DECIZIA DE PUNERE ÎN APLICARE (UE) 2015/1505 A COMISIEI

din 8 septembrie 2015

de stabilire a specificațiilor tehnice și a formatelor pentru listele sigure în temeiul articolului 22 alineatul (5) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE ([1]), în special articolul 22 alineatul (5),

întrucât:

(1) Listele sigure sunt esențiale pentru construirea încrederii între operatorii de piață, deoarece ele indică statutul prestatorului de servicii în momentul supravegherii.

(2) Utilizarea transfrontalieră a semnăturilor electronice a fost facilitată prin Decizia 2009/767/CE a Comisiei ([2]), în care s-a stabilit obligația statelor membre de a crea, a menține și a publica liste sigure cu informații referitoare la prestatorii de servicii de certificare care eliberează certificate calificate publicului în conformitate cu Directiva 1999/93/CE a Parlamentului European și a Consiliului ([3]) și care sunt supravegheați și acreditați de către statele membre.

(3) La articolul 22 din Regulamentul (UE) nr. 910/2014 se prevede că statele membre au obligația să instituie, să mențină și să publice în mod securizat liste sigure semnate sau sigilate electronic într-o formă adecvată pentru prelucrarea automată, precum și obligația să notifice Comisiei organismele responsabile pentru instituirea listelor sigure naționale.

(4) Prestatorul de servicii de încredere și serviciile de încredere pe care le prestează ar trebui să fie considerate calificate în momentul în care prestatorului din lista sigură îi este atribuit statutul de calificat. Pentru a se asigura că prestatorii de servicii pot îndeplini cu ușurință, la distanță și prin mijloace electronice alte obligații care decurg din Regulamentul (UE) nr. 910/2014, în special pe cele prevăzute la articolele 27 și 37, și pentru a se răspunde așteptărilor legitime ale altor prestatori de servicii de certificare care nu eliberează certificate calificate, dar prestează servicii conexe semnăturilor electronice în temeiul Directivei 1999/93/CE și sunt înscriși în liste la 30 iunie 2016, statele membre ar trebui să aibă posibilitatea de a adăuga în listele sigure, la nivel național, și alte servicii de încredere decât cele calificate, dacă prestatorii respectivi doresc acest lucru, cu condiția să se indice clar că serviciile în cauză nu sunt calificate în conformitate cu Regulamentul (UE) nr. 910/2014.

(5) Conform considerentului 25 din Regulamentul (UE) nr. 910/2014, statele membre pot adăuga alte tipuri de servicii de încredere definite la nivel național decât cele definite la articolul 3 alineatul (16) din Regulamentul (UE) nr. 910/2014, cu condiția să se indice clar că serviciile în cauză nu sunt calificate în conformitate cu Regulamentul (UE) nr. 910/2014.

(6) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul comitetului instituit prin articolul 48 din Regulamentul (UE) nr. 910/2014,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Statele membre instituie, publică și mențin liste sigure cu informații referitoare la prestatorii de servicii de încredere calificați pe care îi supraveghează, precum și informații referitoare la serviciile de încredere calificate pe care aceștia le prestează. Listele respective îndeplinesc specificațiile tehnice stabilite în anexa I.

([1]) JO L 257, 28.8.2014, p. 73.

([2]) Decizia 2009/767/CE a Comisiei din 16 octombrie 2009 de stabilire a unor măsuri de facilitare a utilizării procedurilor prin mijloace electronice prin intermediul „ghișeelor unice” în temeiul Directivei 2006/123/CE a Parlamentului European și a Consiliului privind serviciile în cadrul pieței interne (JO L 274, 20.10.2009, p. 36).

([3]) Directiva 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice (JO L 13, 19.1.2000, p. 12).

Articolul 2

Statele membre pot include în listele sigure și informații referitoare la prestatorii de servicii de încredere necalificați, alături de informații referitoare la serviciile de încredere necalificate pe care aceștia le prestează. În listă se indică în mod clar care prestatori de servicii de încredere și care servicii de încredere prestate de aceștia sunt necalificate.

