DECIZIA DE PUNERE ÎN APLICARE A COMISIEI

din 14 octombrie 2013

de modificare a Deciziei 2009/767/CE în ceea ce privește crearea, menținerea și publicarea listelor sigure de prestatori de servicii de certificare supravegheați/acreditați de către statele membre

[notificată cu numărul C(2013) 6543]

(Text cu relevanță pentru SEE)

(2013/662/UE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Directiva 2006/123/CE a Parlamentului European și a Consiliului din 12 decembrie 2006 privind serviciile în cadrul pieței interne [1], în special articolul 8 alineatul (3),

întrucât:

(1) 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 [2] prevede că statele membre trebuie să pună la dispoziție informațiile necesare pentru validarea semnăturilor electronice avansate bazate pe un certificat calificat. Informațiile respective trebuie să fie stabilite în mod uniform cu ajutorul așa-numitelor „liste sigure", care conțin informații cu privire la prestatorii de servicii de certificare care eliberează certificate calificate pentru public, în conformitate cu Directiva 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice [3] și sunt supravegheați/acreditați de către statele membre.

(2) Experiența practică în punerea în aplicare a Deciziei 2009/767/CE de către statele membre a arătat că sunt necesare anumite îmbunătățiri pentru a maximiza beneficiile listelor sigure. Mai mult, Institutul European de Standardizare în Telecomunicații (ETSI) a publicat specificații tehnice noi pentru liste sigure (TS 119 612), care se bazează pe specificațiile incluse în prezent în anexa la decizie, dar care, în același timp, aduc o serie de îmbunătățiri specificațiilor existente.

(3) Prin urmare, Decizia 2009/767/CE ar trebui modificată pentru a se referi la specificațiile tehnice ETSI 119 612 și pentru a încorpora modificări considerate necesare pentru a îmbunătăți și a facilita punerea în aplicare și utilizarea listelor sigure.

(4) Pentru a permite statelor membre să efectueze modificările tehnice necesare la listele sigure actuale, este oportun ca prezenta decizie să se aplice de la 1 februarie 2014.

(5) Măsurile prevăzute în prezenta decizie sunt în conformitate cu avizul Comitetului pe probleme referitoare la Directiva privind serviciile,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Modificări aduse Deciziei 2009/767/CE

Decizia 2009/767/CE se modifică după cum urmează:

1. articolul 2 se modifică după cum urmează:

(a) alineatele (1), (2) și (2a) se înlocuiesc cu următorul text:

„(1) Fiecare stat membru creează, menține și publică, în conformitate cu specificațiile tehnice prevăzute în anexă, o „listă sigură" care conține un minimum de informații referitoare la prestatorii de servicii de certificare care eliberează certificate calificate publicului, pe care statele membre îi supraveghează/acreditează.";

„(2) Statele membre creează și publică o versiune care poate fi prelucrată de calculator a listei sigure în conformitate cu specificațiile prevăzute în anexă. În cazul în care un stat membru decide să publice o versiune lizibilă pentru om a listei sale sigure, versiunea respectivă a listei sigure trebuie să fie în conformitate cu specificațiile din anexă.";

„(2a) Statele membre semnează electronic versiunea care poate fi prelucrată de calculator a listei lor sigure pentru a asigura autenticitatea și integritatea acesteia. În cazul în care un stat membru publică o versiune lizibilă pentru om a listei sigure, acesta trebuie să se asigure că versiunea respectivă a listei sigure conține aceleași date ca și versiunea care poate fi prelucrată de calculator și o semnează electronic cu același certificat utilizat pentru versiunea care poate fi prelucrată de calculator.";

[1] JO L 376, 27.12.2006, p. 36.
[2] JO L 274, 20.10.2009, p. 36.
[3] JO L 13, 19.1.2000, p. 12.

(b) se introduce următorul alineat (2b):

„(2b) Statele membre se asigură că versiunea care poate fi prelucrată de calculator a listei lor sigure este accesibilă la locul de publicare a acesteia în orice moment, fără întrerupere, cu excepția întreruperilor în scopuri de întreținere.";

(c) alineatul (3) se înlocuiește cu următorul text:

„(3) Statele membre transmit Comisiei următoarele informații:

(a) organismul sau organismele responsabile pentru crearea, menținerea și publicarea versiunii care poate fi prelucrată de calculator a listei sigure;

(b) locul în care este publicată versiunea care poate fi prelucrată de calculator a listei sigure;

(c) două sau mai multe certificate de cheie publică ale operatorului de program, cu perioade de valabilitate schimbate de cel puțin trei luni, care corespund cheilor private care pot fi utilizate pentru a semna electronic versiunea care poate fi prelucrată de calculator a listei sigure;

(d) orice modificări ale informațiilor de la literele (a), (b) și (c).";

(d) se introduce următorul alineat (3a):

„(3a) În cazul în care un stat membru publică o versiune lizibilă pentru om a listei sigure, informațiile menționate la alineatul (3) se comunică, de asemenea, în ceea ce privește versiunea lizibilă pentru om.";

2. anexa se înlocuiește cu anexa la prezenta decizie.

Articolul 2

Aplicare

Prezenta decizie se aplică de la 1 februarie 2014.

Articolul 3

Destinatari

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles, 14 octombrie 2013.

