IZVEDBENI SKLEP KOMISIJE (EU) 2015/1505

z dne 8. septembra 2015

o določitvi tehničnih specifikacij in formatov v zvezi z zanesljivimi seznami v skladu s členom 22(5) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES ([1]) ter zlasti člena 22(5) Uredbe,

ob upoštevanju naslednjega:

(1) Zanesljivi seznami so bistveni za vzpostavljanje zaupanja med udeleženci na trgu, saj je iz njih razviden status ponudnika storitev v trenutku nadzora.

(2) Čezmejno uporabo elektronskih podpisov je pospešila Odločba Komisije 2009/767/ES ([2]), ki državam članicam nalaga obveznost, da vzpostavijo, vzdržujejo in objavijo zanesljive sezname, ki vsebujejo informacije v zvezi z overitelji, ki izdajajo kvalificirana potrdila javnosti v skladu z Direktivo 1999/93/ES Evropskega parlamenta in Sveta ([3]) ter so nadzorovani in akreditirani s strani držav članic.

(3) Člen 22 Uredbe (EU) št. 910/2014 državam članicam nalaga obveznost, da v obliki, primerni za avtomatizirano obdelavo, na varen način sestavijo, vodijo in objavijo elektronsko podpisane ali ožigosane zanesljive sezname in Komisijo uradno obvestijo o organih, ki so pristojni za sestavljanje nacionalnih zanesljivih seznamov.

(4) Ponudnik storitev zaupanja in storitve zaupanja, ki jih zagotavlja, bi se morali šteti za kvalificirane, kadar je ponudniku na zanesljivem seznamu dodeljen kvalificiran status. Da se zagotovi, da lahko ponudniki storitev na daljavo in po elektronski poti brez težav izpolnjujejo druge obveznosti iz Uredbe (EU) št. 910/2014, zlasti tiste iz členov 27 in 37, in da se izpolnijo legitimna pričakovanja drugih overiteljev, ki ne izdajajo kvalificiranih potrdil, vendar pa zagotavljajo storitve v zvezi z elektronskimi podpisi na podlagi Direktive 1999/93/ES in so uvrščeni na seznam do 30. junija 2016, bi moralo biti državam članicam omogočeno, da na nacionalni ravni na zanesljive sezname prostovoljno dodajo storitve zaupanja, ki niso kvalificirane, pod pogojem, da se jasno navede, da te storitve zaupanja niso kvalificirane v skladu z Uredbo (EU) št. 910/2014.

(5) V skladu z uvodno izjavo 25 Uredbe (EU) št. 910/2014 lahko države članice dodajo druge vrste nacionalno opredeljenih storitev zaupanja, ki niso opredeljene v členu 3(16) Uredbe (EU) št. 910/2014, pod pogojem, da je jasno navedeno, da te storitve zaupanja niso kvalificirane v skladu z Uredbo (EU) št. 910/2014.

(6) Ukrepi iz tega sklepa so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 48 Uredbe (EU) št. 910/2014 –

SPREJELA NASLEDNJI SKLEP:

Člen 1

Države članice sestavijo, objavijo in vodijo zanesljive sezname, ki vsebujejo informacije o ponudnikih kvalificiranih storitev zaupanja, ki jih nadzorujejo, in informacije o kvalificiranih storitvah zaupanja, ki jih ti zagotavljajo. Navedeni seznami so v skladu s tehničnimi specifikacijami iz Priloge I.

([1]) UL L 257, 28.8.2014, str. 73.

([2]) Odločba Komisije 2009/767/ES z dne 16. oktobra 2009 o vzpostavitvi ukrepov za pospeševanje uporabe postopkov po elektronski poti s pomočjo „enotnih kontaktnih točk“ po Direktivi 2006/123/ES Evropskega parlamenta in Sveta o storitvah na notranjem trgu (UL L 274, 20.10.2009, str. 36).

([3]) Direktiva Evropskega parlamenta in Sveta 1999/93/ES z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis (UL L 13, 19.1.2000, str. 12.)