Articolul 3

(1) În temeiul articolului 22 alineatul (2) din Regulamentul (UE) nr. 910/2014, statele membre semnează sau sigilează electronic forma adecvată pentru prelucrarea automată a listei lor sigure, în conformitate cu specificațiile tehnice stabilite în anexa I.

(2) Dacă își publică electronic lista sigură într-o formă lizibilă pentru om, statele membre se asigură că forma respectivă a listei sigure conține aceleași date ca și forma adecvată pentru prelucrarea automată și o semnează sau sigilează electronic în conformitate cu specificațiile tehnice stabilite în anexa I.

Articolul 4

(1) Statele membre transmit Comisiei informațiile menționate la articolul 22 alineatul (3) din Regulamentul (UE) nr. 910/2014 utilizând modelul din anexa II.

(2) Informațiile menționate la alineatul (1) cuprind două sau mai multe certificate de cheie publică ale operatorului de program, cu perioade de valabilitate decalate în timp de cel puțin trei luni, care corespund cheilor private care pot fi utilizate pentru a semna sau a sigila electronic forma adecvată pentru prelucrarea automată a listei sigure și, când se publică, forma lizibilă pentru om.

(3) În temeiul articolului 22 alineatul (4) din Regulamentul (UE) nr. 910/2014, Comisia pune la dispoziția publicului, printr-un canal sigur către un server web autentificat, informațiile menționate la alineatele (1) și (2), astfel cum au fost notificate de către statele membre, într-o formă semnată sau sigilată care este adecvată pentru prelucrarea automată.

(4) Comisia poate să pună la dispoziția publicului, printr-un canal sigur către un server web autentificat, informațiile menționate la alineatele (1) și (2), astfel cum au fost notificate de către statele membre, într-o formă semnată sau sigilată lizibilă pentru om.

Articolul 5

Prezenta decizie intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezenta decizie este obligatorie în toate elementele sale și se aplică direct în toate statele membre.

Adoptată la Bruxelles, 8 septembrie 2015.

Pentru Comisie

Președintele

Jean-Claude JUNCKER

ANEXA I

SPECIFICAȚII TEHNICE PENTRU UN MODEL COMUN AL LISTELOR SIGURE

CAPITOLUL I

CERINȚE GENERALE

Listele sigure cuprind atât informațiile actuale, cât și toate informațiile istorice cu privire la statutul serviciilor de încredere care figurează în liste, începând cu data includerii unui prestator de servicii de încredere în listele sigure.

Termenii „omologat", „acreditat" și/sau „supravegheat" din prezentele specificații se referă și la sistemele naționale de omologare, dar statele membre furnizează, în lista lor sigură, informații suplimentare cu privire la natura oricărui astfel de sistem național, inclusiv clarificări cu privire la posibilele diferențe față de sistemele de supraveghere aplicate în cazul prestatorilor de servicii de încredere calificați și în cazul serviciilor de încredere calificate pe care aceștia le prestează.

Informațiile furnizate în lista sigură au ca scop principal susținerea validării dispozitivelor de autentificare pentru serviciile de încredere calificate, și anume obiecte fizice sau binare (logice) generate sau emise ca urmare a utilizării unui serviciu de încredere calificat, cum ar fi, în special, semnăturile/sigiliile electronice calificate, semnăturile/sigiliile electronice avansate bazate pe un certificat calificat, mărcile temporale calificate, dovezile de distribuție electronică calificată etc.

CAPITOLUL II

SPECIFICAȚII DETALIATE PENTRU MODELUL COMUN AL LISTELOR SIGURE

Prezentele specificații se bazează pe specificațiile și cerințele cuprinse în documentul intitulat „Specificațiile tehnice ale ETSI 119 612 v2.1.1" (denumit în continuare „ETSI TS 119 612").

