►B ►C1 **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) ◄

(Úř. věst. L 274, 20.10.2009, s. 36)

Ve znění:

		Úřední věstník		
		Č.	Strana	Datum
►M1	Rozhodnutí Komise 2010/425/EU ze dne 28. července 2010	L 199	30	31.7.2010
►M2	Nařízení Komise (EU) č. 519/2013 ze dne 21. února 2013	L 158	74	10.6.2013
►M3	Prováděcí rozhodnutí Komise 2013/662/EU ze dne 14. října 2013	L 306	21	16.11.2013

Opraveno:

►C1 Oprava, Úř. věst. L 299, 14.11.2009, s. 18 (2009/767/ES)
►C2 Oprava, Úř. věst. L 4, 7.1.2011, s. 6 (2009/767/ES)
►C3 Oprava, Úř. věst. L 206, 2.8.2013, s. 18 (2009/767/ES)

▼B
▼C1

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.

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

▼C1

(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 ([1]). 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.

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.

([1]) Úř. věst. L 13, 19.1.2000, s. 12.

▼C1

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

▼M3

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

2. Členské státy zřídí a zveřejní důvěryhodný seznam ve strojově zpracovatelné podobě, a to v souladu se specifikacemi stanovenými v příloze. Pokud se členský stát rozhodne zveřejnit důvěryhodný seznam v podobě čitelné okem, musí být uvedená podoba důvěryhodného seznamu v souladu se specifikacemi stanovenými v příloze.

2a. členské státy elektronicky strojově zpracovatelnou podobu svého důvěryhodného seznamu podepíší tak, aby byla zajištěna jeho pravost a neporušenost. Pokud členský stát vydává podobu důvěryhodného seznamu čitelnou okem, zajistí, aby tato podoba důvěryhodného seznamu obsahovala stejné údaje jako strojově zpracovatelná podoba, a podepíše ji elektronicky se stejným osvědčením, jaké se používá pro strojově čitelnou podobu.

2b. Členské státy zajistí, aby strojově zpracovatelná podoba jejich důvěryhodného seznamu byla na svém místě zveřejnění dostupná kdykoli a bez přerušení, s výjimkou účelů údržby.

3. Členské státy oznámí Komisi tyto informace:

a) subjekt nebo subjekty odpovědné za zřízení, údržbu a zveřejnění důvěryhodného seznamu ve strojově zpracovatelné podobě;

b) místo, kde je strojově zpracovatelná podoba důvěryhodného seznamu zveřejněna;

c) dva nebo více provozovatelů systému osvědčení veřejných klíčů s posunutými dobami platnosti v délce nejméně tří měsíců, která odpovídají soukromým klíčům, které lze použít k elektronickému podpisu strojově zpracovatelné podoby důvěryhodného seznamu;

d) jakékoli změny údajů v písmenech a), b) a c).

▼M3

3a. Pokud členský stát vydává podobu důvěryhodného seznamu čitelnou okem, informace uvedené v odstavci 3 musí být oznámeny také pro podobu čitelnou okem.

▼M1

4. Komise zpřístupní všem členským státům prostřednictvím bezpečného kanálu na ověřený webový server informace uvedené v odstavci 3, jak byly oznámeny členskými státy, v okem čitelné i podepsané strojově zpracovatelné podobě.

▼C1

Článek 3

Použití

Toto rozhodnutí se použije od 28. prosince 2009.

Článek 4

Určení

Toto rozhodnutí se použije od 28. prosince 2009.

▼M3

PŘÍLOHA

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

OBECNÉ POŽADAVKY

1. **Úvod**

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*) ([1]) (dále jen „CSP“), 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.

Účelem 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“) ([2]) podporovaných kvalifikovaným osvědčením ([3]) ([4]).

Povinné informace v důvěryhodném seznamu 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“) ([5]) v souladu s ustanoveními směrnice 1999/93/ES (čl. 3 odst. 2 a 3, čl. 7 odst. 1 písm. a)), včetně, pokud tyto nejsou součástí QC, 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“) ([6]), či nikoli.

Dodatečné informace o dalších ověřovatelích, 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, pokud je nad nimi vykonáván dohled nebo pokud jsou akreditováni podobně jako ověřovatelé, kteří vydávají kvalifikovaná osvědčení nebo jsou schváleni podle odlišného vnitrostátního schvalovacího režimu. Vnitrostátní schvalovací systémy se mohou v některých členských státech odlišovat od systémů dohledu nebo dobrovolných akreditačních systémů použitelných pro ověřovatele vydávající QC, pokud jde o použitelné požadavky nebo odpovědnou organizaci. Pojmy „akreditovaní“ nebo „podléhající dohledu“ v těchto specifikacích se také týkají vnitrostátních schvalovacích systémů, ale další informace o povaze jakýchkoli vnitrostátních systémů poskytnou členské státy ve svém důvěryhodném seznamu, včetně objasnění možných rozdílů oproti systémům akreditace/dohledu použitelným na ověřovatele vydávající QC.

Společná šablona vychází z normy ETSI TS 119 612 v1.1.1 ([7]) (dále jen „ETSI TS 119 612“), jež se zabývá zřizováním, zveřejňováním, umísťováním, ověřováním a celistvostí těchto seznamů a přístupem k nim.

