zrušenia certifikátov, ktorých platnosť uplynula, dodatočné charakteristiky QC, prevzatie kontroly nad CSP iným CSP a iné dodatočné informácie o službách. Napríklad dodatočné charakteristiky QC predstavuje sekvencia jednej alebo viacero n-tíc, pričom každá n-tica poskytuje:

— kritériá na bližšiu identifikáciu (vytriedenie) v certifikačnej službe identifikovanej na základe „Sdi“ tohto konkrétneho súboru kvalifikovaných certifikátov, pre ktorý sa požadujú/poskytujú dodatočné informácie o kvalifikovanom štatúte podpory SSCD a/alebo o ich vydaní právnickej osobe, ako aj

— súvisiace informácie („kvalifikátory“) o tom, či má byť tento súbor kvalifikovaných certifikátov považovaný za „kvalifikovaný“, či je 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),

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

— či ide o službu, ktorá podlieha dohľadu alebo o akreditovanú službu a

— samotnom štatúte dohľadu/akreditácie.

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

Všeobecné usmernenia o úprave údajov:

1. Ak je zaručené [záruka zo strany CSPQC a dohľad/akreditácia zo strany orgánu dohľadu (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 vyhlásenie QcCompliance statement a/alebo QCP OID a neobsahujú vyhlásenie QcSSCD alebo QCP + OID, v takom prípade je príslušný údaj „Sdi“ postačujúci a pole „Sie“ je dobrovoľné a nemá 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 napríklad diferencované rozličnými CSP specific Certificate Policy OIDs alebo prostredníctvom iných informácií špecifických pre CSP v QC, priamo alebo nepriamo, strojovo spracovateľne alebo nie), ale certifikát, ktorý je podporovaný SSCD, 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“ žiadny 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 CSPQC 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“.

Všeobecnou automatickou zásadou je, že pri každom CSP na zozname dôveryhodných informácií o poskytovateľoch musí byť za každý verejný kľúč pre certifikačnú službu CA/QC, teda certifikačnú autoritu (priamo) vydávajúcu QC, jeden záznam o službe. Za určitých výnimočných okolností a pozorne riadených a schválených podmienkach sa orgán dohľadu/akreditačný orgán členského štátu môže rozhodnúť použiť verejný kľúč koreňovej CA alebo CA vyššieho stupňa v rámci PKI CSP (napríklad v kontexte hierarchie CSP CA od koreňovej CA až po niekoľko vydávajúcich CA) namiesto

uvedenia v zozname všetkých podriadených vydávajúcich služieb CA (t. j. v zozname sa uvádza certifikačná autorita, 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 informácií o poskytovateľoch. Dôsledky (výhody a nevýhody) použitia verejného kľúča koreňovej CA alebo CA vyššej úrovne ako hodnoty „Sdi" údajov o službách v zozname dôveryhodných informácií o poskytovateľoch musia členské štáty dôkladne zvážiť a schváliť pri implementácii. 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 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 QC, ktoré sú v skutočnosti podporované SSCD, ale v certifikátoch nemajú strojovo spracovateľný záznam označujúci takúto podporu, dôrazne sa odporúča v QC vydaných v budúcnosti využiť vyhlásenie QcSSCD. Medzičasom (kým neuplynie platnosť posledného QC bez tejto informácie) by sa v zozname dôveryhodných informácií o poskytovateľoch malo využiť pole „Sie" a súvisiace rozšírenie „Qualifications", napríklad vytriediť informácie na identifikáciu súboru(-ov) certifikátov použitím konkrétnych OID vymedzených CSP_{QC}, ktoré CSP_{QC} môžu potenciálne využívať na rozlišovanie medzi rozličnými typmi QC (niektoré podporované SSCD a niektoré nie) a združovanie jednoznačných „informácií na podporu SSCD" s informáciami identifikovanými (vytriedenými) súborom(-mi) certifikátov pomocou „kvalifikátorov".