Dacă în prezentele specificații nu sunt stabilite cerințe specifice, se aplică în întregime cerințele stabilite în secțiunile 5 și 6 din ETSI TS 119 612. Dacă în prezentele specificații sunt stabilite cerințe specifice, acestea prevalează asupra cerințelor corespunzătoare din ETSI TS 119 612. În cazul unor discrepanțe între prezentele specificații și specificațiile din ETSI TS 119 612, prevalează prezentele specificații.

Scheme name (denumirea programului) (secțiunea 5.3.6)

Acest câmp este obligatoriu și trebuie să respecte secțiunea 5.3.6 din TS 119 612, conform căreia pentru program trebuie să se folosească următoarea denumire:

„EN_name_value" = „Listă sigură cu informații referitoare la prestatorii de servicii de încredere calificați care sunt supravegheați de statul membru emitent și informații referitoare la serviciile de încredere calificate pe care aceștia le prestează, în conformitate cu dispozițiile relevante stabilite în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE."

Scheme information URI (URI-ul informațiilor despre program) (secțiunea 5.3.7)

Acest câmp este obligatoriu și trebuie să respecte secțiunea 5.3.7 din TS 119 612, conform căreia „informațiile corespunzătoare despre program" trebuie să cuprindă cel puțin:

(a) informații introductive, comune tuturor statelor membre, cu privire la domeniul și contextul listei sigure, la programul de supraveghere aflat la bază și, când este cazul, la programul (programele) național(e) de omologare (acreditare, de exemplu). Textul comun care trebuie să fie folosit și în care șirul de caractere „[*name of the relevant Member State*]" trebuie să fie înlocuit cu numele statului membru relevant este următorul:

> „Prezenta listă este lista sigură cu informații referitoare la prestatorii de servicii de încredere calificați care sunt supravegheați de [*numele statului membru în cauză*] și informații referitoare la serviciile de încredere calificate pe care aceștia le prestează, în conformitate cu dispozițiile relevante stabilite în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.

Utilizarea transfrontalieră a semnăturilor electronice a fost facilitată prin Decizia 2009/767/CE a Comisiei din 16 octombrie 2009 în care s-a stabilit obligația statelor membre de a crea, a menține și a publica liste sigure cu informații referitoare la prestatorii de servicii de certificare care eliberează certificate calificate publicului în conformitate cu Directiva 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 și care sunt supravegheați și acreditați de către statele membre. Prezenta listă sigură este continuarea listei sigure instituite prin Decizia 2009/767/CE."

Listele sigure sunt elemente esențiale pentru construirea încrederii între operatorii de pe piața electronică, permițând utilizatorilor să stabilească statutul de calificat și istoricul statutului în cazul prestatorilor de servicii de încredere și al serviciilor oferite de aceștia.

Listele sigure ale statelor membre cuprind cel puțin informațiile precizate la articolele 1 și 2 din Decizia de punere în aplicare (UE) 2015/1505 a Comisiei.

Statele membre pot include în listele sigure și informații cu privire la prestatorii de servicii de încredere necalificați, alături de informații cu privire la serviciile de încredere necalificate pe care aceștia le prestează. Trebuie să se indice clar că prestatorii și serviciile în cauză nu sunt calificate în conformitate cu Regulamentul (UE) nr. 910/2014.

Statele membre pot include în listele sigure informații cu privire la serviciile de încredere care sunt definite la nivel național și care sunt de alt tip decât cele definite la articolul 3 alineatul (16) din Regulamentul (UE) nr. 910/2014. Trebuie să se indice clar că prestatorii și serviciile în cauză nu sunt calificate în conformitate cu Regulamentul (UE) nr. 910/2014;

(b) informații specifice cu privire la programul de supraveghere aflat la bază și, când este cazul, la programul (programele) național(e) de omologare (acreditare, de exemplu), în special ([1]):

1. informații cu privire la sistemul național de supraveghere care se aplică în cazul prestatorilor de servicii de încredere calificați și necalificați și în cazul serviciilor de încredere calificate și necalificate pe care aceștia le prestează, în conformitate cu Regulamentul (UE) nr. 910/2014;

2. când este cazul, informații cu privire la sistemele naționale de omologare voluntară aplicabile prestatorilor de servicii de certificare care au emis certificate calificate în temeiul Directivei 1999/93/CE.

