VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2015/1505

z 8. septembra 2015,

ktorým sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov podľa článku 22 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES ([1]), a najmä na jeho článok 22 ods. 5,

keďže:

(1) Dôveryhodné zoznamy sú nevyhnutné na vybudovanie dôvery medzi trhovými subjektmi, pretože určujú štatút poskytovateľa služieb v čase dohľadu.

(2) Cezhraničné používanie elektronických podpisov bolo uľahčené rozhodnutím Komisie 2009/767/ES ([2]), ktorým sa stanovila povinnosť členských štátov vytvoriť, viesť a uverejňovať zoznamy dôveryhodných informácií vrátane informácií o poskytovateľoch certifikačných služieb, ktorí vydávajú kvalifikované certifikáty verejnosti v súlade so smernicou Európskeho parlamentu a Rady 1999/93/ES ([3]) a ktorí sú pod dohľadom určitého členského štátu alebo sú v ňom akreditovaní.

(3) V článku 22 nariadenia (EÚ) č. 910/2014 sa stanovuje povinnosť členských štátov vytvoriť, viesť a uverejňovať dôveryhodné zoznamy, ktoré sú zabezpečeným spôsobom elektronicky podpísané alebo zapečatené vo forme vhodnej na automatizované spracovanie, a poskytnúť Komisii informácie o orgáne zodpovednom za vytvorenie, vedenie a uverejňovanie národných dôveryhodných zoznamov.

(4) Poskytovateľ dôveryhodných služieb a ním poskytované dôveryhodné služby by sa mali považovať za kvalifikované, ak je kvalifikovaný štatút spojený s poskytovateľom v dôveryhodnom zozname. S cieľom zabezpečiť, aby ostatné povinnosti vyplývajúce z nariadenia (EÚ) č. 910/2014, najmä tie, ktoré sú stanovené v článkoch 27 a 37, mohli poskytovatelia služieb ľahko splniť na diaľku a elektronickými prostriedkami a aby sa splnili oprávnené očakávania ostatných poskytovateľov certifikačných služieb, ktorí nevydávajú kvalifikované certifikáty, ale poskytujú služby súvisiace s elektronickými podpismi v zmysle smernice 1999/93/ES a v zozname sú uvedení do 30. júna 2016, by mali mať členské štáty možnosť pridať do dôveryhodných zoznamov aj iné než kvalifikované dôveryhodné služby, a to dobrovoľne, na vnútroštátnej úrovni, za predpokladu, že sa jasne uvedie, že tieto služby nie sú kvalifikované podľa nariadenia (EÚ) č. 910/2014.

(5) V súlade s odôvodnením 25 nariadenia (EÚ) č. 910/2014 môžu členské štáty pridať iné druhy dôveryhodných služieb na vnútroštátnej úrovni než tie, ktoré sú vymedzené v článku 3 ods. 16 nariadenia (EÚ) č. 910/2014, za predpokladu, že sa jasne uvedie, že tieto služby nie sú kvalifikované podľa nariadenia (EÚ) č. 910/2014.

(6) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru uvedeného v článku 48 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Členské štáty vytvoria, vedú a uverejňujú dôveryhodné zoznamy vrátane informácií o kvalifikovaných poskytovateľoch dôveryhodných služieb, nad ktorými vykonávajú dohľad, ako aj informácií o nimi poskytovaných kvalifikovaných dôveryhodných službách. Tieto zoznamy musia byť v súlade s technickými špecifikáciami stanovenými v prílohe I.

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73.

([2]) Rozhodnutie 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 (Ú. v. EÚ L 274, 20.10.2009, s. 36).

([3]) Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy (Ú. v. ES L 13, 19.1.2000, s. 12).

Článok 2

Členské štáty môžu do týchto dôveryhodných zoznamov zaradiť informácie o nekvalifikovaných poskytovateľoch dôveryhodných služieb spolu s informáciami o nimi poskytovaných nekvalifikovaných dôveryhodných službách. V tomto zozname sa musí jasne označiť, ktorí poskytovatelia dôveryhodných služieb nie sú kvalifikovaní a ktoré nimi poskytované dôveryhodné služby nie sú kvalifikované.

