OPRAVY

Oprava rozhodnutí Komise ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu

(Úřední věstník Evropské unie L 274 ze dne 20. října 2009)

Rozhodnutí 2009/767/ES se nahrazuje tímto:

ROZHODNUTÍ KOMISE

ze dne 16. října 2009,

kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu

(oznámeno pod číslem K(2009) 7806)

(Text s významem pro EHP)

(2009/767/ES)

KOMISE EVROPSKÝCH SPOLEČENSTVÍ,

s ohledem na Smlouvu o založení Evropského společenství,

s ohledem na směrnici Evropského parlamentu a Rady 2006/123/ES ze dne 12. prosince 2006 o službách na vnitřním trhu [1], a zejména na čl. 8 odst. 3 uvedené směrnice,

vzhledem k těmto důvodům:

(1) Povinnosti správního zjednodušení uložené členským státům v kapitole II směrnice 2006/123/ES, a zejména v článcích 5 a 8 uvedené směrnice, zahrnují povinnost zjednodušit postupy a formality použitelné na přístup k činnosti poskytování služeb a povinnost zajistit, aby tyto postupy a formality mohly být snadno splněny na dálku a pomocí elektronických prostředků prostřednictvím „jednotného kontaktního místa“.

(2) Jak stanoví článek 8 směrnice 2006/123/ES, musí splnění postupů a formalit prostřednictvím „jednotných kontaktních bodů“ být možné i přes hranice mezi členskými státy.

(3) Aby se splnila povinnost zjednodušit postupy a formality a usnadnit přeshraniční využití „jednotných kontaktních míst“, měly by být postupy s využitím elektronických prostředků založeny na jednoduchých řešeních, a to i pokud jde o využití elektronických podpisů. V případech, kdy se po provedení příslušného posouzení rizik konkrétních postupů a formalit považují za nezbytné vysoká úroveň bezpečnosti nebo podpis odpovídající vlastnoručnímu podpisu, by mohl být od poskytovatelů služeb u některých postupů a formalit vyžadován zaručený elektronický podpis založený na kvalifikovaném osvědčení, ať již s prostředky pro bezpečné vytváření podpisu či bez nich.

(4) Rámec Společenství pro elektronické podpisy byl stanoven směrnicí Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy [2]. Za účelem usnadnění účinného přeshraničního využívání zaručených elektronických podpisů založených na kvalifikovaném osvědčení by se měla podporovat důvěra v tyto elektronické podpisy bez ohledu na to, v kterém členském státě je usazena podepisující osoba nebo ověřovatel, jenž kvalifikované osvědčení vydává. Toho by mohlo být dosaženo tím, že se snazším a důvěryhodným způsobem zpřístupní informace potřebné pro ověřování elektronických podpisů, zejména pak informace týkající se ověřovatelů, nad nimiž je v členském státě vykonáván dohled nebo kteří jsou v členském státě akreditováni, a služeb, jež nabízejí.

(5) Je třeba zajistit, aby členské státy tyto informace zpřístupnily veřejnosti prostřednictvím společné šablony, aby se usnadnilo používání elektronických podpisů a zajistila se vhodná úroveň podrobností, která by příjemci umožnila elektronický podpis ověřit,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Použití a přijímání elektronických podpisů

1. Je-li to opodstatněné na základě příslušného posouzení zahrnutých rizik a v souladu s čl. 5 odst. 1 a 3 směrnice 2006/123/ES, mohou členské státy pro splnění některých postupů a formalit prostřednictvím jednotných kontaktních míst podle článku 8 směrnice 2006/123/ES požadovat, aby poskytovatel služby používal zaručené elektronické podpisy založené na kvalifikovaném osvědčení, ať již s prostředkem pro bezpečné vytváření podpisu nebo bez něj, jak stanoví a upravuje směrnice 1999/93/ES.

[1] Úř. věst. L 376, 27.12.2006, s. 36.

[2] Úř. věst. L 13, 19.1.2000, s. 12.

2. Členské státy přijmou pro splnění postupů a formalit uvedených v odstavci 1 jakýkoli zaručený elektronický podpis založený na kvalifikovaném osvědčení, ať již s prostředkem pro bezpečné vytváření podpisu nebo bez něj, aniž je tím dotčena možnost, aby členské státy omezily toto přijímání na zaručený elektronický podpis založený na kvalifikovaném osvědčení a vytvořený prostředkem pro bezpečné vytváření podpisu, pokud je toto v souladu s posouzením rizik uvedeným v odstavci 1.

3. Členské státy nepodmíní přijetí zaručeného elektronického podpisu založeného na kvalifikovaném osvědčení, ať již s prostředkem pro bezpečné vytváření podpisu nebo bez něj, splněním požadavků, které by pro poskytovatele služby představovaly překážky užití postupů s využitím elektronických prostředků prostřednictvím jednotných kontaktních míst.

4. Odstavec 2 nebrání členským státům v přijímání jiných elektronických podpisů, než jsou zaručené elektronické podpisy založené na kvalifikovaném osvědčení, ať již s prostředkem pro bezpečné vytváření podpisu nebo bez něj.

Článek 2

Zřízení, údržba a zveřejnění důvěryhodných seznamů

1. Každý členský stát v souladu s technickými specifikacemi stanovenými v příloze zřizuje, udržuje a zveřejňuje „důvěryhodný seznam“, jenž obsahuje minimální informace související s ověřovateli, kteří vydávají kvalifikovaná osvědčení pro veřejnost a nad nimiž vykonává dohled nebo jež akreditoval.

2. Členské státy zřídí a zveřejní přinejmenším podobu důvěryhodného seznamu čitelnou okem, a to v souladu se specifikacemi stanovenými v příloze.

3. Členské státy uvědomí Komisi o subjektu odpovědném za zřízení, údržbu a zveřejnění důvěryhodného seznamu, o místě, kde je důvěryhodný seznam zveřejněn, a o jakýchkoli změnách.

Článek 3

Použití

Toto rozhodnutí se použije od 28. prosince 2009.

Článek 4

Určení

Toto rozhodnutí se použije od 28. prosince 2009.

V Bruselu dne 16. října 2009.

Za Komisi

Charlie McCREEVY

člen Komise

PŘÍLOHA

TECHNICKÉ SPECIFIKACE PRO SPOLEČNOU ŠABLONU DŮVĚRYHODNÉHO SEZNAMU OVĚŘOVATELŮ, NAD NIMIŽ JE VYKONÁVÁN DOHLED NEBO KTEŘÍ JSOU AKREDITOVÁNI

PŘEDMLUVA

1. **Obecně**

Cílem společné šablony Důvěryhodného seznamu ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni pro členské státy je zavést jednotný způsob poskytování informací ze strany jednotlivých členských států ohledně stavu dohledu/akreditace osvědčovacích služeb poskytovaných ověřovateli (*Certification Service Providers*, dále jen „CSP“) ([1]), nad nimiž vykonávají dohled nebo kteří jsou jimi akreditováni v souladu s příslušnými ustanoveními směrnice 1999/93/ES. Patří sem poskytování historických informací o stavu dohledu/akreditace osvědčovacích služeb.

Povinné informace v důvěryhodném seznamu (*Trusted List*, dále jen „TL“) musí obsahovat přinejmenším informace o ověřovatelích, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni a kteří vydávají kvalifikovaná osvědčení (*Qualified Certificates*, dále jen „QC“) ([2]) v souladu s ustanoveními směrnice 1999/93/ES (čl. 3 odst. 2 a 3, čl. 7 odst. 1 písm. a)), včetně informací o kvalifikovaných osvědčeních podporujících elektronický podpis a o tom, zda je podpis vytvořen prostředkem pro bezpečné vytváření podpisu (*Secure Signature Creation Device*, dále jen „SSCD“) ([3]), či nikoli.

Dodatečné informace o dalších ověřovatelích, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni a kteří nevydávají kvalifikovaná osvědčení, ale poskytují služby související s elektronickými podpisy (např. ověřovatelé poskytující služby časových razítek a vydávající tokeny časových razítek, ověřovatelé vydávající nekvalifikovaná osvědčení atd.), mohou být do důvěryhodného seznamu zařazeny dobrovolně na vnitrostátní úrovni.

Cílem těchto informací je především podpora validace kvalifikovaných elektronických podpisů (*Qualified Electronic Signatures*, dále jen „QES“) a zaručených elektronických podpisů (*Advanced Electronic Signatures*, dále jen „AdES“) ([4]) podporovaných kvalifikovaným osvědčením ([5]) ([6]).

Navrhovaná společná šablona je slučitelná s prováděním založeným na specifikacích z ETSI TS 102 231 ([7]), které se používají při zřizování, zveřejňování, umísťování a ověřování pravosti takovýchto seznamů a při přístupu k nim a důvěře v ně.

2. **Pokyny pro úpravy zápisů v důvěryhodných seznamech**

2.1. *Důvěryhodný seznam zaměřený na osvědčovací služby, nad nimiž je vykonáván dohled nebo které jsou akreditovány*

Příslušné osvědčovací služby a ověřovatelé v jediném seznamu

Důvěryhodný seznam členského státu je definován jako „Seznam stavu dohledu nebo akreditace osvědčovacích služeb ověřovatelů, nad nimiž vykonává příslušný členský stát dohled nebo kteří jsou příslušným členským státem akreditováni, pokud jde o soulad s příslušnými ustanoveními směrnice 1999/93/ES“.

Takový důvěryhodný seznam musí obsahovat:

— **všechny ověřovatele** ve smyslu definice v čl. 2 odst. 11 směrnice 1999/93/ES, tj. „subjekt nebo právnická či fyzická osoba, která vydává osvědčení nebo poskytuje jiné služby související s elektronickými podpisy“;

— **nad nimiž je vykonáván dohled nebo kteří jsou akreditováni**, pokud jde o soulad s příslušnými ustanoveními směrnice 1999/93/ES.

Z hlediska definic a ustanovení stanovených směrnicí 1999/93/ES, zejména s ohledem na příslušné ověřovatele a jejich systémy dohledu nebo dobrovolné akreditace, lze rozlišit dva druhy ověřovatelů, a to ověřovatele, kteří vydávají kvalifikovaná osvědčení pro veřejnost (CSP_{QC}), a ověřovatele, kteří nevydávají kvalifikovaná osvědčení pro veřejnost, ale poskytují „jiné služby související s elektronickými podpisy“.

([1]) Jak je definováno v čl. 2 odst. 11 směrnice 1999/93/ES.
([2]) Jak je definováno v čl. 2 odst. 10 směrnice 1999/93/ES.
([3]) Jak je definováno v čl. 2 odst. 6 směrnice 1999/93/ES.
([4]) Jak je definováno v čl. 2 odst. 2 směrnice 1999/93/ES.
([5]) Pro AdES podporovaný QC se v tomto dokumentu používá zkratka „$AdES_{QC}$“.
([6]) Je třeba vzít na vědomí, že existuje několik elektronických služeb založených na prostém AdES, jejichž přeshraniční použití by také mělo být usnadněno, a to za předpokladu, že podpůrné osvědčovací služby (např. vydávání nekvalifikovaných osvědčení) tvoří součást služeb, nad nimiž je vykonáván dohled nebo které jsou akreditovány a informace o nichž uvedl členský stát v důvěryhodném seznamu v části určené pro dobrovolné informace.
([7]) ETSI TS 102 231 – *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.*

— **Ověřovatelé vydávající kvalifikovaná osvědčení**

  — o Musí nad nimi vykonávat dohled členský stát, v němž jsou usazeni (pokud jsou usazeni v členském státě), a mohou být také akreditováni, z hlediska souladu s ustanoveními směrnice 1999/93/ES, včetně požadavků přílohy I (požadavky na kvalifikovaná osvědčení) a přílohy II (požadavky pro ověřovatele vydávající kvalifikovaná osvědčení). Ověřovatelé vydávající kvalifikovaná osvědčení, kteří jsou akreditováni v členském státě, musí podléhat také vhodnému systému dohledu tohoto členského státu, ledaže by v něm nebyli usazeni.

  — o Je definován příslušný systém „dohledu“ (resp. systém „dobrovolné akreditace“), který musí splňovat příslušné požadavky směrnice 1999/93/ES, zejména čl. 3 odst. 3, čl. 8 odst. 1, článku 11, 13. bodu odůvodnění (resp. čl. 2 odst. 13, čl. 3 odst. 2, čl. 7 odst. 1 písm. a), čl. 8 odst. 1, článku 11 a 4. a 11.–13. bodu odůvodnění).

— **Ověřovatelé, kteří nevydávají kvalifikovaná osvědčení**

  — o Mohou spadat do systému „dobrovolné akreditace“ (jak je definován ve směrnici 1999/93/ES a v souladu s ní) nebo do „uznaného systému schválení“ definovaného a prováděného na vnitrostátní úrovni pro dohled nad souladem s ustanoveními směrnice a případně též s vnitrostátními ustanoveními souvisejícími s poskytováním osvědčovacích služeb (ve smyslu čl. 2 odst. 11 směrnice).

  — o Některé fyzické nebo binární (logické) objekty vytvořené nebo vydané v důsledku poskytnutí osvědčovací služby mohou mít nárok na zvláštní „kvalifikaci“ na základě svého souladu s ustanoveními a požadavky stanovenými na vnitrostátní úrovni, význam takových „kvalifikací“ však bude pravděpodobně omezen pouze na vnitrostátní úroveň.

Důvěryhodný seznam členského státu musí poskytovat přinejmenším informace o ověřovatelích, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni a kteří vydávají kvalifikovaná osvědčení pro veřejnost (v souladu s ustanoveními směrnice 1999/93/ES (čl. 3 odst. 2 a 3 a čl. 7 odst. 1 písm. a)), informace o kvalifikovaných osvědčeních podporujících elektronický podpis a o tom, zda je podpis vytvořen prostředkem pro bezpečné vytváření podpisu, či nikoli.

Dodatečné informace o dalších službách, nad nimiž je vykonáván dohled nebo které jsou akreditovány, ověřovatelů, kteří nevydávají kvalifikovaná osvědčení pro veřejnost (např. ověřovatelé poskytující služby časových razítek a vydávající tokeny časových razítek, ověřovatelé vydávající nekvalifikovaná osvědčení atd.), mohou být do důvěryhodného seznamu zařazeny dobrovolně na vnitrostátní úrovni.

Cílem důvěryhodného seznamu je:

— poskytnout seznam stavu dohledu nebo akreditace osvědčovacích služeb ověřovatelů, nad nimiž z hlediska souladu s příslušnými ustanoveními směrnice 1999/93/ES vykonává dohled nebo jež akredituje členský stát odpovědný za zřízení a údržbu seznamu, a poskytnout o tomto stavu spolehlivé informace;

— umožnit validaci elektronických podpisů podporovaných osvědčovacími službami uvedenými na seznamu, nad nimiž je vykonáván dohled nebo které jsou akreditovány, ověřovatelů uvedených na seznamu.

Jednotný soubor hodnot stavu dohledu/akreditace

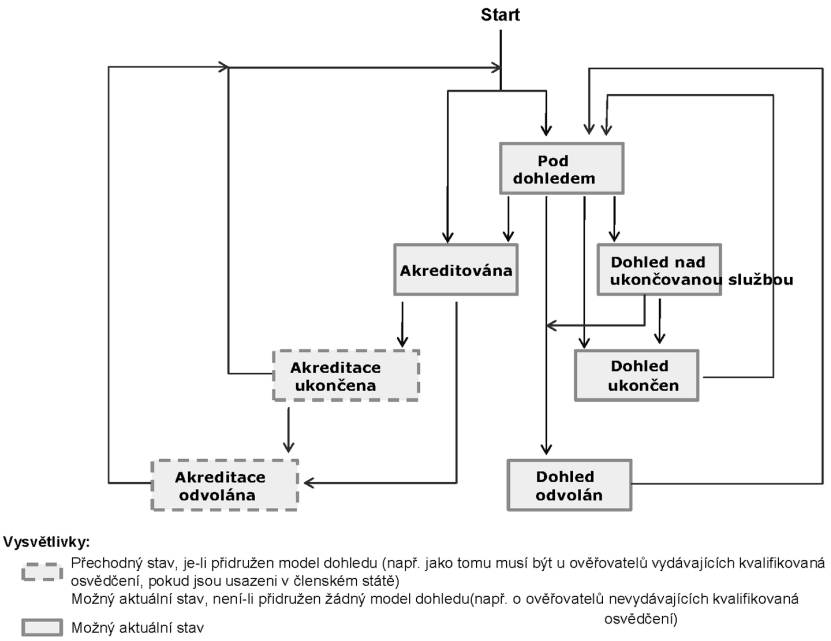
Pro každý členský stát může být zřízen a udržován pouze jediný důvěryhodný seznam, v němž bude uveden stav dohledu nebo akreditace těch osvědčovacích služeb těch ověřovatelů, nad nimiž vykonává členský stát dohled nebo které akreditoval.