([1]) Jak je definováno v čl. 2 odst. 11 směrnice 1999/93/ES.
([2]) Jak je definováno v čl. 2 odst. 2 směrnice 1999/93/ES.
([3]) Pro AdES podporovaný QC se v tomto dokumentu používá zkratka „$AdES_{QC}$“.
([4]) 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.
([5]) Jak je definováno v čl. 2 odst. 10 směrnice 1999/93/ES.
([6]) Jak je definováno v čl. 2 odst. 6 směrnice 1999/93/ES.
([7]) ETSI TS 119 612 v1.1.1 (2013-06) – Electronic Signatures and Infrastructures (ESI); Trusted Lists.

▼M3

2. **Uspořádání společné šablony důvěryhodného seznamu**

Společná šablona důvěryhodného seznamu členského státu je uspořádána podle ETSI TS 119 612 do těchto kategorií informací:

1. Značka (tag) důvěryhodného seznamu usnadňující identifikaci důvěryhodného seznamu při elektronickém vyhledávání;

2. Informace o důvěryhodném seznamu a systému jeho vydávání;

3. 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 pro účely důvěryhodného seznamu není žádný ověřovatel, nad nímž by byl vykonáván dohled nebo který by byl akreditován);

4. U každého ověřovatele jsou údaje o jeho zvláštních důvěryhodných službách, jejichž současný stav je zaznamenán v důvěryhodném seznamu, uvedeny jako sekvence polí jednoznačně identifikujících osvědčovací služby poskytované ověřovatelem, nad nimiž se vykonává dohled nebo které jsou akreditovány, a jejich současný stav (v této sekvenci musí být uveden minimálně jeden zápis);

5. U každé osvědčovací služby na seznamu, nad níž je vykonáván dohled nebo která je akreditována, případně informace o historii jejího stavu;

6. Podpis používaný na důvěryhodném seznamu.

Pokud jde o ověřovatele vydávajícího kvalifikovaná osvědčení, uspořádání důvěryhodného seznamu, a zejména součást s informacemi o službě (podle bodu 4 výše) umožňují, aby doplňkové informace v rozšířených informacích o službě kompenzovaly situace, kdy jsou v rámci kvalifikovaného osvědčení k dispozici nedostatečné (strojově zpracovatelné) informace o jeho „kvalifikovaném“ stavu, jeho případné podpoře prostředkem pro bezpečné vytváření podpisu, a zejména s cílem řešit také skutečnost, že většina (komerčních) ověřovatelů používá jedinou vydávající certifikační autoritu (*Certification Authority*, dále jen „CA“) pro vydávání několika typů osvědčení pro koncové subjekty, a to kvalifikovaných i nekvalifikovaných.

V kontextu služeb vytvoření osvědčení (CA) může být počet zápisů služby na seznamu u ověřovatele snížen, jestliže jedna nebo několik vyšších služeb CA existuje v rámci PKI ověřovatele (například v rámci hierarchie CA od kořenové CA k několika CA vydávajícím osvědčení), uvedením těchto vyšších služeb CA, a nikoli služeb CA vydávajících osvědčení pro koncové subjekty (např. zařazení pouze kořenové CA pro ověřovatele). Avšak v těchto případech se informace o stavu vztahují na celou hierarchii služeb CA pod službou uvedenou na seznamu a musí být zachována a dodržena zásada zajištění jednoznačného spojení mezi osvědčovací službou CSP_{QC} a souborem osvědčení, která mají být určena jako kvalifikovaná osvědčení.

2.1 *Popis informací v každé kategorii*

1. Tag důvěryhodného seznamu

2. Informace o důvěryhodném seznamu a systému jeho vydávání

Součástí této kategorie jsou tyto informace:

— **identifikátor verze formátu** důvěryhodného seznamu,

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

▼M3

— **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 provozovateli (vlastníku) systému** 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 (model systému, pravidla, kritéria, příslušná komunita, typ atd.) nebo o odkazech na taková umístění,

  — o době uchovávání (historických) informací,

— **politika nebo právní upozornění, závazky a odpovědnost** důvěryhodných seznamů,

— **datum a čas vydání** důvěryhodného seznamu,

— **příští plánovaná aktualizace**.

3. Jednoznačné informace pro identifikaci o každém ověřovateli, nad nímž je vykonáván dohled nebo který je akreditován podle systému

Tento soubor informací zahrnuje přinejmenším:

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

— adresu a kontaktní informace ověřovatele,

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

4. U každého ověřovatele na seznamu sekvence 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 zahrnuje u každé osvědčovací služby ověřovatele na seznamu přinejmenším:

— identifikátor typu služby: 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 služby: (obchodní) název této osvědčovací služby,

— digitální identita služby: jednoznačný jedinečný identifikátor osvědčovací služby,

— aktuální stav služby: identifikátor aktuálního stavu služby,

— datum a čas začátku aktuálního stavu,

▼M3

— rozšíření informací o službě, použije-li se: další informace o službě (např. zahrnuté přímo či odkazem na umístění, odkud lze takové informace stáhnout; informace o vymezení služby poskytované provozovatelem systému, informace o přístupu ke službě, informace o definici služby poskytované ověřovatelem a rozšíření informací o službě. Např. u služeb CA/QC volitelně sekvenci n-tic informací, přičemž každá n-tice uvádí:

— kritéria, která se mají použít pro další identifikaci (filtrování) v rámci identifikované důvěryhodné služby přesně těch výstupů služby (tj. souboru (kvalifikovaných) osvědčení), u níž se požadují/poskytují další informace týkající se jejího stavu, údaje o podpoře prostředkem pro bezpečné vytváření podpisu a/nebo vydání právnické osobě, a

— přidružené „kvalifikátory“ poskytující informace o tom, zda tento soubor výstupů služby identifikuje osvědčení, jež se považují za kvalifikovaná, nebo zda tato identifikovaná kvalifikovaná osvědčení z této služby jsou, či nejsou podporována prostředkem pro bezpečné vytváření podpisu, nebo o tom, zda jsou taková kvalifikovaná osvědčení vydávána právnické osobě (standardně se má za to, že se vydávají fyzickým osobám).

5. U každé osvědčovací služby na seznamu historické informace o jejím stavu

6. Podpis vytvořený počítačem pro účely ověřování pravosti přes všechna pole důvěryhodného seznamu kromě samotného podpisu

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

3.1 *Informace o stavu osvědčovacích služeb, nad nimiž je vykonáván dohled nebo které jsou akreditovány, a jejich poskytovatelů v jediném seznamu*

Důvěryhodným seznamem členského státu se rozumí „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 je jednotný nástroj, který používá příslušný členský stát, aby poskytl informace o stavu dohledu nebo akreditace osvědčovacích služeb a jejich poskytovatelů:

— všech ověřovatelů ve smyslu definice v čl. 2 odst. 11 směrnice 1999/93/ES, tj. „subjektu nebo právnické či fyzické osoby, 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 (pomocné) služby související s elektronickými podpisy“.

▼M3

— **Ověřovatelé vydávající kvalifikovaná osvědčení**:

— 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.

— 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., 11.,12. a 13. bodu odůvodnění).

— **Ověřovatelé, kteří nevydávají kvalifikovaná osvědčení**:

— 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 uvedené směrnice a případně též s vnitrostátními ustanoveními souvisejícími s poskytováním osvědčovacích služeb (ve smyslu čl. 2 odst. 11 směrnice 1999/93/ES).

— 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 takové „kvalifikace“ však bude pravděpodobně omezen pouze na vnitrostátní úroveň.

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. Důvěryhodný seznam musí obsahovat alespoň ověřovatele vydávající kvalifikovaná osvědčení. Důvěryhodný seznam může rovněž uvádět stav jiných ověřovacích služeb, nad nimiž je vykonáván dohled nebo které jsou akreditovány podle vnitrostátně stanoveného schvalovacího systému.

3.2 *Jednotný soubor hodnot stavu dohledu/akreditace*

Na důvěryhodném seznamu je skutečnost, že služba je v současné době buď „podrobena dohledu“ nebo „akreditována“, dána hodnotou jejího současného stavu. Kromě toho může být stav dohledu nebo akreditace pozitivní („pod dohledem“, „akreditována“, „dohled nad ukončovanou službou“), ukončený („dohled ukončen“, „akreditace ukončena“), či dokonce odvolaný („dohled odvolán“, „akreditace odvolána“) a nastaví se na odpovídající hodnotu. V průběhu svého trvání může tatáž osvědčovací služba změnit stav dohledu na stav akreditace a naopak ([1]).

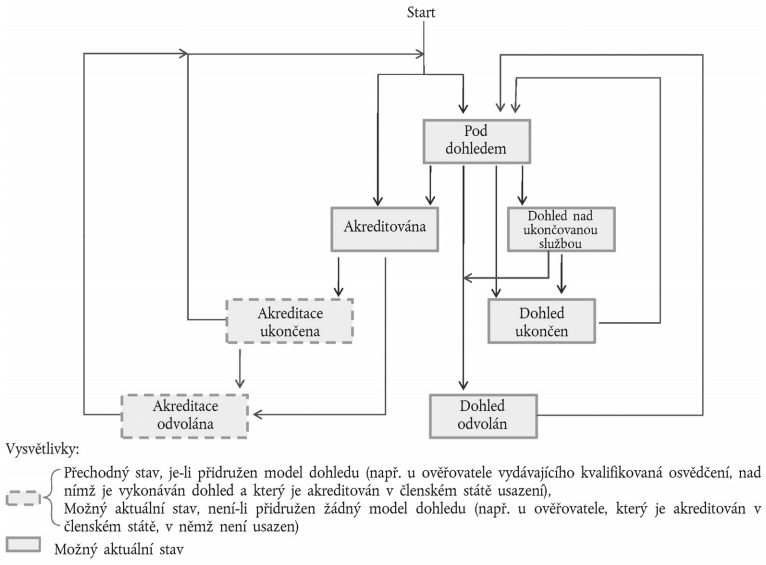
([1]) Např. ověřovatel usazený v členském státě poskytující osvědčovací službu, nad níž zpočátku členský stát (dozorový subjekt) vykonává dohled, se může později rozhodnout, že u stávající dozorované osvědčovací služby přejde k dobrovolné akreditaci. A naopak, ověřovatel v jiném členském státě se může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