Usmernenia o všeobecnom využívaní aplikácií, služieb alebo produktov elektronických podpisov, ktoré sú založené na zozname dôveryhodných informácií o poskytovateľoch 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 strojovo spracovateľných QcStatements (teda QcCompliance) a/alebo QCP(+) OID vymedzených na základe ETSI (čo zaručuje orgán dohľadu/akreditačný orgán – pozri „Všeobecné usmernenia o úprave údajov").

Poznámka: Ak nie sú informácie „Sie" „Qualifications Extension" uvedené alebo ak certifikát konečného subjektu, v prípade ktorého sa požaduje, aby bol QC, nie je „bližšie určený" prostredníctvom príslušného údaja „Sie", v takom prípade „strojovo spracovateľná" informácia v QC, podlieha dohľadu/sa akredituje ako správna. To znamená, že je zaručené, že použitie (alebo nepoužitie) vhodného QcStatement (teda QcCompliance, QcSSCD) a/alebo QCP(+) OID vymedzeného na základe ETSI je v súlade s vyhláseniami $CSP_{QC.}$

— **a ak** sú uvedené informácie „Sie" „Qualifications Extension", potom dodatočne k uvedenému automatickému pravidlu výkladu použitia sa predmetné certifikáty identifikované pomocou rozšírenia informácií „Sie"„Qualifications Extension", ktoré sú zostavené na princípe sekvencie „filtrov" bližšie určujúcich súbor certifikátov, musia byť považované podľa súvisiacich kvalifikátorov poskytujúcich niektoré dodatočné informácie o „podpore SSCD" a/alebo „právnickej osobe ako subjekte" (napríklad certifikáty, ktoré obsahujú konkrétny OID v rozšírení certifikačnej politiky 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.) Uvedené kvalifikátory sú súčasťou tohto súboru „kvalifikátorov" použitých na kompenzáciu za nedostatočné informácie v zodpovedajúcom obsahu QC, ktoré sa používajú na uvedenie:

— údaja o kvalifikovanom štatúte: „QCStatement", čo znamená, že identifikovaný certifikát(-y) je (sú) kvalifikovaný;

A/ALEBO

— údaja o povahe podpory SSCD:

— hodnota kvalifikátora „QCWithSSCD", ktorá znamená, že „QC podporovaný SSCD" alebo

— hodnota kvalifikátora „QCNoSSCD", ktorá znamená, že „QC nie je podporovaný SSCD" alebo

— hodnota kvalifikátora „QCSSCDStatusAsInCert", ktorá znamená, že je zaručené, aby informácia o podpore SSCD bola uvedená v každom QC v rámci informácií „Sdi" – „Sie" poskytnutých v tomto zázname CA/QC;

A/ALEBO

— údaja o vydaní právnickej osobe:

— hodnota kvalifikátora „QCForLegalPerson“, ktorá znamená „certifikát vydaný právnickej osobe“

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

Služby súvisiace so štatútom platnosti certifikátov týkajúce sa QC a v prípade ktorých informáciu súvisiacu so štatútom platnosti certifikátov (napríklad reakcie CRL a OCSP) podpisuje subjekt, ktorého súkromný kľúč nie je certifikovaný v rámci procesu certifikácie, ktorý vedie k CA uvedenému v zozname, ktorá vydáva QC („CA/QC“), sú zahrnuté do zoznamu dôveryhodných informácií o poskytovateľoch uvedením týchto služieb súvisiacich so štatútom platnosti certifikátov ako takých v zozname dôveryhodných informácií o poskytovateľoch (t. j. s typom služby „OCSP/QC“ alebo „CRL/QC“), pretože tieto služby sa môžu považovať za súčasť „kvalifikovaných“ služieb, ktoré podliehajú dohľadu/sú akreditované vo vzťahu k poskytovaniu certifikačných služieb QC. Samozrejme, odpovedajúce subjekty 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 uplatňovať na certifikačné služby vydávajúce nekvalifikované certifikáty (typu služby „CA/PKC“).

Zoznam dôveryhodných informácií o poskytovateľoch zahŕňa služby súvisiace so štatútom platnosti certifikátov, keď pre takéto služby príslušná informácia o lokalite nie je uvedená v certifikátoch konečného subjektu, na ktoré sa vzťahujú služby súvisiace so štatútom platnosti certifikátov.