Skutečnost, že je nad službou aktuálně vykonáván dohled nebo je akreditována, tvoří součást jejího aktuálního stavu („*Current Status*“). Mimo to může být stav dohledu nebo akreditace „probíhající“ („*on-going*“), „v postupu ukončení“ („*in cessation*“), „ukončen“ („*ceased*“), či dokonce „odvolán“ („*revoked*“). V průběhu svého trvání může tatáž osvědčovací služba změnit stav dohledu na stav akreditace a naopak ([1]).

Obrázek 1 níže popisuje předpokládaný pohyb jedné osvědčovací služby mezi možnými stavy dohledu/akreditace:

([1]) Např. ověřovatel usazený v členském státě poskytující osvědčovací službu, nad níž zpočátku členský stát (dozorový subjekt) vykonává dohled, se může později rozhodnout, že u stávající dozorované osvědčovací služby přejde k dobrovolné akreditaci. A naopak, ověřovatel v jiném členském státě se může rozhodnout, že neukončí akreditovanou osvědčovací službu, ale že ji přesune ze stavu akreditace na stav dohledu, např. z obchodních či hospodářských důvodů.

Předpokládané schéma stavu dohledu/akreditace u jediné služby CSP



Obrázek 1

Nad osvědčovací službou vydávající kvalifikovaná osvědčení musí být vykonáván dohled (je-li zřízena v členském státě) a může být dobrovolně akreditována. „Aktuální hodnotou stavu" takové služby uvedené v důvěryhodném seznamu může být jakákoli hodnota stavu zobrazená výše. Je však třeba vzít na vědomí, že „akreditace ukončena" a „akreditace odvolána" musí být hodnotou „přechodný stav" pouze v případě služeb CSP_{QC} zřízených v členském státě, neboť nad takovými službami je vykonáván dohled standardně (i když nejsou nebo již nejsou akreditovány).

Požaduje se, aby členské státy, které zřizují nebo již zřídily „uznané systémy schválení" definované a prováděné na vnitrostátní úrovni pro dohled nad souladem služeb ověřovatelů nevydávajících kvalifikovaná osvědčení s ustanoveními směrnice 1999/93/ES a s případnými vnitrostátními ustanoveními souvisejícími s poskytováním osvědčovacích služeb (ve smyslu čl. 2 odst. 11 směrnice), rozdělily tyto systémy schválení do těchto dvou kategorií:

— „dobrovolná akreditace", jak je definována a upravena směrnicí 1999/93/ES (čl. 2 odst. 13, čl. 3 odst. 2, čl. 7 odst. 1 písm. a), čl. 8 odst. 1, článek 11, 4. a 11.–13. bod odůvodnění);

— „dohled", jak vyžaduje směrnice 1999/93/ES a jak je prováděn vnitrostátními ustanoveními a požadavky v souladu s vnitrostátními zákony.

V souladu s tím může být osvědčovací služba nevydávající kvalifikovaná osvědčení pod dohledem nebo může být dobrovolně akreditována. „Aktuální hodnotou stavu" (viz obrázek 1) takové služby uvedené v důvěryhodném seznamu může být jakákoli hodnota stavu zobrazená výše.

Důvěryhodný seznam musí obsahovat informace o souvisejících systémech dohledu/akreditace, a to zejména:

— informace o systému dohledu vztahujícím se na jakéhokoli CSP_{QC};

— ve vhodných případech informace o vnitrostátním systému „dobrovolné akreditace" vztahujícím se na jakéhokoli CSP_{QC};

— ve vhodných případech informace o systému dohledu vztahujícím se na jakéhokoli ověřovatele nevydávajícího kvalifikovaná osvědčení;

— ve vhodných případech informace o vnitrostátním systému „dobrovolné akreditace" vztahujícím se na jakéhokoli ověřovatele nevydávajícího kvalifikovaná osvědčení.

Dva poslední soubory informací jsou zásadně důležité pro to, aby mohly strany spoléhající se na osvědčení posoudit úroveň kvality a bezpečnosti systémů dohledu/akreditace použitých na vnitrostátní úrovni na ověřovatele nevydávající kvalifikovaná osvědčení. Když se v důvěryhodném seznamu uvádějí informace ohledně stavu dohledu/akreditace u služeb ověřovatelů nevydávajících kvalifikovaná osvědčení, uvedou se výše uvedené soubory informací na úrovni důvěryhodného

seznamu prostřednictvím „*Scheme information URI*“ („URI – informace o systému“, bod 5.3.7 – informace poskytované členským státem), „*Scheme type/community/rules*“ („Typ/společenství/pravidla systému“, bod 5.3.9 – prostřednictvím textu společného pro všechny členské státy a volitelných informací poskytovaných členským státem) a „*TSL policy/legal notice*“ („Politika/právní upozornění TSL“, bod 5.3.11 – text společný pro všechny členské státy související se směrnicí 1999/93/ES, společně s možností, aby členský stát doplnil svůj specifický text/odkazy). Další informace o „kvalifikaci“ definované na úrovni vnitrostátních systémů dohledu/akreditace pro ověřovatele nevydávající kvalifikovaná osvědčení lze ve vhodných případech poskytnout na úrovni služby (např. pro odlišení různých úrovní kvality/bezpečnosti) prostřednictvím použití rozšíření „*additionalServiceInformation*“ („další informace o službě“, bod 5.8.2) jako součásti „*Service information extension*“ („Rozšíření informací o službě“, bod 5.5.9). Další informace o příslušných technických specifikacích jsou uvedeny v podrobných specifikacích v kapitole I.

Přestože v členském státě mohou být za dohled nad osvědčovacími službami a za jejich akreditaci odpovědné různé subjekty členského státu, předpokládá se, že pro jednu osvědčovací službu bude existovat pouze jediný zápis (identifikovaný její „Digitální identitou služby“ („*Service digital identity*“) podle ETSI TS 102 231 [1]) a že bude stav jejího dohledu/akreditace odpovídajícím způsobem aktualizován. Význam výše znázorněných stavů je popsán v souvisejícím bodě 5.5.4 podrobných technických specifikací v kapitole I.

2.2. *Zápisy v důvěryhodném seznamu, jejichž cílem je usnadnit validaci kvalifikovaných elektronických podpisů a zaručených elektronických podpisů podporovaných kvalifikovaným osvědčením*

Nejdůležitější částí vytvoření důvěryhodného seznamu je zřízení jeho povinné části, jmenovitě „Seznamu služeb“ („*List of services*“) podle ověřovatelů vydávajících kvalifikovaná osvědčení tak, aby správně odrážel přesnou situaci každé takové osvědčovací služby vydávající kvalifikovaná osvědčení a aby se zajistilo, že jsou informace poskytované v každém zápisu dostatečné pro usnadnění validace QES a $AdES_{QC}$ (ve spojení s obsahem kvalifikovaného osvědčení koncového subjektu vydaného ověřovatelem v rámci osvědčovací služby uvedené v tomto zápisu).

Vzhledem k tomu, že dosud neexistuje žádný skutečně interoperabilní přeshraniční profil kvalifikovaného osvědčení, mohou požadované informace zahrnovat i jiné informace než „Digitální identita služby“ („*Service digital identity*“) jediné (kořenové) certifikační autority, zejména informace o identifikaci stavu vydaného osvědčení a o tom, zda byly podporované podpisy vytvořeny prostředkem pro bezpečné vytváření podpisu. Subjekt, který je v členském státě pověřen zřízením, úpravou a údržbou důvěryhodného seznamu (tj. provozovatel systému podle ETSI TS 102 231), musí tedy zohlednit aktuální profil a obsah osvědčení v každém vydaném kvalifikovaném osvědčení u CSP_{QC}, kteří jsou uvedeni v důvěryhodném seznamu.

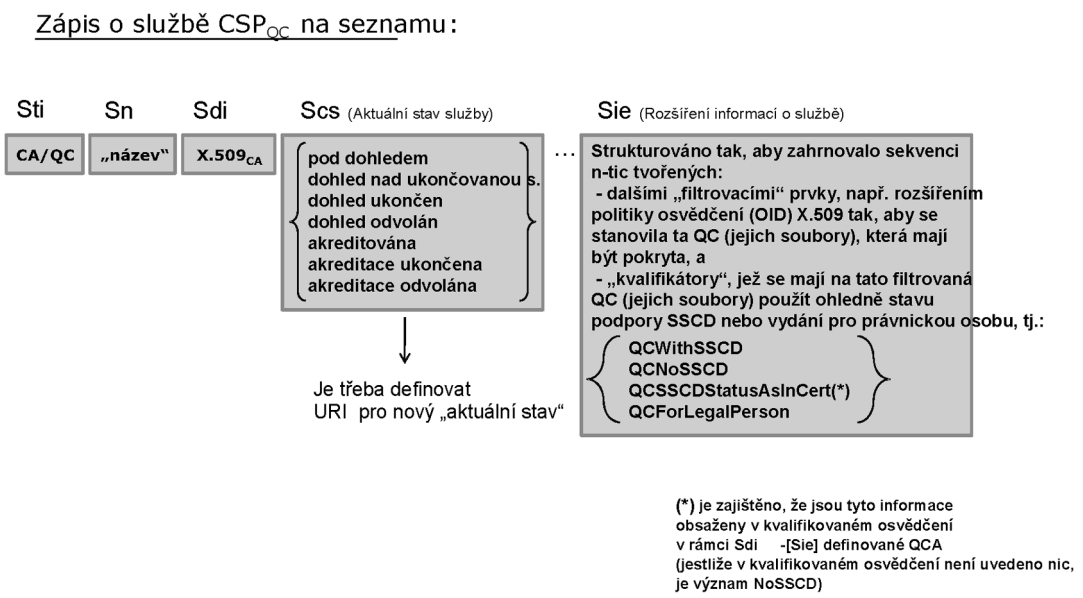
V ideálním případě by každé vydané kvalifikované osvědčení mělo obsahovat prohlášení o shodě kvalifikovaného osvědčení (*QcCompliance*) [2] definované ETSI, pokud se tvrdí, že jde o kvalifikované osvědčení, a mělo by obsahovat prohlášení QcSSCD, pokud se tvrdí, že je podporováno SSCD pro vytváření elektronických podpisů nebo že každé vydané kvalifikované osvědčení obsahuje QCP/QCP + identifikátory předmětu (OID) politiky osvědčení definované v ETSI TS 101 456 [3]. Používání různých norem ze strany ověřovatelů, široký výklad těchto norem a také nedostatečná informovanost o existenci a přednosti normativních technických specifikací nebo norem vede k odlišnostem ve skutečném obsahu aktuálně vydávaných kvalifikovaných osvědčení (např. využití, či nevyužití prohlášení o kvalifikovaných osvědčeních definovaných ETSI), a v důsledku toho brání přijímajícím stranám, aby se jednoduše spoléhaly na osvědčení podepisující osoby (a související řetězec/cestu) při posuzování, alespoň ve strojově čitelné podobě, toho, zda se o osvědčení podporujícím elektronický podpis tvrdí, že je kvalifikovaným osvědčením, a zda je či není spojené s prostředkem pro bezpečné vytváření podpisu, jímž byl elektronický podpis vytvořen.

Vyplnění polí „Identifikátor typu služby“ („*Service type identifier*“, „Sti“), „Název služby“ („*Service name*“, „Sn“) a „Digitální identita služby“ („*Service digital identity*“, „Sdi“) [4] informacemi uvedenými v poli „Rozšíření informací o službě“ („*Service information extensions*“, „Sie“) umožňuje, aby navrhovaná společná šablona důvěryhodného seznamu plně stanovila zvláštní typ kvalifikovaného osvědčení vydaného ověřovatelem ze seznamu vydávajícím kvalifikovaná osvědčení a aby poskytla informace o skutečnosti, zda je, či není podporováno prostředkem pro bezpečné vytváření podpisu (jestliže tato informace ve vydaném kvalifikovaném osvědčení chybí). S tímto zápisem je samozřejmě spjata určitá informace o „Aktuálním stavu služby“ („*Service current status*“, „Scs“). Toto je znázorněno na obrázku 2 níže.

Zanesení služby do seznamu tím, že se poskytne pouze „Sdi“ (kořenové) certifikační autority, by znamenalo, že je zajištěno (ověřovatelem vydávajícím kvalifikovaná osvědčení, ale také dozorovým/akreditačním subjektem odpovědným za dohled nad tímto ověřovatelem nebo za jeho akreditaci), aby osvědčení jakéhokoli koncového subjektu vydané v rámci této (hierarchie) (kořenové) certifikační autority obsahovalo dostatečné množství ETSI definovaných a strojově zpracovatelných informací pro posouzení toho, zda jde o kvalifikované osvědčení a zda je podporováno prostředkem pro bezpečné vytváření podpisu. Například v případě, kdy tvrzení o podpoře prostředkem pro bezpečné vytváření podpisu není pravdivé (např. v kvalifikovaném osvědčení není uveden strojově zpracovatelný údaj podle normy ETSI o tom, zda je podporováno prostředkem pro bezpečné vytváření podpisu), pak lze ze zápisu na seznam pouze pro „Sdi“ dané (kořenové) certifikační autority vyvodit pouze to, že kvalifikovaná osvědčení vydaná v rámci hierarchie této (kořenové) certifikační autority nejsou podporována žádným prostředkem pro bezpečné vytváření podpisu. Aby mohla být taková kvalifikovaná osvědčení považována za podporovaná prostředkem pro bezpečné vytváření podpisu, měla by být tato skutečnost uvedena v poli „Sie“ (to rovněž znamená, že jsou zaručena ověřovateli vydávajícími kvalifikovaná osvědčení, nad nimiž dozorový subjekt vykonává dohled nebo kteří jsou akreditováni akreditačním subjektem).

[1] ETSI TS 102 231- *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.*
[2] Viz ETSI TS 101 862 - *Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.*
[3] ETSI TS 101 456 - *Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.*
[4] Tj. minimálně osvědčení X.509 v3 vydávající kvalifikované certifikační autority nebo výše postavené certifikační autority.

Obecné zásady – Pravidla pro úpravu– CSP_{QC} zápisy (služby na seznamu)



Obrázek 2:

Zápis o službě u ověřovatele vydávajícího kvalifikovaná osvědčení zapsaného na důvěryhodném seznamu provedeném v podobě TSL Tyto technické specifikace pro společnou šablonu důvěryhodných seznamů umožňují zkombinovat pět hlavních částí informací v zápisu o službě:

— „Identifikátor typu služby" („Sti"), např. identifikace certifikační autority vydávající kvalifikovaná osvědčení („CA/QC");

— „Název služby" („Sn");

— „Digitální identita služby" („Sdi") – informace identifikující službu na seznamu, např. (minimálně) osvědčení X.509v3 certifikační autority vydávající kvalifikovaná osvědčení;

— u služeb CA/QC volitelně „Rozšíření informací o službě" („Sie") – informace umožňující zahrnout sekvenci jedné nebo více n-tic, přičemž každá z nich obsahuje:

  — kritéria, která se mají použít pro další identifikaci (filtrování) v rámci osvědčovací služby identifikované pomocí „Sdi" přesně té služby (tj. souboru kvalifikovaných osvědčení), u níž se požadují/poskytují další informace týkající se údaje o podpoře prostředkem pro bezpečné vytváření podpisu (nebo vydání pro právnickou osobu) a

  — přidružené informace („kvalifikátory") o tom, zda je tento dále identifikovaný soubor služeb kvalifikovaných osvědčení podporován prostředkem pro bezpečné vytváření podpisu, nebo o tom, zda jsou tyto přidružené informace součástí kvalifikovaného osvědčení v rámci standardizované strojově zpracovatelné podoby, a informace týkající se skutečnosti, že jsou taková kvalifikovaná osvědčení vydávána pro právnické osoby (standardně se má za to, že se vydávají pouze pro fyzické osoby).

— „aktuální stav" – informace o tomto zápisu o službě týkající se:

  — toho, zda jde o službu, nad níž je vykonáván dohled, nebo o akreditovanou službu a

  — samotného stavu dohledu/akreditace.

2.3. *Pokyny k úpravě a použití zápisů o službách CSP_{QC}*

Obecné pokyny k úpravě znějí takto:

1. Jestliže je zajištěno (záruku poskytuje CSP_{QC} pod dohledem dozorového subjektu (*Supervisory Body*, dále jen „SB") nebo akreditovaný akreditačním subjektem (*Accreditation Body*, dále jen „AB")), že u služby uvedené na seznamu a identifikované pomocí „Sdi" obsahuje jakékoli kvalifikované osvědčení podporované prostředkem pro bezpečné vytváření podpisu prohlášení QcCompliance definované ETSI a obsahuje prohlášení QcSSCD nebo QCP + identifikátor předmětu (*Object Identifier*, dále jen „OID"), pak je použití vhodného „Sdi" dostačující a pole „Sie" lze využít volitelně a nemusí obsahovat informace o podpoře prostředkem pro bezpečné vytváření podpisu.

