ROZHODNUTÍ KOMISE

ze dne 28. července 2010,

kterým se mění rozhodnutí 2009/767/ES, co se týče zřízení, údržby a zveřejnění důvěryhodných seznamů ověřovatelů, nad nimiž je vykonáván dohled nebo kteří jsou akreditováni členskými státy

(oznámeno pod číslem K(2010) 5063)

(Text s významem pro EHP)

(2010/425/EU)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

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) Přeshraniční používání zaručených elektronických podpisů založených na kvalifikovaném osvědčení a vytvořených s prostředkem pro bezpečné vytváření podpisu nebo bez něj bylo usnadněno rozhodnutím Komise 2009/767/ES 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 [2], jež zavazuje členské státy, aby zpřístupnily informace potřebné pro ověřování elektronických podpisů. Členské státy musí zvláště v takzvaných „důvěryhodných seznamech" zpřístupnit informace o ověřovatelích, kteří vydávají kvalifikovaná osvědčení pro veřejnost v souladu se směrnicí Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy [3] a nad nimiž vykonávají dohled nebo jež akreditovaly, a o jejich nabízených službách.

(2) Ve spolupráci s Evropským ústavem pro telekomunikační normy (ETSI) byla podniknuta řada praktických zkoušek, aby se členským státům umožnilo ověřit, zda jsou jejich důvěryhodné seznamy v souladu se specifikacemi stanovenými v příloze rozhodnutí 2009/767/ES. Tyto zkoušky ukázaly, že k zajištění funkčních a interoperabilních důvěryhodných seznamů je třeba učinit technické změny technických specifikací v příloze rozhodnutí 2009/767/ES.

(3) Tyto zkoušky také potvrdily potřebu, aby členské státy zpřístupnily veřejnosti nejen verze důvěryhodných seznamů čitelné okem, jak vyžaduje rozhodnutí 2009/767/ES, ale také jejich strojově zpracovatelné podoby. Pokud mají členské státy velký počet ověřovatelů, manuální používání okem čitelné podoby provedení důvěryhodných seznamů může být poměrně složité a časově náročné. Zveřejňování strojově zpracovatelných podob důvěryhodných seznamů usnadní jejich používání tím, že umožní jejich automatizované zpracování, čímž rozšíří jejich používání ve veřejných elektronických službách.

(4) K usnadnění přístupu k vnitrostátním důvěryhodným seznamům by členské státy měly oznámit Komisi informace týkající se umístění a ochrany jejich důvěryhodných seznamů. Komise by měla tuto informaci zabezpečeným způsobem zpřístupnit ostatním členským státům.

(5) Výsledky těchto praktických zkoušek důvěryhodných seznamů členských států by měly být zohledněny, aby se umožnilo automatické používání těchto seznamů a usnadnil se k nim přístup.

(6) Rozhodnutí 2009/767/ES by proto mělo být odpovídajícím způsobem změněno.

(7) Aby se členským státům umožnilo provést do jejich současných důvěryhodných seznamů požadované technické změny, bude vhodné použít toto rozhodnutí od 1. prosince 2010.

(8) Opatření tohoto rozhodnutí jsou v souladu se stanoviskem výboru pro směrnici o službách,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Změny rozhodnutí 2009/767/ES

Rozhodnutí 2009/767/ES se mění takto:

[1] Úř. věst. L 376, 27.12.2006, s. 36.
[2] Úř. věst. L 274, 20.10.2009, s. 36.
[3] Úř. věst. L 13, 19.1.2000, s. 12.