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	1. poskytovateľ certifikačnej služby, ktorý vytvára a prideľuje certifikáty s verejným kľúčom, alebo 2. technická služba na vydávanie certifikátov, ktorú využíva poskytovateľ certifikačnej služby, ktorý vytvára a prideľuje certifikáty s verejným kľúčom. *POZNÁMKA*: Pozri odsek 4 normy EN 319 411-2 [1] s ďalšími vysvetlivkami pojmu certifikačnej autority.
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	Týka sa dohľadu stanoveného v článku 3 ods. 3 smernice 1999/93/ES. V smernici 1999/93/ES 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 uvedenej smernice.
dobrovoľná akreditácia	akreditácia	Ako je vymedzené v článku 2 ods. 13 smernice 1999/93/ES.
zoznam dôveryhodných informácií o poskytovateľoch	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.

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 119 612.
dôveryhodná služba		Služba, ktorá zvyšuje dôveru voči elektronickým transakciám (bežne, ale nie nevyhnutne pomocou kryptografických techník alebo dôverného materiálu) [ETSI TS 119 612]. *POZNÁMKA*: Tento pojem sa používa v širšom zmysle ako certifikačná služba vydávajúca certifikáty alebo poskytujúca iné služby týkajúce sa elektronických podpisov.
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. Príklady binárnych TrST sú certifikáty, zoznamy zrušených certifikátov (CRL), tokeny časovej pečiatky (TST) a odpovedí online protokolu štatútu certifikátov (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.

([1]) ISO 319411:-2: Elektronické podpisy a infraštruktúry (ESI); Politické a bezpečnostné požiadavky na poskytovateľov dôveryhodných služieb vydávajúcich certifikáty; Časť 2: Politické požiadavky na poskytovateľov certifikačných služieb vydávajúcich kvalifikované certifikáty.

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]).

KAPITOLA I

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

Tieto špecifikácie sú založené na špecifikáciách a požiadavkách uvedených v ETSI TS 119 612 v1.1.1 (ďalej len „ETSI TS 119 612“).

Ak sa v týchto špecifikáciách neuvádza žiadna osobitná požiadavka, UPLATŇUJÚ SA požiadavky v ETSI TS 119 612 odseky 5 a 6 v celom rozsahu. Ak sa v týchto špecifikáciách uvádzajú osobitné požiadavky, PREVLÁDAJÚ nad zodpovedajúcimi požiadavkami ETSI TS 119 612. V prípade rozdielov medzi týmito špecifikáciami a špecifikáciami v ETSI TS 119 612 SÚ normatívnymi špecifikáciami tieto špecifikácie.

Scheme operator name (odsek 5.3.4)

Toto pole JE prítomné a JE V SÚLADE so špecifikáciami odseku 5.3.4. normy TS 119 612.

([1]) IETF RFC 2119: „Kľúčové slová, ktoré sa majú použiť v RFC a ktoré majú naznačovať úrovne požiadaviek“.

Krajiny MÔŽU mať oddelené orgány dohľadu a akreditačné orgány, ako aj dodatočné orgány zodpovedné za akékoľvek operatívne súvisiace činnosti. Určenie prevádzkovateľa schémy (Scheme operator) zoznamu dôveryhodných informácií o poskytovateľoch členských štátov spadá do kompetencie členských štátov. Vychádza sa z predpokladu, že orgán dohľadu, 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 SA IDENTIFIKUJÚ v informácii o schéme ako súčasti zoznamu dôveryhodných informácií o poskytovateľoch vrátane informácií špecifických pre danú schému uvedených pomocou „Scheme information URI“ (odsek 5.3.7).

Scheme name (odsek 5.3.6)

Toto pole JE prítomné a JE V SÚLADE so špecifikáciami odseku 5.3.6. normy TS 119 612, v ktorom sa pre schému POUŽÍVA tento názov:

„EN_name_value“ = „Zoznam štatútov dohľadu nad certifikačnými službami/štatútov akreditácie certifikačných služieb poskytovateľov certifikačných služieb, ktorí podliehajú dohľadu prevádzkovateľa referenčnej schémy dotknutého členského štátu/ktorých prevádzkovateľ referenčnej schémy dotknutého členského štátu akreditoval vzhľadom na dodržiavanie príslušných ustanovení smernice Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy“.