2. Jestliže je zajištěno (záruku poskytuje CSP_{QC} pod dohledem SB nebo akreditovaný AB), že u služby uvedené na seznamu a identifikované pomocí „Sdi“ jakékoli kvalifikované osvědčení nepodporované prostředkem pro bezpečné vytváření podpisu obsahuje prohlášení QcCompliance nebo QCP OID a je navrženo tak, aby neobsahovalo prohlášení QcSSCD nebo QCP + OID, pak je použití vhodného „Sdi“ dostačující a pole „Sie“ lze využít volitelně a nemusí obsahovat informace o podpoře prostředkem pro bezpečné vytváření podpisu (což znamená, že není podporováno prostředkem pro bezpečné vytváření podpisu).

3. Jestliže je zajištěno (záruku poskytuje CSP_{QC} pod dohledem SB nebo akreditovaný AB), že u služby uvedené na seznamu a identifikované pomocí „Sdi“ obsahuje kterékoli kvalifikované osvědčení prohlášení QcCompliance a některá z těchto kvalifikovaných osvědčení mají být podporována prostředkem pro bezpečné vytváření podpisu (toto lze rozlišit například různými identifikátory předmětu politiky osvědčení specifickými pro jednotlivé ověřovatele nebo prostřednictvím jiných informací v kvalifikovaném osvědčení specifických pro jednotlivé ověřovatele, přímo či nepřímo, zda jsou strojově zpracovatelná, či nikoli), ale NEOBSAHUJÍ prohlášení QcSSCD ani ETSI QCP (+) OID, pak nemusí být použití vhodného „Sdi“ dostačující A musí být využito pole „Sie“, aby se poskytla výslovná informace o podpoře prostředkem pro bezpečné vytváření podpisu spolu s možným rozšířením informací tak, aby identifikovaly pokrytý soubor osvědčení. To bude pravděpodobně vyžadovat, aby byly při využívání pole „Sie“ zahrnuty pro totéž „Sdi“ různé „hodnoty informací o podpoře prostředkem pro bezpečné vytváření podpisu“.

4. Jestliže je zajištěno (záruku poskytuje CSP_{QC} pod dohledem SB nebo akreditovaný AB), že u služby uvedené na seznamu a identifikované pomocí „Sdi“ žádné kvalifikované osvědčení neobsahuje prohlášení QcCompliance, QCP OID, prohlášení QcSSCD ani QCP + OID, ale je zajištěno, že některá z těchto osvědčení pro koncové subjekty vydaná v rámci tohoto „Sdi“ mají být kvalifikovanými osvědčeními nebo mají být podporována prostředkem pro bezpečné vytváření podpisu (to lze rozlišit například různými identifikátory předmětu politiky osvědčení specifickými pro jednotlivé CSP_{QC} nebo prostřednictvím jiných informací v kvalifikovaném osvědčení specifických pro jednotlivé CSP_{QC}, přímo či nepřímo, zda jsou strojově zpracovatelná, či nikoli), pak použití vhodného „Sdi“ není dostačující A pole „Sie“ musí být využito tak, aby zahrnovalo výslovné informace o podpoře prostředkem pro bezpečné vytváření podpisu. To bude pravděpodobně vyžadovat, aby byly při využívání pole „Sie“ zahrnuty pro totéž „Sdi“ různé „hodnoty informací o podpoře prostředkem pro bezpečné vytváření podpisu“.

Obecnou standardní zásadou je, že pro ověřovatele uvedeného na důvěryhodném seznamu musí být pro typ osvědčovací služby CA/QC uveden jeden zápis o službě na jedno osvědčení X.509v3, tj. certifikační autorita (přímo) vydávající kvalifikovaná osvědčení. Za pečlivě promyšlených okolností a za pečlivě řízených podmínek se může dozorový subjekt /akreditační subjekt členského státu rozhodnout, že se osvědčení X.509v3 kořenové CA nebo CA vyšší úrovně (tj. certifikační autority, která kvalifikovaná osvědčení pro koncové subjekty přímo nevydává, ale osvědčuje hierarchii nižších CA až po CA vydávající kvalifikovaná osvědčení pro koncové subjekty) použije jako „Sdi“ jediného zápisu v seznamu služeb ověřovatele uvedeného na seznamu. Důsledky (výhody a nevýhody) takového použití X.509v3 kořenové CA nebo vyšší CA jako hodnot „Sdi“ v zápisech o službách v důvěryhodném seznamu musí členské státy pečlivě zvážit a schválit. Navíc musí členské státy při použití této povolené výjimky ze standardní zásady poskytnout dokumentaci potřebnou pro usnadnění zřízení a ověření cesty osvědčení.

Pro znázornění obecných pokynů pro úpravu lze podat tento příklad: V kontextu CSP_{QC} využívajícího jednu kořenovou CA, v rámci níž různé CA vydávají kvalifikovaná i nekvalifikovaná osvědčení, ale u nějž kvalifikovaná osvědčení obsahují pouze prohlášení o souladu kvalifikovaného osvědčení a žádný údaj o tom, zda je podporován prostředkem pro bezpečné vytváření podpisu, by uvedení „Sdi“ kořenové CA při uplatnění pravidel vysvětlených výše znamenalo pouze to, že kvalifikované osvědčení vydané v rámci této hierarchie kořenové CA NENÍ podporováno prostředkem pro bezpečné vytváření podpisu. Jestliže tato kvalifikovaná osvědčení ve skutečnosti jsou podporována prostředkem pro bezpečné vytváření podpisu, důrazně se doporučuje využít v budoucích vydaných kvalifikovaných osvědčeních prohlášení QcSSCD. Prozatím (dokud nebude ukončena platnost posledního kvalifikovaného osvědčení, které obsahuje tyto informace) by měl TSL využívat pole „Sie“ a přidružené rozšíření „*Qualifications*“, např. filtrovat osvědčení prostřednictvím specifických OID definovaných CSP_{QC}, které mohou CSP_{QC} využívat k rozlišení různých typů kvalifikovaných osvědčení (některých podporovaných prostředkem pro bezpečné vytváření podpisu), a zahrnout výslovné „Informace o podpoře prostředkem pro bezpečné vytváření podpisu“ („*SSCD support information*“) ohledně osvědčení filtrovaných za použití „Kvalifikátorů“ („*Qualifiers*“).

Obecné pokyny k použití aplikací, služeb nebo produktů elektronického podpisu, které jsou založeny na provedení důvěryhodného seznamu v podobě TSL, znějí takto:

Zápis „CA/QC“ v „Sti“ (obdobně jako zápis CA/QC, který je dále použitím rozšíření „Sie“ *additionalServiceInformation* kvalifikován jako „RootCA/QC“),

— udává, že z CA identifikované „Sdi“ (obdobně uvnitř hierarchie CA počínaje kořenovou CA identifikovanou „Sdi“) jsou všechna vydaná osvědčení pro koncové subjekty kvalifikovanými osvědčeními, **jestliže** jsou za kvalifikovaná vydávána v příslušných prohlášeních QcStatements (tj. QcC, QcSSCD) nebo v ETSI definovaných QCP (+) OID (a to je zajištěno dozorovým/akreditačním subjektem, viz „obecné pokyny k úpravě“ výše)

Poznámka: Není-li v „Sie“ uvedena žádná informace o „kvalifikaci“ nebo pokud osvědčení koncového subjektu vydávané za kvalifikované osvědčení není „dále identifikováno“ prostřednictvím souvisejícího zápisu v „Sie“, pak se informace o „strojovém zpracování“, které jsou obsaženy v kvalifikovaném osvědčení, považují dohledem/akreditací za přesné. To znamená, že u použití (nebo nepoužití) vhodných prohlášení QcStatements (tj. QcC, QcSSCD) nebo ETSI definovaných QCP (+) OID je zajištěno, že jsou v souladu s tím, co tvrdí CSP_{QC}.

— **a JESTLIŽE** je informace o „kvalifikaci“ v „Sie“ přítomna, pak – navíc k výše uvedenému pravidlu výkladu standardního použití – se ta osvědčení, která jsou identifikována použitím tohoto zápisu „kvalifikace“ v „Sie“, který je postaven na zásadě sekvence „filtrů“, jež dále identifikují soubor osvědčení a poskytují další informace o „podpoře prostředkem pro bezpečné vytváření podpisu“ nebo o „právnické osobě jako subjektu“ (např. osvědčení obsahující specifický identifikátor předmětu v rozšíření politiky osvědčení nebo se specifickým vzorcem „použití klíče“ nebo filtrována použitím specifické hodnoty, která se má objevit v jednom specifickém poli nebo rozšíření osvědčení atd.), mají posuzovat podle následujícího souboru „kvalifikátorů“, čímž se vyváží nedostatek informací v příslušném kvalifikovaném osvědčení, tj.:

— o mají uvádět informace o podpoře prostředkem pro bezpečné vytváření podpisu:

  — hodnota kvalifikátoru „QCWithSSCD“ znamená „kvalifikované osvědčení podporované prostředkem pro bezpečné vytváření podpisu“ nebo

  — hodnota kvalifikátoru „QCNoSSCD“ znamená „kvalifikované osvědčení nepodporované prostředkem pro bezpečné vytváření podpisu“ nebo

  — hodnota kvalifikátoru „QCSSCDStatusAsInCert“ znamená, že je zajištěno, aby informace o podpoře prostředkem pro bezpečné vytváření podpisu byla u tohoto zápisu CA/QC obsažena v informacích poskytnutých v „Sdi“ – „Sie“ kvalifikovaného osvědčení;

  NEBO

— o mají uvádět informace o vydání pro právnickou osobu:

  — hodnota kvalifikátoru „QCForLegalPerson“ znamená „osvědčení vydáno právnické osobě“.

2.4. *Služby podporující služby „CA/QC“, které nejsou součástí „Sdi“ „CA/QC“*

Měly by být pokryty též případy, kdy jsou odpovědi CRL a OCSP podepsány klíči, které nepocházejí od CA, jež kvalifikované osvědčení vydala („CA/QC“). To je možno pokrýt uvedením těchto služeb na seznam, jako je provedení důvěryhodného seznamu v podobě TSL (tj. „identifikátor typu služby“ se dále kvalifikuje rozšířením „*additionalServiceInformation*“, které odráží, že je služba OCSP nebo CRL součástí poskytnutí kvalifikovaného osvědčení, např. typ služby „OCSP/QC“ nebo „CRL/QC“), neboť lze tyto služby považovat za součást „kvalifikovaných“ služeb pod dohledem/akreditovaných služeb týkajících se poskytnutí osvědčovacích služeb kvalifikovaného osvědčení. Samozřejmě odpovídající subjekty protokolu OCSP nebo vydavatelé CRL, jejichž osvědčení jsou podepsána CA v rámci hierarchie služeb CA/QC uvedených na seznamu, se mají považovat za „platné“ a v souladu s hodnotou stavu služby CA/QC uvedené na seznamu.

Obdobná ustanovení se mohou vztahovat na osvědčovací služby vydávající nekvalifikovaná osvědčení (typy „CA/PKC“) za použití standardních typů služeb OCSP a CRL podle ETSI TS 102 231.

Je třeba vzít na vědomí, že provedení důvěryhodného seznamu v podobě TSL MUSÍ zahrnovat odvolávací služby, jestliže v poli AIA koncových osvědčení nejsou přítomny příslušné informace nebo jestliže není podepsáno CA uvedenou na seznamu.

2.5. *Směrem k interoperabilnímu profilu kvalifikovaného osvědčení*

Obecným pravidlem je, že je nutno usilovat o co největší zjednodušení (snížení počtu) zápisů o službách (různá „Sdi“). To však musí být v rovnováze se správnou identifikací služeb, které souvisejí s vydáváním kvalifikovaných osvědčení a poskytováním důvěryhodné informace o tom, zda jsou tato kvalifikovaná osvědčení podporována prostředkem pro bezpečné vytváření podpisu, pokud taková informace ve vydaném kvalifikovaném osvědčení chybí.

V ideálním případě by se použití pole „Sie“ a rozšíření „kvalifikace“ mělo (přísně) omezit na ty specifické případy, které musí být takto řešeny, neboť kvalifikovaná osvědčení by měla obsahovat dostatečné informace ohledně údajného stavu kvalifikace a podpory prostředkem pro bezpečné vytváření podpisu.

Členské státy by v nejvyšší možné míře měly prosazovat přijetí a používání interoperabilních profilů kvalifikovaných osvědčení.

3. **Uspořádání společné šablony důvěryhodného seznamu**

Navrhovaná společná šablona důvěryhodného seznamu členského státu bude uspořádána do těchto kategorií informací:

1. informace o důvěryhodném seznamu a systému jeho vydávání;

2. sekvence polí s jednoznačnými informacemi pro identifikaci o každém ověřovateli v rámci systému, nad nímž je vykonáván dohled nebo který je akreditován (tato sekvence polí je volitelná, tj. pokud se nepoužije, bude seznam považován za prázdný, což znamená, že v přidruženém členském státě v souvislosti s působností důvěryhodného seznamu není žádný ověřovatel, nad nímž by byl vykonáván dohled nebo který by byl akreditován);

3. u každého ověřovatele na seznamu sekvence polí s jednoznačnou identifikací osvědčovací služby poskytované ověřovatelem, nad níž je vykonáván dohled nebo která je akreditována (v této sekvenci musí být uveden minimálně jeden zápis);

4. u každé osvědčovací služby na seznamu, nad níž je vykonáván dohled nebo která je akreditována, identifikace aktuálního stavu služby a jeho historie.

Pokud jde o ověřovatele vydávajícího kvalifikovaná osvědčení, musí jednoznačná identifikace osvědčovací služby, která má být uvedena na seznam a nad níž je vykonáván dohled nebo která je akreditována, zohlednit situace, kdy v kvalifikovaném osvědčení není k dispozici dostatek informací o jeho „kvalifikovaném" stavu, jeho případné podpoře prostředkem pro bezpečné vytváření podpisu, a zejména s cílem přizpůsobit se skutečnosti, že většina (obchodních) ověřovatelů používá jedinou vydávající kvalifikovanou CA pro vydávání několika typů osvědčení pro koncové subjekty, a to kvalifikovaných i nekvalifikovaných.

Počet zápisů v seznamu na uznaného ověřovatele by bylo možno snížit tam, kde existují služby vyšší CA, např. v kontextu obchodní hierarchie CA od kořenové CA až k vydávajícím CA. I v těchto případech však musí být zachována a zajištěna zásada zajištění jednoznačné vazby mezi osvědčovací službou CSP_{QC} a souborem osvědčení, která mají být identifikována jako kvalifikovaná.

1. *Informace o důvěryhodném seznamu a systému jeho vydávání*

Součástí této kategorie jsou tyto informace:

— **značka** (tag) důvěryhodného seznamu usnadňující identifikaci důvěryhodného seznamu při elektronickém vyhledávání a v podobě čitelné okem také pro potvrzení jeho účelu;

— **formát a identifikátor verze formátu** důvěryhodného seznamu;

— **číslo sekvence (nebo vydání)** důvěryhodného seznamu;

— **informace o typu** důvěryhodného seznamu (např. pro identifikaci skutečnosti, že tento důvěryhodný seznam poskytuje informace o stavu dohledu/akreditace osvědčovacích služeb ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni z hlediska souladu s ustanoveními směrnice 1999/93/ES členským státem, na nějž se odkazuje);

— **informace o vlastnictví** důvěryhodného seznamu (např. název, adresa, kontaktní informace atd. subjektu členského státu, který odpovídá za zřízení, bezpečné zveřejnění a údržbu důvěryhodného seznamu);

— **informace o souvisejících systémech dohledu/akreditace**, k nimž jsou důvěryhodné seznamy přidruženy, mimo jiné:

  — o zemi, na niž se vztahují,

  — o informacích o umístění informací ohledně systémů (modely systémů, pravidla, kritéria, příslušné společenství, typ atd.) nebo o odkazech na taková umístění,

  — o době uchovávání (historických) informací.

— **o politice nebo právním upozornění, závazcích a odpovědnosti** důvěryhodných seznamů;

— **datum a čas vydání** důvěryhodného seznamu a **příští plánované aktualizace**.