Aceste informații specifice trebuie să includă pentru fiecare program de bază menționat mai sus cel puțin următoarele:

1. o descriere generală;

2. informații cu privire la procedura urmată pentru sistemul național de supraveghere și, când este cazul, pentru omologarea în cadrul unui sistem național de omologare;

3. informații cu privire la criteriile după care sunt supravegheați sau, când este cazul, omologați prestatorii de servicii de încredere;

4. informații cu privire la criteriile și regulile aplicate pentru selectarea supraveghetorilor/auditorilor și pentru stabilirea modului în care aceștia evaluează prestatorii de servicii de încredere și serviciile de încredere prestate;

5. când este cazul, alte date de contact și informații generale cu privire la funcționarea programului.

Scheme type/community/rules (Tipul/comunitatea/regulile programului) (secțiunea 5.3.9)

Acest câmp este obligatoriu și trebuie să respecte secțiunea 5.3.9 din TS 119 612.

Câmpul trebuie să conțină numai URI-uri în engleza britanică.

([1]) Aceste seturi de informații au o importanță esențială pentru evaluarea de către beneficiari a nivelului de calitate și de siguranță al sistemelor respective. Aceste seturi de informații se furnizează la nivelul listei sigure prin utilizarea actualelor „Scheme information URI" (secțiunea 5.3.7 – informații furnizate de statul membru), „Scheme type/community/rules" (secțiunea 5.3.9 – prin utilizarea unui text comun tuturor statelor membre) și „TSL policy/legal notice" (secțiunea 5.3.11 – un text comun tuturor statelor membre, fiecare stat membru având posibilitatea de a adăuga texte/referințe care îi sunt specifice). Informațiile suplimentare cu privire la aceste sistem pentru serviciile de încredere necalificate și pentru serviciile de încredere (calificate) care sunt definite la nivel național pot fi furnizate la nivelul fiecărui serviciu, când este cazul și dacă este necesar (de exemplu pentru a se distinge între mai multe niveluri de calitate/siguranță), prin utilizarea „Scheme service definition URI" (secțiunea 5.5.6).

Câmpul trebuie să conțină cel puțin două URI-uri:

1. Un URI comun tuturor listelor sigure ale statelor membre, care trimite la un text descriptiv aplicabil tuturor listelor sigure, după cum urmează:

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

   Text descriptiv:

   „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. Un URI specific pentru fiecare listă sigură a unui stat membru care trimite la un text descriptiv aplicabil listei sigure a statului membru respectiv:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC unde CC = codul țării ISO 3166-1 ([1]) alpha-2 utilizat în câmpul „Scheme territory" (secțiunea 5.3.10)

— unde utilizatorii găsesc politica/regulile specifice ale statului membru respectiv, pe baza cărora sunt evaluate serviciile de încredere incluse în listă, în conformitate cu regimul de supraveghere al statului membru și, când este cazul, cu sistemul de omologare al acestuia;

— unde utilizatorii găsesc o descriere specifică oferită de statul membru respectiv cu privire la modul de utilizare și de interpretare a conținutului listei sigure în ceea ce privește serviciile de încredere necalificate care figurează în listă și/sau serviciile de încredere definite la nivel național. Acesta poate fi utilizat pentru a indica o eventuală divizare în cadrul sistemului național de omologare în ceea ce privește CSP care nu eliberează QC și modul în care se utilizează „Scheme service definition URI" (secțiunea 5.5.6) și câmpul „Service information extension" (secțiunea 5.5.9) în acest scop.