Scheme information URI (odsek 5.3.7)

Toto pole JE prítomné a JE V SÚLADE so špecifikáciami odseku 5.3.7. normy TS 119 612, v ktorom „príslušné informácie o schéme“ ZAHŔŇAJÚ minimálne:

— Úvodné informácie spoločné pre všetky členské štáty o rozsahu a súvislostiach zoznamu dôveryhodných informácií o poskytovateľoch a schémach dohľadu/akreditačných schémach, na ktorých sú založené. Spoločný text, ktorý sa má použiť, je ďalej uvedený text, v ktorom SA reťazec znakov „[*názov príslušného členského štátu*]“ NAHRADÍ názvom príslušného členského štátu:

„Tento zoznam je „Zoznam dôveryhodných informácií o poskytovateľoch certifikačných služieb, ktorí podliehajú dohľadu/sú akreditovaní“, ktorí poskytujú informácie o štatúte dohľadu nad certifikačnými službami/akreditácie certifikačných služieb zo strany poskytovateľov certifikačných služieb (CSP), ktorí podliehajú dohľadu *[názov príslušného členského štátu]*/sú akreditovaní [*názov príslušného členského štátu*] vzhľadom na dodržiavanie príslušných ustanovení smernice Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy.

Cieľom zoznamu dôveryhodných informácií o poskytovateľoch 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 [*názov príslušného členského štátu*]/sú akreditovaní [*názov príslušného členského štátu*] zodpovedným za zostavenie a vedenie zoznamu o súlade s príslušnými ustanoveniami v smernici 1999/93/ES,

— umožňovať dôveryhodné overovanie elektronických podpisov podporovaných tými certifikačnými službami podliehajúcimi dohľadu/tými akreditovanými certifikačnými službami, ktoré poskytujú CSP na zozname.

Zoznam dôveryhodných informácií o poskytovateľoch členského štátu poskytuje minimálne informácie o CSP, ktorí podliehajú dohľadu/sú akreditovaní a vydávajú kvalifikované certifikáty v súlade s ustanoveniami stanovenými v smernici 1999/93/ES [článok 3 ods. 3 a 2 a článok 7 ods. 1 písm. a)], ako aj informácie o QC podporujúcich elektronický podpis a o tom, či je podpis vytvorený bezpečným zariadením na vytvorenie podpisu.

CSP vydávajúci kvalifikované certifikáty (QC) uvedení na tomto zozname podliehajú dohľadu [*názov príslušného členského štátu*] a môžu byť takisto akreditovaní vzhľadom na dodržiavanie ustanovení stanovených v smernici 1999/93/ES, ako aj dodržiavanie požiadaviek prílohy I (požiadavky na QC) a požiadaviek prílohy II (požiadavky na CSP vydávajúcich QC). Platný systém „dohľadu“ (prípadne systém „dobrovoľnej akreditácie“) je vymedzený a musí spĺňať príslušné požiadavky v smernici 1999/93/ES, predovšetkým požiadavky stanovené v článku 3 ods. 3, článku 8 ods. 1, článku 11, (prípadne článku 2 ods. 13, článku 3 ods. 2, článku 7 ods. 1 písm. a), článku 8 ods. 1 a článku 11).

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

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

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

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

  Tieto konkrétne informácie ZAHŔŇAJÚ pri každej uvedenej základnej schéme minimálne:

  — všeobecný opis,

  — informácie o postupe orgánu dohľadu/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 akreditovaní.

— V prípade potreby konkrétne informácie o špecifických „kvalifikáciách“, na ktoré môžu byť oprávnené niektoré z fyzických alebo binárnych (logických) objektov vygenerované alebo vydané v dôsledku poskytovania certifikačnej služby, a to 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 na dobrovoľnom základe poskytnúť špecifické informácie členských štátov o schéme, a to:

— informácie o kritériách a pravidlách uplatnených pri výbere osôb vykonávajúcich dohľad/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.