1) Článek 2 se mění takto:

a) Odstavec 2 se nahrazuje tímto:

„2. Členské státy zřídí a zveřejní důvěryhodný seznam jak v podobě čitelné okem, tak ve strojově zpracovatelné podobě, a to v souladu se specifikacemi stanovenými v příloze.“

b) Vkládá se nový odstavec 2a, který zní:

„2a. Členské státy strojově zpracovatelnou podobu svého důvěryhodného seznamu elektronicky podepíší a podobu důvěryhodného seznamu čitelnou okem přinejmenším zveřejní prostřednictvím bezpečného kanálu, aby se zajistila pravost a neporušenost seznamu.“

c) Odstavec 3 se nahrazuje tímto:

„3. Členské státy oznámí Komisi tyto informace:

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

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

c) osvědčení pro veřejný klíč používané k provedení bezpečného kanálu, kterým je zveřejňována okem čitelná podoba důvěryhodného seznamu, nebo pokud je okem čitelná podoba seznamu elektronicky podepsána, osvědčení pro veřejný klíč, které bylo použito k podpisu;

d) osvědčení pro veřejný klíč použité k elektronickému podpisu strojově zpracovatelné podoby důvěryhodného seznamu;

e) jakékoli změny údajů v písmenech a) až d).“

d) Doplňuje se nový odstavec 4, který zní:

„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.“

2) Příloha se mění v souladu s přílohou tohoto rozhodnutí.

Článek 2

Použití

Toto rozhodnutí se použije ode dne 1. prosince 2010.

Článek 3

Určení

Toto rozhodnutí je určeno členským státům.

V Bruselu dne 28. července 2010.

Za Komisi

Michel BARNIER

člen Komise

PŘÍLOHA

Příloha rozhodnutí 2009/767/ES se mění takto:

1) Kapitola I se mění takto:

a) Ve druhém pododstavci se první a druhá věta nahrazují tímto:

„Tyto specifikace se zakládají na specifikacích a požadavcích uvedených v ETSI TS 102 231 v.3.1.2. Není-li v těchto specifikacích uveden žádný specifický požadavek, MUSÍ se plně uplatnit požadavky ETSI TS 102 231 v.3.1.2.“

b) V oddíle „TSL tag (bod 5.2.1)“ se zrušuje druhý pododstavec.

c) Pododstavec následující po nadpise oddílu „TSL sequence number (bod 5.3.2)“ se nahrazuje tímto:

„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. Při zvýšení hodnoty výše uvedeného tagu „TSL version identifier“ NESMÍ být číslo „1“ znovu použito.“

d) První pododstavec následující po nadpise „TSL type (bod 5.3.3)“ se nahrazuje tímto:

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

e) Třetí pododstavec následující po nadpise „TSL type (bod 5.3.3)“ se nahrazuje tímto:

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

f) Ve druhém pododstavci následujícím po nadpise oddílu „Scheme operator name (bod 5.3.4)“ se druhá věta nahrazuje tímto:

„Je na každém členském státě, aby určil provozovatele systému „Scheme operator“ pro provedení TL členského státu v podobě TSL.“

g) Čtvrtý pododstavec následující po nadpise oddílu „Scheme operator name (bod 5.3.4)“ se nahrazuje tímto:

„Jmenovaný provozovatel systému „Scheme Operator“ (bod 5.3.4) je entitou, která podepisuje TSL.“

h) Čtvrtá odrážka následující po nadpise oddílu „Scheme name (bod 5.3.6)“ se nahrazuje tímto:

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

i) První pododstavec následující po nadpise oddílu „Service type identifier (bod 5.5.1)“ se nahrazuje tímto:

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

j) Pátá odrážka následující po nadpise oddílu „Service current status (bod 5.5.4)“ se nahrazuje tímto:

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

k) Devátá odrážka následující po nadpise oddílu „Service current status (bod 5.5.4)“ se nahrazuje tímto:

„— **Dohled nad ukončovanou službou:** Služba identifikovaná v „Service digital identity“ (bod 5.5.3) poskytovaná ověřovatelem („CSP“) 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 („CSP“)) v „Scheme service definition URI“ (bod 5.5.6) a v rozšíření „TakenOverBy“ (bod L.3.2) zápisu o službě.“

l) Pátý pododstavec následující po nadpise oddílu „Service information extensions (bod 5.5.9)“ se nahrazuje tímto:

„V kontextu provedení XML musí být specifický obsah takových dalších informací šifrován za použití souborů xsd uvedených v příloze C ETSI TS 102 231.“

m) Oddíl nazvaný „Service digital identity (bod 5.6.3)“ se nahrazuje tímto:

„Service digital identity (bod 5.6.3)

Toto pole je POVINNÉ a specifikuje přinejmenším jedno zastoupení digitálního identifikátoru (tj. osvědčení X.509v3) používaného v „TSP Service Information – Service digital identity“ (bod 5.5.3), ve stejném formátu a se stejným významem, jak je definuje ETSI TS 102 231, bod 5.5.3.