Článok 3

1. Podľa článku 22 ods. 2 nariadenia (EÚ) č. 910/2014 členské štáty elektronicky podpisujú alebo zapečaťujú formu dôveryhodného zoznamu vhodnú na automatizované spracovanie v súlade s technickými špecifikáciami stanovenými v prílohe I.

2. Ak členský štát elektronicky uverejní formu dôveryhodného zoznamu čitateľnú ľudským okom, musí zabezpečiť, aby táto forma dôveryhodného zoznamu obsahovala rovnaké údaje ako forma vhodná na automatizované spracovanie, a elektronicky ju podpíše alebo zapečatí v súlade s technickými špecifikáciami stanovenými v prílohe I.

Článok 4

1. Členské štáty oznamujú Komisii informácie uvedené v článku 22 ods. 3 nariadenia (EÚ) č. 910/2014 podľa vzoru v prílohe II.

2. Informácie uvedené v odseku 1 zahŕňajú dva alebo viac certifikátov s verejným kľúčom prevádzkovateľa schémy s dobou platnosti posunutou aspoň o 3 mesiace, ktoré zodpovedajú súkromným kľúčom, ktoré sa môžu používať na elektronicky podpísanú alebo zapečatenú formu dôveryhodného zoznamu vhodnú na automatizované spracovanie a na formu čitateľnú ľudským okom po uverejnení.

3. Podľa článku 22 ods. 4 nariadenia (EÚ) č. 910/2014 Komisia prostredníctvom zabezpečeného kanálu na overenom webovom serveri sprístupňuje verejnosti informácie oznámené členskými štátmi uvedené v odsekoch 1 a 2 v elektronicky podpísanej alebo zapečatenej forme vhodnej na automatizované spracovanie.

4. Komisia môže prostredníctvom zabezpečeného kanálu na overenom webovom serveri sprístupniť verejnosti informácie oznámené členskými štátmi uvedené v odsekoch 1 a 2 v elektronicky podpísanej alebo zapečatenej forme čitateľnej ľudským okom.

Článok 5

Toto rozhodnutie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto rozhodnutie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 8. septembra 2015

Za Komisiu

predseda

Jean-Claude JUNCKER

PRÍLOHA I

TECHNICKÉ ŠPECIFIKÁCIE SPOLOČNÉHO VZORU PRE DÔVERYHODNÉ ZOZNAMY

KAPITOLA I

VŠEOBECNÉ POŽIADAVKY

Dôveryhodné zoznamy obsahujú súčasné aj všetky historické informácie o štatúte dôveryhodných služieb uvedených v zoznamoch, datujúce sa od začlenenia poskytovateľa dôveryhodnej služby do dôveryhodných zoznamov.

Pojmy „schválený“, „akreditovaný“ a/alebo „podliehajúci dohľadu“ v súčasných špecifikáciách takisto zahŕňajú vnútroštátne schémy schvaľovania, ale dodatočné informácie o povahe všetkých týchto vnútroštátnych schém poskytnú členské štáty vo svojom dôveryhodnom zozname vrátane objasnenia možných rozdielov oproti schémam dohľadu uplatňovaným na kvalifikovaných poskytovateľov dôveryhodných služieb a nimi poskytované kvalifikované dôveryhodné služby.

Informácie uvedené v dôveryhodnom zozname sú zamerané v prvom rade na podporu validácie tokenov kvalifikovaných dôveryhodných služieb, t. j. fyzických alebo binárnych (logických) objektov vygenerovaných alebo vydaných v dôsledku využitia dôveryhodnej služby, napr. menovite kvalifikovaných elektronických podpisov/pečatí alebo zdokonalených elektronických podpisov/pečatí podporovaných kvalifikovaným certifikátom, kvalifikovaných časových pečiatok, kvalifikovaných elektronických potvrdení o doručení atď.

KAPITOLA II

PODROBNÉ ŠPECIFIKÁCIE SPOLOČNÉHO VZORU PRE DÔVERYHODNÉ ZOZNAMY

Tieto špecifikácie sú založené na špecifikáciách a požiadavkách stanovených v ETSI TS 119 612 v2.1.1 (ďalej len „ETSI TS 119 612“).