Scheme type/community/rules (odsek 5.3.9)

Toto pole JE prítomné a JE V SÚLADE so špecifikáciami odseku 5.3.9. normy TS 119 612, pričom zahŕňa aspoň dva URI:

— URI spoločný pre všetky zoznamy dôveryhodných informácií o poskytovateľoch členských štátov, ktorý odkazuje na opisný text, ktorý JE uplatniteľný na všetky zoznamy dôveryhodných informácií o poskytovateľoch takýmto spôsobom:

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

  Opisný text:

  „*Účasť na schéme*

  Každý členský štát musí vytvoriť „Zoznam dôveryhodných informácií o poskytovateľoch certifikačných služieb, ktorí podliehajú dohľadu/sú akreditovaní“, v rámci ktorého sa poskytujú informácie o štatúte dohľadu nad certifikačnými službami/akreditácie certifikačných služieb od poskytovateľov certifikačných služieb (CSP), ktorí podliehajú dohľadu príslušného členského štátu/sú akreditovaní príslušným členským štátom vzhľadom na dodržiavanie príslušných ustanovení smernice Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy.

  Pri implementácii takýchto zoznamov dôveryhodných informácií o poskytovateľoch sa takisto odkazuje na zoznam liniek (ukazovateľov) na zoznam dôveryhodných informácií o poskytovateľoch každého členského štátu vypracovaný Európskou komisiou.

  Politika/pravidlá posudzovania služieb na zozname

  Zoznam dôveryhodných informácií o poskytovateľoch členského štátu musí poskytovať minimálne informácie o CSP podliehajúcich dohľadu/akreditovaných CSP vydávajúcich kvalifikované certifikáty v súlade s ustanoveniami stanovenými v smernici 1999/93/ES [článok 3 ods. 2 a 3 a článok 7 ods. 1 písm. a)], ako aj informácie o QC podporujúcich elektronický podpis a o tom, či je podpis vytvorený bezpečným zariadením na vytvorenie podpisu.

([1]) Posledné dva súbory informácií sú mimoriadne dôležité pre strany spoliehajúce sa na posúdenie kvality a stupňa bezpečnosti týchto systémov dohľadu/akreditácie uplatniteľné na CSP nevydávajúcich QC. Tieto súbory informácií sa uvádzajú na úrovni zoznamu dôveryhodných informácií o poskytovateľoch pomocou súčasných „Scheme information URI“ (odsek 53.7 – 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 v prípade potreby a ak sa o to požiada, môžu poskytovať na úrovni služby (napríklad na účely odlíšenia viacerých úrovní kvality/bezpečnosti) pomocou „Scheme service definition URI“ (odsek 5.5.6).

CSP vydávajúci kvalifikované certifikáty (QC) musia podliehať dohľadu členského štátu, v ktorom sú usadení (ak sú usadení v členskom štáte), a môžu byť takisto akreditovaní vzhľadom na dodržiavanie ustanovení stanovených v smernici 1999/93/ES, ako aj na dodržiavanie požiadaviek prílohy I (požiadavky na QC) a požiadaviek prílohy II (požiadavky na CSP vydávajúcich QC). CSP vydávajúci QC, ktorí sú akreditovaní v členskom štáte, musia patriť do príslušného systému dohľadu daného členského štátu okrem prípadu, keď nie sú usadení v danom členskom štáte. Platný systém „dohľadu" (prípadne systém „dobrovoľnej akreditácie") je vymedzený a musí spĺňať príslušné požiadavky v smernici 1999/93/ES, predovšetkým požiadavky stanovené v článku 3 ods. 3, článku 8 ods. 1, článku 11, (prípadne článku 2 ods. 13, článku 3 ods. 2, článku 7 ods. 1 písm. a), článku 8 ods. 1, článku 11).