2. *Jednoznačné informace pro identifikaci o každém ověřovateli uznaném systémem*

Tento soubor informací bude zahrnovat přinejmenším toto:

— název organizace ověřovatele tak, jak je užit v úřední zákonné registraci (v závislosti na praxi jednotlivých členských států může zahrnovat UID organizace ověřovatele);

— adresu a kontaktní informace ověřovatele;

— další informace o ověřovateli, ať již zahrnuté přímo nebo odkazem na umístění, odkud lze takové informace stáhnout.

3. *U každého ověřovatele na seznamu sekvenci polí s jednoznačnou identifikací osvědčovací služby poskytované ověřovatelem, nad níž je vykonáván dohled nebo která je akreditována z hlediska směrnice 1999/93/ES*

Tento soubor informací bude zahrnovat u každé osvědčovací služby ověřovatele na seznamu přinejmenším toto:

— identifikátor typu osvědčovací služby (např. identifikátor toho, že osvědčovací službou ověřovatele, nad níž je vykonáván dohled nebo která je akreditována, je certifikační autorita vydávající kvalifikovaná osvědčení);

— (obchodní) název této osvědčovací služby;

— jednoznačný jedinečný identifikátor osvědčovací služby;

— další informace o osvědčovací službě (např. zahrnuté přímo či odkazem na umístění, odkud lze takové informace stáhnout, informace o přístupu týkající se služby);

— u služeb CA/QC volitelně sekvenci n-tic informací, přičemž každá n-tice poskytuje:

i. kritéria, která se mají použít pro další identifikaci (filtrování) v rámci osvědčovací služby identifikované pomocí „Sdi" přesně té služby (tj. souboru kvalifikovaných osvědčení), u níž se požadují/poskytují další informace týkající se údaje o podpoře prostředkem pro bezpečné vytváření podpisu (nebo vydání pro právnickou osobu) a

ii. přidružené „kvalifikátory" poskytující informace o tom, zda je takto dále identifikovaný soubor kvalifikovaných osvědčení podporován prostředkem pro bezpečné vytváření podpisu, nebo o tom, zda jsou taková kvalifikovaná osvědčení vydávána pro právnické osoby (standardně se má za to, že se vydávají pouze pro fyzické osoby).

5. *U každé osvědčovací služby na seznamu identifikace aktuálního stavu služby a jeho historie*

Tento soubor informací bude zahrnovat přinejmenším toto:

— identifikátor aktuálního stavu

— datum a čas začátku aktuálního stavu

— historické informace o tomto stavu.

4. **Definice a zkratky**

Pro účely tohoto dokumentu se použijí tyto definice a zkratky:

Výraz	Zkratka	Definice
Ověřovatel	CSP	Jak je definováno v čl. 2 odst. 11 směrnice 1999/93/ES.
Certifikační autorita	CA	CA je ověřovatelem a může k vydávání osvědčení pro koncové subjekty používat několik technických soukromých podpisových klíčů CA, ke každému z nichž je přidruženo osvědčení. CA je orgánem, který je důvěryhodný pro jednoho nebo více uživatelů pro tvorbu a přidělování osvědčení. Volitelně také CA může vytvářet uživatelské klíče [ETSI TS 102 042]. CA se považuje za identifikovanou prostřednictvím identifikačních informací přítomných v poli Vydavatel osvědčení CA souvisejícího (osvědčujícího) veřejného klíče spojeného se soukromým podepisovacím klíčem CA, který může CA použít k vydání osvědčení pro subjekty. CA může mít několik podepisovacích klíčů. Každý podepisovací klíč je jedinečně identifikován jedinečným identifikátorem, který tvoří součást pole Identifikátor klíče autority v osvědčení CA.
Certifikační autorita vydávající kvalifikovaná osvědčení	CA/QC	CA, která splňuje požadavky stanovené v příloze II směrnice 1999/93/ES a vydává kvalifikovaná osvědčení, která splňují požadavky stanovené v příloze I směrnice 1999/93/ES.
Osvědčení	Osvědčení	Jak je definováno v čl. 2 odst. 9 směrnice 1999/93/ES.
Kvalifikované osvědčení	QC	Jak je definováno v čl. 2 odst. 10 směrnice 1999/93/ES.
Podepisující osoba	Podepisující osoba	Jak je definováno v čl. 2 odst. 3 směrnice 1999/93/ES.

Výraz	Zkratka	Definice
Dohled	Dohled	Výraz „dohled“ se používá ve smyslu směrnice 1999/93/ES (čl. 3 odst. 3). Směrnice po členských státech vyžaduje, aby zavedly odpovídající systém, který umožní dohled nad ověřovateli, kteří jsou usazeni na jeho území a kteří vydávají kvalifikovaná osvědčení pro veřejnost, čímž zajistí dohled nad souladem s ustanoveními směrnice.
Dobrovolná akreditace	Akreditace	Jak je definováno v čl. 2 odst. 13 směrnice 1999/93/ES.
Důvěryhodný seznam	TL	Označuje seznam, v němž je uveden stav dohledu/akreditace osvědčovacích služeb ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni odkazovaným členským státem z hlediska souladu s ustanoveními směrnice 1999/93/ES.
Seznam stavu důvěryhodných služeb	TSL	Podepsaný seznam používaný jako základ pro prezentaci informací o stavu důvěryhodných služeb podle specifikací stanovených v ETSI TS 102 231.
Důvěryhodná služba		Služba, která posiluje důvěryhodnost a jistotu v elektronických transakcích (obvykle – nikoli však výhradně – za použití šifrovacích technik nebo za pomoci důvěrných materiálů) (ETSI TS 102 231).
Poskytovatel důvěryhodné služby	TSP	Subjekt provozující jednu nebo více (elektronických) důvěryhodných služeb (tento termín má širší použití než CSP).
Token důvěryhodné služby	TrST	Fyzický nebo binární (logický) objekt vygenerovaný nebo vydaný jako výsledek použití důvěryhodné služby. Příklady binárních TrST jsou osvědčení, CRL, tokeny časových razítek a odpovědi OCSP.
Kvalifikovaný elektronický podpis	QES	AdES podporovaný QC, který je vytvořen SSCD, jak je definováno v článku 2 směrnice 1999/93/ES.
Zaručený elektronický podpis	AdES	Jak je definováno v čl. 2 odst. 2 směrnice 1999/93/ES.
Zaručený elektronický podpis podporovaný kvalifikovaným osvědčením	$AdES_{QC}$	Značí elektronický podpis, který splňuje požadavky na AdES a je podporován QC, jak je definováno v článku 2 směrnice 1999/93/ES.
Prostředek pro bezpečné vytváření podpisu	SSCD	Jak je definováno v čl. 2 odst. 6 směrnice 1999/93/ES.

KAPITOLA I

PODROBNÉ SPECIFIKACE PRO SPOLEČNOU ŠABLONU „DŮVĚRYHODNÉHO SEZNAMU OVĚŘOVATELŮ, NAD KTERÝMI JE VYKONÁVÁN DOHLED NEBO KTEŘÍ JSOU AKREDITOVÁNI“

V následující části tohoto dokumentu se výrazy „MUSÍ“, „NESMÍ“, „POVINNÝ“ „MĚL BY“, „NEMĚL BY“, „MŮŽE“ a „VOLITELNÝ“ mají vykládat v souladu s RFC 2119 [1].

Tyto specifikace se zakládají na specifikacích a požadavcích uvedených v ETSI TS 102 231 v3.1.1 (2009-06). Není-li v těchto specifikacích uveden žádný specifický požadavek, MUSÍ se plně uplatnit požadavky ETSI TS 102 231. Jsou-li v těchto specifikacích uvedeny specifické požadavky, pak MUSÍ mít přednost před odpovídajícími požadavky ETSI TS 102 231, ačkoli jsou vyplněny specifikacemi ohledně formátu specifikovanými v ETSI TS 102 231. V případě nesrovnalostí mezi těmito specifikacemi a specifikacemi ETSI TS 102 231 jsou normativní tyto specifikace.

Jazyková podpora MUSÍ být provedena a poskytnuta alespoň v angličtině (EN) a dodatečně volitelně též v jednom či více národních jazycích.

Datum-čas MUSÍ uvádět v souladu s bodem 5.1.4 ETSI TS 102 231.

URI se MUSÍ použít v souladu s bodem 5.1.5 ETSI TS 102 231.

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

Informace o systému vydávání důvěryhodného seznamu

Tag

TSL tag (bod 5.2.1)

Toto pole je POVINNÉ a MUSÍ být v souladu s bodem 5.2.1 ETSI TS 102 231.

V souvislosti s prováděním XML zpřístupnil ETSI soubor xsd, který je v aktuálním stavu uveden v příloze 1.

Scheme Information

TSL version identifier (bod 5.3.1)

Toto pole je POVINNÉ a MUSÍ být nastaveno na „3“ (celé číslo).

TSL sequence number (bod 5.3.2)

Toto pole je POVINNÉ. Specifikuje pořadové číslo TSL. Tato celočíselná hodnota začíná číslem „1“ při prvním vydání TSL a při každém následujícím vydání se zvyšuje o 1. Při zvýšení hodnoty výše uvedeného tagu „*TSL version identifier*“ nesmí být číslo „1“ znovu použito.

TSL type (bod 5.3.3)

Toto pole specifikuje typ TSL a je POVINNÉ. MUSÍ být nastaveno na http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLtype/generic (obecný).

Poznámka 1: Aby byl dodržen soulad s bodem 5.3.3 ETSI TS 102 231 a aby se uvedl specifický typ TSL a zároveň se odkázalo na existenci těchto specifikací upravujících zřízení provedení důvěryhodného seznamu členských států ([1]) v podobě TSL a umožnilo se, aby syntaktický analyzátor stanovil, jakou podobu následujících polí ([2]) lze očekávat, pokud mají tato pole specifický (nebo variantní) význam podle typu TSL, který zastupují (v tomto případě jde o důvěryhodný seznam členského státu), MUSÍ být výše specifikovaný URI zaznamenán a popsán takto:

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

Popis: Provedení v podobě TSL seznamu stavů dohledu/akreditace osvědčovacích služeb ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni odkazovaným členským státem odpovědným za provedení v podobě TSL z hlediska souladu s příslušnými ustanoveními směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy, a to prostřednictvím přímého dozoru (ať již dobrovolného nebo povinného).

Scheme operator name (bod 5.3.4)

Toto pole je POVINNÉ. Specifikuje název subjektu členského státu odpovědného za zřízení, zveřejnění a údržbu vnitrostátního důvěryhodného seznamu. Specifikuje úřední název, pod nímž přidružená právnická osoba nebo pověřená osoba (např. u úřadů státní správy) přidružená k tomuto subjektu působí. MUSÍ jít o název uvedený v úřední zákonné registraci nebo povolení, jemuž mají být adresována veškerá úřední sdělení. Jde o sekvenci vícejazyčných řetězců znaků, který bude povinně proveden v angličtině (EN) a volitelně v jednom či více národních jazycích.

Poznámka: Země MŮŽE mít odlišné subjekty pro dohled a pro akreditaci, a dokonce i další subjekty pro jakékoli související provozní činnosti. Je na každém členské státě, aby pověřil provozovatele systému provedení TL členského státu v podobě TSL. Očekává se, že dozorový subjekt, akreditační subjekt a provozovatel systému (pokud jde o samostatné subjekty) budou mít každý své vlastní povinnosti a závazky.

([1]) Tj. „seznam stavu dohledu/akreditace osvědčovacích služeb ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni odkazovaným členským státem z hlediska souladu s ustanoveními směrnice 1999/93/ES“ (zkráceně „důvěryhodný seznam“).

([2]) To znamená pole specifikovaná ETSI TS 102 231- *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information* a „profilovaná“ těmito specifikacemi tak, aby se specifikovalo zřízení důvěryhodného seznamu členského státu.

Jestliže za dohled, akreditaci nebo provozní hlediska odpovídají různé subjekty, MUSÍ to být jasně vyjádřeno a uvedeno v informacích o systému jako součást TL, včetně informací specifických pro systém uvedených v „*Scheme information URI*“ (bod 5.3.7).

Očekává se, že jmenovaný provozovatel systému podepisuje TSL (bod 5.3.4).

Scheme operator address (bod 5.3.5)

Toto pole je POVINNÉ. Specifikuje se v něm adresa právnické osoby nebo pověřené organizace uvedené v poli „*Scheme operator name*“ (bod 5.3.4) pro poštovní i elektronickou komunikaci. Zahrnuje jak „*PostalAddress*“ (tj. ulici, obec, [stát nebo provincii], [poštovní směrovací číslo] a kód země ve formátu ISO 3166-1 alpha-2) v souladu s bodem 5.3.5.1, tak „*ElectronicAddress*“ (tj. e-mail nebo URI internetové stránky) v souladu s bodem 5.3.5.2.

Scheme name (bod 5.3.6)

Toto pole je povinné a specifikuje název, pod nímž systém působí. Jde o sekvenci vícejazyčných řetězců znaků (s povinným jazykem EN a volitelně s jedním či více národními jazyky) definovaný takto:

— EN verze je řetězec znaků uspořádaný takto:

CC:EN_název_hodnota

kde

— „CC“ = kód země ve formátu ISO 3166-1 alpha-2 použitý v poli „*Scheme territory*“ (bod 5.3.10);

— „:“ = je použita jako oddělovací znak;

— „EN_název_hodnota“ = „seznam stavu dohledu/akreditace osvědčovacích služeb ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni odkazovaným členským státem z hlediska souladu s příslušnými ustanoveními směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy“.

— Jakákoli jazyková verze členského státu MUSÍ být řetězcem znaků s tímto uspořádáním:

CC:název_hodnota

kde

— „CC“ = kód země ve formátu ISO 3166-1 alpha-2 použitý v poli „*Scheme territory*“ (bod 5.3.10);

— „:“ = je použita jako oddělovací znak;

— „název_hodnota“ = úřední překlad výše uvedeného „EN_název_hodnota“ do národního jazyka.

Název systému se požaduje výhradně pro identifikaci systému, na nějž odkazuje „*Scheme information URI*“, prostřednictvím názvu, a také aby se zajistilo, aby v případě, kdy provozovatel systému provozuje více než jeden systém, měl každý z těchto systémů jiný název.

Členské státy a provozovatelé systémů zajistí, aby v případě, že členský stát nebo provozovatel systému provozují více než jeden systém, měl každý z těchto systémů jiný název.

Scheme information URI (bod 5.3.7)

Toto pole je povinné a specifikuje URI, kde mohou uživatelé (strany spoléhající se na osvědčení) získat informace specifické pro daný systém (povinně EN a volitelně jeden či více národních jazyků). Jde o sekvenci vícejazyčných ukazatelů (s povinným jazykem EN a volitelně s jedním či více národními jazyky). Odkazovaná adresa URI MUSÍ poskytnout cestu k informacím popisujícím „vhodné informace o systému“.

„Vhodné informace o systému“ MUSÍ zahrnovat přinejmenším:

— Všeobecné úvodní informace, které jsou společné pro všechny členské státy, týkající se rozsahu působnosti a kontextu důvěryhodného seznamu a souvisejících systémů dohledu/akreditace. Použitý společný text má znít takto:

Tento seznam je provedením „Důvěryhodného seznamu ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni“ [*název příslušného členského státu*] v podobě TSL, v němž se poskytují informace o stavu dohledu/akreditace osvědčovacích služeb ověřovatelů (CSP), nad nimiž vykonává [*název příslušného členského státu*] dohled nebo kteří jsou jím/jí akreditováni z hlediska souladu s příslušnými ustanoveními směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.

Cílem důvěryhodného seznamu je:

— poskytnout seznam stavu dohledu nebo akreditace osvědčovacích služeb ověřovatelů, nad nimiž z hlediska souladu s příslušnými ustanoveními směrnice 1999/93/ES vykonává dohled nebo jež akredituje [*název příslušného členského státu*], a poskytnout o tomto stavu spolehlivé informace;

— umožnit validaci elektronických podpisů podporovaných osvědčovacími službami uvedenými na seznamu, nad nimiž je vykonáván dohled nebo které jsou akreditovány, ověřovatelů uvedených na seznamu.

Důvěryhodný seznam členského státu poskytuje přinejmenším informace o ověřovatelích, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni a kteří vydávají kvalifikovaná osvědčení v souladu s ustanoveními směrnice 1999/93/ES (čl. 3 odst. 2 a 3, čl. 7 odst. 1 písm. a)), včetně informací o kvalifikovaných osvědčeních podporujících elektronický podpis a o tom, zda je podpis vytvořen prostředkem pro bezpečné vytváření podpisu či nikoli.