▼M3

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

Obrázek 1

Předpokládaný průběh stavu dohledu/akreditace u jediné služby CSP



Pokud je usazena v členském státě, musí být nad osvědčovací službou vydávající kvalifikovaná osvědčení vykonáván dohled (členským státem, v němž je usazena) a může být dobrovolně akreditována. Stav takové služby uvedené v důvěryhodném seznamu musí mít jednu z výše zobrazených hodnot stavu jako „aktuální hodnotu stavu“ v souladu se svým skutečným stavem a musí se případně změnit podle vývoje stavu zobrazeného výše. „Akreditace ukončena“ i „akreditace odvolána“ však musí být hodnotou „přechodný stav“, pokud je odpovídající služba CSP_{QC} uvedena v důvěryhodném seznamu členského státu usazení, neboť nad takovou službou je vykonáván dohled standardně (i když není nebo již není akreditována); pokud je odpovídající služba vedena na seznamu (akreditována) v jiném členském státě, než ve kterém je usazena, mohou být tyto hodnoty hodnotami konečnými.

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 v souladu s ustanoveními směrnice 1999/93/ES a s případnými vnitrostátními ustanoveními souvisejícími s poskytováním osvědčovacích služeb (ve smyslu čl. 2 odst. 11 směrnice 1999/93/ES) musí tyto systémy schválení rozdělit 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., 11.,12. a 13. bod odůvodnění),

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

V souladu s tím může být osvědčovací služba nevydávající kvalifikovaná osvědčení pod dohledem nebo může být dobrovolně akreditována. Stav takové služby uvedené v důvěryhodném seznamu musí mít jednu z výše zobrazených hodnot

▼M3

stav jako svou „aktuální hodnotu stavu“ (viz obrázek 1) v souladu se svým skutečným stavem a musí se případně změnit podle vývoje stavu zobrazeného 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 odkazující na směrnici 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 v příslušných případech poskytnout na úrovni služby (např. pro odlišení různých úrovní kvality/bezpečnosti) prostřednictvím použití rozšíření „*additionalServiceInformation*“ („další informace o službě“, bod 5.5.9.4) 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 tohoto členského státu, předpokládá se, že pro jednu osvědčovací službu musí existovat pouze jediný zápis a že musí být stav jejího dohledu/akreditace odpovídajícím způsobem aktualizován.

3.3 *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 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).

▼M3

Požadované informace by mohly obsahovat jiné informace než „digitální identitu služby“ jediné (kořenové) CA, zejména informace pro identifikaci kvalifikovaného stavu osvědčení vydaných takovou službou CA a informace o tom, zda jsou, či nejsou vytvořeny podpisy podporované prostředkem pro bezpečné vytváření podpisu. Subjekt, který je v členském státě pověřen zřízením, úpravou a údržbou důvěryhodného seznamu, musí tedy zohlednit aktuální profil a obsah osvědčení v každém vydaném kvalifikovaném osvědčení u služby CSP_{QC}, kteří jsou uvedeni v důvěryhodném seznamu.

V ideálním případě by každé vydané kvalifikované osvědčení mělo obsahovat prohlášení o shodě kvalifikovaného osvědčení (QcCompliance) ([1]) 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 EN 319 411-2 ([2]). 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“) u zápisu služby v důvěryhodném seznamu informacemi uvedenými v poli „Rozšíření informací o službě“ („*Service information extensions*“, „Sie“) umožňuje plně stanovit zvláštní typ kvalifikovaného osvědčení vydaného ověřovatelem ze seznamu vydávajícím kvalifikovaná osvědčení a poskytuje informace o tom, zda je, či není podporováno prostředkem pro bezpečné vytváření podpisu (jestliže tato informace ve vydaném kvalifikovaném osvědčení chybí). S tímto zápisem je 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, nebo není 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 se uvedlo, že taková kvalifikovaná osvědčení musí být považována za podporovaná prostředkem pro bezpečné vytváření podpisu, mělo by se použít pole „Sie“ (to rovněž znamená, že tyto informace jsou zaručeny ověřovateli vydávajícími kvalifikovaná osvědčení, nad nimiž dozorový subjekt vykonává dohled nebo kteří jsou akreditováni akreditačním subjektem).

([1]) Viz ETSI EN 319 412-5 (Electronic Signatures and Infrastructures (ESI): Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile), pokud jde o definici takového prohlášení.