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

CSP nevydávajúci QC, ale poskytujúci doplnkové služby 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 uvedenej smernice a prípadne s vnútroštátnymi ustanoveniami týkajúcimi sa poskytovania certifikačných služieb (v zmysle článku 2 ods. 11 smernice 1999/93/ES). Niektoré z fyzických alebo binárnych (logických) objektov vygenerované alebo vydané v dôsledku poskytovania certifikačnej služby môžu byť oprávnené na základe svojho súladu s ustanoveniami a požiadavkami platnými na vnútroštátnej úrovni, ale význam takejto „kvalifikácie" sa pravdepodobne obmedzí iba na vnútroštátnu úroveň.

Výklad zoznamu dôveryhodných informácií o poskytovateľoch

Usmernenia o všeobecnom využívaní aplikácií, služieb alebo produktov elektronických podpisov, ktoré sú založené na zozname dôveryhodných informácií o poskytovateľoch podľa prílohy k rozhodnutiu Komisie [odkaz na súčasné rozhodnutie], sú takéto:

Záznam „CA/QC" „Service type identifier" („Sti") (podobne ako záznam CA/QC ďalej kvalifikovaný ako „RootCA/QC" prostredníctvom využívania „Service information extension" („Sie") rozšírenia additionalServiceInformation)

— znamená, že všetky vydané certifikáty konečného subjektu, ktoré vydala CA na základe „Service digital identifier" (Sdi) (podobne v rámci hierarchie CA počnúc koreňovou CA identifikovanou na základe „Sdi") od zodpovedajúcich CSP (pozri súvisiace informačné polia TSP) sú kvalifikované certifikáty (QC) **za predpokladu**, že sa tak uvádza na samotnom certifikáte prostredníctvom použitia vhodných QcStatements vymedzených na základe EN 319 412-5 (t. j. QcCompliance, QcSSCD atď.) a/alebo QCP(+) OID vymedzených na základe EN 319 411-2 (čo je zaručené vydaním CSP a zaistené orgánom dohľadu/akreditačným orgánom členského štátu),

Poznámka: ak nie sú informácie „Sie" „Qualifications Extension" uvedené alebo ak certifikát konečného subjektu, v prípade ktorého sa požaduje, aby bol QC, nie je „bližšie určený" prostredníctvom príslušného údaja „Sie" „Qualifications Extension", v takom prípade „strojovo spracovateľná" informácia v QC podlieha dohľadu/sa akredituje ako správna. To znamená, že je zaručené, že použitie (alebo nepoužitie) vhodného QcStatement (teda QcCompliance, QcSSCD) a/alebo QCP(+) OID vymedzeného na základe ETSI je v súlade s vyhláseniami CSP vydávajúcimi QC.

— **a AK** sú informácie „Sie" „Qualifications Extension" uvedené, potom dodatočne k uvedenému automatickému pravidlu výkladu použitia sa predmetné certifikáty identifikované pomocou záznamov „Sie" „Qualifications Extension", ktoré sú zostavené na princípe sekvencie „filtrov" bližšie identifikujúcich súbor certifikátov, musia zohľadňovať v súlade so súvisiacimi kvalifikátormi poskytujúcimi niektoré dodatočné informácie o kvalifikovanom štatúte „podpory SSCD" a/alebo „právnickej osoby ako subjektu" (napríklad certifikáty, ktoré obsahujú konkrétny OID v rozšírení certifikačnej politiky 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.). Uvedené kvalifikátory sú súčasťou tohto súboru „kvalifikátorov" použitých na kompenzáciu za nedostatočné informácie v zodpovedajúcom obsahu QC, ktoré sa používajú na uvedenie:

— údaja o kvalifikovanom štatúte: „QCStatement", čo znamená, že identifikovaný certifikát(-y) je (sú) kvalifikovaný,,

A/ALEBO

— údaja o povahe podpory SSCD:

— hodnoty kvalifikátora „QCWithSSCD“, ktorá znamená, že „QC je podporovaný SSCD“ alebo

— hodnoty kvalifikátora „QCNoSSCD“, ktorá znamená, že „QC nie je podporovaný SSCD“ alebo

— hodnoty kvalifikátora „QCSSCDStatusAsInCert“, ktorá znamená, že je zaručené, aby informácia o podpore SSCD bola uvedená v každom QC v rámci informácií „Sdi“ – „Sie“ poskytnutých v tomto zázname CA/QC,