Statele membre POT defini și utiliza URI-uri suplimentare prin extinderea URI-ului specific al statului membru, menționat mai sus (cu alte cuvinte URI-uri definite pornind de la acest URI ierarhic specific).

TSL policy/legal notice (Politica/avizul juridic al TSL) (secțiunea 5.3.11)

Acest câmp este obligatoriu și trebuie să respecte secțiunea 5.3.11 din TS 119 612. Câmpul conține politica/avizul juridic privind statutul juridic al programului sau cerințele juridice respectate de program în temeiul jurisdicției în care este stabilit și/sau eventualele constrângeri și condiții în care lista sigură este menținută și publicată. Informațiile sunt

([1]) ISO 3166-1:2006: „Coduri pentru reprezentarea numelor țărilor și ale subdiviziunilor acestora – Partea 1: Codurile țărilor".

prezentate sub forma unei secvențe de șiruri de caractere multilingve (a se vedea secțiunea 5.1.4) care redă, obligatoriu în engleza britanică și opțional în una sau mai multe limbi naționale, textul efectiv al politicii respective sau al avizului respectiv, după următoarea structură:

1. O primă parte obligatorie, comună tuturor listelor sigure ale statelor membre, în care se precizează cadrul juridic aplicabil și a cărei versiune în limba engleză este următoarea:

   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.

   Textul în limba națională a (limbile naționale ale) unui stat membru:

   Cadrul juridic aplicabil pentru prezenta listă sigură este Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.

2. O a doua parte, opțională, specifică fiecărei listei sigure, în care se menționează trimiterile la cadrele juridice naționale aplicabile în cazul respectiv.

Service current status (Statutul actual al serviciului) (secțiunea 5.5.4)

Acest câmp este obligatoriu și trebuie să respecte secțiunea 5.5.4 din TS 119 612.

În cazul serviciilor care sunt introduse în listele sigure ale statelor membre ale UE în ziua dinaintea zilei de aplicare a Regulamentul (UE) nr. 910/2014 (și anume 30 iunie 2016), migrația valorii „Service current status” se efectuează la data aplicării regulamentului (și anume 1 iulie 2016), astfel cum se specifică în anexa J la ETSI TS 119 612.

CAPITOLUL III

CONTINUITATEA LISTELOR SIGURE

Certificatele care trebuie notificate Comisiei în conformitate cu articolul 4 alineatul (2) din prezenta decizie trebuie să îndeplinească cerințele stabilite în secțiunea 5.7.1 din ETSI TS 119 612 și, în momentul emiterii, să îndeplinească următoarele condiții:

— să prezinte o diferență de cel puțin trei luni în ultima lor zi de valabilitate („Nu după”); și

— să fie create pe baza unor perechi noi de chei. Perechile de chei utilizate anterior nu trebuie să fie certificate din nou.

În cazul expirării unuia dintre certificatele cu cheie publică la care s-ar putea recurge pentru validarea semnăturii sau a sigiliului listei sigure care a fost notificată Comisiei și publicată în lista centrală de indicatori a Comisiei, statele membre trebuie:

— să emită, fără întârziere, o nouă listă sigură semnată sau sigilată cu o cheie privată al cărei certificat cu cheie publică nu a expirat, în cazul în care lista sigură publicată la momentul respectiv a fost semnată sau sigilată cu o cheie privată al cărei certificat cu cheie publică a expirat;

— când este necesar, să genereze noi perechi de chei care ar putea fi utilizate pentru semnarea sau sigilarea listei sigure și să asigure generarea certificatelor corespunzătoare cu cheie publică;

— să notifice prompt Comisiei noua listă de certificate cu cheie publică corespunzătoare cheilor private care ar putea fi utilizate pentru semnarea sau sigilarea listei sigure.