Ak sa v týchto špecifikáciách nestanovuje žiadna osobitná požiadavka, uplatňujú sa požiadavky ETSI TS 119 612 časti 5 a 6 v celom rozsahu. Ak sa v týchto špecifikáciách stanovujú osobitné požiadavky, majú prednosť pred zodpovedajúcimi požiadavkami ETSI TS 119 612. V prípade rozdielov medzi týmito špecifikáciami a špecifikáciami ETSI TS 119 612 majú prednosť tieto špecifikácie.

Názov schémy („Scheme name“) (odsek 5.3.6)

Toto pole je prítomné a je v súlade so špecifikáciami odseku 5.3.6. normy TS 119 612, v ktorom sa pre schému používa tento názov:

„EN_name_value“ = „Dôveryhodný zoznam vrátane informácií týkajúcich sa kvalifikovaných poskytovateľov dôveryhodných služieb, ktorí sú pod dohľadom členského štátu pôvodu, spolu s informáciami týkajúcimi sa nimi poskytovaných kvalifikovaných dôveryhodných služieb v súlade s príslušnými ustanoveniami uvedenými v nariadení Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.“

URI informácií o schéme („Scheme information URI“) (odsek 5.3.7)

Toto pole je prítomné a je v súlade so špecifikáciami odseku 5.3.7. normy TS 119 612, v ktorom „príslušné informácie o schéme“ zahŕňajú minimálne:

a) Úvodné informácie spoločné pre všetky členské štáty o rozsahu a súvislostiach dôveryhodného zoznamu, schéme, ktorá je základom dohľadu, a v prípade potreby aj príslušnú vnútroštátnu schému (príslušné vnútroštátne schémy) schvaľovania (napr. akreditáciu). Spoločný text, ktorý sa má použiť, je ďalej uvedený text, v ktorom sa reťazec znakov „[*názov príslušného členského štátu*]“ nahradí názvom príslušného členského štátu:

> „Tento zoznam je dôveryhodným zoznamom vrátane informácií týkajúcich sa kvalifikovaných poskytovateľov dôveryhodných služieb, ktorí sú pod dohľadom [*názov príslušného členského štátu*], spolu s informáciami týkajúcimi sa nimi poskytovaných kvalifikovaných dôveryhodných služieb v súlade s príslušnými ustanoveniami uvedenými v nariadení Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

Cezhraničné používanie elektronických podpisov bolo uľahčené rozhodnutím Komisie 2009/767/ES zo 16. októbra 2009, ktorým sa stanovila povinnosť členských štátov vytvoriť, viesť a uverejňovať zoznamy dôveryhodných informácií vrátane informácií o poskytovateľoch certifikačných služieb, 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 a ktorí sú pod dohľadom určitého členského štátu alebo sú v ňom akreditovaní. Súčasný dôveryhodný zoznam je pokračovaním zoznamu dôveryhodných informácií vytvoreného podľa rozhodnutia 2009/767/ES.“

Dôveryhodné zoznamy sú základnými prvkami pri budovaní dôvery medzi elektronickými trhovými subjektmi vďaka tomu, že používateľom umožňujú určiť kvalifikovaný štatút a históriu štatútu poskytovateľov dôveryhodných služieb a ich služieb.

Dôveryhodné zoznamy členských štátov obsahujú prinajmenšom informácie uvedené v článkoch 1 a 2 vykonávacieho rozhodnutia Komisie (EÚ) 2015/1505.

Členské štáty môžu do dôveryhodných zoznamov zaradiť informácie o nekvalifikovaných poskytovateľoch dôveryhodných služieb spolu s informáciami o nimi poskytovaných nekvalifikovaných dôveryhodných službách. Jasne sa musí uviesť, že nie sú kvalifikovaní podľa nariadenia (EÚ) č. 910/2014.