A/ALEBO

— údaja o vydaní právnickej osobe:

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

Všeobecné pravidlo výkladu každého záznamu typu „Sti“ je, že služba v zozname pomenovaná podľa poľa „Sn“ a jednoznačne identifikovaná podľa hodnoty poľa „Sdi“ má aktuálny štatút dohľadu/akreditácie podľa hodnoty poľa „Scs“, a to od dátumu uvedeného v „Current status starting date and time (Dátum a čas, odkedy aktuálny štatút začal platiť)“. Osobitné pravidlá výkladu pre všetky dodatočné informácie vzhľadom na službu v zozname (napríklad pole „Service information extensions“) možno nájsť podľa potreby v špecifickom URI členského štátu v rámci súčasného poľa „Scheme type/community/rules“.

Uveďte prosím odkaz na Technické špecifikácie spoločného vzoru „Zoznamu dôveryhodných informácií o poskytovateľoch certifikačných služieb, ktorí podliehajú dohľadu/sú akreditovaní“ v prílohe k rozhodnutiu Komisie 2009/767/ES vzhľadom na ďalšie podrobnosti o poliach, opis a význam implementácie zoznamov dôveryhodných informácií o poskytovateľoch členských štátov.“

— URI špecifické pre zoznam dôveryhodných informácií o poskytovateľoch každého členského štátu, ktorý je odkazom na opisný text, ktorý JE uplatniteľný na TL tohto členského štátu:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, kde CC = ISO 3166-1 ([1]) alpha-2 kód krajiny používaný v poli „Scheme territory“ (odsek 5.3.10)

— Keď majú používatelia 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.

— Keď majú používatelia prístup k osobitnému opisu členského štátu, ako používať a vykladať obsah zoznamu dôveryhodných informácií o poskytovateľoch 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 na vysvetlenie, ako sa na tento účel používajú polia „Scheme service definition URI“ (odsek 5.5.6) a „Service information extension“ (odsek 5.5.9).

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

TSL policy/legal notice (odsek 5.3.11)

Toto pole JE prítomné a JE V SÚLADE so špecifikáciami odseku 5.3.11 normy TS 119 612, keď politické/právne upozornenie týkajúce sa právneho štatútu schémy alebo právnych požiadaviek, ktoré schéma spĺňa, na území, pod ktorého právomoc spadá, a/alebo obmedzenia a podmienky, za ktorých sa zoznam dôveryhodných informácií o poskytovateľoch vedie a uverejňuje, JE viacjazyčný reťazec znakov (vo formáte „plain text“) pozostávajúci z dvoch častí:

1. Prvej, povinnej časti, spoločnej pre zoznamy dôveryhodných informácií o poskytovateľoch všetkých členských štátov (v angličtine UK ako povinnom jazyku a prípadne v jednom alebo viacerých štátnych 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 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.

([1]) ISO 3166-1:2006: „Kódy názvov krajín a ich častí – 1. časť: Kódy krajín“.

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

2. Druhá, dobrovoľná časť, špecifická pre každý zoznam dôveryhodných informácií o poskytovateľoch (v angličtine UK ako povinnom jazyku a prípadne v jednom alebo viacerých národných jazykoch) s odkazmi na osobitné platné vnútroštátne právne rámce (napríklad najmä vtedy, ak sa týkajú vnútroštátnych schém dohľadu/akreditácie CSP, ktorí nevydávajú QC).

KAPITOLA II

KONTINUITA ZOZNAMOV DÔVERYHODNÝCH INFORMÁCIÍ O POSKYTOVATEĽOCH

Certifikáty, ktoré treba oznámiť Komisii podľa článku 3 písm. c) súčasného rozhodnutia BUDÚ VYDANÉ tak, aby:

— medzi ich lehotami platnosti boli minimálne tri mesiace,

— boli vytvorené s novými pármi kľúčov, pretože žiadne predtým použité páry kľúčov sa opakovane necertifikujú.

