# ROZHODNUTIE KOMISIE

## z 28. júla 2010,

## ktorým sa mení a dopĺňa rozhodnutie 2009/767/ES, pokiaľ ide o zostavenie, vedenie a uverejňovanie zoznamov dôveryhodných informácií o poskytovateľoch certifikačných služieb, ktorí sú pod dohľadom členského štátu alebo sú v ňom akreditovaní

*[oznámené pod číslom K(2010) 5063]*

**(Text s významom pre EHP)**

(2010/425/EÚ)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

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

keďže:

(1) Cezhraničné využívanie zdokonaleného elektronického podpisu založeného na kvalifikovanom certifikáte, vytvoreného bezpečným zariadením na vytvorenie podpisu alebo bez neho, bolo uľahčené rozhodnutím Komisie 2009/767/ES zo 16. októbra 2009, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu [2], na základe ktorého sú členské štáty povinné sprístupniť informácie, ktoré sú potrebné na overenie elektronického podpisu. Členské štáty musia vo svojich tzv. zoznamoch dôveryhodných informácií sprístupniť predovšetkým informácie o poskytovateľoch certifikačných služieb pod dohľadom členského štátu alebo v ňom akreditovaných, ktorí vydávajú kvalifikované certifikáty verejnosti v súlade so smernicou Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy [3], a o službách, ktoré poskytujú.

(2) V Európskom inštitúte pre telekomunikačné normy (European Telecommunications Standards Institute – ETSI) boli vykonané viaceré praktické testy, aby sa členským štátom umožnila kontrola zhody ich zoznamov dôveryhodných informácií so špecifikáciami uvedenými v prílohe k rozhodnutiu 2009/767/ES. Tieto testy ukázali, že je potrebné vykonať niekoľko zmien technických špecifikácií v prílohe k rozhodnutiu 2009/767/ES, aby sa zaistila funkčnosť a interoperabilita zoznamov dôveryhodných informácií.

(3) Týmito testami sa takisto potvrdilo, že je potrebné, aby členské štáty sprístupnili verejnosti nielen verzie svojich zoznamov dôveryhodných informácií čitateľné ľudským okom v súlade s rozhodnutím 2009/767/ES, ale aj v ich strojovo spracovateľnej podobe. Manuálne používanie podoby zoznamov dôveryhodných informácií čitateľných ľudským okom môže byť relatívne komplexné a časovo náročné, ak v členských štátoch pôsobí vysoký počet poskytovateľov certifikačných služieb. Uverejňovaním zoznamov dôveryhodných informácií v strojovo spracovateľnej podobe sa uľahčí ich používanie, umožní sa ich automatizované spracovanie, čím sa rozšíri ich využívanie vo verejných elektronických službách.

(4) Aby sa uľahčil prístup k vnútroštátnym zoznamom dôveryhodných informácií, členské štáty by mali oznámiť Komisii informácie týkajúce sa lokality, kde sa zoznamy nachádzajú, a ich ochrany. Tieto informácie by Komisia mala sprístupniť ostatným členským štátom bezpečným spôsobom.

(5) Výsledky týchto praktických testov zoznamov dôveryhodných informácií členských štátov by sa mali zohľadniť, aby sa umožnilo automatizované používanie týchto zoznamov a uľahčil sa k nim prístup.

(6) Rozhodnutie 2009/767/ES by sa preto malo zodpovedajúcim spôsobom zmeniť a doplniť.

(7) S cieľom umožniť členským štátom vykonať technické zmeny v súčasných zoznamoch dôveryhodných informácií je vhodné, aby sa rozhodnutie uplatňovalo od 1. decembra 2010.

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

PRIJALA TOTO ROZHODNUTIE:

*Článok 1*

**Zmeny a doplnenia rozhodnutia 2009/767/ES**

Rozhodnutie 2009/767/ES sa mení a dopĺňa takto:

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

1. Článok 2 sa mení a dopĺňa takto:

a) Odsek 2 sa nahrádza takto:

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

b) Vkladá sa tento odsek 2a:

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

c) Odsek 3 sa nahrádza takto:

„3. Členské štáty oznamujú Komisii tieto informácie:

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

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

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

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

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

d) Dopĺňa sa tento odsek 4:

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

2. Príloha sa mení a dopĺňa v súlade s prílohou k tomuto rozhodnutiu.

*Článok 2*

**Uplatňovanie**

Toto rozhodnutie sa uplatňuje od 1. decembra 2010.

*Článok 3*

**Adresáti**

Toto rozhodnutie je určené členským štátom.