Členské štáty môžu do dôveryhodných zoznamov zaradiť informácie aj o iných druhoch dôveryhodných služieb vymedzených na vnútroštátnej úrovni než tie, ktoré sú vymedzené v článku 3 ods. 16 nariadenia (EÚ) č. 910/2014. Jasne sa musí uviesť, že nie sú kvalifikované podľa nariadenia (EÚ) č. 910/2014.

b) Konkrétne informácie o schéme, ktorá je základom dohľadu, a v prípade potreby aj o príslušnej vnútroštátnej schéme (príslušných vnútroštátnych schémach) schvaľovania (napr. akreditácia), najmä ([1]):

1. Informácie o vnútroštátnom systéme dohľadu, ktoré sa vzťahujú na kvalifikovaných a nekvalifikovaných poskytovateľov dôveryhodných služieb a nimi poskytované kvalifikované a nekvalifikované dôveryhodné služby, ako ich upravuje nariadenie (EÚ) č. 910/2014;

2. Prípadne informácie o vnútroštátnych dobrovoľných akreditačných schémach, ktoré sa týkajú poskytovateľov certifikačných služieb vydávajúcich kvalifikované certifikáty podľa smernice 1999/93/ES;

Tieto konkrétne informácie zahŕňajú pri každej uvedenej základnej schéme minimálne:

1. Všeobecný opis;

2. Informácie o postupe dodržiavanom pre vnútroštátny systém dohľadu a prípadne pre schvaľovanie podľa vnútroštátnej schémy schvaľovania.

3. Informácie o kritériách, podľa ktorých sa vykonáva a v prípade potreby schvaľuje dozor nad poskytovateľmi dôveryhodných služieb.

4. Informácie o kritériách a pravidlách uplatnených pri výbere osôb vykonávajúcich dohľad alebo audítorov a pri vymedzení spôsobu, akým majú posudzovať poskytovateľov dôveryhodných služieb a nimi poskytované dôveryhodné služby.

5. V prípade potreby aj iné kontaktné a všeobecné informácie, ktoré sa týkajú prevádzkovania schémy.

Typ schémy/komunity/pravidlá („Scheme type/community/rules“) (odsek 5.3.9)

Toto pole je prítomné a je v súlade so špecifikáciami odseku 5.3.9 normy TS 119 612.

Zahŕňa len URI v britskej angličtine.

([1]) Uvedené súbory informácií sú pre závislé strany mimoriadne dôležité na posúdenie kvality a stupňa bezpečnosti týchto systémov. Uvedené súbory informácií sa uvádzajú na úrovni dôveryhodného zoznamu prostredníctvom súčasných „Scheme information URI“ (odsek 5.3.7 – informácie, ktoré poskytujú členské štáty), „Scheme type/community/rules“ (odsek 5.3.9 – prostredníctvom textu spoločného pre všetky členské štáty) a „TSL policy/legal notice“ (odsek 5.3.11 – text spoločný pre všetky členské štáty spolu s možnosťou doplniť texty/referencie špecifické pre daný členský štát). Dodatočné informácie o takýchto systémoch nekvalifikovaných dôveryhodných služieb a (kvalifikovaných) dôveryhodných služieb definovaných na vnútroštátnej úrovni sa v prípade potreby a ak je to uplatniteľné môžu poskytovať na úrovni služby (napríklad na účely odlíšenia viacerých úrovní kvality/bezpečnosti) pomocou „Scheme service definition URI“ (odsek 5.5.6).

Zahŕňa minimálne dve URI:

1. URI spoločný pre všetky dôveryhodné zoznamy členských štátov, ktorý odkazuje na opisný text uplatniteľný na všetky dôveryhodné zoznamy nasledujúcim spôsobom:

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

   Opisný text:

   „Participation in a scheme

   Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in 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.

   The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

   Policy/rules for the assessment of the listed services

   Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

   The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505.

   The trusted lists include both current and historical information about the status of listed trust services.

   Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) schemes) under which the trust service providers and the trust services that they provide are listed.

   Interpretation of the Trusted List

   The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

   The ‚qualified' status of a trust service is indicated by the combination of the ‚Service type identifier' (‚Sti') value in a service entry and the status according to the ‚Service current status' field value as from the date indicated in the ‚Current status starting date and time'. Historical information about such a qualified status is similarly provided when applicable.

   Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

   A ‚CA/QC' ‚Service type identifier' (‚Sti') entry (possibly further qualified as being a ‚RootCA-QC' through the use of the appropriate ‚Service information extension' (‚Sie') additionalServiceInformation Extension)

   — indicates that any end-entity certificate issued by or under the CA represented by the ‚Service digital identifier' (‚Sdi') CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

     — the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),

     — the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. ‚undersupervision', ‚supervisionincessation', ‚accredited' or ‚granted') for that entry.