V prípade poškodenia alebo vyradenia JEDNÉHO zo súkromných kľúčov zodpovedajúceho verejnému kľúču, ktorý by sa mohol použiť na overenie podpisu v zozname dôveryhodných informácií a ktorý bol oznámený Komisii a uverejnený v centrálnych zoznamoch ukazovateľov Komisie, členské štáty:

— ZNOVU VYDAJÚ, a to bez zdržania, nový zoznam dôveryhodných informácií o poskytovateľoch podpísaný nepoškodeným súkromným kľúčom v prípade, ak bol zoznam dôveryhodných informácií o poskytovateľoch podpísaný poškodeným alebo vyradeným súkromným kľúčom,

— okamžite OZNÁMIA Komisii nový zoznam certifikátov s verejnými kľúčmi zodpovedajúcimi súkromným kľúčom, ktoré by sa mohli použiť na podpísanie zoznamu dôveryhodných informácií o poskytovateľoch.

V prípade poškodenia alebo vyradenia VŠETKÝCH súkromných kľúčov zodpovedajúcich verejným kľúčom, ktoré by sa mohli použiť na overenie podpisu v zozname dôveryhodných informácií a ktoré boli oznámené Komisii a uverejnené v centrálnych zoznamoch ukazovateľov Komisie, členské štáty:

— VYGENERUJÚ nové páry kľúčov, ktoré by sa mohli použiť na podpísanie zoznamu dôveryhodných informácií o poskytovateľoch a ich zodpovedajúce certifikáty s verejným kľúčom,

— ZNOVU VYDAJÚ, a to bez zdržania, nový zoznam dôveryhodných informácií o poskytovateľoch podpísaný jedným z tých nových súkromných kľúčov, ktorých zodpovedajúci certifikát s verejným kľúčom sa má oznámiť,

— okamžite OZNÁMIA Komisii nový zoznam certifikátov s verejnými kľúčmi zodpovedajúcimi súkromným kľúčom, ktoré by sa mohli použiť na podpísanie zoznamu dôveryhodných informácií o poskytovateľoch.

KAPITOLA III

ŠPECIFIKÁCIE ĽUDSKÝM OKOM ČITATEĽNEJ FORMY ZOZNAMU DÔVERYHODNÝCH INFORMÁCIÍ O POSKYTOVATEĽOCH

Ak sa stanoví a uverejní ľudským okom čitateľná forma zoznamu dôveryhodných informácií o poskytovateľoch, MALA BY byť poskytnutá vo formáte dokumentu PDF podľa ISO 32000 ([1]), ktorý MUSÍ byť naformátovaný podľa profilu PDF/A (ISO 19005 ([2])).

Obsah ľudským okom čitateľnej formy zoznamu dôveryhodných informácií o poskytovateľoch vo formáte PDF/A BY MAL spĺňať tieto požiadavky:

— v štruktúre formy HR BY SA MAL odrážať logický model opísaný v ETSI TS 119 612,

— každé zahrnuté pole BY MALO byť zobrazené a uvádzať:

  — názov poľa (napríklad „Service type identifier“),

  — hodnotu poľa (napríklad „QA/QC“),

  — podľa potreby význam (opis) hodnoty poľa (napríklad „certifikačná autorita vydávajúca certifikáty s verejným kľúčom.“),

  — podľa potreby viacero verzií v štátnych jazykoch, ako sa stanovuje v zozname dôveryhodných informácií o poskytovateľoch,

([1]) ISO 32000-1:2008: Správa dokumentov – PDF (Portable document format) – 1. časť: PDF 1.7
([2]) ISO 19005-2:2011: Správa dokumentov – Formát pre dlhodobú archiváciu elektronických textových dokumentov – 2. časť: Používanie normy ISO 32000-1 (PDF/A-2)

— – 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

  — 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 dať ľahko vytlačiť,

— formu HR MUSÍ podpísať prevádzkovateľ schémy podľa základného profilu podpisov PAdES ([1]).

([1]) ETSI TS 103 172 (marec 2012) – Elektronické podpisy a infraštruktúry (ESI – Electronic Signatures and Infrastructures); Základný profil PAdES