Ověřovatel vydávající kvalifikovaná osvědčení uvedený na tomto seznamu je pod dohledem [*název příslušného členského státu*] a může být akreditován z hlediska souladu s ustanoveními směrnice 1999/93/ES, včetně požadavků přílohy I (požadavky na QC) a přílohy II (požadavky na ověřovatele vydávající kvalifikovaná osvědčení). Je definován příslušný systém „dohledu“ (resp. systém „dobrovolné akreditace“), který musí splňovat příslušné požadavky směrnice 1999/93/ES, zejména čl. 3 odst. 3, čl. 8 odst. 1, článku 11 (resp. čl. 2 odst. 13, čl. 3 odst. 2, čl. 7 odst. 1 písm. a), čl. 8 odst. 1, článku 11).

Dodatečné informace o dalších ověřovatelích, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni a kteří nevydávají kvalifikovaná osvědčení, ale poskytují služby související s elektronickými podpisy (např. ověřovatelé poskytující služby časových razítek a vydávající tokeny časových razítek, ověřovatelé vydávající nekvalifikovaná osvědčení atd.), jsou do tohoto provedení v podobě TSL zařazeni dobrovolně na vnitrostátní úrovni.

— Specifické informace o souvisejících systémech dohledu/akreditace, zejména tyto [1]:

— informace o systému dohledu vztahujícím se na jakéhokoli CSP_{QC};

— ve vhodných případech informace o vnitrostátním systému dobrovolné akreditace vztahujícím se na jakéhokoli CSP_{QC};

— ve vhodných případech informace o systému dohledu vztahujícím se na jakéhokoli ověřovatele nevydávajícího kvalifikovaná osvědčení;

— ve vhodných případech informace o vnitrostátním systému dobrovolné akreditace vztahujícím se na jakéhokoli ověřovatele nevydávajícího kvalifikovaná osvědčení.

— Tyto specifické informace MUSÍ u každého souvisejícího systému uvedeného výše zahrnovat přinejmenším:

— obecný popis;

— informace o postupech dozorového/akreditačního subjektu při dohledu nad ověřovateli nebo při jejich akreditaci a ověřovatelů při dohledu/akreditaci;

— informace o kritériích, podle nichž je nad ověřovateli vykonáván dohled nebo podle nichž jsou akreditováni.

— Ve vhodných případech specifické informace o specifických „kvalifikacích“, na něž mohou mít některé fyzické nebo binární (logické) objekty vytvořené nebo vydané v důsledku poskytnutí osvědčovací služby nárok na základě svého souladu s ustanoveními a požadavky stanovenými na vnitrostátní úrovni, včetně významu takových „kvalifikací“ a souvisejících vnitrostátních ustanovení a požadavků.

[1] Dva poslední soubory informací jsou životně důležité pro to, aby mohly strany spoléhající se na osvědčení posoudit úroveň kvality a bezpečnosti systémů dohledu/akreditace. Tyto soubory informací se poskytnou na úrovni důvěryhodného seznamu prostřednictvím „*Scheme information URI*“ (bod 5.3.7 – informace poskytované členským státem), „*Scheme type/community/rules*“ (bod 5.3.9 – prostřednictvím textu společného pro všechny členské státy) a „*TSL policy/legal notice*“ (bod 5.3.11 – text společný pro všechny členské státy související se směrnicí 1999/93/ES, společně s možností, aby členský stát doplnil svůj specifický text/odkazy). Další informace o vnitrostátních systémech dohledu/akreditace pro ověřovatele nevydávající kvalifikovaná osvědčení lze ve vhodných a požadovaných případech poskytnout na úrovni služby (např. pro odlišení různých úrovní kvality/bezpečnosti) prostřednictvím použití rozšíření „*Scheme service definition URI*“ (bod 5.5.6).

Členské státy MOHOU dále o systémech dobrovolně poskytnout dodatečné specifické informace. Ty zahrnují:

— informace o kritériích a pravidlech použitých pro výběr osob vykonávajících dohled/audit a definování toho, jak nad ověřovateli vykonávají dohled (kontrolu) nebo jak u nich provádějí akreditaci (audit);

— jiné kontaktní a obecné informace, které se vztahují k fungování systému.

Status determination approach (bod 5.3.8)

Toto pole je povinné a specifikuje identifikátor přístupu ke stanovení stavu. Použije se tento specifický URI, tak jak je zaznamenán a popsán zde:

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

Popis: U služeb uvedených na seznamu stanovuje jejich stav provozovatel systému sám nebo v zastoupení v rámci vhodného systému pro odkazovaný členský stát, který umožňuje „dohled" (a ve vhodných případech „dobrovolnou akreditaci") u ověřovatelů, kteří jsou usazeni na jeho území (nebo ve třetí zemi v případě „dobrovolné akreditace") a kteří vydávají kvalifikovaná osvědčení pro veřejnost podle čl. 3 odst. 3 (resp. čl. 3 odst. 2 nebo čl. 7 odst. 1 písm. a)) směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy, a ve vhodných případech umožňuje dohled nebo akreditaci u ověřovatelů, kteří nevydávají kvalifikovaná osvědčení, v souladu s vnitrostátně definovanými a zřízenými „uznanými systémy schválení" provedenými na vnitrostátní úrovni pro dohled nad souladem služeb ověřovatelů nevydávajících kvalifikovaná osvědčení s ustanoveními směrnice 1999/93/ES a případně s rozšířenými vnitrostátními ustanoveními týkajícími se takových osvědčovacích služeb.

Scheme type/community/rules (bod 5.3.9)

Toto pole je povinné a obsahuje přinejmenším tyto zapsané URI:

— URI společný pro všechny důvěryhodné seznamy členských států a vedoucí k popisnému textu, který se vztahuje na všechny důvěryhodné seznamy:

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

  — který poukazuje na systém členského státu (identifikovaný prostřednictvím „*TSL type*" (bod 5.3.3) a „*Scheme name*" (bod 5.3.6)) v systému systémů (tj. ukazatelů seznamů TSL všech členských států, které zveřejňují a udržují důvěryhodný seznam v podobě TSL);

  — kde mohou uživatelé získat politiky/pravidla pro posouzení služeb uvedených na seznamu a kde lze stanovit typ TSL (viz bod 5.3.3);

  — kde mohou uživatelé získat návod k použití a výkladu obsahu důvěryhodného seznamu provedeného TSL. Tato pravidla použití jsou společná pro všechny důvěryhodné seznamy členských států, nezávisle na typu služby uvedené na seznamu a na systémech dohledu/akreditace.

  Popisný text:

  „**Účast v systému**

  Každý členský stát musí vytvořit „Důvěryhodný seznam ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni", v němž se poskytují informace o stavu dohledu/akreditace osvědčovacích služeb ověřovatelů (CSP), nad nimiž vykonává příslušný členský stát dohled nebo kteří jsou jím akreditováni z hlediska souladu s příslušnými ustanoveními směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.

  Na tento důvěryhodný seznam v podobě TSL se také odkazuje v seznamu odkazů (ukazatelů) na provedení důvěryhodných seznamů jednotlivých členských států v podobě TSL vypracovaném Komisí.

  Politiky/pravidla pro posuzování služeb uvedených na seznamu

  Důvěryhodný seznam členského státu musí poskytovat minimální informace o ověřovatelích, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni a kteří vydávají kvalifikovaná osvědčení v souladu s ustanoveními směrnice 1999/93/ES (čl. 3 odst. 2 a 3, čl. 7 odst. 1 písm. a)), včetně informací o kvalifikovaných osvědčeních podporujících elektronický podpis a o tom, zda je podpis vytvořen prostředkem pro bezpečné vytváření podpisu, či nikoli.

Nad ověřovateli vydávajícími kvalifikovaná osvědčení musí vykonávat dohled členský stát, v němž jsou usazeni (pokud jsou usazeni v členském státě), a mohou být také akreditováni z hlediska souladu s ustanoveními směrnice 1999/93/ES, včetně požadavků přílohy I (požadavky na kvalifikovaná osvědčení) a přílohy II (požadavky pro ověřovatele vydávající kvalifikovaná osvědčení). Ověřovatelé vydávající kvalifikovaná osvědčení, kteří jsou akreditováni v členském státě, musí podléhat také vhodnému systému dohledu tohoto členského státu, ledaže by v něm nebyli usazeni. Je definován příslušný systém „dohledu“ (resp. systém „dobrovolné akreditace“), který musí splňovat příslušné požadavky směrnice 1999/93/ES, zejména čl. 3 odst. 3, čl. 8 odst. 1, článku 11 (resp. čl. 2 odst. 13, čl. 3 odst. 2, čl. 7 odst. 1 písm. a), čl. 8 odst. 1, článku 11).

Dodatečné informace o dalších ověřovatelích, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni a kteří nevydávají kvalifikovaná osvědčení, ale poskytují služby související s elektronickými podpisy (např. ověřovatelé poskytující služby časových razítek a vydávající tokeny časových razítek, ověřovatelé vydávající nekvalifikovaná osvědčení atd.), mohou být do tohoto provedení v podobě TSL zařazeni dobrovolně na vnitrostátní úrovni.

Ověřovatelé, kteří nevydávají kvalifikovaná osvědčení, ale poskytují související služby, mohou spadat do systému „dobrovolné akreditace“ (jak je definován ve směrnici 1999/93/ES a v souladu s ní) nebo do „uznaného systému schválení“ definovaného a prováděného na vnitrostátní úrovni pro dohled nad souladem s ustanoveními směrnice 1999/93/ES a případně též s vnitrostátními ustanoveními souvisejícími s poskytováním osvědčovacích služeb (ve smyslu čl. 2 odst. 11 směrnice). Některé fyzické nebo binární (logické) objekty vytvořené nebo vydané v důsledku poskytnutí osvědčovací služby mohou mít nárok na získání zvláštní „kvalifikace“ na základě svého souladu s ustanoveními a požadavky stanovenými na vnitrostátní úrovni, význam takových „kvalifikací“ však bude pravděpodobně omezen pouze na vnitrostátní úroveň.

Výklad důvěryhodného seznamu v podobě TSL

Obecné pokyny pro uživatele aplikací, služeb nebo produktů elektronického podpisu, které jsou založeny na důvěryhodném seznamu v podobě TSL podle přílohy rozhodnutí Komise [odkaz na toto rozhodnutí], znějí takto:

Zápis „CA/QC“ v „Identifikátoru typu služby“ („Sti“) (obdobně jako zápis CA/QC, který je dále použitím rozšíření „Rozšíření informací o službě“ („Sie“) *additionalServiceInformation* kvalifikován jako „RootCA/QC“

— udává, že z CA identifikované „Digitální identitou služby“ („Sdi“) (obdobně uvnitř hierarchie CA počínaje kořenovou CA identifikovanou „Sdi“) od příslušného ověřovatele (viz přidružená pole informací TSP) jsou všechna vydaná osvědčení pro koncové subjekty kvalifikovanými osvědčeními (QC), **jestliže** jsou za kvalifikovaná vydávána v příslušných prohlášeních QcStatements (tj. QcC, QcSSCD) definovaných ETSI TS 101 862 nebo QCP (+) OID definovaných ETSI TS 101 456 (a toto je zaručeno vydávajícím ověřovatelem a zajištěno dozorovým/akreditačním subjektem)

Poznámka: Není-li v „Sie“ uvedena žádná informace o „kvalifikaci“ nebo pokud osvědčení koncového subjektu vydávané za kvalifikované osvědčení není „dále identifikováno“ prostřednictvím souvisejícího zápisu v „Sie“, pak se informace o „strojovém zpracování“, které jsou obsaženy v kvalifikovaném osvědčení, považují dohledem/akreditací za přesné. To znamená, že u použití (nebo nepoužití) vhodných prohlášení QcStatements (tj. QcC, QcSSCD) nebo ETSI definovaných QCP (+) OID je zajištěno, že jsou v souladu s tím, co tvrdí CSP_{QC}.

— **a JESTLIŽE** je informace o „kvalifikaci“ v „Sie“ přítomna, pak – navíc k výše uvedenému pravidlu výkladu standardního použití – se ta osvědčení, která jsou identifikována použitím tohoto zápisu „kvalifikace“ v „Sie“, který je postaven na zásadě sekvence „filtrů“, jež dále identifikují soubor osvědčení, musí posuzovat podle přidružených „kvalifikátorů“ poskytujících další informace o „podpoře prostředkem pro bezpečné vytváření podpisu“ nebo o „právnické osobě jako subjektu“ (např. osvědčení obsahující specifický identifikátor předmětu v rozšíření politiky osvědčení nebo se specifickým vzorcem „použití klíče“ nebo filtrována použitím specifické hodnoty, která se má objevit v jednom specifickém poli nebo rozšíření osvědčení atd.). Tyto kvalifikátory tvoří součást následujícího souboru „kvalifikátorů“ využívaných k vyvážení nedostatku informací v příslušném obsahu kvalifikovaného osvědčení, které se využívají:

  — k uvedení informace o podpoře prostředkem pro bezpečné vytváření podpisu:

    — hodnota kvalifikátoru „QCWithSSCD“ znamená „kvalifikované osvědčení podporované prostředkem pro bezpečné vytváření podpisu“ nebo

    — hodnota kvalifikátoru „QCNoSSCD“ znamená „kvalifikované osvědčení nepodporované prostředkem pro bezpečné vytváření podpisu“ nebo

    — hodnota kvalifikátoru „QCSSCDStatusAsInCert“ znamená, že je zajištěno, aby informace o podpoře prostředkem pro bezpečné vytváření podpisu byla u tohoto zápisu CA/QC obsažena v informacích poskytnutých v „Sdi“ – „Sie“ kvalifikovaného osvědčení;

  NEBO

  — k uvedení informace o vydání právnické osobě:

    — hodnota kvalifikátoru „QCForLegalPerson“ znamená „osvědčení vydáno právnické osobě“.

Obecné pravidlo výkladu pro jakýkoli jiný typ zápisu „Sti“ zní, že služba uvedená na seznamu pojmenovaná podle hodnoty pole „Sn“ a jedinečně identifikovaná hodnotou pole „Sdi“ má aktuální stav dohledu/akreditace podle hodnoty pole „Scs“ od data uvedeného v „Datum a čas začátku aktuálního stavu služby“. Specifická pravidla výkladu pro jakékoli další informace týkající se služby uvedené na seznamu (např. pole „Rozšíření informací o službě“) lze v případě potřeby nalézt na specifické URI členského státu jako součást tohoto pole „Typ/společenství/pravidla systému“.

Pro další podrobnosti ohledně polí, popisu a významu provedení důvěryhodných seznamů členských států v podobě TSL se prosím obracejte na technické specifikace společné šablony „Důvěryhodného seznamu ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni“ v příloze rozhodnutí Komise [odkaz na toto rozhodnutí].“

— URI specifický pro každý důvěryhodný seznam členského státu a vedoucí k popisnému textu, který se vztahuje na důvěryhodný seznam tohoto členského státu:

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

kdy „CC“ = kód země ve formátu ISO 3166-1 alpha-2 použitý v poli „*Scheme territory*“ (bod 5.3.10)

— kde mohou uživatelé získat specifické politiky/pravidla odkazovaného členského státu, podle nichž jsou služby uvedené na seznamu posuzovány z hlediska souladu s příslušným systémem dohledu a systémy dobrovolné akreditace;

— kde mohou uživatelé získat specifický popis odkazovaného členského státu toho, jak používat a vykládat obsah provedení důvěryhodného seznamu v podobě TSL s ohledem na osvědčovací služby, které nesouvisejí s vydáváním kvalifikovaných osvědčení. Lze jej využít k poukázání na možnou nesourodost mezi vnitrostátními systémy dohledu/akreditace souvisejícími s ověřovateli nevydávajícími kvalifikovaná osvědčení a tím, jak jsou pro tyto účely využívána pole „*Scheme service definition URI*“ (bod 5.5.6) a „*Service information extension*“.

Členské státy MOHOU na základě výše uvedeného URI specifického pro jednotlivé členské státy definovat další URI (tj. URI definované na základě tohoto hierarchického specifického URI).

Scheme territory (bod 5.3.10)

V kontextu těchto specifikací je toto pole povinné a specifikuje zemi, v níž je systém zřízen (kód země ve formátu ISO 3166-1 alpha-2).

TSL policy/legal notice (bod 5.3.11)

V kontextu těchto specifikací je toto pole povinné a specifikuje politiku systému nebo poskytuje oznámení o právním postavení systému nebo o zákonných požadavcích, které musí systém splňovat v rámci své příslušnosti, nebo o jakýchkoli omezeních nebo podmínkách, za nichž je důvěryhodný seznam udržován nebo zveřejňován.

Jde o vícejazyčný řetězec znaků (prostý text) složený ze dvou částí:

— V první, povinné části společné pro všechny důvěryhodné seznamy členských států (s povinným jazykem EN a volitelně s jedním či více národními jazyky) se uvádí, že platným právním rámcem je směrnice 1999/93/ES a její příslušné prováděcí právní předpisy členských států uvedených v poli „*Scheme territory*“.