Člen 2

Države članice lahko v zanesljive sezname vključijo informacije o ponudnikih nekvalificiranih storitev zaupanja, skupaj z informacijami o nekvalificiranih storitvah zaupanja, ki jih ti zagotavljajo. Iz zanesljivega seznama je jasno razvidno, kateri ponudniki storitev zaupanja in katere storitve zaupanja, ki jih ti zagotavljajo, niso kvalificirani.

Člen 3

1. V skladu s členom 22(2) Uredbe (EU) št. 910/2014 države članice elektronsko podpišejo ali ožigosajo obliko, primerno za avtomatizirano obdelavo svojega zanesljivega seznama v skladu s tehničnimi specifikacijami iz Priloge I.

2. Če država članica elektronsko objavi zanesljivi seznam v človeku berljivi obliki, zagotovi, da ta oblika zanesljivega seznama vsebuje enake podatke kot oblika, primerna za avtomatizirano obdelavo, ter jo elektronsko podpiše ali ožigosa v skladu s tehničnimi specifikacijami iz Priloge I.

Člen 4

1. Države članice Komisiji uradno sporočijo informacije iz člena 22(3) Uredbe (EU) št. 910/2014 z uporabo predloge iz Priloge II.

2. Informacije iz odstavka 1 vsebujejo dve ali več potrdil javnih ključev upravljavca sheme z najmanj trimesečnimi izmeničnimi obdobji veljavnosti, ki ustrezajo zasebnim ključem, ki se lahko uporabljajo za elektronsko podpisovanje ali žigosanje oblike, primerne za avtomatizirano obdelavo zanesljivega seznama, in človeku berljive oblike, kadar se objavi.

3. V skladu s členom 22(4) Uredbe (EU) št. 910/2014 Komisija prek varnega kanala na avtenticiranem spletnem strežniku javnosti da na voljo informacije iz odstavkov 1 in 2, kot so jih uradno sporočile države članice, v podpisani ali ožigosani obliki, primerni za avtomatizirano obdelavo.

4. Komisija prek varnega kanala na avtenticiranem spletnem strežniku javnosti lahko da na voljo informacije iz odstavkov 1 in 2, kot so jih uradno sporočile države članice, v podpisani ali ožigosani človeku berljivi obliki.

Člen 5

Ta sklep začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta sklep je v celoti zavezujoč in se neposredno uporablja v vseh državah članicah.

V Bruslju, 8. septembra 2015

Za Komisijo

Predsednik

Jean-Claude JUNCKER

PRILOGA I

TEHNIČNE SPECIFIKACIJE ZA SKUPNO PREDLOGO ZA ZANESLJIVE SEZNAME

POGLAVJE I

SPLOŠNE ZAHTEVE

Zanesljivi seznami vključujejo veljavne in pretekle informacije o statusu navedenih storitev zaupanja od vključitve ponudnika storitev zaupanja v zanesljive sezname.

Izrazi „potrjen“, „akreditiran“ in/ali „nadzorovan“ v teh specifikacijah zajemajo tudi nacionalne sheme potrjevanja, vendar bodo države članice zagotovile dodatne informacije o naravi vsake take nacionalne sheme v svojem zanesljivem seznamu, vključno s pojasnili o mogočih razlikah glede na sheme nadzora, ki se uporabljajo za ponudnike kvalificiranih storitev zaupanja in kvalificirane storitve zaupanja, ki jih ti zagotavljajo.

Glavni cilj informacij zanesljivega seznama je podpreti potrjevanje veljavnosti žetonov kvalificiranih storitev zaupanja, tj. fizičnih ali binarnih (logičnih) objektov, ki se generirajo ali izdajo ob uporabi kvalificirane storitve zaupanja, in sicer na primer kvalificiranih elektronskih podpisov/žigov, naprednih elektronskih podpisov/žigov, podprtih s kvalificiranim potrdilom, kvalificiranih časovnih žigov, kvalificiranih evidenc elektronske dostave itd.

POGLAVJE II

PODROBNE SPECIFIKACIJE ZA SKUPNO PREDLOGO ZA ZANESLJIVE SEZNAME

Te specifikacije temeljijo na specifikacijah in zahtevah iz ETSI TS 119 612 v 2.1.1 (v nadaljnjem besedilu: ETSI TS 119 612).

