

PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2015/1505**ze dne 8. září 2015,****kterým se stanoví technické specifikace a formáty důvěryhodných seznamů podle čl. 22 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu****(Text s významem pro EHP)**

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES ⁽¹⁾, a zejména na čl. 22 odst. 5 uvedeného nařízení,

vzhledem k těmto důvodům:

- (1) Důvěryhodné seznamy jsou nezbytné při budování důvěry mezi tržními subjekty, jelikož udávají status poskytovatele služeb v okamžiku dohledu.
- (2) Přeshraniční používání elektronických podpisů bylo usnadněno rozhodnutím Komise 2009/767/ES ⁽²⁾, které pro členské státy zavedlo povinnost zřídit, udržovat a zveřejňovat důvěryhodné seznamy obsahující informace o poskytovatelích certifikačních služeb, kteří vydávají kvalifikované certifikáty pro veřejnost v souladu se směrnicí Evropského parlamentu a Rady 1999/93/ES ⁽³⁾ a nad nimiž vykonávají dohled nebo je akreditovaly členské státy.
- (3) Podle článku 22 nařízení (EU) č. 910/2014 musí členské státy zabezpečeným způsobem zřizovat, udržovat a zveřejňovat důvěryhodné seznamy, které jsou opatřeny elektronickým podpisem nebo elektronickou pečetí, a to ve formě vhodné pro automatické zpracování, a oznámit Komisi subjekty odpovědné za zřízení vnitrostátních důvěryhodných seznamů.
- (4) Poskytovatel služeb vytvářejících důvěru a jím poskytované služby vytvářející důvěru by měly být považovány za kvalifikované, pokud je poskytovateli na důvěryhodném seznamu přiřazen status kvalifikovaného poskytovatele. S cílem zajistit, aby poskytovatelé služeb mohli snadno na dálku a pomocí elektronických prostředků plnit ostatní povinnosti vyplývající z nařízení (EU) č. 910/2014, zejména ty, které jsou stanoveny v člancích 27 a 37, a za účelem naplnění oprávněných očekávání jiných poskytovatelů certifikačních služeb, kteří sice nevydávají kvalifikované certifikáty, avšak poskytují služby související s elektronickými podpisy podle směrnice 1999/93/ES a jsou do 30. června 2016 zahrnuti do seznamu, měly by mít členské státy možnost dobrovolně na vnitrostátní úrovni doplnit na důvěryhodné seznamy služby vytvářející důvěru jiné než kvalifikované, pokud je jasně uvedeno, že nejsou kvalifikované v souladu s nařízením (EU) č. 910/2014.
- (5) V souladu s 25. bodem odůvodnění nařízení (EU) č. 910/2014 mohou členské státy doplnit i jiné typy vnitrostátně definovaných služeb vytvářejících důvěru než ty, které jsou uvedeny v čl. 3 bodu 16 nařízení (EU) č. 910/2014, za předpokladu, že je jasně uvedeno, že nejsou kvalifikované v souladu s nařízením (EU) č. 910/2014.
- (6) Opatření stanovená tímto rozhodnutím jsou v souladu se stanoviskem výboru zřízeného článkem 48 nařízení (EU) č. 910/2014,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Členské státy zřídí, zveřejní a udržují důvěryhodné seznamy obsahující informace o kvalifikovaných poskytovatelích služeb vytvářejících důvěru, nad nimiž vykonávají dohled, jakož i informace o kvalifikovaných službách vytvářejících důvěru, které tyto poskytovatelé poskytují. Tyto seznamy musí být v souladu s technickými specifikacemi stanovenými v příloze I.

⁽¹⁾ Úř. věst. L 257, 28.8.2014, s. 73.

⁽²⁾ Rozhodnutí 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 (Úř. věst. L 274, 20.10.2009, s. 36).

⁽³⁾ Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy (Úř. věst. L 13, 19.1.2000, s. 12).

Článek 2

Členské státy mohou do důvěryhodných seznamů zahrnout informace o nekvalifikovaných poskytovatelích služeb vytvářejících důvěru spolu s informacemi o nekvalifikovaných službách vytvářejících důvěru, které tito poskytovatelé poskytují. Seznam musí jasně uvádět, kteří poskytovatelé služeb vytvářejících důvěru a které jimi poskytované služby vytvářející důvěru nejsou kvalifikované.