— **and IF** ‚Sie' ‚Qualifications Extension' information is present, then in addition to the above default rule, those certificates that are identified through the use of ‚Sie' ‚Qualifications Extension' information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the ‚SSCD support' and/or ‚Legal person as subject' (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific ‚Key usage' pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of ‚Qualifiers' used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

  — to indicate the qualified certificate nature:

    — ‚QCStatement' meaning the identified certificates) is(are) qualified under Directive 1999/93/EC;

    — ‚QCForESig' meaning the identified certificates), when claimed or stated as qualified certificates), is (are) qualified certificates) for electronic signature under Regulation (EU) No 910/2014;

    — ‚QCForESeal' meaning the identified certificates), when claimed or stated as qualified certificates), is (are) qualified certificates) for electronic seal under Regulation (EU) No 910/2014;

    — ‚QCForWSA' meaning the identified certificates), when claimed or stated as qualified certificates), is (are) qualified certificates) for web site authentication under Regulation (EU) No 910/2014.

  — to indicate that the certificate is not to be considered as qualified:

    — ‚NotQualified' meaning the identified certificates) is(are) not to be considered as qualified; And/or

  — to indicate the nature of the SSCD support:

    — ‚QCWithSSCD' meaning the identified certificates), when claimed or stated as qualified certificates), have their private key residing in an SSCD, or

    — ‚QCNoSSCD' meaning the identified certificates), when claimed or stated as qualified certificates), have not their private key residing in an SSCD, or

    — ‚QCSSCDStatusAsInCert' meaning the identified certificates), when claimed or stated as qualified certificates), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

  — to indicate the nature of the QSCD support:

    — ‚QCWithQSCD' meaning the identified certificates), when claimed or stated as qualified certificates), have their private key residing in a QSCD, or

    — ‚QCNoQSCD' meaning the identified certificates), when claimed or stated as qualified certificates), have not their private key residing in a QSCD, or

    — ‚QCQSCDStatusAsInCert' meaning the identified certificates), when claimed or stated as qualified certificates), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

    — ‚QCQSCDManagedOnBehalf' indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; And/or

— to indicate issuance to Legal Person:

— ‚QCForLegalPerson' meaning the identified certificates), when claimed or stated as qualified certificates), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

— if none of the id-etsi-qcs 1 statement, QCP OID or QCP+ OID information is included in an end-entity certificate, and

— if no ‚Sie' ‚Qualifications Extension' information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a ‚QCStatement' qualifier, or

— an ‚Sie' ‚Qualifications Extension' information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a ‚NotQualified' qualifier,

then the certificate is not to be considered as qualified.

‚Service digital identifiers' are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other ‚Sti' type entry is that, for that ‚Sti' identified service type, the listed service named according to the ‚Service name' field value and uniquely identified by the ‚Service digital identity' field value has the current qualified or approval status according to the ‚Service current status' field value as from the date indicated in the ‚Current status starting date and time'.

Specific interpretation rules for any additional information with regard to a listed service (e.g. ‚Service information extensions' field) may be found, when applicable, in the Member State specific URI as part of the present ‚Scheme type/community/rules' field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists."

2. URI špecifický pre dôveryhodný zoznam každého členského štátu odkazujúci na opisný text, ktorý je uplatniteľný na dôveryhodný zoznam daného členského štátu:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, kde CC = ISO 3166-1 ([1]) alpha-2 kód krajiny používaný v poli „Scheme territory" (odsek 5.3.10)

— Prostredníctvom tohto URI môžu používatelia získať prístup k osobitným politikám/pravidlám dotknutého členského štátu, podľa ktorých sa dôveryhodné služby na zozname posudzujú v súlade s režimom dohľadu daného členského štátu a v prípade potreby aj jeho schémou schvaľovania.

— Prostredníctvom tohto URI môžu používatelia získať prístup k osobitnému opisu členského štátu týkajúcemu sa toho, ako používať a vykladať obsah dôveryhodného zoznamu vzhľadom na uvedené nekvalifikované dôveryhodné služby a/alebo dôveryhodné služby definované na vnútroštátnej úrovni. Toto sa môže využiť na znázornenie možnej nesúrodosti vnútroštátneho systému schvaľovania súvisiaceho s poskytovateľmi certifikovaných služieb, ktorí nevydávajú kvalifikovaný certifikát, a na vysvetlenie, ako sa na tento účel používajú polia „Scheme service definition URI" (odsek 5.5.6) a „Service information extension" (odsek 5.5.9).