Kadar v teh specifikacijah niso navedene posebne zahteve, v celoti veljajo zahteve iz razdelkov 5 in 6 ETSI TS 119 612. Kadar so v teh specifikacijah navedene posebne zahteve, prevladajo nad ustreznimi zahtevami iz ETSI TS 119 612. V primeru neskladij med temi specifikacijami in specifikacijami iz ETSI TS 119 612 prevladajo te specifikacije.

Ime sheme (razdelek 5.3.6)

To polje mora biti vključeno in v skladu s specifikacijami iz razdelka 5.3.6 TS 119 612, v katerem se za shemo uporablja naslednje ime:

„EN_name_value“ = „zanesljivi seznam, ki vsebuje informacije o ponudnikih kvalificiranih storitev zaupanja, ki jih nadzirajo države članice izdajateljice, skupaj z informacijami o kvalificiranih storitvah zaupanja, ki jih ti zagotavljajo, v skladu z ustreznimi določbami iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES.“

URI za informacije o shemi (razdelek 5.3.7)

To polje mora biti vključeno in v skladu s specifikacijami iz razdelka 5.3.7 TS 119 612, v katerem „ustrezne informacije o shemi“ zajemajo najmanj:

(a) za vse države članice enake uvodne informacije o obsegu in ozadju zanesljivega seznama, osnovni shemi nadzora in, kadar je to primerno, nacionalnih shemah potrjevanja (npr. akreditacijskih). Uporabi se spodnje besedilo, v katerem se znakovni niz „[*ime zadevne države članice*]“ nadomesti z imenom zadevne države članice:

„Ta seznam je zanesljivi seznam, ki vsebuje informacije o ponudnikih kvalificiranih storitev zaupanja, ki jih nadzira [*ime zadevne države članice*], skupaj z informacijami o kvalificiranih storitvah zaupanja, ki jih ti zagotavljajo, v skladu z ustreznimi določbami iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES.

Čezmejno uporabo elektronskih podpisov je pospešila Odločba Komisije 2009/767/ES z dne 16. oktobra 2009, ki državam članicam nalaga obveznost, da vzpostavijo, vzdržujejo in objavijo zanesljive sezname, ki vsebujejo informacije v zvezi z overitelji, ki izdajajo kvalificirana potrdila javnosti v skladu z Direktivo Evropskega parlamenta in Sveta 1999/93/ES z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis ter so nadzorovani/akreditirani s strani držav članic. Ta zanesljivi seznam je nadaljevanje zanesljivega seznama, ki je bil vzpostavljen z Odločbo 2009/767/ES."

Zanesljivi seznami so bistveni elementi za vzpostavljanje zaupanja med udeleženci na elektronskem trgu, ki uporabnikom omogočajo, da preverijo, ali imajo ponudniki ter njihove storitve kvalificirani status ter kakšen je bil njihov pretekli status.

Zanesljivi seznami države članice vključujejo najmanj informacije, navedene v členih 1 in 2 Izvedbenega sklepa Komisije (EU) 2015/1505.

Države članice lahko v zanesljive sezname vključijo informacije o nekvalificiranih ponudnikih storitev zaupanja, skupaj z informacijami o nekvalificiranih storitvah zaupanja, ki jih ti zagotavljajo. Jasno mora biti navedeno, da niso kvalificirani v skladu z Uredbo (EU) št. 910/2014.

Države članice lahko v zanesljive sezname vključijo informacije o nacionalno opredeljenih storitvah zaupanja, ki niso opredeljene na podlagi člena 3(16) Uredbe (EU) št. 910/2014. Jasno mora biti navedeno, da niso kvalificirane v skladu z Uredbo (EU) št. 910/2014.

(b) Posebne informacije o osnovni shemi nadzora in, kadar je to primerno, nacionalnih shemah potrjevanja (npr. akreditacije), zlasti ([1]):

1. informacije o nacionalnem sistemu nadzora, ki se uporablja za ponudnike kvalificiranih in nekvalificiranih storitev zaupanja ter kvalificirane in nekvalificirane storitve zaupanja, ki jih ti zagotavljajo, kakor je določeno v Uredbi (EU) št. 910/2014;

2. informacije, kadar je to primerno, o nacionalnih shemah za prostovoljno akreditacijo, ki se uporabljajo za overitelje, ki so izdali kvalificirana potrdila na podlagi Direktive 1999/93/ES.