Článek 3

1. Podle čl. 22 odst. 2 nařízení (EU) č. 910/2014 opatří členské státy formu vhodnou pro automatické zpracování svých důvěryhodných seznamů elektronickým podpisem nebo elektronickou pečetí v souladu s technickými specifikacemi stanovenými v příloze I.
2. Pokud členský stát elektronicky zveřejní formu důvěryhodného seznamu čitelnou okem, zajistí, aby tato forma důvěryhodného seznamu obsahovala stejné údaje jako forma vhodná pro automatické zpracování, a opatří ji elektronickým podpisem nebo elektronickou pečetí v souladu s technickými specifikacemi stanovenými v příloze I.

Článek 4

1. Členské státy oznámí Komisi údaje uvedené v čl. 22 odst. 3 nařízení (EU) č. 910/2014 za použití šablony v příloze II.
2. Informace uvedené v odstavci 1 zahrnují dva nebo více certifikáty veřejných klíčů provozovatele systému s posunutými dobami platnosti v délce nejméně tří měsíců, které odpovídají soukromým klíčům, jež lze použít pro elektronický podpis nebo elektronickou pečeť u formy důvěryhodného seznamu vhodné pro automatické zpracování a v případě zveřejnění u formy čitelné okem.
3. Podle čl. 22 odst. 4 nařízení (EU) č. 910/2014 zpřístupní Komise veřejnosti bezpečnou cestou na ověřeném webovém serveru informace uvedené v odstavcích 1 a 2 oznámené členskými státy ve formě vhodné pro automatické zpracování opatřené podpisem nebo pečetí.
4. Komise může zpřístupnit veřejnosti bezpečnou cestou na ověřeném webovém serveru informace uvedené v odstavcích 1 a 2 oznámené členskými státy ve formě čitelné okem opatřené podpisem nebo pečetí.

Článek 5

Toto rozhodnutí vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto rozhodnutí je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 8. září 2015.

Za Komisi
předseda
Jean-Claude JUNCKER

PŘÍLOHA I

TECHNICKÉ SPECIFIKACE PRO SPOLEČNOU ŠABLONU DŮVĚRYHODNÝCH SEZNAMŮ

KAPITOLA I

OBECNÉ POŽADAVKY

Důvěryhodné seznamy musí obsahovat jak aktuální informace o statutu služeb vytvářejících důvěru zařazených na seznam, tak i všechny tyto informace z minulosti, počínaje zařazením poskytovatele služeb vytvářejících důvěru na důvěryhodné seznamy.

Pojmy „schválení“, „akreditování“ a/nebo „podléhající dohledu“ v těchto specifikacích se vztahují i na vnitrostátní schvalovací systémy, ale další informace o povaze jakýchkoli takových vnitrostátních systémů poskytnou členské státy ve svém důvěryhodném seznamu, včetně objasnění možných rozdílů oproti systémům dohledu použitelným pro kvalifikované poskytovatele služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru.

Hlavním účelem informací poskytnutých v důvěryhodném seznamu je podpora ověřování tokenů kvalifikovaných služeb vytvářejících důvěru, tj. fyzických nebo binárních (logických) objektů vytvořených nebo vydaných v důsledku použití kvalifikované služby vytvářející důvěru, například kvalifikovaných elektronických podpisů/pečetí, zaručených elektronických podpisů/pečetí podporovaných kvalifikovaným certifikátem, kvalifikovaných časových razítek, kvalifikovaných důkazů o elektronickém doručování atd.

KAPITOLA II

PODROBNÉ SPECIFIKACE PRO SPOLEČNOU ŠABLONU DŮVĚRYHODNÝCH SEZNAMŮ

Tyto specifikace vycházejí ze specifikací a požadavků uvedených v ETSI TS 119 612 v2.1.1 (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 mají přednost tyto specifikace.

Název systému (Scheme name) (bod 5.3.6)

Toto pole je povinné a musí být v souladu se specifikacemi TS 119 612 bodem 5.3.6, kde se pro systém používá tento název:

„EN_name_value“ = „Důvěryhodný seznam obsahující informace o kvalifikovaných poskytovatelích služeb vytvářejících důvěru, nad nimiž vykonává dohled vydávající členský stát, spolu s informacemi o kvalifikovaných službách vytvářejících důvěru poskytovaných těmito poskytovateli, v souladu s příslušnými ustanoveními nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.“

URI informací o systému (Scheme information URI) (bod 5.3.7)

Toto pole je povinné a musí být v souladu se specifikacemi TS 119 612 bodem 5.3.7, kde „vhodné informace o systému“ musí zahrnovat přinejmenším:

- Úvodní informace společné pro všechny členské státy, týkající se rozsahu působnosti a kontextu důvěryhodného seznamu, souvisejícího systému dohledu a případně vnitrostátního schvalovacího systému (vnitrostátních schvalovacích systémů) (např. akreditace). Společný text, který má být použit, je uveden níže, přičemž řetězec znaků „[název příslušného členského státu]“ v něm musí být nahrazen názvem příslušného členského státu:

„Tento seznam je důvěryhodným seznamem obsahujícím informace o kvalifikovaných poskytovatelích služeb vytvářejících důvěru, nad nimiž vykonává dohled [název příslušného členského státu], spolu s informacemi o kvalifikovaných službách vytvářejících důvěru poskytovaných těmito poskytovateli, v souladu s příslušnými ustanoveními nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.“

Přeshraniční používání elektronických podpisů bylo usnadněno rozhodnutím Komise 2009/767/ES ze dne 16. října 2009, které pro členské státy zavedlo povinnost zřídit, udržovat a zveřejňovat důvěryhodné seznamy obsahující informace o poskytovatelích certifikačních služeb, kteří veřejnosti vydávají kvalifikované certifikáty v souladu se směrnicí Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy a nad nimiž vykonávají dohled nebo je akreditovaly členské státy. Tento důvěryhodný seznam je pokračováním důvěryhodného seznamu vypracovaného na základě rozhodnutí 2009/767/ES.“

Důvěryhodné seznamy jsou nezbytnými prvky při budování důvěry mezi tržními subjekty, jelikož uživatelům umožňují určit, zda poskytovatelé služeb vytvářejících důvěru a jimi poskytované služby mají status kvalifikovaných poskytovatelů a kvalifikovaných služeb, a rovněž jim poskytují informace o historii statutu.

Důvěryhodné seznamy členských států obsahují alespoň informace uvedené v člancích 1 a 2 prováděcího rozhodnutí (EU) 2015/1505.

Členské státy mohou do důvěryhodných seznamů zahrnout informace o nekvalifikovaných poskytovatelích služeb vytvářejících důvěru, spolu s informacemi o nekvalifikovaných službách vytvářejících důvěru, které tyto poskytovatele poskytují. Je třeba jasně uvést, že poskytovatelé či služby nejsou kvalifikované v souladu s nařízením (EU) č. 910/2014.

Členské státy mohou do důvěryhodných seznamů zahrnout informace o jiných typech vnitrostátně definovaných služeb vytvářejících důvěru než těch, které jsou uvedeny v čl. 3 bodu 16 nařízení (EU) č. 910/2014. Je třeba jasně uvést, že poskytovatelé či služby nejsou kvalifikované v souladu s nařízením (EU) č. 910/2014.

b) Specifické informace o souvisejícím systému dohledu a případně vnitrostátním schvalovacím systému (vnitrostátních schvalovacích systémech) (např. akreditace), zejména (!):

- 1) informace o vnitrostátním systému dohledu platném pro kvalifikované i nekvalifikované poskytovatele služeb vytvářejících důvěru a jimi poskytované kvalifikované i nekvalifikované služby vytvářející důvěru, jak jsou upraveny nařízením (EU) č. 910/2014;
- 2) případně informace o vnitrostátních systémech dobrovolné akreditace platných pro poskytovatele certifikačních služeb, kteří vydali kvalifikované certifikáty podle směrnice 1999/93/ES.

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

- 1) obecný popis;
- 2) informace o postupu používaném ve vnitrostátním systému dohledu a případně při schvalování podle vnitrostátního schvalovacího systému;
- 3) informace o kritériích, podle nichž poskytovatelé služeb vytvářejících důvěru podléhají dohledu nebo jsou případně schváleni;
- 4) informace o kritériích a pravidlech použitých pro výběr osob vykonávajících dohled/audit a definování toho, jak posuzují služby vytvářející důvěru a jejich poskytovatele;
- 5) případně jiné kontaktní a obecné informace, které se vztahují k fungování systému.

Typ systému/komunita/pravidla (Scheme type/community/rules) (bod 5.3.9)

Toto pole je povinné a musí být v souladu se specifikacemi TS 119 612 bodem 5.3.9.

Zahrnuje pouze jednotné identifikátory zdroje (URI) v britské angličtině.

(!) Tyto soubory informací jsou zásadně důležité pro to, aby mohly spoléhající se strany posoudit úroveň kvality a bezpečnosti takových systémů. Tyto soubory informací se poskytnou na úrovni důvěryhodného seznamu prostřednictvím aktuálních informací v polích „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, společně s možností, aby každý členský stát doplnil svůj specifický text/odkazy). Další informace o takových systémech pro nekvalifikované služby vytvářející důvěru a vnitrostátně definované (kvalifikované) služby vytvářející důvěru lze ve vhodných a požadovaných případech poskytnout na úrovni služby (např. pro odlišení různých úrovní kvality/bezpečnosti) použitím pole „Scheme service definition URI“ (bod 5.5.6).