([2]) ETSI EN 319 411-2 – Electronic Signatures and Infrastructures (ESI): Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

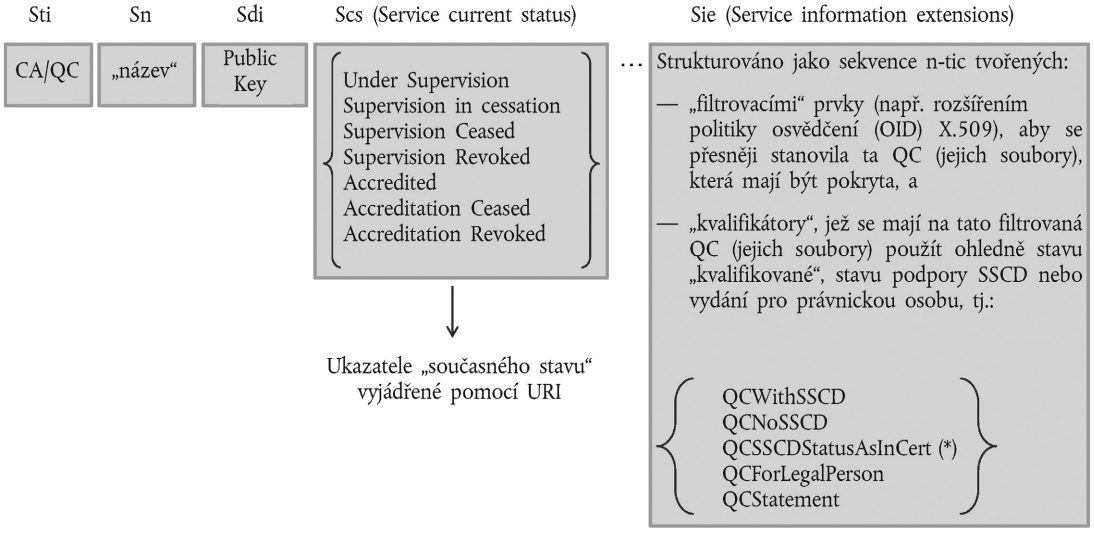
▼M3

Obrázek 2

Zápis o službě u služby ověřovatele vydávajícího kvalifikovaná osvědčení a zapsaného na důvěryhodném seznamu

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

Zápis o službě CSP_{QC} na seznamu:



(*) znamená, že je zajištěno, že tyto informace jsou obsaženy v každém QC v rámci Sdi-[Sie] definované CA/QC (pokud v QC není uvedeno nic, je význam NoSSCD)

Tyto technické specifikace pro společnou šablonu důvěryhodných seznamů umožňují zkombinovat v zápisu o službě pět hlavních částí informací:

— „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) veřejný klíč certifikační autority vydávající kvalifikovaná osvědčení,

— u služeb CA/QC volitelné informace „Rozšíření informací o službě“ („Sie“), které umožní zahrnutí řady specifických informací souvisejících se službou týkajících se stavu zrušení u osvědčení, jejichž doba platnosti vypršela, další znaky kvalifikovaných osvědčení, převzetí ověřovatele jiným ověřovatelem a další dodatečné informace o službě. Například dodatečné znaky kvalifikovaných osvědčení jsou zastoupeny sekvencí 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 „kvalifikovaném“ stavu, podpoře prostředkem pro bezpečné vytváření podpisu (nebo vydání pro právnickou osobu), a

  — přidružené informace („kvalifikátory“) o tom, zda se tento soubor kvalifikovaných osvědčení považuje za „kvalifikovaný“, zda je, nebo není 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

▼M3

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.

3.4 *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 a/nebo QCP OID a neobsahuje 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 osvědčení podporované prostředkem pro bezpečné vytváření podpisu NEOBSAHUJE 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 kvalifikaci. To bude pravděpodobně vyžadovat, aby byly při využívání pole „Sie“ zahrnuty pro totéž „Sdi“ různé „hodnoty informací o podpoře prostředkem pro bezpečné vytváření podpisu“.

▼M3

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 jeden veřejný klíč, tj. na certifikační autoritu (přímo) vydávající kvalifikovaná osvědčení. Za určitých výjimečných okolností a v pečlivě řízených podmínkách může kontrolní subjekt/akreditační orgán členského státu rozhodnout, že se jako „Sdi“ použije jediný zápis v seznamu služeb od tohoto ověřovatele na seznamu, veřejný klíč kořenové CA nebo CA vyšší úrovně v rámci PKI ověřovatele (např. v rámci hierarchie ověřovatelových CA od kořenové CA k několika vydávajícím CA) namísto uvádění všech podřízených vydávajících služeb CA (tj. zařazení na seznam certifikační autority nevydávající kvalifikovaná osvědčení přímo pro koncové subjekty, ale osvědčující hierarchii CA k CA vydávajícím kvalifikovaná osvědčení pro koncové subjekty). Důsledky (výhody a nevýhody) použití takového veřejného klíče kořenové CA nebo vyšší CA jako hodnoty „Sdi“ v zápisech o službách v důvěryhodném seznamu musí členské státy při provádění pečlivě zvážit. Navíc musí členské státy při použití této povolené výjimky ze standardní zásady poskytnout dokumentaci potřebnou pro usnadnění zřízení a ověření cesty osvědčení. Například 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 žádné z kvalifikovaných osvědčení vydané v rámci této hierarchie kořenové CA není podporováno prostředkem pro bezpečné vytváření podpisu. Pokud existují kvalifikovaná osvědčení, která jsou skutečně podporována prostředkem pro bezpečné vytváření podpisu, avšak bez strojově zpracovatelného prohlášení o této podpoře obsažené v osvědčení, důrazně se doporučuje využít prohlášení QcSSCD v kvalifikovaných osvědčeních vydávaných v budoucnosti. Prozatím (dokud nebude ukončena platnost posledního kvalifikovaného osvědčení, které neobsahuje tyto informace) by měl věrohodný seznam využívat pole „Sie“ a přidružené rozšíření „*Qualifications Extension*“, např. poskytovat filtrování informací s cílem identifikovat soubor či soubory 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 některých nikoli), a přidružit výslovné „Informace o podpoře prostředkem pro bezpečné vytváření podpisu“ („*SSCD support information*“) k těmto identifikovaným (filtrovaným) osvědčením za použití „Kvalifikátorů“ („*Qualifiers*“).