Te posebne informacije za vsako zgoraj navedeno osnovno shemo vključujejo najmanj:

1. splošni opis;

2. informacije o postopku, ki se upošteva za nacionalni sistem nadzora in, kadar je to primerno, za potrjevanje na podlagi nacionalne sheme potrjevanja;

3. informacije o merilih za nadzor ali, kadar je to primerno, za potrjevanje ponudnikov storitev zaupanja;

4. informacije o merilih in pravilih, ki se uporabljajo za izbiro nadzornikov/revizorjev in za opredelitev, kako naj ocenjujejo ponudnike storitev zaupanja in storitve zaupanja, ki jih ti zagotavljajo;

5. kadar je to primerno, druge kontaktne in splošne informacije, ki se uporabljajo za izvajanje sheme.

Vrsta sheme/skupnost/pravila (razdelek 5.3.9)

To polje mora biti vključeno in v skladu s specifikacijami iz razdelka 5.3.9. TS 119 612.

Vključuje izključno URI v britanski angleščini.

([1]) Navedena podatkovna niza sta za zanašajoče se stranke bistvenega pomena za ocenjevanje ravni kakovosti in varnosti takih sistemov. Ta dva podatkovna niza se zagotavljata na ravni zanesljivega seznama v poljih „Informacije o shemi URI" (razdelek 5.3.7 – informacije, ki jih zagotovi država članica), „Vrsta sheme/skupnost/pravila" (razdelek 5.3.9 – skupno besedilo za vse države članice) in „Politika/pravno obvestilo v zvezi s seznamom o statusu storitev zaupanja" (razdelek 5.3.11 – skupno besedilo za vse države članice, z možnostjo za vsako državo članico, da doda besedilo/sklice, ki so zanjo posebni). Dodatne informacije o takih sistemih za nekvalificirane storitve zaupanja in nacionalno opredeljene (kvalificirane) storitve zaupanja se lahko zagotavljajo na ravni storitve, kadar je to primerno in potrebno (npr. za razlikovanje med več ravnmi kakovosti/varnosti), v polju „URI za opredelitev storitev sheme" (razdelek 5.5.6).

Vključuje najmanj dva URI:

1. URI, ki je skupen vsem zanesljivim seznamom držav članic, z napotilom na opisno besedilo, ki velja za vse zanesljive sezname, in sicer:

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

   Opisno besedilo:

   „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) scheme(s) 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 certificate(s) is(are) qualified under Directive 1999/93/EC;

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

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

— ‚QCForWSA' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is(are) qualified certificate(s) 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 certificate(s) is(are) not to be considered as qualified; and/or

— to indicate the nature of the SSCD support:

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

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

— ‚QCSSCDStatusAsInCert' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), 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 certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

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

— ‚QCQSCDStatusAsInCert' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), 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 certificate(s), when claimed or stated as qualified certificate(s), 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, ki je specifičen za zanesljivi seznam vsake države članice, z napotilom na opisno besedilo, ki velja za zanesljivi seznam te države članice:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, pri čemer je CC = ISO 3166-1 ([1]) dvočrkovna oznaka države, ki se uporablja v polju „Država sheme" (razdelek 5.3.10),

— podatki o tem, kje lahko uporabniki najdejo posebne politike/pravila za zadevno državo članico, v skladu s katerimi se storitve zaupanja v zanesljivem seznamu ocenjujejo v skladu s sistemom nadzora države članice in, kadar je to primerno, shemo potrjevanja,

— podatki o tem, kje lahko uporabniki najdejo posebni opis za zadevno državo članico glede načina uporabe in razlage vsebine zanesljivega seznama v zvezi z navedenimi nekvalificiranimi storitvami zaupanja in/ali nacionalno opredeljenimi storitvami zaupanja. Ta opis se lahko uporabi za navedbo morebitne razdrobljenosti v nacionalnih sistemih potrjevanja v zvezi z overitelji, ki ne izdajajo kvalificiranih potrdil, in kako se v ta namen uporabljata polji „URI za opredelitev storitev sheme" (razdelek 5.5.6) in „Razširitve informacij o storitvah" (razdelek 5.5.9).