Musí zahrnovat nejméně dva identifikátory URI:

- 1) URI společný pro všechny důvěryhodné seznamy členských států, který odkazuje na popisný text, jež 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 vypracovat důvěryhodný seznam obsahující informace o kvalifikovaných poskytovatelích služeb vytvářejících důvěru, nad nimiž vykonává dohled, spolu s informacemi o kvalifikovaných službách vytvářejících důvěru poskytovaných těmito poskytovateli, v souladu s příslušnými ustanoveními nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

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

Členské sáty musí vykonávat dohled nad kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými na území členského státu, který provedl určení, jak je stanoveno v kapitole III nařízení (EU) č. 910/2014, s cílem zajistit, aby tito kvalifikovaní poskytovatelé služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru splňovali požadavky stanovené v tomto nařízení.

Důvěryhodné seznamy členských států obsahují alespoň informace uvedené v člancích 1 a 2 prováděcího rozhodnutí (EU) 2015/1505.

Důvěryhodné seznamy obsahují jak aktuální informace o statutu služeb vytvářejících důvěru zařazených na seznam, tak i všechny tyto informace z minulosti.

Každý důvěryhodný seznam členského státu musí uvádět informace o vnitrostátním systému dohledu a případně vnitrostátním schvalovacím systému (vnitrostátních schvalovacích systémech) (např. akreditace), v jejichž rámci jsou poskytovatelé služeb vytvářejících důvěru a jimi poskytované služby vytvářející důvěru uvedeny.

Výklad důvěryhodného seznamu

Obecné pokyny pro uživatele aplikací, služeb nebo produktů, které vycházejí z důvěryhodného seznamu zveřejněného v souladu s nařízením (EU) č. 910/2014, jsou následující:

Status ‚kvalifikované‘ služby vytvářející důvěru je uveden kombinací hodnoty ‚Service type identifier‘ (Identifikátor typu služby, ‚Sti‘) v záznamu o službě a statutu uvedeného v poli ‚Service current status‘ (Aktuální status služby) ode dne uvedeného v poli ‚Current status starting date and time‘ (Datum a čas začátku aktuálního statutu). Případně se rovněž poskytují historické informace o takovém kvalifikovaném statutu.

Pokud jde o kvalifikované poskytovatele služeb vytvářejících důvěru, kteří vydávají kvalifikované certifikáty pro elektronické podpisy, elektronické pečete a/nebo pro autentizaci internetových stránek:

Záznam ‚CA/QC‘ ‚Service type identifier‘ (‚Sti‘) (s možností jeho další kvalifikace jako ‚RootCA-QC‘ pomocí rozšíření informace o službě jako součást ‚Service information extension‘ (‚Sie‘)

— uvádí, že jakýkoliv certifikát koncového subjektu vydaný certifikační autoritou nebo jejím jménem, reprezentovaný identifikátorem ‚Service digital identifier‘ (‚Sdi‘), veřejným klíčem certifikační autority a jejím jménem/názvem (oba údaje o certifikační autoritě se považují za trust anchor input), je kvalifikovaným certifikátem za předpokladu, že obsahuje alespoň jeden z těchto údajů:

- prohlášení id-etsi-qcs-QcCompliance (id-etsi-qcs 1) definované podle ETSI,
- certifikační politika OID 0.4.0.1456.1.1 (QCP+) definovaná podle ETSI,

— certifikační politika OID 0.4.0.1456.1.2 (QCP) definovaná podle ETSI,

a za předpokladu, že toto zajistí orgán dohledu daného členského státu prostřednictvím platného statutu služby (tj. ‚undersupervision‘, ‚supervisionincessation‘, ‚akreditovaný‘ nebo ‚schválený‘).

— **a JESTLIŽE** je uvedena informace ‚Sie‘ ‚Qualifications Extension‘, pak – navíc k výše uvedenému pravidlu standardního použití – se ty certifikáty, které jsou identifikovány použitím informace ‚Sie‘ ‚Qualifications Extension‘, která je postavena na zásadě sekvence ‚filtrů‘, jež dále identifikují soubor certifikátů, musí posuzovat podle přidružených ‚kvalifikátorů‘ poskytujících další informace o kvalifikovaném statutu, ‚podpoře SSCD‘ nebo o ‚právní osobě jako subjektu‘ (např. certifikát obsahující specifický identifikátor OID v rozšíření certifikační politiky a/nebo se specifickým vzorcem ‚použití klíče‘ a/nebo filtrován použitím specifické hodnoty, která se má objevit v jednom specifickém poli nebo rozšíření certifikátu atd.). Tyto kvalifikátory tvoří součást následujícího souboru ‚kvalifikátorů‘ využívaných k vyvážení nedostatku informací v příslušném obsahu kvalifikovaného certifikátu a využívají se:

— k uvedení údajů o povaze kvalifikovaného certifikátu:

— ‚QCStatement‘, což znamená, že označený certifikát (označené certifikáty) je kvalifikovaný (jsou kvalifikované) podle směrnice 1999/93/ES;

— ‚QCForESig‘, což znamená, že označený certifikát (označené certifikáty), pokud je označen či stanoven (jsou označeny či stanoveny) za kvalifikovaný(é), je kvalifikovaným certifikátem (jsou kvalifikovanými certifikáty) pro elektronický podpis podle nařízení (EU) č. 910/2014;

— ‚QCForESeal‘, což znamená, že označený certifikát (označené certifikáty), pokud je označen či stanoven (jsou označeny či stanoveny) za kvalifikovaný(é), je kvalifikovaným certifikátem (jsou kvalifikovanými certifikáty) pro elektronickou pečeť podle nařízení (EU) č. 910/2014;

— ‚QCForWSA‘, což znamená, že označený certifikát (označené certifikáty), pokud je označen či stanoven (jsou označeny či stanoveny) za kvalifikovaný(é), je kvalifikovaným certifikátem (jsou kvalifikovanými certifikáty) pro autentizaci internetových stránek podle nařízení (EU) č. 910/2014;

— k uvedení, že certifikát nelze považovat za kvalifikovaný:

— ‚NotQualified‘, což znamená, že označený certifikát (označené certifikáty) nelze považovat za kvalifikovaný(é) a/nebo

— k uvedení údajů o povaze podpory SSCD:

— ‚QCWithSSCD‘, což znamená, že označený certifikát (označené certifikáty), pokud je označen či stanoven (jsou označeny či stanoveny) za kvalifikovaný(é), mají svůj soukromý klíč v SSCD nebo

— ‚QCNoSSCD‘, což znamená, že označený certifikát (označené certifikáty), pokud je označen či stanoven (jsou označeny či stanoveny) za kvalifikovaný(é), nemá (nemají) svůj soukromý klíč v SSCD nebo

— ‚QCSSCDStatusAsInCert‘, což znamená, že označený certifikát (označené certifikáty), pokud je označen či stanoven (jsou označeny či stanoveny) za kvalifikovaný(é), obsahuje(i) řádné strojově zpracovatelné informace o tom, zda má (mají) či nemá (nemají) svůj soukromý klíč v SSCD;

— k uvedení údajů o povaze podpory QSCD:

— ‚QCWithQSCD‘, což znamená, že označený certifikát (označené certifikáty), pokud je označen či stanoven (jsou označeny či stanoveny) za kvalifikovaný(é), mají svůj soukromý klíč v QSCD nebo

— ‚QCNoQSCD‘, což znamená, že označený certifikát (označené certifikáty), pokud je označen či stanoven (jsou označeny či stanoveny) za kvalifikovaný(é), nemá (nemají) svůj soukromý klíč v QSCD nebo

— ‚QCQSCDStatusAsInCert‘, což znamená, že označený certifikát (označené certifikáty), pokud je označen či stanoven (jsou označeny či stanoveny) za kvalifikovaný(é), obsahuje(i) řádné strojově zpracovatelné informace o tom, zda má (mají) či nemá (nemají) svůj soukromý klíč v QSCD;

— ‚QCQSCDManagedOnBehalf‘, což znamená, že všechny certifikáty označené na základě platného seznamu kritérií, pokud jsou označeny či stanoveny za kvalifikované, mají svůj soukromý klíč v QSCD, kde soukromý klíč vytvoří a spravuje kvalifikovaný TSP jménem subjektu, jehož totožnost je potvrzena v certifikátu a/nebo

— k uvedení údajů o vydání právnické osobě:

- ‚QCForLegalPerson‘, což znamená, že označený certifikát (označené certifikáty), pokud je označen či stanoven (jsou označeny či stanoveny) za kvalifikovaný(é), je vydán (jsou vydány) právnické osobě podle směrnice 1999/93/ES;

Pozn.: Informace poskytnuté v důvěryhodném seznamu lze považovat za správné, což znamená, že:

- pokud nejsou v certifikátu koncového subjektu uvedeny žádné informace o prohlášení id-etsi-qcs 1, QCP OID či QCP+ OID a
- pokud není v záznamu o službě, kterému odpovídá trust anchor CA/QC, uvedena žádná informace ‚Sie‘ ‚Qualifications Extension‘, která kvalifikuje certifikát kvalifikátorem ‚QCStatement‘, nebo
- pokud je v záznamu o službě, kterému odpovídá trust anchor CA/QC, uvedena informace ‚Sie‘ ‚Qualifications Extension‘, která kvalifikuje certifikát kvalifikátorem ‚NotQualified‘,

potom nelze certifikát považovat za kvalifikovaný.