Obecné pokyny k použití aplikací, služeb nebo produktů elektronického podpisu, které jsou založeny na důvěryhodném seznamu odpovídajícímu těmto technickým specifikacím, 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 příslušném strojem zpracovatelném prohlášení QcStatement (tj. QcCompliance) nebo v ETSI definovaných QCP (+) OID (a to je zajištěno dozorovým/akreditačním subjektem, viz „obecné pokyny k úpravě“ výše).

Pozn.: Není-li v „Sie“ uvedena žádná informace o „rozšíření kvalifikací“ nebo pokud osvědčení koncového subjektu vydávané za kvalifikované osvědčení není „dále identifikováno“ prostřednictvím souvisejících „rozšíření kvalifikací“ 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. QcCompliance, QcSSCD) nebo ETSI definovaných QCP (+) OID je zajištěno, že jsou v souladu s tím, co tvrdí CSP_{QC};

▼M3

— a JESTLIŽE je informace o „rozšíření kvalifikací“ v „Sie“ přítomna, pak – navíc k výše uvedenému pravidlu výkladu standardního použití – se ta osvědčení, která jsou identifikována použitím této informace o „rozšíření kvalifikace“ v „Sie“, která je postavena na zásadě sekvence „filtrů“, jež dále identifikují soubor osvědčení, musí posuzovat podle přidružených „kvalifikátorů“ poskytujících další informace o kvalifikovaném stavu, „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 označení kvalifikovaného stavu: prohlášení „QCStatement“, jímž se rozumí, že označené osvědčení či označená osvědčení je (jsou) kvalifikované (kvalifikovaná),

NEBO

— 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“.

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

Služby ověřování platnosti stavu osvědčení související s kvalifikovanými osvědčeními, u nichž jsou informace o platnosti stavu osvědčení (např. CRL a odpovědi OCSP) podepsány subjektem, jehož soukromý klíč není osvědčen v rámci osvědčovacího postupu vedoucího k CA zařazené na seznam, jež vydává kvalifikovaná osvědčení („CA/QC“), se zařadí do důvěryhodného seznamu uvedením těchto služeb ověřování platnosti stavu osvědčení jako takových v důvěryhodném seznamu (tj. s typem služby „OCSP/QC“ nebo „CRL/QC“), neboť tyto služby mohou být považovány za součást „kvalifikovaných“ služeb, nad nimiž je vykonáván dohled nebo které jsou akreditovány v souvislosti s poskytováním osvědčovacích služeb QC. Odpovídající subjekty protokolu OCSP nebo vydavatelé CRL, jejichž osvědčení jsou podepsána CA v rámci hierarchie služeb CA/QC uvedených na seznamu, se samozřejmě 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 (typ služby „CA/PKC“).

Důvěryhodný seznam musí obsahovat služby ověřování stavu platnosti osvědčení, pokud související informace o umístění takových služeb nejsou obsaženy v osvědčeních pro koncové subjekty, na něž se vztahují služby ověřování stavu platnosti osvědčení.

▼M3

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	1) ověřovatel, který vytváří a přiděluje osvědčení pro veřejný klíč. nebo 2) služba vytváření technického osvědčení, kterou používá ověřovatel vytvářející a přiřazující osvědčení pro veřejný klíč. *POZN.*: Viz bod 4 normy EN 319 411-2 ([1]) pro další vysvětlení pojmu certifikační autority.
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.
Dohled	Dohled	Týká se dohledu ve smyslu čl. 3 odst. 3 směrnice 1999/93/ES. Směrnice 1999/93/ES po členských státech vyžaduje, aby zavedly odpovídající systém, který umožní dohled nad ověřovateli, kteří jsou usazeni na jejich území a kteří vydávají kvalifikovaná osvědčení pro veřejnost, čímž zajistí dohled nad souladem s ustanoveními uvedené 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 119 612.
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 119 612). *POZN.*: Tento termín má širší použití než osvědčovací služby vydávající osvědčení nebo poskytující další služby související s elektronickými podpisy.

▼M3

Výraz	Zkratka	Definice
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, seznamy zneplatněných osvědčení (dále jen „CRL“), tokeny časových razítek (TST) a odpovědi online protokolu o stavu osvědčení (OCSP).
Kvalifikovaný elektronický podpis	QES	AdES podporovaný QC, který je vytvořen prostředkem pro bezpečné vytváření podpisu, 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.

([1]) EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

V následujících kapitolách se výrazy „MUSÍ“, „NESMÍ“, „JE POVINNÉ“, „MĚL BY“, „NEMĚL BY“, „DOPORUČENÝ“, „MŮŽE“ a „VOLITELNÝ“ mají vykládat v souladu s RFC 2119 ([1]).