Države članice LAHKO razširijo zgoraj naveden poseben URI za državo članico, tako da opredelijo in uporabijo dodatne URI (tj. URI, opredeljen na podlagi tega hierarhičnega posebnega URI).

Politika/pravno obvestilo v zvezi s seznamom o statusu storitev zaupanja (razdelek 5.3.11)

To polje mora biti vključeno in v skladu s specifikacijami iz razdelka 5.3.11 TS 119 612, v katerem je politika/pravno obvestilo v zvezi s pravnim statusom sheme ali pravnimi zahtevami, ki jih shema izpolnjuje v okviru pristojnosti, v kateri je bila vzpostavljena, in/ali kakršnimi koli omejitvami ter pogoji, na podlagi katerih se zanesljivi seznam vodi in

([1]) ISO 3166-1:2006: „Kode za predstavljanje imen držav in njihovih podrejenih enot – 1. del: Kode držav".

objavi, izražena z zaporedjem večjezikovnih znakovnih nizov (glej razdelek 5.1.4), ki v britanski angleščini kot obveznem jeziku in izbirno v enem ali več nacionalnih jezikih navaja dejansko besedilo take politike ali obvestilo, ki je sestavljeno na naslednji način:

1. prvi obvezni del, skupen vsem zanesljivim seznamom držav članic, v katerem je naveden veljaven pravni okvir v angleščini:

   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.

   Besedilo v nacionalnem jeziku države članice:

   Pravni okvir, ki se uporablja za ta zanesljivi seznam je Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES;

2. drugi, neobvezni del, ki je poseben za vsak zanesljivi seznam in navaja sklicevanje na nacionalni pravni okvir, ki se uporablja.

Trenutni status storitve (razdelek 5.5.4)

To polje mora biti vključeno in v skladu s specifikacijami iz razdelka 5.5.4. TS 119 612.

Migracija vrednosti „Trenutni status storitve“ storitev, ki so uvrščene na zanesljivi seznam držav članic EU od datuma pred začetkom veljavnosti Uredbe (EU) št. 910/2014 (tj. 30. junija 2016), se izvrši na datum začetka uporabe Uredbe (tj. 1. julija 2016), kot je določeno v Prilogi J k ETSI TS 119 612.

POGLAVJE III

NEPREKINJENA VELJAVNOST ZANESLJIVIH SEZNAMOV

Potrdila, ki se uradno sporočijo Komisiji v skladu s členom 4(2) tega sklepa, morajo izpolnjevati zahteve iz razdelka 5.7.1 ETSI TS 119 612 in se izdajo tako, da:

— so do njihovega končnega datuma veljavnosti najmanj trije meseci („NotAfter“),

— so bili generirani na podlagi novih parov ključev. Predhodno uporabljeni pari ključev se ne smejo ponovno potrjevati.

V primeru izteka veljavnosti enega od potrdil javnih ključev, ki se lahko uporabljajo za potrjevanje veljavnosti podpisa ali žiga zanesljivega seznama, ki je bil uradno sporočen Komisiji in je objavljen v osrednjem seznamu kazalcev Komisije, države članice:

— v primeru, da je bil trenutno objavljeni zanesljivi seznam podpisan ali ožigosan z zasebnim ključem, katerega potrdilo javnega ključa je poteklo, brez odlašanja ponovno izdajo nov zanesljivi seznam, podpisan ali ožigosan z zasebnim ključem, katerega uradno sporočeno potrdilo javnega ključa ni poteklo,

— na zahtevo generirajo nove pare ključev, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama, in generirajo ustrezna potrdila javnih ključev,

— nemudoma Komisiji uradno sporočijo nov seznam potrdil javnih ključev, ki ustrezajo zasebnim ključem, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama.