V Bruseli 28. júla 2010

*Za Komisiu*

Michel BARNIER

*člen Komisie*

*PRÍLOHA*

Príloha k rozhodnutiu 2009/767/ES sa mení a dopĺňa takto:

1. Kapitola I sa mení a dopĺňa takto:

a) Prvá a druhá veta druhého odseku sa nahrádza takto:

„Tieto špecifikácie sú založené na špecifikáciách a požiadavkách uvedených v ETSI TS 102 231 v.3.1.2. Ak sa v týchto špecifikáciách neuvádza žiadna osobitná požiadavka, UPLATŇUJÚ SA požiadavky v ETSI TS 102 231 v.3.1.2 v celom rozsahu."

b) Druhý odsek oddielu „TSL tag (odsek 5.2.1)" sa vypúšťa.

c) Odsek, ktorý nasleduje po názve oddielu „TSL sequence number (odsek 5.3.2)", sa nahrádza takto:

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

d) Prvý odsek, ktorý nasleduje po názve oddielu „TSL type (odsek 5.3.3)", sa nahrádza takto:

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

e) Tretí odsek, ktorý nasleduje po názve oddielu „TSL type (odsek 5.3.3)", sa nahrádza takto:

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

f) Druhá veta druhého odseku, ktorý nasleduje po názve oddielu „Scheme operator name (odsek 5.3.4)", sa nahrádza takto:

„Určenie prevádzkovateľa schémy (scheme operator) TSL implementácie TL členských štátov spadá do kompetencie členských štátov."

g) Štvrtý odsek, ktorý nasleduje po názve oddielu „Scheme operator name (odsek 5.3.4)", sa nahrádza takto:

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

h) Štvrtá zarážka, ktorá nasleduje po názve oddielu „Scheme name (odsek 5.3.6)", sa nahrádza takto:

' "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) Prvý odsek, ktorý nasleduje po názve oddielu „Service type identifier (odsek 5.5.1)", sa nahrádza takto:

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

j) Piata zarážka, ktorá nasleduje po názve oddielu „Service current status (odsek 5.5.4)", sa nahrádza takto:

„— **Akreditácia** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited),".

k) Deviata zarážka, ktorá nasleduje po názve oddielu „Service current status (odsek 5.5.4)", sa nahrádza takto:

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

l) Piaty odsek, ktorý nasleduje po názve oddielu „Service information extensions (odsek 5.5.9)“, sa nahrádza takto:

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

m) Oddiel s názvom „Service digital identity (odsek 5.6.3)“ sa nahrádza takto:

„Service digital identity (odsek 5.6.3).

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

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

n) Oddiel s názvom „Signed TSL“ sa nahrádza takto:

„**Signed TSL**

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

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

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

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

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

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

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

o) Druhý odsek, ktorý nasleduje po názve oddielu „Scheme identification (odsek 5.7.2)“, sa nahrádza takto:

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

p) Druhý odsek, ktorý nasleduje po názve oddielu „rozšírenie additional ServiceInformation (odsek 5.8.2)“ sa nahrádza takto:

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

q) Oddiel s názvom „Qualifications Extension (odsek L.3.1)“ sa nahrádza takto:

„Qualifications Extension (odsek L.3.1)

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

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

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

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

r) Po oddiele Qualifications Extension (odsek L.3.1) sa vkladá tento oddiel TakenOverBy Extension (odsek L.3.2):

„TakenOverBy Extension (odsek L.3.2)

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

2. Kapitola II sa nahrádza takto:

„KAPITOLA II

Členské štáty v rámci zostavovania svojich zoznamov dôveryhodných informácií použijú:

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

kódy jazykov a krajín v súlade s tabuľkou uvedenou nižšie;

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

| Skrátený názov (zdrojový jazyk) | Skrátený názov (angličtina) | Kód krajiny | Kód jazyka | Poznámky | Transliterácia do latinky |
|---|---|---|---|---|---|
| Belgique/België | Belgium | BE | nl, fr, de | | |
| България (*) | Bulgaria | BG | bg | | bg-Latn |
| Česká republika | Czech Republic | CZ | cs | | |
| Danmark | Denmark | DK | da | | |
| Deutschland | Germany | DE | de | | |
| Eesti | Estonia | EE | et | | |
| Éire/Ireland | Ireland | IE | ga, en | | |
| Ελλάδα (*) | Greece | EL | el | kód krajiny, ktorý odporúča EÚ | el-Latn |
| España | Spain | ES | es | aj katalánčina (ca), baskičtina (eu), galícijčina (gl) | |
| France | France | FR | fr | | |
| Italia | Italy | IT | it | | |
| Κύπρος/Kıbrıs (*) | Cyprus | CY | el, tr | | el-Latn |
| Latvija | Latvia | LV | lv | | |

| Skrátený názov (zdrojový jazyk) | Skrátený názov (angličtina) | Kód krajiny | Kód jazyka | Poznámky | Transliterácia do latinky |
|---|---|---|---|---|---|
| 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 krajiny, ktorý odporúča EÚ | |
| Ísland | Iceland | IS | is | | |
| Liechtenstein | Liechtenstein | LI | de | | |
| Norge/Noreg | Norway | NO | no, nb, nn | | |

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

3. Kapitola III sa vypúšťa.

4. Do kapitoly IV sa po úvodnej vete: „Obsah formy HR TSL implementácie zoznamu dôveryhodných poskytovateľov vo formáte PDF/A BY MAL spĺňať tieto požiadavky:“ vkladá táto zarážka:

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

— nepovinný obrázok vlajky členského štátu,

— medzera,

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

— medzera,

— ‚(‘,

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

— ‚): ‘ako koniec zátvorky a oddeľovací znak,

— medzera,

— ‚Trusted List‘,

— nepovinné logo prevádzkovateľa schémy členského štátu.“