Anglické znění společného textu:

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

Text v národním jazyce/jazycích členského státu: [úřední překlad(y) výše uvedeného anglického textu:

Platným právním rámcem pro toto provedení důvěryhodného seznamu ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni, v podobě TSL pro [název příslušného členského státu] je směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy a její provedení v právních předpisech [název příslušného členského státu]].

— Ve druhé, volitelné části specifické pro jednotlivé důvěryhodné seznamy (s povinným jazykem EN a volitelně s jedním či více národními jazyky) se uvádějí odkazy na specifické platné vnitrostátní právní rámce (např. zejména pokud jde o vnitrostátní systémy dohledu/akreditace pro ověřovatele nevydávají kvalifikovaná osvědčení).

Historical information period (bod 5.3.12)

Toto pole je povinné a specifikuje trvání doby (celočíselně), pro niž se v TSL poskytují historické informace. Tato celočíselná hodnota se vyjadřuje počtem dní a v kontextu těchto specifikací MUSÍ být vyšší nebo rovna 3 653 (tj. provedení důvěryhodného seznamu členského státu v podobě TSL MUSÍ obsahovat historické informace minimálně pro deset let). Vyšší hodnoty by měly řádně zohledňovat zákonné požadavky na uchovávání dat v členském státě uvedeném v „*Scheme Territory*“ (bod 5.3.10).

Pointers to other TSLs (bod 5.3.13)

V kontextu těchto specifikací je toto pole povinné a zahrnuje ukazatel – pokud je k dispozici – na seznam odkazů (ukazatelů) vypracovaný EK, který je v souladu s ETSI TS 102 231 a který odkazuje na provedení důvěryhodných seznamů členských států v podobě TSL. Použijí se specifikace ETSI TS 102 231 bod 5.3.13 a zároveň se požaduje využití volitelné digitální identity vydavatele TSL, na který se odkazuje, ve formátu podle bodu 5.5.3.

Poznámka: Dokud se čeká na provedení seznamu odkazů na provedení důvěryhodných seznamů členských států v podobě TSL vypracovaného EK, který je v souladu s ETSI TS 102 231, toto pole se NESMÍ použít.

List issue date and time (bod 5.3.14)

Toto pole je povinné a specifikuje datum a čas (koordinovaný světový čas (UTC) vyjádřený jako „Zulu“) vydání TSL, hodnota data a času se použije podle ETSI TS 102 231 bodu 5.1.4.

Next update (bod 5.3.15)

Toto pole je povinné a specifikuje nejzazší datum a čas (koordinovaný světový čas (UTC) vyjádřený jako „Zulu“), kdy bude vydán příští TSL nebo kdy bude ukončena platnost TSL (hodnota data a času se použije podle ETSI TS 102 231 bodu 5.1.4).

Pokud nedošlo k žádným průběžným změnám ve stavu TSP nebo služeb pokrytých systémem, MUSÍ být TSL znovu vydán do data, kdy bude ukončena platnost předchozího TSL.

V kontextu těchto specifikací NESMÍ rozdíl mezi daty a časy uvedenými v „*Next update*“ a „*List issue date and time*“ překročit **šest (6)** měsíců.

Distribution points (bod 5.3.16)

Toto pole je volitelné. Použije-li se, specifikuje umístění, kde je zveřejněno provedení důvěryhodného seznamu v podobě TSL a kde lze nalézt aktuální TSL. Pokud je specifikováno několik míst, MUSÍ všechna poskytovat identické kopie aktuálního TSL nebo jeho aktualizovanou verzi. Pokud se toto pole použije, má formát neprázdné sekvence řetězců, přičemž každý z nich je v souladu s RFC 3986 [1].

Scheme extensions (bod 5.3.17)

Toto pole je volitelné a v kontextu těchto specifikací se nepoužije.

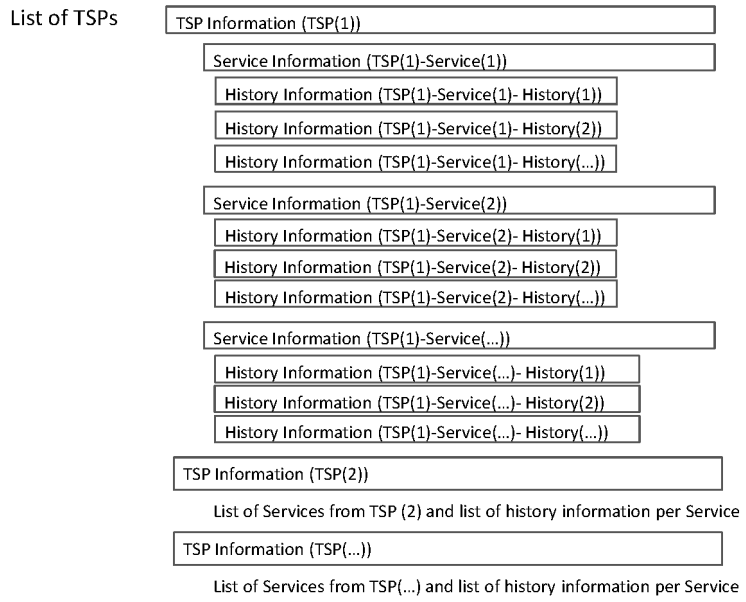
List of Trust Service Providers

Toto pole je volitelné.

V případě, že nebyl v kontextu systému členského státu vykonáván dohled nad žádným ověřovatelem ani nebyl žádný ověřovatel akreditován, NESMÍ být toto pole přítomno. Je však dohodnuto, že i když členský stát nemá pod dohledem žádného ověřovatele ani nemá žádného ověřovatele akreditovaného, MUSÍ TSL provést, a to za nepřítomnosti tohoto pole. Nepřítomnost ověřovatelů na tomto seznamu znamená, že v zemi specifikované v „*Scheme Territory*“ se nenachází žádný ověřovatel pod dohledem ani žádný akreditovaný ověřovatel.

V případě, že v rámci systému je či byla pod dohledem/akreditována jedna či více služeb ověřovatelů, obsahuje toto pole sekvenci identifikující každého ověřovatele poskytujícího jednu či více těchto služeb, nad nimiž je/byl vykonáván dohled nebo které jsou/byly akreditovány, s podrobnostmi o stavu dohledu/akreditace a stavu historie každé ze služeb ověřovatelů (na obrázku níže TSP = CSP).

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



Seznam TSP je uspořádán tak, jak je zobrazeno na obrázku výše. U každého TSP je zde sekvence polí nesoucích informace o TSP („*TSP Information*“) následována seznamem služeb. U každé z těchto služeb na seznamu je zde sekvence polí nesoucích informace o službě („*Service Information*“) a sekvence polí o historii stavu schválení služby („*Service approval history*“).

TSP Information

TSP(1)

TSP name (bod 5.4.1)

Toto pole je povinné a specifikuje název právnické osoby odpovědné za služby ověřovatelů v rámci systému, nad nimiž je či byl vykonáván dohled nebo kteří jsou či byli akreditováni. Jde o sekvenci vícejazyčných řetězců znaků (s povinným jazykem EN a volitelně s jedním či více národními jazyky). Tímto názvem MUSÍ být název uvedený v úřední zákonné registraci, jemuž mají být adresována veškerá úřední sdělení.

TSP trade name (bod 5.4.2)

Toto pole je volitelné, je-li přítomno, specifikuje alternativní název, pod nímž ověřovatel vystupuje ve specifickém kontextu poskytování svých služeb, které se mají nacházet v tomto TSL pod zápisem jeho „*TSP name*“ (bod 5.4.1).

Poznámka: Jestliže jediná právnická osoba ověřovatele poskytuje služby pod různými obchodními názvy nebo v různých specifických kontextech, může se vyskytovat tolik zápisů ověřovatele, kolik je specifických kontextů (např. zápisy Název/Obchodní název). Alternativně lze uvést na seznamu každého ověřovatele (právnickou osobu) pouze jednou a poskytnout u něj informace o specifickém kontextu služby. Je na provozovateli systému členského státu, aby s ověřovatelem prodiskutoval a dohodl nejvhodnější přístup.

TSP address (bod 5.4.3)

Toto pole je povinné a specifikuje se v něm adresa právnické osoby nebo pověřené organizace uvedené v poli „*TSP name*“ (bod 5.4.1) pro poštovní i elektronickou komunikaci. Zahrnuje jak „*PostalAddress*“ (tj. ulici, obec, [stát nebo provincii], [poštovní směrovací číslo] a kód země ve formátu ISO 3166-1 alpha-2) v souladu s bodem 5.3.5.1, tak „*ElectronicAddress*“ (tj. e-mail nebo URI internetové stránky) v souladu s bodem 5.3.5.2.

TSP information URI (bod 5.4.4)

Toto pole je povinné a specifikuje URI, kde mohou uživatelé (např. strany spoléhající se na osvědčení) získat specifické informace o ověřovateli. Jde o sekvenci vícejazyčných ukazatelů (s povinným jazykem EN a volitelně s jedním či více národními jazyky). Odkazovaný URI MUSÍ obsahovat cestu k informacím popisujícím všeobecné obchodní podmínky ověřovatele, jeho postupy, právní náležitosti, politiky péče o zákazníka a další obecné informace, které se týkají všech jeho služeb uvedených v TSL pod jeho zápisem jako ověřovatele.

Poznámka: Jestliže jediná právnická osoba ověřovatele poskytuje služby pod různými obchodními názvy nebo v různých specifických kontextech a jestliže se to odráží v tolika zápisech TSP, kolik je specifických kontextů, specifikuje toto pole informace týkající se specifického souboru služeb uvedených pod konkrétním zápisem TSP/TradeName.

TSP information extensions (bod 5.4.5)

Toto pole je volitelné, je-li přítomno, může jej provozovatel systému v souladu se specifikacemi ETSI TS 102 231 (bod 5.4.5) použít k poskytnutí specifických informací, které se mají vykládat podle pravidel specifického systému.

List of Services

Toto pole je povinné a obsahuje sekvenci identifikující každou z uznaných služeb ověřovatele a stav schválení (a historii tohoto stavu) dané služby. Musí zde být uvedena nejméně jedna služba (i když jsou informace o ní zcela historické povahy).

Vzhledem k tomu, že v rámci těchto specifikací je uchovávání informací o službách uvedených na seznamu povinné, MUSÍ se historické informace uchovávat i přesto, že by aktuální stav služby za normálních podmínek její uvedení na seznamu nevyžadoval (např. služba byla zrušena). Pro zachování historie tak ověřovatel MUSÍ být zahrnut i přesto, že jeho jediná služba na seznamu je v takovém stavu.

Service Information

TSP(1) Service(1)

Service type identifier (bod 5.5.1)

Toto pole je povinné a specifikuje identifikátor typu služby podle typu těchto specifikací TSL (tj. „/eSigDir-1999-93-EC-TrustedList/TSLtype/generic“).

Pokud služba na seznamu souvisí s vydáváním kvalifikovaných služeb, bude citován URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC (certifikační autorita vydávající kvalifikovaná osvědčení).

Pokud služba uvedená na seznamu souvisí s vydáváním tokenů důvěryhodné služby, které nejsou kvalifikovanými osvědčeními ani nepodporují vydávání kvalifikovaných osvědčení, pak je citovaným URI jeden z URI definovaných v ETSI 102 231 a uvedený v jeho bodě D.2, co se týče tohoto pole. Toto se použije i v případě tokenů důvěryhodných služeb, nad nimiž je vykonáván dohled nebo které jsou akreditovány z hlediska plnění specifických kvalifikací podle vnitrostátních zákonů členských států (např. tzv. tokeny kvalifikovaných časových razítek v DE nebo HU), citovaným URI je jeden z URI definovaných v ETSI 102 231 a uvedený v jeho bodě D.2, co se týče tohoto pole (např. TSA pro vnitrostátně definované tokeny kvalifikovaných časových razítek). Pokud je to vhodné, MOHOU být takové specifické vnitrostátní kvalifikace tokenů důvěryhodných služeb zaznamenány v zápisu o službě a pro tento účel se použije rozšíření *additionalServiceInformation* (bod 5.8.2) v bodě 5.5.9 („*Service information extension*“).

Obecnou standardní zásadou je, že u osvědčovacích služeb uvedených na seznamu a poskytovaných ověřovatelem z důvěryhodného seznamu (např. certifikační autorita (přímo) vydávající kvalifikovaná osvědčení) MUSÍ existovat jeden zápis na jedno osvědčení X.509v3 (např. pro typ osvědčovací služby CA/QC). Za pečlivě promyšlených okolností a za pečlivě řízených a schválených podmínek se MŮŽE dozorový subjekt/akreditační subjekt členského státu rozhodnout, že se osvědčení X.509v3 kořenové CA nebo CA vyšší úrovně (tj. certifikační autority, která kvalifikovaná osvědčení pro koncové subjekty přímo nevydává, ale osvědčuje hierarchii nižších CA až po CA vydávající kvalifikovaná osvědčení pro koncové subjekty) použije jako „Sdi“ jediného zápisu v seznamu služeb ověřovatele uvedeného na seznamu. Důsledky (výhody a nevýhody) použití takového osvědčení X.509v3 kořenové CA nebo vyšší CA jako hodnoty „Sdi“ v zápisech o službách v důvěryhodném seznamu musí členské státy pečlivě zvážit a schválit [1]. Navíc MUSÍ členské státy při použití takové povolené výjimky ze standardní zásady poskytnout dokumentaci potřebnou pro usnadnění zřízení a ověření cesty osvědčení.

[1] Použití osvědčení X.509v3 kořenové CA jako hodnoty „Sdi“ služby uvedené na seznamu přinutí provozovatele systému, aby z hlediska „stavu dohledu/akreditace“ posuzoval celý soubor osvědčovacích služeb v rámci takové kořenové CA jako celek. Např. jakákoli změna stavu vyžadovaná od jedné CA uvedené v rámci kořenové hierarchie bude vyžadovat, aby tuto změnu stavu přijala celá hierarchie.

Poznámka 1: Stejně jako odpovídající subjekty OCSP a vydavatelé CRL tvořící součást osvědčovacích služeb CSP_{QC} a podléhající používání příslušných samostatných klíčů k podepisování odpovědí OCSP a CRL MOHOU být TSP uvedeny v této šabloně TSL, a to použitím této kombinace URI:

— hodnota „*Service type identifier*“ (bod 5.5.1):

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

v kombinaci s touto hodnotou „*Service information extension*“ (bod 5.5.9) v rozšíření *additionalServiceInformation* (bod 5.8.2):

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

popis: poskytovatel informací o stavu osvědčení provozující server OCSP jako součást služby ověřovatele vydávajícího kvalifikovaná osvědčení.

— hodnota „*Service type identifier*“ (bod 5.5.1):

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

v kombinaci s touto hodnotou „*Service information extension*“ (bod 5.5.9) v rozšíření *additionalServiceInformation* (bod 5.8.2):

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

popis: poskytovatel informací o stavu osvědčení provozující CRL jako součást služby ověřovatele vydávajícího kvalifikovaná osvědčení.

— hodnota „*Service type identifier*“ (bod 5.5.1):

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

v kombinaci s touto hodnotou „*Service information extension*“ (bod 5.5.9) v rozšíření *additionalServiceInformation* (bod 5.8.2):

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

popis: kořenová certifikační autorita, od níž lze stanovit cestu osvědčení až k certifikační autoritě vydávající kvalifikovaná osvědčení.

— hodnota „*Service type identifier*“ (bod 5.5.1):

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

v kombinaci s touto hodnotou „*Service information extension*“ (bod 5.5.9) v rozšíření *additionalServiceInformation* (bod 5.8.2):

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

popis: služba časového razítka jako součást služby ověřovatele vydávajícího kvalifikovaná osvědčení, který vydává tokeny časových razítek (TST), jež lze v postupu ověřování kvalifikovaného podpisu použít k tomu, aby se zjistila a rozšířila platnost podpisu, když je kvalifikované osvědčení odvoláno nebo skončila jeho platnost.

Service name (bod 5.5.2)

Toto pole je povinné a specifikuje název, pod nímž ověřovatel identifikovaný v „*TSP name*“ (bod 5.4.1) poskytuje službu identifikovanou v „*Service type identifier*“ (bod 5.5.1). Jde o sekvenci vícejazyčných řetězců znaků (s povinným jazykem EN a volitelně s jedním či více národními jazyky).

Service digital identity (bod 5.5.3)

Toto pole je povinné a specifikuje přinejmenším jedno zastoupení digitálního identifikátoru jedinečného pro službu, jejíž typ je specifikován v „*Service type identifier*“ (bod 5.5.1), jímž je služba jednoznačně identifikována.