V primeru, da je kompromitiran ali deaktiviran eden od zasebnih ključev, ki ustreza potrdilu javnega ključa, ki se lahko uporabi za potrjevanje veljavnosti podpisa ali žiga zanesljivega seznama, in ki je bil uradno sporočen Komisiji ter objavljen v osrednjem seznamu kazalcev Komisije, države članice:

— brez odlašanja ponovno izdajo nov zanesljivi seznam, podpisan ali ožigosan z nekompromitiranim zasebnim ključem, če je bil objavljeni zanesljivi seznam podpisan ali ožigosan s kompromitiranim ali deaktiviranim zasebnim ključem,

— na zahtevo generirajo nove pare ključev, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama, in generirajo ustrezna potrdila javnih ključev,

— nemudoma Komisiji uradno sporočijo nov seznam potrdil javnih ključev, ki ustrezajo zasebnim ključem, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama.

V primeru, da so kompromitirani ali deaktivirani vsi zasebni ključi, ki ustrezajo potrdilom javnega ključa, ki se lahko uporabijo za potrjevanje veljavnosti podpisa zanesljivega seznama, in ki so bili uradno sporočeni Komisiji ter objavljeni v osrednjem seznamu kazalcev Komisije, države članice:

— generirajo nove pare ključev, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama, in generirajo ustrezna potrdila javnih ključev,

— brez odlašanja ponovno izdajo nov zanesljivi seznam, podpisan ali ožigosan z enim od navedenih novih zasebnih ključev, katerega ustrezno potrdilo javnega ključa je treba uradno sporočiti,

— nemudoma Komisiji uradno sporočijo nov seznam potrdil javnih ključev, ki ustrezajo zasebnim ključem, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama.

POGLAVJE IV

TEHNIČNE SPECIFIKACIJE ZA ČLOVEKU BERLJIVO OBLIKO ZANESLJIVEGA SEZNAMA

Kadar je pripravljena in objavljena človeku berljiva oblika zanesljivega seznama, se zagotavlja v obliki datoteke Portable Document Format (PDF) v skladu z ISO 32000 ([1]), katere format mora ustrezati profilu PDF/A (ISO 19005 ([2])).

Vsebina zanesljivega seznama v človeku berljivi obliki na podlagi PDF/A mora izpolnjevati naslednje zahteve:

— struktura človeku berljive oblike upošteva logični model, opisan v TS 119 612,

— prikazano je vsako vsebovano polje, ki vključuje:

  — naziv polja (npr. „Identifikator vrste storitve“),

  — vrednost polja (npr. „http://uri.etsi.org/TrstSvc/Svctype/CA/QC}“),

  — pomen (opis) vrednosti polja, kadar je to primerno (npr. „Storitev generiranja potrdil, s katero se generirajo in podpisujejo kvalificirana potrdila na podlagi identitete in drugih značilnosti, ki jih preverjajo zadevne registracijske službe.“),

  — kadar je to primerno, več različic v naravnih jezikih, kot so določene v zanesljivem seznamu,

— naslednja polja in ustrezne vrednosti digitalnih potrdil ([3]), če so izpolnjene v polju „Digitalna identiteta storitve“, morajo biti prikazane vsaj v človeku v berljivi obliki:

  — Različica

  — Serijska številka potrdila

  — Algoritem za podpis

  — Izdajatelj – vsa ustrezna polja z razločevalnimi imeni

  — Obdobje veljavnosti

  — Imetnik – vsa ustrezna polja z razločevalnimi imeni

([1]) ISO 32000-1:2008: Upravljanje dokumentov – Portable document format – del 1: PDF 1.7.
([2]) ISO 19005-2:2011: Upravljanje dokumentov – Format datoteke elektronskega dokumenta za dolgotrajno hrambo – del 2: Uporaba ISO 32000-1 (PDF/A-2).
([3]) Priporočilo ITU-T X.509 | ISO/IEC 9594-8: Informacijska tehnologija – Medsebojno povezovanje odprtih sistemov – Register: Strukture potrdil javnih ključev in atributov (glej http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— Javni ključ

— Identifikator izdajateljevega ključa

— Identifikator imetnikovega ključa

— Uporaba ključa

— Razširjena uporaba ključa

— Oznaka politike potrdila – vse enolične oznake politike in identifikatorji politike

— Določitve politike

— Alternativno ime imetnika

— Atributi direktorija imetnika

— Osnovne omejitve

— Politične omejitve

— Objava registra preklicanih potrdil ([1])

— Dostop do podatkov o overitelju

— Dostop do podatkov o imetniku

— Izjave, da je potrdilo kvalificirano ([2])

— Zgoščeni algoritem

— Zgoščena vrednost potrdila

— Človeku berljiva oblika mora biti enostavna za tiskanje.