Členské štáty MÔŽU vymedziť a používať dodatočné URI, ktoré je rozšírením uvedeného URI špecifického pre daný členský štát (t. j. URI vymedzené na základe tohto hierarchického špecifického URI).

Politické/právne upozornenie TSL (TSL policy/legal notice) (odsek 5.3.11)

Toto pole je prítomné a je v súlade so špecifikáciami odseku 5.3.11 normy TS 119 612, keď politické/právne upozornenie týkajúce sa právneho štatútu schémy alebo právnych požiadaviek, ktoré schéma spĺňa, na území, pod ktorého právomoc spadá, a/alebo obmedzenia a podmienky, za ktorých sa zoznam dôveryhodných informácií

([1]) ISO 3166-1:2006: „Kódy názvov krajín a ich častí – 1. časť: Kódy krajín".

o poskytovateľoch vedie a uverejňuje, je sekvencia viacjazyčných reťazcov znakov (pozri odsek 5.1.4) uvádzajúca povinne v britskej angličtine a nepovinne v jednom alebo viacerých národných jazykoch samotný text takejto politiky alebo upozornenia v nasledujúcej podobe:

1. Prvá, povinná časť, spoločná pre dôveryhodné zoznamy všetkých členských štátov, uvádza uplatniteľný právny rámec, ktorého anglické znenie je nasledovné:

   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.

   Znenie v národnom jazyku (národných jazykoch) členského štátu:

   Uplatniteľným právnym rámcom tohto dôveryhodného zoznamu je nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

2. Druhá, nepovinná časť, špecifická pre každý dôveryhodný zoznam, s odkazmi na osobitné uplatniteľné vnútroštátne právne rámce.

Aktuálny štatút služby (Service current status) (odsek 5.5.4)

Toto pole je prítomné a je v súlade so špecifikáciami odseku 5.5.4 normy TS 119 612.

Migrácia hodnoty „Service current status“ pre služby uvedené v dôveryhodnom zozname VŠEÚ ku dňu predchádzajúcemu dátumu uplatňovania nariadenia (EÚ) č. 910/2014 (t. j. 30. júna 2016) sa vykoná v deň uplatňovania nariadenia (t. j. 1. júla 2016), ako sa uvádza v prílohe J k ETSI TS 119 612.

KAPITOLA III

KONTINUITA DÔVERYHODNÝCH ZOZNAMOV

Certifikáty, ktoré treba oznámiť Komisii v súlade s článkom 4 ods. 2 tohto rozhodnutia, musia spĺňať požiadavky odseku 5.7.1 ETSI TS 119 612 a musia byť vydané tak, aby:

— mali aspoň trojmesačný rozdiel v konečnom dátume platnosti („Not After“),

— boli vytvorené s novými pármi kľúčov. Páry kľúčov používané predtým sa nesmú opätovne certifikovať.

V prípade vypršania platnosti jedného z certifikátov verejného kľúča, ktorý by sa mohol použiť na validáciu podpisu alebo pečate v dôveryhodnom zozname a ktorý bol oznámený Komisii a uverejnený v centrálnych zoznamoch ukazovateľov Komisie, členské štáty:

— v prípade, ak bol aktuálne uverejnený dôveryhodný zoznam podpísaný alebo zapečatený súkromným kľúčom, ktorého certifikát verejného kľúča stratil platnosť, znovu vydajú, a to bez zdržania, nový dôveryhodný zoznam podpísaný alebo zapečatený súkromným kľúčom, ktorého certifikát verejného kľúča nestratil platnosť,

— na požiadanie vygenerujú nové páry kľúčov, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu, a vygenerujú pre ne príslušné certifikáty verejného kľúča,

— okamžite oznámia Komisii nový zoznam certifikátov verejného kľúča zodpovedajúcich súkromným kľúčom, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu.