V těchto specifikacích je digitálním identifikátorem použitým v tomto poli příslušné osvědčení X.509v3 zastupující veřejný klíč (klíče), který ověřovatel používá pro poskytování služeb specifikovaných v „*Service type identifier*“ (bod 5.5.1) (tj. klíč používaný kořenovou CA/QC, klíč používaný k podepisování osvědčení ([1]) nebo případně k vydávání tokenů časových razítek nebo podepisování CRL nebo podepisování odpovědí OCSP). Toto související osvědčení X.509v3 MUSÍ být použito jako minimální požadovaný digitální identifikátor (zastupující veřejný klíč (klíče), který ověřovatel používá pro poskytování služby uvedené na seznamu). Další identifikátory je MOŽNÉ použít, jak je uvedeno níže, ale všechny MUSÍ odkazovat na stejnou identitu (tj. na související osvědčení X.509v3):

a) jedinečné jméno (DN) osvědčení, jež lze použít k ověření elektronických podpisů služby ověřovatele specifikované v „*Service type identifier*“ (bod 5.5.1);

b) identifikátor souvisejícího veřejného klíče (tj. hodnota *SubjectKeyIdentifier* neboli SKI X.509v3);

c) související veřejný klíč.

Obecnou standardní zásadou je, že digitální identifikátor (tj. související osvědčení X.509v3) NESMÍ být v důvěryhodném seznamu přítomen více než jednou, tj. pro osvědčovací službu v rámci osvědčovacích služeb uvedených na seznamu poskytovaných ověřovatelem z důvěryhodného seznamu MUSÍ existovat pouze jeden zápis na jedno osvědčení X.509v3. A opačně, jako hodnota „Sdi“ MUSÍ být jedno osvědčení X.509v3 použito pouze v jediném zápisu o službě.

Poznámka 1: Jediným případem, kdy se výše uvedená obecná standardní zásada nesmí použít, je situace, kdy je k vydávání různých typů tokenů důvěryhodných služeb, na něž se vztahují různé systémy dohledu/akreditace, použito jediné osvědčení X.509v3, například když ověřovatel používá jediné osvědčení X.509v3 na jedné straně k vydávání kvalifikovaných osvědčení v rámci příslušného systému dohledu a na druhé straně k vydávání nekvalifikovaných osvědčení v rámci jiného stavu dohledu/akreditace. V tomto případě by se v uvedeném příkladě použily dva zápisy s odlišnými hodnotami „Sti“ (např. v uvedeném příkladě CA/QC a CA/PKC, v tomto pořadí) a stejnou hodnotou „Sdi“ (související osvědčení X.509v3).

Provedení závisí na ASN.1 nebo XML a MUSÍ být v souladu se specifikacemi ETSI TS 102 231 (pro ASN.1 viz příloha A ETSI TS 102 231 a pro XML viz příloha B ETSI TS 102 231).

Poznámka 2: Pokud je třeba poskytnout další informace o „kvalifikaci“ ohledně identifikovaného zápisu o službě, pak provozovatel systému ve vhodných případech MUSÍ zvážit použití rozšíření „*additionalServiceInformation*“ (bod 5.8.2) v poli „*Service information extension*“ (bod 5.5.9), a to podle cíle poskytování takových dalších informací o „kvalifikaci“. Navíc může provozovatel systému volitelně použít bod 5.5.6 („*Scheme service definition URI*“).

Service current status (bod 5.5.4)

Toto pole je povinné a specifikuje identifikátor stavu služby prostřednictvím jednoho z těchto URI:

— **pod dohledem („*Under Supervision*“)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision);

— **dohled nad ukončovanou službou („*Supervision of Service in Cessation*“)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

— **dohled ukončen („*Supervision Ceased*“)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— **dohled odvolán („*Supervision Revoked*“)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked);

— **akreditována („*Accredited*“)** (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited);

— **akreditace ukončena („*Accreditation Ceased*“)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— **akreditace odvolána („*Accreditation Revoked*“)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

Výše uvedené stavy se v kontextu těchto specifikací vykládají takto:

— ***Pod dohledem:*** Služba identifikovaná v „*Service digital identity*“ (bod 5.5.3) poskytovaná ověřovatelem (CSP) identifikovaným v „*TSP name*“ (bod 5.4.1) je v současnosti pod dohledem členského státu identifikovaného v „*Scheme territory*“ (bod 5.3.10), v němž je ověřovatel usazen, z hlediska souladu s ustanoveními směrnice 1999/93/ES.

([1]) Může to být osvědčení CA vydávající osvědčení pro koncové subjekty (např. CA/PKC, CA/QC) **nebo** osvědčení důvěryhodné kořenové CA, od níž lze najít cestu až ke kvalifikovaným osvědčením pro koncové subjekty. V závislosti na tom, zda lze tyto informace a informace nacházející se v každém osvědčení pro koncový subjekt vydaném touto důvěryhodnou kořenovou CA použít k jednoznačnému stanovení vhodných vlastností jakéhokoli kvalifikovaného osvědčení, může být potřeba doplnit tyto informace („*Service digital identity*“) údaji v „*Service information extensions*“ (viz bod 5.5.9).

— ***Dohled nad ukončovanou službou:*** Služba identifikovaná v „*Service digital identity*“ (bod 5.5.3) poskytovaná ověřovatelem identifikovaným v „*TSP name*“ (bod 5.4.1) je v současnosti ve fázi ukončování, ale dokud nebude dohled ukončen nebo odvolán, je stále ještě pod dohledem. V případě, že odpovědnost za zajištění této fáze ukončování převzala jiná právnická osoba, než je uvedeno v „*TSP name*“, uvede se identifikace takovéto nové nebo rezervní právnické osoby (rezervního ověřovatele) v bodě 5.5.6 zápisu o službě.

— ***Dohled ukončen:*** Platnost posouzení dohledu uplynula a služba identifikovaná v „*Service digital identity*“ (bod 5.5.3) nebyla posouzena znovu. Služba v současnosti již není pod dohledem od data aktuálního stavu, neboť se má za to, že přestala fungovat.

— ***Dohled odvolán:*** Služba ověřovatele byla pod dohledem, ale poté již ona sama a možná též ověřovatel přestali být v souladu s ustanoveními směrnice 1999/93/ES, jak stanoví členský stát identifikovaný v „*Scheme territory*“ (bod 5.3.10), v němž je ověřovatel usazen. V souladu s tím bylo požadováno, aby bylo ukončeno působení služby a aby byla považována za ukončenou z výše uvedených důvodů.

Poznámka 1: Hodnota stavu „Dohled odvolán“ („*Supervision Revoked*“) může být konečným stavem, i když poté ověřovatel zcela přestane vykonávat svou činnost; v takovém případě již není třeba přecházet k hodnotě „Dohled nad ukončovanou službou“ („*Supervision of Service in Cessation*“) nebo „Dohled ukončen“ („*Supervision Ceased*“). Jediným způsobem, jak změnit stav „Dohled odvolán“, je vrátit se z nesouladu s ustanoveními směrnice 1999/93/ES k souladu s nimi podle příslušného platného systému dohledu členského státu odpovědného za důvěryhodný seznam a znovu dosáhnout stavu „Pod dohledem“ („*Under Supervision*“). Ke stavu „Dohled nad ukončovanou službou“ nebo „Dohled ukončen“ dochází, pouze když ověřovatel přímo ukončí své související služby pod dohledem, nikoli když byl dohled odvolán.

— ***Akreditována:*** Akreditační subjekt vykonal jménem členského státu identifikovaného v „*Scheme territory*“ (bod 5.3.10) posouzení pro akreditaci a bylo shledáno, že služba identifikovaná v „*Service digital identity*“ (bod 5.5.3) poskytovaná ověřovatelem ([1]) identifikovaným v „*TSP name*“ (bod 5.4.1) je v souladu s ustanoveními směrnice 1999/93/ES.

Poznámka 2: Při použití v kontextu ověřovatele vydávajícího kvalifikovaná osvědčení, který je usazen v „*Scheme territory*“ (bod 5.3.10), se následující dva stavy „Akreditace odvolána“ („*Accreditation Revoked*“) a „Akreditace ukončena“ („*Accreditation Ceased*“) MUSÍ považovat za „přechodné“ a NESMÍ se použít jako hodnota „Aktuálního stavu služby“, neboť v případě použití po nich MUSÍ v „Informacích o historii schválení služby“ nebo v „Aktuálním stavu služby“ bezprostředně následovat stav „Pod dohledem“, případně následovaný některým dalším stavem dohledu definovaným výše a znázorněným v obrázku 1. Při použití v kontextu ověřovatele nevydávajícího kvalifikovaná osvědčení, kdy jde pouze o přidružený systém „dobrovolné akreditace“ bez přidruženého systému dohledu, nebo v kontextu ověřovatele vydávajícího kvalifikovaná osvědčení, který není usazen v „*Scheme territory*“ (bod 5.3.10) (např. je usazen ve třetí zemi), lze tyto stavy „Akreditace odvolána“ a „Akreditace ukončena“ použít jako hodnotu „Aktuálního stavu služby“.

— ***Akreditace ukončena:*** Platnost posouzení akreditace uplynula a služba identifikovaná v „*Service digital identity*“ (bod 5.5.3) nebyla posouzena znovu.

— ***Akreditace odvolána:*** Služba identifikovaná v „*Service digital identity*“ (bod 5.5.3) poskytovaná ověřovatelem (CSP) identifikovaným v „*TSP name*“ (bod 5.4.1) byla původně v souladu s kritérii systému, ale již ona sama a možná též její poskytovatel přestali být v souladu s ustanoveními směrnice 1999/93/ES.

Poznámka 3: U ověřovatelů vydávajících kvalifikovaná osvědčení se musí použít naprosto shodné hodnoty jako u ověřovatelů nevydávajících kvalifikovaná osvědčení (např. u poskytovatelů služeb časových razítek vydávajících tokeny časových razítek, ověřovatelů vydávajících nekvalifikovaná osvědčení atd.). Pro rozlišení příslušných systémů dohledu/akreditace se použije „*Service Type identifier*“ (bod 5.5.1).

Poznámka 4: Další informace o „kvalifikaci“ týkající se stavu definované na úrovni vnitrostátních systémů dohledu/akreditace pro ověřovatele nevydávající kvalifikovaná osvědčení lze ve vhodných a požadovaných případech poskytnout na úrovni služby (např. pro odlišení různých úrovní kvality/bezpečnosti). Provozovatelé systémů MUSÍ použít rozšíření „*additionalServiceInformation*“ (bod 5.8.2) pole „*Service information extension*“ (bod 5.5.9) v souladu s účelem poskytnutí takových dalších informací o „kvalifikaci“. Navíc může provozovatel systému volitelně použít bod 5.5.6 („*Scheme service definition URI*“).

Current status starting date and time (bod 5.5.5)

Toto pole je povinné a specifikuje datum a čas, odkdy platí aktuální stav schválení (hodnota data a času podle definice v ETSI TS 102 231 bod 5.4.1).

Scheme service definition URI (bod 5.5.6)

Toto pole je volitelné, je-li přítomno, specifikuje URI, kde mohou strany spoléhající se na osvědčení získat informace specifické pro danou službu poskytované provozovatelem systému jako sekvence vícejazyčných ukazatelů (s povinným jazykem EN a volitelně s jedním či více národními jazyky).

([1]) Vezměte na vědomí, že tento akreditovaný ověřovatel může být usazen v jiném členském státě, než je stát identifikovaný v „*Scheme territory*“ provedení důvěryhodného seznamu v podobě TSL, nebo ve třetí zemi (viz čl. 7 odst. 1 písm. a) směrnice 1999/93/ES.)

Použije-li se, MUSÍ odkazovaná adresa URI poskytnout cestu k informacím popisujícím službu podle specifikací v systému. Toto MŮŽE ve vhodných případech zahrnovat zejména:

a) URI uvádějící identitu rezervního ověřovatele pro případ dohledu nad službou ukončovanou za účasti rezervního poskytovatele (viz „*Service current status*“ bod 5.5.4);

b) URI vedoucí k dokumentům poskytujícím další informace týkající se použití některých vnitrostátně definovaných specifických kvalifikací tokenů důvěryhodných služeb, nad nimiž je vykonáván dohled nebo které jsou akreditovány, poskytujících službu v souladu s použitím uvedeným v poli „*Service information extension*“ (bod 5.5.9) s rozšířením „*additionalServiceInformation*“ definovaným v bodě 5.8.2.

Service supply points (bod 5.5.7)

Toto pole je volitelné, je-li přítomno, specifikuje URI, kde mohou mít strany spoléhající se na osvědčení přístup ke službě prostřednictvím sekvence řetězců znaků, jejichž syntax MUSÍ být v souladu s RFC 3986.

TSP service definition URI (bod 5.5.8)

Toto pole je volitelné, je-li přítomno, specifikuje URI, kde mohou strany spoléhající se na osvědčení získat informace specifické pro danou službu poskytované TSP jako sekvence vícejazyčných ukazatelů (s povinným jazykem EN a volitelně s jedním či více národními jazyky). Odkazovaná adresa URI MUSÍ poskytnout cestu k informacím popisujícím službu podle specifikací TSP.

Service information extensions (bod 5.5.9)

V kontextu těchto specifikací je toto pole volitelné, ale MUSÍ být přítomno, pokud informace poskytnuté v „*Service digital identity*“ (bod 5.5.3) nejsou dostatečné pro jednoznačnou identifikaci kvalifikovaných osvědčení vydaných v rámci této služby nebo pokud informace přítomné v souvisejících kvalifikovaných osvědčeních neumožňují strojové zpracování identifikace skutečností o tom, zda kvalifikované osvědčení je, či není podporováno prostředkem pro bezpečné vytváření podpisu ([1]).

V kontextu těchto specifikací, pokud je toto pole povinné, např. pro služby CA/QC, MUSÍ se použít a uspořádat volitelné pole informací „*Service information extensions*“ („Sie“) podle rozšíření „Kvalifikací“ definovaného v ETSI TS 102 231 příloze L.3.1, a to jako sekvence jedné či více n-tic, přičemž každá n-tice poskytuje:

— (filtry) Informace, které se mají použít pro další identifikaci v rámci osvědčovací služby identifikované pomocí „Sdi“ přesně té služby (tj. souboru kvalifikovaných osvědčení), u níž se požadují/poskytují další informace týkající se existence/neexistence podpory prostředkem pro bezpečné vytváření podpisu (nebo vydání pro právnickou osobu) a

— Přidružené informace („kvalifikátory“) o tom, zda je tento dále identifikovaný soubor služeb kvalifikovaných osvědčení podporován prostředkem pro bezpečné vytváření podpisu (pokud tato informace zní „QCSSCDStatusAsInCert“, znamená to, že jsou tyto přidružené informace součástí kvalifikovaného osvědčení v rámci strojově zpracovatelné podoby standardizované ETSI ([2]), nebo informace týkající se skutečnosti, že jsou taková kvalifikovaná osvědčení vydávána pro právnické osoby (standardně se má za to, že se vydávají pouze pro fyzické osoby).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): značí, že ověřovatel zajišťuje a členský stát kontroluje (model dohledu, dozorový subjekt) nebo akredituje (model akreditace, akreditační subjekt), že jakékoli kvalifikované osvědčení vydané v rámci služby (QCA) identifikované v „*Service digital identity*“ (bod 5.5.3) a dále identifikované výše uvedenými informacemi (filtry) použitými pro další identifikaci přesně toho souboru kvalifikovaných osvědčení v rámci služeb identifikovaných „Sdi“, u nějž se požadují tyto další informace o (ne)existenci podpory prostředkem pro bezpečné vytváření podpisu, **JE** podporováno prostředkem pro bezpečné vytváření podpisu (tj. že soukromý klíč spojený s veřejným klíčem v osvědčení je uložen v prostředku pro bezpečné vytváření podpisu v souladu s přílohou III směrnice 1999/93/ES);

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD): značí, že ověřovatel zajišťuje a členský stát kontroluje (model dohledu, dozorový subjekt) nebo akredituje (model akreditace, akreditační subjekt), že jakékoli kvalifikované osvědčení vydané v rámci služby (kořenová CA/QC nebo CA/QC) identifikované v „*Service digital identity*“ (bod 5.5.3) a dále identifikované výše uvedenými informacemi (filtry) použitými pro další identifikaci přesně toho souboru kvalifikovaných osvědčení v rámci služeb identifikovaných „Sdi“, u nějž se požadují tyto další informace o (ne)existenci podpory prostředkem pro bezpečné vytváření podpisu, **NENÍ** podporováno prostředkem pro bezpečné vytváření podpisu (tj. že soukromý klíč spojený s veřejným klíčem v osvědčení není uložen v prostředku pro bezpečné vytváření podpisu v souladu s přílohou III směrnice 1999/93/ES);

([1]) Viz oddíl 2.2 tohoto dokumentu.
([2]) Toto odkazuje na vhodnou kombinaci ETSI definovaných prohlášení QcCompliance, prohlášení QcSSCD [ETSI TS 101 862] nebo QCP/QCP + ETSI definovaných OID [ETSI TS 101 456].