KAPITOLA I

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

Tyto specifikace se zakládají na specifikacích a požadavcích uvedených v ETSI TS 119 612 v1.1.1 (dále jen „ETSI TS 119 612“).

Není-li v těchto specifikacích uveden žádný specifický požadavek, MUSÍ se plně uplatnit požadavky bodů 5 a 6 ETSI TS 119 612. V případech, kdy jsou v těchto specifikacích uvedeny zvláštní požadavky, MUSÍ mít přednost před odpovídajícími požadavky ETSI TS 119 612. V případě nesrovnalostí mezi těmito specifikacemi a specifikacemi ETSI TS 119 612 jsou normativní tyto specifikace.

Scheme operator name (bod 5.3.4)

Toto pole JE POVINNÉ a MUSÍ být v souladu se specifikacemi bodu 5.3.4 TS 119 612.

Země MŮŽE mít odlišné subjekty pro dohled a pro akreditaci, a dokonce i další subjekty pro jakékoli související provozní činnosti. Je na každém členském státě, aby určil provozovatele systému důvěryhodného seznamu členského státu.

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

▼M3

Očekává se, že dozorový subjekt, akreditační subjekt a provozovatel systému (pokud jde o samostatné subjekty) budou mít každý své vlastní povinnosti a závazky.

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

Scheme name (bod 5.3.6)

Toto pole JE POVINNÉ a MUSÍ být v souladu se specifikacemi bodu 5.3.6 TS 119 612, kde se pro systém MUSÍ použít tento název:

„EN_název_hodnota“= „seznam stavu dohledu/akreditace osvědčovacích služeb ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni odkazovaným členským státem provozovatele systému 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“.

Scheme information URI (bod 5.3.7)

Toto pole JE POVINNÉ a MUSÍ být v souladu se specifikacemi bodu 5.3.7 TS 119 612, kde „vhodné informace o systému“ MUSÍ zahrnovat přinejmenším:

— Úvodní informace společné pro všechny členské státy, týkající se rozsahu působnosti a kontextu důvěryhodného seznamu a souvisejících systémů dohledu/akreditace. Společný text, který má být použit, je text níže, v němž řetězec znaků „[*název příslušného členského státu*]“ MUSÍ být nahrazen názvem příslušného členského státu:

„Tento seznam je „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 [*název příslušného členského státu*] 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.

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 důvěryhodnou 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, pokud to není součástí kvalifikovaných osvědčení, informací o kvalifikovaných osvědčeních podporujících elektronický podpis a o tom, zda je podpis vytvořen prostředkem pro bezpečné vytváření podpisu, či nikoli.

▼M3

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 souladu s požadavky 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 důvěryhodného seznamu zařazeny 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 zásadně důležité pro to, aby mohly strany spoléhající se na osvědčení posoudit úroveň kvality a bezpečnosti systémů dohledu/akreditace použitých na ověřovatele nevydávající kvalifikovaná osvědčení. 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).

▼M3

Členské státy MOHOU dále o systémech dobrovolně poskytnout dodatečné specifické informace, například:

— 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.

Scheme type/community/rules (bod 5.3.9)

Toto pole JE POVINNÉ být aktuální a MUSÍ být v souladu se specifikacemi bodu 5.3.9 TS 119 612 a MUSÍ zahrnovat nejméně dva URI:

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

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

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 se také odkazuje v seznamu odkazů (ukazatelů) na provedení důvěryhodných seznamů jednotlivých členských států vypracovaném Komisí.

Politiky/pravidla pro posuzování služeb uvedených na seznamu

Důvěryhodný seznam členského státu musí poskytovat 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.

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 souladu s požadavky 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 důvěryhodného seznamu zařazeny dobrovolně na vnitrostátní úrovni.

▼M3

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 1999/93/ES). 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

Obecné pokyny pro uživatele aplikací, služeb nebo produktů elektronického podpisu, které jsou založeny na důvěryhodném seznamu 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. QcCompliance, QcSSCD, atd.) definovaných EN 319 412-5 nebo QCP (+) OID definovaných EN 319 411-2 (a toto je zaručeno vydávajícím ověřovatelem a zajištěno dozorovým/akreditačním subjektem)

  Pozn.: Není-li v „Sie“ uvedena žádná informace o „rozšíření kvalifikací“ nebo pokud osvědčení koncového subjektu vydávané za kvalifikované osvědčení není „dále identifikováno“ prostřednictvím souvisejících informací o „rozšíření kvalifikací“ 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. QcCompliance, QcSSCD atd.) nebo ETSI definovaných QCP (+) OID je zajištěno, že jsou v souladu s tím, co tvrdí CSP_{QC}.

— a JESTLIŽE je informace o „rozšíření kvalifikací“ v „Sie“ přítomna, pak – navíc k výše uvedenému pravidlu výkladu standardního použití – se ta osvědčení, která jsou identifikována použitím této informace o „rozšíření kvalifikace“ v „Sie“, která je postavena na zásadě sekvence „filtrů“, jež dále identifikují soubor osvědčení, musí posuzovat podle přidružených „kvalifikátorů“ poskytujících další informace o kvalifikovaném stavu, „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 označení kvalifikovaného stavu: prohlášení „QCStatement“, jímž se rozumí, že označené osvědčení či označená osvědčení je (jsou) kvalifikované (kvalifikovaná);

▼M3

NEBO

— 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/komunita/pravidla systému“.