V prípade poškodenia alebo vyradenia jedného zo súkromných kľúčov zodpovedajúceho certifikátom verejného kľúča, ktorý by sa mohol použiť na validáciu podpisu alebo pečate v dôveryhodnom zozname a ktorý bol oznámený Komisii a uverejnený v centrálnych zoznamoch ukazovateľov Komisie, členské štáty:

— znovu vydajú, a to bezodkladne, nový dôveryhodný zoznam podpísaný alebo zapečatený nepoškodeným súkromným kľúčom v prípade, ak bol uverejnený dôveryhodný zoznam podpísaný poškodeným alebo vyradeným súkromným kľúčom,

— na požiadanie vygenerujú nové páry kľúčov, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu, a vygenerujú pre ne príslušné certifikáty verejného kľúča,

— okamžite oznámia Komisii nový zoznam certifikátov verejného kľúča zodpovedajúcich súkromným kľúčom, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu.

V prípade poškodenia alebo vyradenia všetkých súkromných kľúčov zodpovedajúcich certifikátom verejných kľúčov, ktoré by sa mohli použiť na overenie podpisu v dôveryhodnom zozname a ktoré boli oznámené Komisii a uverejnené v centrálnych zoznamoch ukazovateľov Komisie, členské štáty:

— vygenerujú nové páry kľúčov, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu, a vygenerujú pre ne príslušné certifikáty verejného kľúča,

— znovu vydajú, a to bezodkladne, nový dôveryhodný zoznam podpísaný alebo zapečatený jedným z tých nových súkromných kľúčov, ktorých zodpovedajúci certifikát s verejným kľúčom sa má oznámiť,

— okamžite oznámia Komisii nový zoznam certifikátov verejného kľúča zodpovedajúcich súkromným kľúčom, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu.

KAPITOLA IV

ŠPECIFIKÁCIE FORMY DÔVERYHODNÉHO ZOZNAMU ČITATEĽNEJ ĽUDSKÝM OKOM

Ak sa stanoví a uverejní forma dôveryhodného zoznamu čitateľná ľudským okom, poskytne sa vo formáte dokumentu PDF podľa ISO 32000 ([1]), ktorý sa naformátuje podľa profilu PDF/A (ISO 19005 ([2])).

Obsah formy dôveryhodného zoznamu čitateľnej ľudským okom vo formáte PDF/A musí spĺňať tieto požiadavky:

— v štruktúre formy čitateľnej ľudským okom by sa mal odrážať logický model opísaný v norme TS 119 612,

— každé zahrnuté pole je zobrazené a uvádza:

  — názov poľa (napríklad „*Service type identifier*“),

  — hodnotu poľa (napríklad „http://uri.etsi.org/TrstSvc/Svctype/CA/QC“),

  — v prípade potreby význam (opis) hodnoty poľa, (napr. „*Služba na vydávanie certifikátov, ktorá vytvára a podpisuje kvalifikované certifikáty na základe identity a ostatných atribútov overených príslušnými registračnými službami*.“),

  — v prípade potreby viacero jazykových verzií, ako sa stanovuje v dôveryhodnom zozname.

— Na forme čitateľnej ľudským okom sa uvedú minimálne tieto polia a zodpovedajúce hodnoty digitálnych certifikátov ([3]), ak sú uvedené v poli „Service digital identity“:

  — Verzia,

  — Sériové číslo certifikátu,

  — Algoritmus podpisu,

  — Vydavateľ – všetky dôležité rozlíšiteľné názvové polia,

  — Doba platnosti,

  — Subjekt – všetky dôležité rozlíšiteľné názvové polia,

([1]) ISO 32000-1:2008: Správa dokumentov – PDF (Portable document format) – 1. časť: PDF 1.7.
([2]) ISO 19005-2:2011: Správa dokumentov – Formát pre dlhodobú archiváciu elektronických textových dokumentov – 2. časť: Používanie normy ISO 32000-1 (PDF/A-2).
([3]) Odporúčanie ITU-T X.509 | ISO/IEC 9594-8: Informačné technológie – prepojenia otvorených systémov – adresár: Certifikačné rámce verejného kľúča a atribútu (pozri http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— Verejný kľúč,

— Identifikátor kľúča orgánu,

— Identifikátor kľúča subjektu,

— Používanie kľúča,

— Rozšírené používanie kľúča,

— Certifikačné politiky – všetky identifikátory a kvalifikátory politiky,

— Mapovanie politiky,

— Alternatívny názov subjektu,

— Vlastnosti adresára subjektu,

— Základné obmedzenia,

— Politické obmedzenia,

— Distribučné body CRL ([1]),

— Prístup k informáciám pre orgán,

— Prístup k informáciám pre subjekt,

— Vyhlásenia kvalifikovaného certifikátu ([2]),

— Hašovací algoritmus,

— Hašovacia hodnota certifikátu.