Poznámka: Pro hodnotu osvědčení X.509v3 používanou v „Sdi“ (bod 5.5.3) služby musí existovat pouze jediný zápis o službě v důvěryhodném seznamu na hodnotu „Sti:Sie/additionalServiceInformation“. Informace „Sdi“ (bod 5.6.3) používaná v informacích o historii schválení služby spojených se zápisem o službě a informace „Sdi“ (bod 5.5.3) použitá v tomto zápise o službě se MUSÍ vztahovat k téže hodnotě osvědčení X.509v3. Pokud se u služby uvedené na seznamu mění „Sdi“ (tj. obnovení nebo překlíčování osvědčení X.509v3 např. pro CA/PKC nebo CA/QC) nebo se vytváří nové „Sdi“ pro takovou službu, i pokud jsou hodnoty pro spojené „Sti“, „Sn“ a [„Sie“] stejné, znamená to, že „Scheme Operator“ MUSÍ vytvořit zápis o službě odlišný od předchozího zápisu.“

n) Oddíl nazvaný „Signed TSL“ se nahrazuje tímto:

„**Signed TSL**

Okem čitelnou podobu provedení důvěryhodného seznamu v podobě TSL zřízenou podle těchto specifikací a zejména kapitoly IV, BY MĚL podepsat „Scheme operator name“ (bod 5.3.4), aby byla zajištěna pravost a neporušenost seznamu (*). Formát podpisu BY MĚL být PAdES část 3 (ETSI TS 102 778-3 (**)), ale MŮŽE být PAdES část 2 (ETSI TS 102 778-2 (***)) v kontextu zvláštního modelu důvěry založeného na zveřejnění osvědčení používaných k podpisu důvěryhodných seznamů.

Strojově zpracovatelnou podobu provedení důvěryhodného seznamu v podobě TSL zřízenou podle těchto specifikací MUSÍ podepsat „Scheme operator name“ (bod 5.3.4), aby byla zajištěna pravost a neporušenost seznamu. Formát strojově zpracovatelné podoby důvěryhodného seznamu v podobě TSL zřízené podle těchto specifikací, MUSÍ být XML a MUSÍ být v souladu se specifikacemi uvedenými v příloze B a C ETSI TS 102 231.

Formát podpisu MUSÍ být XAdES BES nebo EPES, jak je definují specifikace ETSI TS 101903 pro provedení XML. Takové provedení elektronického podpisu MUSÍ splňovat požadavky uvedené v ETSI TS 102 231 v příloze B (****). Další všeobecné požadavky ohledně tohoto podpisu jsou uvedeny v následujících oddílech.

(*) V případě, že okem čitelná podoba provedení důvěryhodného seznamu v podobě TSL není podepsána, její pravost a neporušenost MUSÍ být zaručena příslušným komunikačním kanálem s rovnocennou úrovní bezpečnosti. Pro tento účel se doporučuje použít TSL (IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2“) a otisk osvědčení kanálu TSL MUSÍ být členským státem zpřístupněn uživatelům TSL mimo pásmo.

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

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

(****) Podpisové osvědčení provozovatele systému je povinné chránit jedním ze způsobů specifikovaných v ETSI TS 101903 a ds:keyInfo by mělo případně obsahovat příslušný řetězec osvědčení.“

o) Druhý pododstavec následující po nadpise oddílu „Scheme identification (bod 5.7.2)“ se nahrazuje tímto:

„V kontextu těchto specifikací MUSÍ přidělený odkaz zahrnovat „TSL type“ (bod 5.3.3), „Scheme name“ (bod 5.3.6) a hodnotu rozšíření SubjectKeyIdentifier osvědčení použitého provozovatelem systému „Scheme operator“ k elektronickému podepsání TSL.“

p) Druhý pododstavec následující po nadpise oddílu „Rozšíření additionalServiceInformation (bod 5.8.2)“ se nahrazuje tímto:

„Nepřímý odkaz URI BY MĚL vést k okem čitelné podobě informací (minimálně v EN a volitelně v jednom či více národních jazycích), které jsou považovány za vhodné a dostatečné k tomu, aby strana spoléhající se na osvědčení porozuměla rozšíření, a které zejména vysvětlují význam daných URI a specifikují možné hodnoty serviceInformation a význam každé hodnoty.“

q) Oddíl nazvaný „Qualifications Extension (clause L.3.1)“ se nahrazuje tímto:

„Qualifications Extension (bod L.3.1)

Popis: Toto pole je VOLITELNÉ, ale MUSÍ být přítomno, je-li jeho použití POVINNÉ, např. u služeb RootCA/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 souvisejicich kvalifikovanch osvédčenich neumožňuji strojově zpracovatelnou identifikaci skutečnosti o tom, zda je kvalifikované osvědčení „QC“ podporováno zařízením pro bezpečné vytváření podpisu „SSCD“.

Je-li toto rozšíření na úrovni služby použito, MUSÍ se použít pouze v poli definovaném v „Service information extension“ (bod 5.5.9) a MUSÍ být v souladu se specifikacemi uvedenými v ETSI TS 102 231 v příloze L.3.1.“

r) Za oddíl Qualifications Extension (bod L.3.1) se doplňuje nový oddíl TakenOverBy Extension (bod L.3.2), který zní:

„TakenOverBy Extension (bod L.3.2)

Popis: Toto rozšíření je VOLITELNÉ, ale MUSÍ být přítomno, pokud službu, která byla původně právní odpovědností CSP, přebírá jiný TSP a jejím účelem je formálně prohlásit právní odpovědnost služby a umožnit ověřovacímu softwaru zobrazit uživateli některou právní podrobnost. Informace poskytnutá v tomto rozšíření MUSÍ být soudržná se souvisejícím použitím bodu 5.5.6 a MUSÍ být v souladu se specifikacemi v ETSI TS 102 231 v příloze L.3.2.“

2) Kapitola II se nahrazuje tímto zněním:

„KAPITOLA II

Při sestavování důvěryhodných seznamů členské státy použijí:

kódy jazyků psané malými písmeny a kódy zemí psané velkými písmeny;

kódy jazyků a zemí podle níže uvedené tabulky.

Pokud je přítomna latinka (se správným kódem jazyka), je latinská transliterace se souvisejícími specifikovanými jazykovými kódy připojena v níže uvedené tabulce.

Zkrácený název (v původním jazyce)	Zkrácený název (v angličtině)	Kód země	Kód jazyka	Poznámky	Latinská transliterace
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	Kód země doporučený EU	el-Latn
España	Spain	ES	es	také katalánština (ca), baskičtina (eu), galicijština (gl)	
France	France	FR	fr		
Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		

Zkrácený název (v původním jazyce)	Zkrácený název (v angličtině)	Kód země	Kód jazyka	Poznámky	Latinská transliterace
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Kód země doporučený EU	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Latinská transliterace: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.“

3) Kapitola III se zrušuje.

4) V kapitole IV se za návětí: „Obsah PDF/A postavený na základě okem čitelné podoby provedení důvěryhodného seznamu v podobě TSL BY MĚL splňovat tyto požadavky:“ vkládá nová odrážka, která zní:

„— název okem čitelné podoby důvěryhodných seznamů bude vytvořen jako sřetězení následujících prvků

— nepovinný obrázek národní vlajky členského státu,

— mezera,

— zkrácený název země v původním jazyce/původních jazycích (jak je uveden v prvním sloupci tabulky v kapitole II),

— mezera,

— „(“,

— zkrácený název země v angličtině (jak je uveden ve druhém sloupci tabulky v kapitole II) uvnitř závorek,

— „):“ jako uzavírající závorka a oddělovací znaménko:

— mezera,

— „Trusted List“,

— nepovinné logo provozovatele systému „Scheme operator“ v daném členském státě.“