Další podrobnosti ohledně polí, popisu a významu důvěryhodných seznamů členských států viz technické specifikace společné šablony „Důvěryhodného seznamu ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni“ v příloze rozhodnutí Komise 2009/767/ES.“

— 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/TrustedList/schemerules/CC, kde CC = kód země ve formátu ISO 3166-1 ([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 důvěryhodného seznamu s ohledem na osvědčovací služby, které nesouvisejí s vydáváním kvalifikovaných osvědčení. Lze jej využít k poukázání na možnou nesourodost

([1]) ISO 3166-1:2006: „Kódy pro názvy zemí a jejich částí. Část 1: Kódy zemí“.

▼M3

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*“ (bod 5.5.9).

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

TSL policy/legal notice (bod 5.3.11)

Toto pole JE POVINNÉ a MUSÍ být v souladu se specifikacemi z bodu 5.3.11 TS 119 612, kde oznámení/právní upozornění o právním postavení systému nebo o zákonných požadavcích, které musí systém splňovat v rámci jurisdikce, v níž je usazen, nebo o jakýchkoli omezeních a podmínkách, za nichž je důvěryhodný seznam udržován nebo zveřejňován, MUSÍ být vícejazyčný řetězec znaků (prostý text) složený ze dvou částí:

1. V první, povinné části společné pro všechny důvěryhodné seznamy členských států (s povinným jazykem britskou angličtinou 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 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 Českou republiku 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 České republiky].

2. Ve druhé, volitelné části specifické pro jednotlivé důvěryhodné seznamy (s povinným jazykem britskou angličtinou 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 nevydávající kvalifikovaná osvědčení).

KAPITOLA II

KONTINUITA DŮVĚRYHODNÝCH SEZNAMŮ

Osvědčení, která se Komisi oznamují podle čl. 3 písm. c) tohoto rozhodnutí, MUSÍ být vystavena tak, aby:

— měla minimálně tři měsíce mezi svými daty platnosti,

— byla vytvořena na nových párech klíčů, neboť žádný dříve použitý pár klíčů nesmí být znovu osvědčen.

V případě prozrazení či vyřazení JEDNOHO ze soukromých klíčů odpovídajícího veřejnému klíči, který by mohl být použit pro validaci podpisu z důvěryhodného

▼M3

seznamu a který byl oznámen Evropské komisi a je zveřejněn v ústředních seznamech ukazatelů Komise, MUSÍ členské státy:

— neprodleně znovu vydat nový důvěryhodný seznam podepsaný neprozrazeným soukromým klíčem v případě, že zveřejněný důvěryhodný seznam byl podepsán prozrazeným nebo vyřazeným soukromým klíčem,

— neprodleně oznámit Komisi nový seznam osvědčení pro veřejný klíč odpovídajících soukromým klíčům, které by mohly být využity k podpisu důvěryhodného seznamu.

V případě prozrazení či vyřazení VŠECH soukromých klíčů odpovídajících veřejným klíčům, které by mohl být použity pro validaci podpisu z důvěryhodného seznamu a které byly oznámeny Evropské komisi a jsou zveřejněny v ústředních seznamech ukazatelů Komise, MUSÍ členské státy:

— vytvořit nové páry klíčů, které by mohly být použity k podpisu důvěryhodného seznamu, a jejich odpovídající osvědčení pro veřejný klíč,

— neprodleně znovu vydat nový důvěryhodný seznam podepsaný jedním z těchto nových soukromých klíčů a jehož příslušné osvědčení pro veřejný klíč má být oznámeno,

— neprodleně oznámit Komisi nový seznam osvědčení pro veřejný klíč odpovídajících soukromým klíčům, které by mohly být využity k podpisu důvěryhodného seznamu.

KAPITOLA III

SPECIFIKACE PRO OKEM ČITELNOU PODOBU DŮVĚRYHODNÉHO SEZNAMU

Pokud je sestavena a zveřejněna podoba důvěryhodného seznamu čitelná okem, MĚLA BY být poskytnuta v podobě dokumentu PDF podle normy ISO 32000 ([1]), který MUSÍ mít formát podle profilu PDF/A (ISO 19005 ([2])).

Obsah okem čitelné podoby důvěryhodného seznamu na základě PDF/A BY MĚL splňovat tyto požadavky:

— struktura okem čitelné podoby BY MĚLA odrážet logický model popsaný v TS 119 612,

— 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“),

  — případně význam (popis) hodnoty pole (např. „certifikační autorita vydávající osvědčení pro veřejný klíč“),

  — je-li to třeba, znění v několika přirozených jazycích podle důvěryhodného seznamu,

— 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

([1]) ISO 32000-1:2008: Document management – Portable document format – Part 1: PDF 1.7.

([2]) ISO 19005-2:2011: Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2).

▼**M3**

— Vydavatel

— Platnost od

— Platnost 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 čitelná podoba MUSÍ být podepsána provozovatelem systému podle výchozího profilu pro podpisy PAdES ([1]).

([1]) ETSI TS 103 172 (March 2012) - Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.