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): značí, že ověřovatel zajišťuje a členský stát kontroluje (model dohledu, dozorový subjekt) nebo akredituje (model akreditace, akreditační subjekt), že jakékoli kvalifikované osvědčení vydané v rámci služby (CA/QC) identifikované v „*Service digital identity*“ (bod 5.5.3) a dále identifikované výše uvedenými informacemi (filtry) použitými pro další identifikaci přesně toho souboru kvalifikovaných osvědčení v rámci služeb identifikovaných „Sdi“, u nějž se požadují tyto další informace o (ne)existenci podpory prostředkem pro bezpečné vytváření podpisu, MUSÍ obsahovat strojově zpracovatelnou informaci o tom, zda je kvalifikované osvědčení podporováno prostředkem pro bezpečné vytváření podpisu;

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): značí, že ověřovatel zajišťuje a členský stát kontroluje (model dohledu, dozorový subjekt) nebo akredituje (model akreditace, akreditační subjekt), že jakékoli kvalifikované osvědčení vydané v rámci služby (QCA) identifikované v „*Service digital identity*“ (bod 5.5.3) a dále identifikované výše uvedenými informacemi (filtry) použitými pro další identifikaci přesně toho souboru kvalifikovaných osvědčení v rámci služeb identifikovaných „Sdi“, u nějž se požadují tyto další informace o vydání pro právnickou osobu, **JSOU** vydána pro právnické osoby.

Tyto kvalifikátory se mají použít pouze jako rozšíření, pokud je typ služby http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Toto pole je specifické podle provedení (ASN.1 nebo XML) a MUSÍ být v souladu se specifikacemi uvedenými v příloze L.3.1 ETSI TS 102 231.

V kontextu provedení XML musí být specifický obsah takových dalších informací šifrován za použití souboru xsd uvedeného v kapitole 3.

Service Approval History

Toto pole je volitelné, ale MUSÍ být použito, jestliže „*Historical information period*“ (bod 5.3.12) není prázdné. V kontextu těchto specifikací tedy systém MUSÍ uchovávat historické informace. V případě, že jsou historické informace určeny k uchovávání, ale služba nemá před aktuálním stavem žádnou historii (tj. provozovatel systému neuchoval první zaznamenaný stav nebo historické informace), MUSÍ být toto pole prázdné. Jinak MUSÍ být u každé změny v aktuálním stavu služby TSP, k níž došlo v období historických informací, jak je specifikováno v ETSI TS 102 231, bod 5.3.12, poskytnuta informace o schválení předchozího stavu, a to v sestupném pořadí podle data a času změny stavu (tj. data a času, od nějž začalo platit následující schválení stavu).

Jde o sekvenci historických informací, jak je definováno níže.

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

Service type identifier (bod 5.6.1)

Toto pole je povinné a specifikuje identifikátor typu služby, ve formátu a s významem použitým v „*TSP Service Information – Service type identifier*“ (bod 5.5.1).

Service name (bod 5.6.2)

Toto pole je povinné a specifikuje název, pod nímž ověřovatel poskytl službu identifikovanou v „*TSP Service Information – Service type identifier*“ (bod 5.5.1), ve formátu a s významem použitým v „*TSP Service Information – Service name*“ (bod 5.5.2). Tento bod nevyžaduje, aby byl název stejný jako název specifikovaný v bodě 5.5.2. Změna názvu MŮŽE být jednou z okolností vyžadujících nový stav.

Service digital identity (bod 5.6.3)

Toto pole je povinné a specifikuje přinejmenším jedno zastoupení digitálního identifikátoru jedinečného pro službu specifikovanou v „*TSP Service Information – Service digital identity*“ (bod 5.5.3), ve stejném formátu a se stejným významem.

Service previous status (bod 5.6.4)

Toto pole je povinné a specifikuje identifikátor předchozího stavu služby, ve formátu a s významem použitým v „*TSP Service Information – Service current status*“ (bod 5.5.4).

Previous status starting date and time (bod 5.6.5)

Toto pole je povinné a specifikuje datum a čas, od nějž začal platit dotčený předchozí stav, ve formátu a s významem použitým v „*TSP Service Information – Service current status starting date and time*“ (bod 5.5.5).

Service information extensions (bod 5.6.6)

Toto pole je volitelné a provozovatelé systému jej MOHOU použít k poskytnutí specifických informací souvisejících se službou, ve formátu a s významem použitým v „*TSP Service Information – Service information extensions*“ (bod 5.5.9).

TSP(1) Služba(1) Historie(2)

Stejně pro TSP(1) Služba(1) Historie(2) (před Historie 1)

…

TSP(1) Služba(2)

Stejně pro TSP(1) Služba 2 (podle potřeby)

TSP(1) Služba(2) Historie(1)

…

Informace o TSP(2)

Stejně pro TSP(2) (podle potřeby)

Stejně pro TSP 2 Služba 1

Stejně pro TSP 2 Služba 1 Historie 1

…

Signed TSL

TSL zřízený podle těchto specifikací BY MĚL ([1]) být podepsán „*Scheme operator name*“ (bod 5.3.4), aby byla zajištěna jeho pravost a neporušenost.

Doporučuje se, aby formát podpisu byl CAdES BES/EPES pro provedení ASN.1 a XAdES BES/EPES, jak je definováno ve specifikacích ETSI TS 101 903, pro provedení XML ([2]). Takové provedení elektronického podpisu MUSÍ splňovat požadavky uvedené v ETSI TS 102 231 v příloze A, respektive B.

Další všeobecné požadavky ohledně podpisu jsou uvedeny v následujících oddílech.

Scheme identification (bod 5.7.2)

Toto pole je povinné a specifikuje odkaz přidělený provozovatelem systému, který jedinečně identifikuje systém popsaný v těchto specifikacích a zřízený TSL, a MUSÍ být zahrnuto do výpočtu podpisu. Má být řetězec znaků nebo řetězec bitů.

V kontextu těchto specifikací MUSÍ být přidělený odkaz sřetězením „*TSL type*“ (bod 5.3.3), „*Scheme name*“ (bod 5.3.6) a rozšíření osvědčení *SubjectKeyIdentifier* použitých provozovatelem systému k elektronickému podepsání TSL.

Signature algorithm identifier (bod 5.7.3)

Toto pole je povinné a specifikuje šifrovací algoritmus, který byl použit k vytvoření podpisu. V závislosti na použitém algoritmu MŮŽE toto pole vyžadovat další parametry. Toto pole MUSÍ být zahrnuto do výpočtu podpisu.

([1]) Provedení důvěryhodných seznamů členských států plně v souladu s ETSI TS 102 231, a tedy elektronicky podepsaných, lze považovat za ideální cíl pro všechny členské státy, aby se zaručil skutečně interoperabilní, on-line a strojově zpracovatelný rámec pro usnadnění validace a přeshraničního použití QES a $AdES_{QC}$, přesto však bude členským státům z praktických důvodů povoleno, aby provedly prozatímní podobu svých důvěryhodných seznamů podle těchto technických specifikací, pokud zajistí šíření těchto prozatímních podob důvěryhodných seznamů bezpečnými kanály.

([2]) Je povinné chránit podpisové osvědčení provozovatele systému jedním ze způsobů specifikovaných v ETSI TS 101 733, respektive ETSI TS 101 903.

Signature value (bod 5.7.4)

Toto pole je povinné a obsahuje skutečnou hodnotu digitálního podpisu. Všechna pole TSL (kromě samotného podpisu) MUSÍ být zahrnuta do výpočtu podpisu.

TSL extensions (bod 5.8)

Rozšíření **expiredCertsRevocationInfo** (bod 5.8.1)

Toto rozšíření je volitelné. Je-li použito, MUSÍ být v souladu se specifikacemi ETSI TS 102 231, bod 5.8.1.

Rozšíření **additionalServiceInformation** (bod 5.8.2)

Toto je volitelné rozšíření, je-li použito, MUSÍ se použít pouze na úrovni služby a pouze v poli definovaném v bodě 5.5.9 („*Service information extension*"). Používá se k poskytnutí dalších informací o službě. Jde o sekvenci jedné nebo více n-tic, přičemž každá n-tice poskytuje:

a) URI identifikující další informace, např.:

— URI uvádějící některé specifické kvalifikace definované na vnitrostátní úrovni pro službu poskytování tokenů důvěryhodné služby, nad níž je vykonáván dohled nebo která je akreditována, např.:

— specifická úroveň nesourodosti bezpečnosti/kvality, pokud jde o vnitrostátní systém dohledu/akreditace pro ověřovatele nevydávající kvalifikovaná osvědčení (např. RGS*/**/*** ve FR, specifický stav „dohledu" stanovený vnitrostátními právními předpisy pro specifické ověřovatele vydávající kvalifikovaná osvědčení v DE), viz poznámka 4 u „*Service current status*" – bod 5.5.4;

— nebo specifický právní stav poskytování tokenů důvěryhodné služby, nad nímž je vykonáván dohled nebo které je akreditováno (např. „kvalifikovaný TST" definovaný na vnitrostátní úrovni jako v DE nebo HU);

— nebo význam specifického identifikátoru politiky přítomného v osvědčení X.509v3 uvedeném v poli „Sdi";

— nebo zaznamenaný URI, jak je specifikováno v „*Service type identifier*", bod 5.5.1, za účelem dalšího specifikování služby identifikované „Sti" jako služba, jež tvoří součást služeb ověřovatele vydávajícího kvalifikovaná osvědčení (např. OCSP-QC, CRL-QC a kořenová CA-QC);

b) volitelný řetězec obsahující hodnotu serviceInformation ve významu specifikovaném systémem (např. *, ** nebo ***);

c) jakékoli další volitelné informace uvedené ve formátu specifickém pro systém.

Nepřímý odkaz URI BY MĚL vést k okem čitelné podobě dokumentů, které obsahují všechny podrobnosti požadované pro porozumění rozšíření, a které zejména vysvětlují význam daných URI a specifikují možné hodnoty serviceInformation a význam každé hodnoty.

Qualifications Extension (bod L.3.1)

Popis: Toto pole je volitelné, ale MUSÍ být přítomno, je-li jeho použití povinné, např. u služeb kořenové CA/QC nebo CA/QC, a pokud

— informace uvedené v „service digital identity" nejsou dostatečné pro jednoznačnou identifikaci kvalifikovaných osvědčení vydaných touto službou;

— informace uvedené v souvisejících kvalifikovaných osvědčeních neumožňují strojově zpracovatelnou identifikaci skutečností o tom, zda je kvalifikované osvědčení podporováno zařízením pro bezpečné vytváření podpisu.

Je-li toto rozšíření na úrovni služby použito, MUSÍ se použít pouze v poli definovaném v „*Service information extension*" (bod 5.5.9).

Formát: Neprázdná sekvence jednoho či více *Qualification-elements* (bod L.3.1.2), jak je definováno v příloze L.3 ETSI TS 102 231.

KAPITOLA II

SOUBOR XSD ETSI TÝKAJÍCÍ SE ETSI TS 102 231 VERZE 3

Tyto informace se poskytují v současném stavu. Vyskytnou-li se při používání tohoto souboru xsd potíže, je třeba je nahlásit ETSI, aby je mohl napravit.

```
<?xml version='1,0' encoding='UTF-8'?>
<!-- edited with XML Spy v4,1 U (http://www.xmlspy.com) by Juan Carlos
Cruellas (UPC Dpt. Arquitectura de Computadors) -->
<!-- ****** NOTICE ******
Tato verze tohoto dokumentu NENÍ formálně schválenou publikací vydanou
ETSI.
Tento dokument je Â'rozpracovaným zněnímÂ' vypracovaným TC ESI STF 290
a byl revidován s cílem opravit chyby a vynechávky nalezené ve
stávající formální publikaci ETSI a také vyřešit otázky výkladu
vznesené při zavádění na základě uvedené publikace, které se nepovažují
za diskutabilní ani nemění základní strukturu TSL definovanou
v původním dokumentu TS 102 231 a odpovídajícím souboru XSD.
-->
<xsd:schema targetNamespace='http://uri.etsi.org/02231/v2#"
xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
xmlns:xsd='http://www.w3.org/2001/XMLSchema'
xmlns:ds='http://www.w3.org/2000/09/xmldsig#"
xmlns:tsl='http://uri.etsi.org/02231/v2#"
elementFormDefault='qualified' attributeFormDefault='unqualified'>
        <!-- Imports -->
        <xsd:import namespace='http://www.w3.org/XML/1998/namespace'
schemaLocation='http://www.w3.org/2001/xml.xsd'/>
        <xsd:import namespace='http://www.w3.org/2000/09/xmldsig#"
schemaLocation='http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd'/>
        <!-- Begin auxiliary types -->
        <!--InternationalNamesType-->
        <xsd:complexType name='InternationalNamesType'>
        <xsd:sequence>
        <xsd:element name='Name' type='tsl:MultiLangNormStringType'
maxOccurs='unbounded'/>
        </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name='MultiLangNormStringType'>
        <xsd:simpleContent>
        <xsd:extension base='tsl:NonEmptyNormalizedString'>
        <xsd:attribute ref='xml:lang' use='required'/>
        </xsd:extension>
        </xsd:simpleContent>
        </xsd:complexType>
        <xsd:complexType name='MultiLangStringType'>
        <xsd:simpleContent>
        <xsd:extension base='tsl:NonEmptyString'>
        <xsd:attribute ref='xml:lang' use='required'/>
        </xsd:extension>
        </xsd:simpleContent>
        </xsd:complexType>
        <xsd:simpleType name='NonEmptyString'>
        <xsd:restriction base='xsd:string'>
        <xsd:minLength value='1'/>
        </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name='NonEmptyNormalizedString'>
      <xsd:restriction base='xsd:normalizedString'>
```

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

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

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

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

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

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

KAPITOLA III

SOUBOR XSD TÝKAJÍCÍ SE KÓDOVÁNÍ POLE „SIE“

Tyto informace se poskytují v současném stavu.

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

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

KAPITOLA IV

SPECIFIKACE PRO OKEM ČITELNOU PODOBU PROVEDENÍ DŮVĚRYHODNÉHO SEZNAMU V PODOBĚ TSL

Okem čitelná podoba provedení důvěryhodného seznamu v podobě TSL MUSÍ být veřejně dostupná a přístupná elektronickými prostředky. MĚLA BY být poskytnuta v podobě dokumentu PDF podle normy ISO 32000, který MUSÍ mít formát podle profilu PDF/A (ISO 19005).

Obsah PDF/A postavený na základě okem čitelné podoby provedení důvěryhodného seznamu v podobě TSL BY MĚL splňovat tyto požadavky:

— struktura okem čitelné podoby BY MĚLA odrážet logický model popsaný v oddíle 5.1.2 ETSI TS 102 231;

— MĚLA BY být zobrazena všechna přítomná pole a MĚLO BY u nich být uvedeno toto:

  — název pole (např. „Identifikátor typu služby“);

  — hodnota pole (např. „CA/QC“);

  — je-li to třeba, význam (popis) hodnoty pole, a to zejména podle přílohy D ETSI TS 102 231 nebo podle stávajících specifikací pro zaznamenané URI (např. „Certifikační autorita vydávající osvědčení veřejných klíčů“);

  — je-li to třeba, znění v několika přirozených jazycích podle provedení důvěryhodného seznamu v podobě TSL;

— okem čitelná podoba BY MĚLA zobrazovat minimálně tato pole a příslušné hodnoty digitálních osvědčení přítomných v poli „Digitální identita služby“:

  — Verze

  — Sériové číslo

  — Algoritmus podpisu

  — Vydavatel

  — Platí od

  — Platí do

  — Subjekt

  — Veřejný klíč

  — Politiky osvědčení

  — Identifikátor klíče subjektu

  — Distribuční místa CRL

  — Identifikátor klíče autority

  — Použití klíče

  — Základní omezení

  — Algoritmus otisku

  — Otisk

— okem čitelná podoba BY MĚLA být snadno tisknutelná;

— okem čitelnou podobu JE MOŽNO podepisovat elektronicky; při podpisu MUSÍ být podepsána provozovatelem systému podle stejných specifikací podpisu jako pro provedení důvěryhodného seznamu v podobě TSL.