— Človeku berljivo obliko podpiše ali ožigosa upravljavec sheme v skladu z naprednim podpisom PDF, določenim v členih 1 in 3 Izvedbenega sklepa Komisije (EU) 2015/1505.

([1]) RFC 5280: Potrdilo o infrastrukturi javnih ključev internet X. 509 PKI in profil registra preklicanih potrdil.
([2]) RFC 3739 internet X.509 PKI: Profil kvalificiranih potrdil.

PRILOGA II

PREDLOGA ZA URADNA OBVESTILA DRŽAV ČLANIC

Informacije, ki jih morajo države članice uradno sporočiti v skladu s členom 4(1) tega sklepa, vsebujejo naslednje podatke in vse njihove morebitne spremembe:

1. Država članica, ki uporablja kode ISO 3166-1 ([1]) Alpha 2 z naslednjimi izjemami:

   (a) koda države za Združeno kraljestvo je „UK“;

   (b) koda države za Grčijo je „EL“.

2. Organ oz. organi, odgovorni za sestavljanje, vodenje in objavo oblike zanesljivih seznamov, ki je primerna za avtomatizirano obdelavo, in zanesljivih seznamov v človeku berljivi obliki:

   (a) ime upravljavca sheme: zagotovljene informacije morajo biti enake vrednosti polja „Ime upravljavca sheme“ v zanesljivem seznamu, in sicer v vseh jezikih, ki se uporabljajo v zanesljivem seznamu (z ujemanjem velikih oziroma malih črk);

   (b) neobvezne informacije le za interno uporabe Komisije, kadar je treba stopiti v stik z zadevnim organom (informacije ne bodo objavljene na zbirnem seznamu Evropske komisije zanesljivih seznamov):

      — naslov upravljavca sheme,

      — kontaktni podatki odgovornih oseb (ime in priimek, telefon, e-naslov).

3. Kraj, kjer je objavljena oblika, primerna za avtomatizirano obdelavo zanesljivega seznama (*kraj, kjer je objavljen veljavni zanesljivi seznam*).

4. Kraj, kadar je to primerno, kjer je objavljen zanesljivi seznam v človeku berljivi obliki (*kraj, kjer je objavljen veljavni zanesljivi seznam*). Če zanesljivi seznam v človeku berljivi obliki ni več objavljen, se to navede.

5. Potrdila javnih ključev, ki ustrezajo zasebnim ključem, ki se lahko uporabljajo za elektronsko podpisovanje ali žigosanje oblike zanesljivega seznama, primerne za avtomatizirano obdelavo, in človeku berljive oblike zanesljivih seznamov: navedena potrdila se zagotovijo kot potrdila DER, prekodirana na način Base 64 v format PEM (Privacy Enhanced Mail). Ob uradnem obvestilu o spremembi se navedejo dodatne informacije, če se z novim potrdilom zamenja določeno potrdilo na seznamu Komisije in če se uradno sporočeno potrdilo doda k obstoječim, ne da bi se katero potrdilo zamenjalo.

6. Datum predložitve podatkov, ki se uradno sporočijo v točkah 1 do 5.

Podatki, uradno sporočeni v skladu s točkami 1, 2(a), 3, 4 in 5, se vključijo v zbirni seznam Evropske komisije zanesljivih seznamov, ki zamenja predhodno uradno sporočene informacije, vključene v navedeni zbirni seznam.

([1]) ISO 3166-1: „Kode za predstavljanje imen držav in njihovih podrejenih enot – 1. del: Kode držav“.