V souvislosti s ověřováním elektronických podpisů či pečeti, v jejichž případě se má certifikát podepisující či pečeti osoby ověřit na základě informací z důvěryhodného seznamu, se jako trust anchor použijí ‚Service digital identifiers‘, což znamená, že jako informace pro trust anchor jsou potřebné jen veřejný klíč a příslušný název subjektu. Pokud je veřejný klíč na identifikaci služby zastoupený víc než jedním certifikátem, musí se tyto certifikáty považovat za certifikáty trust anchor obsahující totožné informace s ohledem na informace, které se vyžadují striktně jako informace pro trust anchor.

Obecné pravidlo výkladu pro jakýkoli jiný záznam typu ‚Sti‘ zní, že identifikovaná služba typu ‚Sti‘ uvedená na seznamu pojmenovaná podle hodnoty pole ‚Service name‘ a jedinečně identifikovaná hodnotou pole ‚Service digital identity‘ má aktuální status kvalifikace či schválení podle hodnoty pole ‚Service current status‘, a to od data uvedeného v položce ‚Current status starting date and time‘.

Specifická pravidla výkladu pro jakékoli další informace týkající se služby uvedené na seznamu (např. pole ‚Service information extensions‘) lze v případě potřeby nalézt na specifickém URI členského státu jako součást uvedeného pole ‚Scheme type/community/rules‘.

Další podrobnosti o polích, popisu a významu důvěryhodných seznamů členských států viz příslušné sekundární právní předpisy podle nařízení (EU) č. 910/2014.“

- 2) URI specifický pro každý důvěryhodný seznam členského státu odkazující na popisný text, který se vztahuje na důvěryhodný seznam tohoto členského státu:

<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC>, kde CC = dvoupísmenný kód země podle ISO 3166-1 ⁽¹⁾ použitý v poli „Scheme territory“ (bod 5.3.10)

- kde mohou uživatelé získat specifické politiky/pravidla příslušného členského státu, podle nichž jsou služby vytvářející důvěru uvedené na seznamu posuzovány z hlediska souladu se systémem dohledu a případně schvalovacími systémy členského státu;
- kde mohou uživatelé získat specifický popis vypracovaný příslušným členským státem o tom, jak používat a vykládat obsah důvěryhodného seznamu s ohledem na nekvalifikované služby vytvářející důvěru uvedené na seznamu a/nebo na vnitrostátně definované služby vytvářející důvěru. Toho lze využít k poukázání na možnou nesourodost mezi vnitrostátními schvalovacími systémy souvisejícími s ověřovateli nevydávajícími kvalifikované certifikáty 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 definovat a používat další URI, které jsou rozšířením výše uvedeného URI specifického pro jednotlivé členské státy (tj. URI definované na základě tohoto hierarchického specifického URI).

Politické/právní upozornění TSL (TSL policy/legal notice) (bod 5.3.11)

Toto pole je povinné a musí být v souladu se specifikacemi TS 119 612 bodem 5.3.11, kde politické/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,

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

musí být vícejazyčné řetězce znaků (viz bod 5.1.4) uvádějící povinně v britské angličtině a nepovinně v jednom či více národních jazycích samotný text takové politiky nebo upozornění v této podobě:

- 1) První, povinná část, společná pro všechny důvěryhodné seznamy členských států, uvádí platný právní rámec, jehož anglické znění je následující:

The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Text v národním jazyce/jazycích členského státu:

Platným právním rámcem pro stávající důvěryhodný seznam je nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

- 2) Druhá, nepovinná část, specifická pro každý důvěryhodný seznam s odkazy na specifické platné vnitrostátní právní rámce

Aktuální status služby (Service current status) (bod 5.5.4)

Toto pole je povinné a musí být v souladu se specifikacemi TS 119 612 bodem 5.5.4.

Migrace hodnoty „Service current status“ pro služby uvedené na důvěryhodném seznamu EUMS ke dni předcházejícímu datu vstupu nařízení (EU) č. 910/2014 v platnost (tj. 30. června 2016) se vykoná v den vstupu nařízení v platnost (tj. 1. července 2016), jak je uvedeno v příloze J k ETSI TS 119 612.