În cazul compromiterii sau al desființării uneia dintre cheile private corespunzătoare unuia dintre certificatele cu cheie publică la care s-ar putea recurge pentru validarea semnăturii sau a sigiliului listei sigure care a fost notificată Comisiei și publicată în lista centrală de indicatori a Comisiei, statele membre trebuie:

— să emită, fără întârziere, o nouă listă sigură semnată sau sigilată cu o cheie privată necompromisă în cazurile în care lista sigură publicată a fost semnată sau sigilată cu o cheie privată compromisă sau desființată;

— când este necesar, să genereze noi perechi de chei care ar putea fi utilizate pentru semnarea sau sigilarea listei sigure și să asigure generarea certificatelor corespunzătoare cu cheie publică;

— să notifice prompt Comisiei noua listă de certificate cu cheie publică corespunzătoare cheilor private care ar putea fi utilizate pentru semnarea sau sigilarea listei sigure.

În cazul compromiterii sau desființării tuturor cheilor private corespunzătoare certificatelor cu cheie publică la care s-ar putea recurge pentru validarea semnăturii listei sigure care a fost notificată Comisiei și publicată în lista centrală de indicatori a Comisiei, statele membre trebuie:

— să genereze noi perechi de chei care ar putea fi utilizate pentru semnarea sau sigilarea listei sigure și să asigure generarea certificatelor corespunzătoare cu cheie publică;

— să emită, fără întârziere, o nouă listă sigură semnată sau sigilată cu una dintre cheile private noi al căror certificat corespunzător cu cheie publică urmează a fi notificat;

— să notifice prompt Comisiei noua listă de certificate cu cheie publică corespunzătoare cheilor private care ar putea fi utilizate pentru semnarea sau sigilarea listei sigure.

CAPITOLUL IV

SPECIFICAȚII PRIVIND FORMA LIZIBILĂ PENTRU OM A LISTEI SIGURE

În cazul în care se creează și se publică o formă lizibilă pentru om a listei sigure, aceasta trebuie să fie prezentată ca document PDF (Portable Document Format) conform ISO 32000 ([1]) care trebuie formatat conform profilului PDF/A (ISO 19005 ([2])).

Conținutul listei sigure în forma lizibilă pentru om bazată pe PDF/A trebuie să respecte următoarele cerințe:

— structura formei lizibile pentru om trebuie să reflecte modelul logic descris în TS 119 612;

— fiecare câmp existent trebuie să fie afișat și să cuprindă:

  — denumirea câmpului (de exemplu, „Service type identifier”);

  — valoarea câmpului (de exemplu, „http://uri.etsi.org/TrstSvc/Svctype/CA/QC”);

  — sensul (descrierea) valorii câmpului, atunci când este cazul (de exemplu „A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.”);

  — versiuni în mai multe limbi naturale, astfel cum sunt prevăzute în lista sigură, atunci când este cazul;

— în forma lizibilă pentru om trebuie să fie afișate cel puțin următoarele câmpuri și valori corespunzătoare ale certificatelor digitale ([3]), dacă sunt prezente în câmpul „Service digital identity”:

  — versiunea;

  — seria certificatului;

  — algoritmul semnăturii;

  — emitentul – toate câmpurile relevante ale numelui distinctiv;

  — perioada de valabilitate;

  — subiectul – toate câmpurile relevante ale numelui distinctiv;

([1]) ISO 32000-1:2008: Managementul documentelor – Formatul documentelor portabile – Partea 1: PDF 1.7

([2]) ISO 19005-2:2011: Managementul documentelor – Formatul de fișier al documentelor electronice pentru o conservare pe termen lung – Partea 2: Utilizarea ISO 32000-1 (PDF/A-2)

([3]) Recomandarea ITU-T X.509 | ISO/IEC 9594-8: Tehnologia informației – Interconectarea sistemelor deschise – Catalogul: Cadrul-general al certificatelor cu cheie publică și atribut (a se vedea http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509)

— cheia publică;

— identificatorul cheii autorității;