— Forma čitateľná ľudským okom sa musí dať ľahko vytlačiť.

— Formu čitateľnú ľudským okom podpíše alebo zapečatí prevádzkovateľ schémy podľa zdokonalených podpisov PDF vymedzených v článkoch 1 a 3 vykonávacieho rozhodnutia Komisie (EÚ) 2015/1505.

([1]) RFC 5280: Profil certifikátu Internet X.509 PKI a profil CRL.
([2]) RFC 3739: Internet X.509 PKI: Profil kvalifikovaného certifikátu.

PRÍLOHA II

VZOR OZNÁMENÍ ČLENSKÝCH ŠTÁTOV

Informácie, ktoré majú členské štáty oznamovať podľa článku 4 ods. 1 predmetného rozhodnutia obsahujú tieto údaje a akékoľvek ich zmeny:

1. Členský štát, s použitím kódu ISO 3166-1 ([1]) alpha-2 s týmito výnimkami:

   a) Kódom krajiny pre Spojené kráľovstvo je „UK".

   b) Kódom krajiny pre Grécko je „EL".

2. Orgán(-y) zodpovedný(-é) za zostavenie, vedenie a uverejňovanie formy dôveryhodných zoznamov vhodnej na automatizované spracovanie a formy dôveryhodných zoznamov čitateľnej ľudským okom:

   a) Meno prevádzkovateľa schémy: poskytnutá informácia sa musí zhodovať – rozlišujú sa veľké a malé písmená – s menom prevádzkovateľa schémy („Scheme operator name") v zozname dôveryhodných informácií vo všetkých jazykoch, ktoré sa v ňom používajú.

   b) Nepovinné údaje iba na vnútorné účely Komisie v prípadoch, keď je potrebné kontaktovať príslušný orgán (v zozname dôveryhodných zoznamov, ktorý zostavila EK, nebudú tieto informácie uverejnené):

      — adresa prevádzkovateľa schémy;

      — kontaktné údaje o zodpovednej(-ých) osobe(-ách) (meno, telefón, emailová adresa).

3. Lokalita, kde je uverejnený dôveryhodný zoznam vo forme vhodnej na automatizované spracovanie (*lokalita, kde je uverejnený v súčasnosti platný dôveryhodný zoznam*).

4. V prípade potreby lokalita, kde je uverejnený dôveryhodný zoznam vo forme čitateľnej ľudským okom (*lokalita, kde je uverejnený v súčasnosti platný dôveryhodný zoznam*). Ak dôveryhodný zoznam vo forme čitateľnej ľudským okom už nie je uverejnený, je potrebné túto skutočnosť uviesť.

5. Certifikáty verejného kľúča zodpovedajúce súkromným kľúčom, ktoré sa môžu používať na elektronické podpísanie alebo zapečatenie formy dôveryhodných zoznamov vhodnej na automatizované spracovanie a formy dôveryhodných zoznamov čitateľnej ľudským okom: tieto certifikáty sa predkladajú ako certifikáty DER kódované vo formáte Privacy Enhanced Mail Base64. Pri oznamovaní zmeny sa uvedú dodatočné informácie v prípade, keď je v zozname Komisie potrebné nahradiť osobitný certifikát novým certifikátom, a v prípade, keď je k existujúcemu certifikátu alebo certifikátom potrebné pridať oznámený certifikát bez akejkoľvek náhrady.

6. Dátum predloženia údajov oznamovaných v bodoch 1 až 5.

Údaje oznámené podľa bodu 1, bodu 2 písm. a) a bodov 3, 4 a 5 sa musia pridať do zoznamu dôveryhodných zoznamov, ktorý zostavuje EK, namiesto predtým oznámených informácií v uvedenom zozname.

([1]) ISO 3166-1: „Kódy názvov krajín a ich častí – 1. časť: Kódy krajín".