KAPITOLA III

KONTINUITA DŮVĚRYHODNÝCH SEZNAMŮ

Certifikáty, které se oznamují Komisi podle čl. 4 odst. 2 tohoto rozhodnutí, musí splňovat požadavky ETSI TS 119 612 bodu 5.7.1 a vydávají se tak, aby:

- rozdíl v jejich konečném datu platnosti („Not After“) byl alespoň tři měsíce,
- byly vytvořeny s novými páry klíčů. Již použité páry klíčů nesmí být znovu certifikovány.

V případě skončení platnosti jednoho z certifikátů veřejných klíčů, který by se mohl použít pro ověření podpisu nebo pečete z důvěryhodného seznamu a který byl oznámen Komisi a je zveřejněn v ústředních seznamech ukazatelů Komise, musí členské státy:

- v případě, že byl aktuálně zveřejněný důvěryhodný seznam podepsán či zapečetěn soukromým klíčem, u něž skončila platnost certifikátu veřejného klíče, neprodleně znovu vydat nový důvěryhodný seznam podepsaný či zapečetěný soukromým klíčem, jehož oznámený certifikát veřejného klíče je stále platný;
- v případě potřeby vytvořit nové páry klíčů, které by mohly být použity k podpisu důvěryhodného seznamu či jeho opatření pečeti, a vytvořit odpovídající certifikáty veřejných klíčů;
- neprodleně oznámit Komisi nový seznam certifikátů veřejných klíčů odpovídajících soukromým klíčům, které by mohly být využity k podpisu důvěryhodného seznamu nebo jeho opatření pečeti.

V případě prozrazení či vyřazení jednoho ze soukromých klíčů odpovídajícího jednomu z certifikátů veřejných klíčů, který by mohl být použit pro ověření podpisu či pečete z důvěryhodného seznamu a který byl oznámen Komisi a je zveřejněn v ústředním seznamu ukazatelů Komise, musí členské státy:

- neprodleně znovu vydat nový důvěryhodný seznam podepsaný či zapečetěný neprozrazeným soukromým klíčem v případech, kdy zveřejněný důvěryhodný seznam byl podepsán či zapečetěn prozrazeným nebo vyřazeným soukromým klíčem;

- v případě potřeby vytvořit nové páry klíčů, které by mohly být použity k podpisu důvěryhodného seznamu či jeho opatření pečeti, a vytvoří odpovídající certifikáty veřejných klíčů;
- neprodleně oznámit Komisi nový seznam certifikátů veřejných klíčů odpovídajících soukromým klíčům, které by mohly být využity k podpisu důvěryhodného seznamu nebo jeho opatření pečeti.

V případě prozrazení či vyřazení všech soukromých klíčů odpovídajících certifikátům veřejných klíčů, které by mohly být použity pro ověření podpisu z důvěryhodného seznamu a které byly oznámeny Komisi a jsou zveřejněny v ústředním seznamu ukazatelů Komise, musí členské státy:

- vytvořit nové páry klíčů, které by mohly být použity k podpisu důvěryhodného seznamu či jeho opatření pečeti, a vytvoří odpovídající certifikáty veřejných klíčů;
- neprodleně znovu vydat nový důvěryhodný seznam podepsaný nebo zapečetěný jedním z těchto nových soukromých klíčů a jehož příslušný certifikát veřejného klíče má být oznámen;
- neprodleně oznámit Komisi nový seznam certifikátů veřejných klíčů odpovídajících soukromým klíčům, které by mohly být využity k podpisu důvěryhodného seznamu nebo jeho opatření pečeti.

KAPITOLA IV

SPECIFIKACE PRO OKEM ČITELNOU PODOBU DŮVĚRYHODNÉHO SEZNAMU

Pokud je sestavena a zveřejněna podoba důvěryhodného seznamu čitelná okem, musí 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 musí splňovat tyto požadavky:

- Struktura okem čitelné podoby musí odrážet logický model popsany v TS 119 612.
- Musí být zobrazena všechna přítomná pole, v nichž je třeba uvést toto:
 - název pole (např. „*Service type identifier*“);
 - hodnota pole (např. „<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>“);
 - případně význam (popis) hodnoty pole (např. „*Služba na vydávání certifikátů, která vytváří a podepisuje kvalifikované certifikáty na základě identity a ostatních atributů ověřených příslušnými registračními službami*“);
 - je-li to třeba, znění ve vícero jazykových verzích podle důvěryhodného seznamu.
- Okem čitelná podoba musí zobrazovat minimálně tato pole a příslušné hodnoty digitálních certifikátů ⁽³⁾, pokud jsou uvedeny v poli „*Service digital identity*“:
 - Verze
 - Pořadové číslo certifikátu
 - Algoritmus podpisu
 - Vydavatel – všechna příslušná pole jedinečného jména
 - Doba platnosti
 - Subjekt – všechna příslušná pole jedinečného jména

⁽¹⁾ ISO 32000-1:2008: Document management – Portable document format – Part 1: PDF 1.7 (Správa dokumentů – Portable Document Format – Část 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) (Správa dokumentů – Formát pro dlouhodobou archivaci elektronických dokumentů – Část 2: Použití ISO 32000-1 (PDF/A-2)).