— identificatorul cheii subiectului;

— utilizarea cheii;

— utilizarea extinsă a cheii;

— politicile de certificare – toți identificatorii politicilor și toate calificativele politicilor;

— mapările de politici;

— numele alternativ al subiectului;

— atributul catalogului subiectului;

— restricțiile de bază;

— restricțiile de politici;

— punctele de distribuire ale CRL ([1]);

— accesul la informații despre autoritate;

— accesul la informații despre subiect;

— declarațiile certificatului calificat ([2]);

— algoritmul hash;

— valoarea hash a certificatului;

— forma lizibilă pentru om trebuie să fie ușor de imprimat;

— forma lizibilă pentru om trebuie să fie semnată sau sigilată de către operatorul programului în conformitate cu semnătura avansată pentru PDF prevăzută la articolele 1 și 3 din Decizia de punere în aplicare (UE) 2015/1505.

([1]) RFC 5280: internet X. 509 – Certificatul PKI și profilul CRL
([2]) RFC 3739: internet X. 509 – PKI: Profilul certificatelor calificate

ANEXA II

MODEL PENTRU NOTIFICĂRILE EFECTUATE DE STATELE MEMBRE

Informațiile pe care statele membre le notifică în temeiul articolului 4 alineatul (1) din prezenta decizie cuprind următoarele elemente, precum și orice modificare adusă acestora:

1. Statul membru, indicat cu ajutorul codurilor ISO 3166-1 ([1]) alfa-2, cu următoarele excepții:

   (a) codul de țară pentru Regatul Unit este „UK”;

   (b) codul de țară pentru Grecia este „EL”.

2. Organismul/organismele responsabil(e) pentru instituirea, menținerea și publicarea listelor sigure în forma adecvată pentru prelucrarea automată și în forma lizibilă pentru om:

   (a) denumirea operatorului programului: informațiile furnizate trebuie să fie identice – cu respectarea regimului de litere mici și mari – cu valoarea „Scheme operator name” din lista sigură în toate limbile utilizate în această listă;

   (b) informații opționale numai pentru uzul intern al Comisiei în cazurile în care trebuie contactat organismul competent (informațiile nu vor fi publicate în inventarul listelor sigure, realizat de Comisia Europeană):

      — adresa operatorului sistemului;

      — datele de contact ale persoanei (persoanelor) responsabile (numele, numărul de telefon, adresa de e-mail).

3. Locul unde este publicată lista sigură în forma adecvată pentru prelucrarea automată *(locul unde este publicată lista sigură curentă)*.

4. Dacă este cazul, locul unde este publicată lista sigură în forma lizibilă pentru om *(locul unde este publicată lista sigură curentă)*. Dacă lista sigură nu se mai publică în forma lizibilă pentru om, indicarea acestui lucru.

5. Certificatele cu cheie publică corespunzătoare cheilor private care pot fi utilizate pentru semnarea sau sigilarea electronică a listelor sigure în forma adecvată pentru prelucrarea automată și în forma lizibilă pentru om: certificatele respective se transmit sub formă de certificate DER Privacy Enhanced Mail Base64. Pentru notificarea unei modificări, informații suplimentare în cazul în care un anumit certificat din lista Comisiei urmează să fie înlocuit cu un certificat nou și în cazul în care la certificatul (certificatele) existent(e) se adaugă un certificat notificat, fără a avea loc vreo înlocuire.

6. Data notificării informațiilor menționate la punctele 1-5.

Informațiile menționate la punctul 1, punctul 2 litera (a) și punctele 3, 4 și 5 se înscriu, după ce au fost notificate, în inventarul listelor sigure, realizat de Comisia Europeană, înlocuind informațiile notificate anterior care fuseseră înscrise în acest inventar.

([1]) ISO 3166-1: „Coduri pentru reprezentarea numelor țărilor și ale subdiviziunilor acestora – Partea 1: Codurile țărilor”.