⁽³⁾ Doporučení ITU-T X.509 | ISO/IEC 9594-8: Informační technologie – Propojení otevřených systémů – Adresář: Certifikační rámce veřejných klíčů a atributů (viz <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>).

- Veřejný klíč
- Identifikátor klíče autority
- Identifikátor klíče subjektu
- Použití klíče
- Rozšířené použití klíče
- Politiky certifikace – všechny politické identifikátory a kvalifikátory
- Mapování politiky
- Alternativní název/jméno subjektu
- Atributy adresáře subjektu
- Základní omezení
- Politická omezení
- Distribuční místa CRL ⁽¹⁾
- Přístup orgánu k informacím
- Přístup subjektu k informacím
- Prohlášení ke kvalifikovanému certifikátu ⁽²⁾
- Hašovací algoritmus
- Hašovací hodnota certifikátu
- Okem čitelná podoba musí být snadno tisknutelná.
- Provozovatel systému okem čitelnou podobu podepíše či ji opatří pečetí za použití zaručeného podpisu PDF vymezeného v článcích 1 a 3 prováděcího rozhodnutí (EU) 2015/1505.

⁽¹⁾ RFC 5280: Internet X.509 PKI Certificate a CRL Profile

⁽²⁾ RFC 3739: Internet X.509 PKI: Qualified Certificate Profile

PŘÍLOHA II

ŠABLONA OZNÁMENÍ ČLENSKÝCH STÁTŮ

Informace, které mají členské státy oznámit podle čl. 4 odst. 1 tohoto rozhodnutí, musí zahrnovat následující údaje a jejich veškeré změny:

- 1) Členský stát, vyjádřeno dvoupísmenným kódem ISO 3166-1 ⁽¹⁾, s těmito výjimkami:
 - a) Pro Spojené království se použije kód „UK“.
 - b) Pro Řecko se použije kód „EL“.
- 2) Subjekt/subjekty odpovědné za zřízení, údržbu a zveřejňování formy důvěryhodných seznamů vhodné pro automatické zpracování a formy čitelné okem:
 - a) Název/jméno provozovatele systému: poskytnutý údaj musí být totožný, včetně rozlišení velkých a malých písmen, s hodnotou pole „Scheme operator name“ důvěryhodného seznamu ve všech jazycích, které jsou v seznamu použity.
 - b) Nepovinné údaje určené k internímu použití Komisí pouze v případech, kdy je nutno kontaktovat příslušný subjekt (informace nebudou zveřejněny v seznamu důvěryhodných seznamů vypracovaném Evropskou komisí):
 - adresa provozovatele systému,
 - kontaktní údaje odpovědné osoby/odpovědných osob (jméno, telefon, e-mail).
- 3) Místo, kde je zveřejněna forma důvěryhodného seznamu vhodná pro automatické zpracování (*místo, kde je zveřejněn aktuální důvěryhodný seznam*).
- 4) Případně místo, kde je zveřejněna forma důvěryhodného seznamu čitelná okem (*místo, kde je zveřejněn aktuální důvěryhodný seznam*). V případě, že se forma důvěryhodného seznamu čitelná okem již nezveřejňuje, se tato skutečnost uvede.
- 5) Certifikáty veřejných klíčů, které odpovídají soukromým klíčům a jež lze použít pro elektronický podpis nebo elektronickou pečeť u formy důvěryhodného seznamu vhodné pro automatické zpracování a u formy čitelné okem: tyto certifikáty se vydávají jako certifikáty DER kódované ve formátu „Privacy Enhanced Mail Base64“. U oznámení změny se uvedou dodatečné informace v případě, že konkrétní certifikát na seznamu Komise má být nahrazen novým certifikátem, a v případě, že oznámený certifikát je třeba doplnit ke stávajícím(u) bez jakékoliv náhrady.
- 6) Datum poskytnutí údajů oznámených v bodech 1 až 5.

Údaje oznámené podle bodu 1, bodu 2 písm. a) a bodů 3, 4 a 5 musí být zahrnuty do seznamu důvěryhodných seznamů vypracovaného Evropskou komisí, čímž nahradí původně oznámené informace uvedené v daném seznamu.

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