Pentru Comisie

Michel BARNIER

Membru al Comisiei

ANEXĂ

SPECIFICAȚII TEHNICE PENTRU UN MODEL COMUN AL „LISTEI SIGURE A PRESTATORILOR DE SERVICII DE CERTIFICARE SUPRAVEGHEAȚI/ACREDITAȚI”

CERINȚE GENERALE

1. **Introducere**

Scopul modelului comun al „Listei sigure a prestatorilor de servicii de certificare supravegheați/acreditați” întocmită de statele membre este de a institui o modalitate comună prin care fiecare stat membru oferă informații despre statutul supravegherii/acreditării serviciilor de certificare furnizate de prestatorii de servicii de certificare [1] (CSP) care sunt supravegheați/acreditați de către statele membre în vederea conformității cu dispozițiile relevante ale Directivei 1999/93/CE. Aceasta include furnizarea de informații istorice cu privire la statutul supravegherii/acreditării serviciilor de certificare supravegheate/acreditate.

Astfel de informații au ca scop principal susținerea validării semnăturilor electronice calificate (QES) și a semnăturilor electronice avansate (AdES) [2] bazate pe un certificat calificat [3] [4].

Informațiile obligatorii din lista sigură (TL) trebuie să cuprindă, cel puțin, informații privind CSP supravegheați/acreditați care eliberează certificate calificate (QC) [5] în conformitate cu dispozițiile Directivei 1999/93/CE [articolul 3 alineatele (2) și (3) și articolul 7 alineatul (1) litera (a)], inclusiv, în cazul în care acestea nu fac parte din QC, informații despre QC care stau la baza unei semnături electronice și despre eventuala utilizare a unui dispozitiv securizat de creare a semnăturii (SSCD) pentru crearea semnăturii electronice [6].

Informații suplimentare privind alți CSP care nu eliberează QC, dar prestează servicii legate de semnăturile electronice (de exemplu, CSP care furnizează servicii de marcare temporală și eliberează jetoane de marcare temporală, CSP care eliberează certificate necalificate etc.) pot fi incluse în lista sigură la nivel național în mod voluntar, cu condiția ca aceștia să fie acreditați/supravegheați într-un mod similar cu CSP care eliberează QC sau să fie aprobați în cadrul unui sistem diferit de omologare la nivel național. În unele state membre, sistemele naționale de omologare pot diferi de sistemele de supraveghere sau de acreditare voluntară aplicabile pentru CSP care eliberează QC în ceea ce privește cerințele aplicabile și/sau organizația responsabilă. Termenii „acreditat” și/sau „supravegheat” din prezentele specificații acoperă, de asemenea, sistemele naționale de omologare, iar statele membre vor furniza informații suplimentare cu privire la natura oricăror sisteme naționale în lista lor sigură, inclusiv clarificări cu privire la posibilele diferențe față de sistemele de acreditare/supraveghere aplicate la CSP care eliberează QC.

Modelul comun se bazează pe ETSI TS 119 612 v1.1.1 [7] (denumit în continuare ETSI TS 119 612), care se referă la crearea, publicarea, localizarea, accesul, autentificarea și integritatea unor astfel de liste.

2. **Structura modelului comun pentru lista sigură**

Modelul comun pentru lista sigură a unui stat membru este structurat conform ETSI TS 119 612 în următoarele categorii de informații:

1. o etichetă a listei sigure care facilitează identificarea listei sigure în timpul căutărilor electronice;

2. informații privind lista sigură și sistemul de publicare a acesteia;

3. o secvență de câmpuri care conțin informații de identificare neechivoce cu privire la fiecare CSP supravegheat/acreditat din cadrul programului (secvența este opțională, și anume, dacă aceasta nu este utilizată, lista va fi considerată goală, însemnând că niciun CSP nu este supravegheat sau acreditat în statul membru asociat în contextul domeniului listei sigure);

4. pentru fiecare CSP inclus pe listă, detaliile serviciilor sale de încredere specifice al căror statut actual este înregistrat în lista sigură sunt furnizate ca o secvență de câmpuri care identifică neechivoc serviciile de certificare supravegheate/acreditate furnizate de CSP și statutul lor actual (secvența trebuie să aibă minimum o intrare);

[1] Conform definiției de la articolul 2 punctul 11 din Directiva 1999/93/CE.
[2] Conform definiției de la articolul 2 punctul 2 din Directiva 1999/93/CE.
[3] Pentru o AdES bazată pe un QC, se va folosi pe parcursul prezentului document acronimul „$AdES_{QC}$”.
[4] Trebuie menționat că există un număr de servicii electronice bazate pe AdES simplă, a căror utilizare transfrontalieră va fi, de asemenea, facilitată, cu condiția ca serviciile de certificare ce susțin respectiva semnătură (de exemplu, eliberarea de certificate necalificate) să facă parte din serviciile supravegheate/acreditate incluse de un stat membru pe lista lor sigură, printre informațiile furnizate în mod voluntar.
[5] Conform definiției de la articolul 2 punctul 10 din Directiva 1999/93/CE.
[6] Conform definiției de la articolul 2 punctul 6 din Directiva 1999/93/CE.
[7] ETSI TS 119 612 v1.1.1 (2013-06) – Semnături și infrastructuri electronice (*Electronic Signatures and Infrastructures* – ESI); Liste sigure.

5. pentru fiecare serviciu de certificare supravegheat/acreditat inclus pe listă, informațiile cu privire la istoricul statutului, atunci când este cazul;

6. semnătura aplicată pe lista sigură.

În contextul unui CSP care eliberează QC, structura listei sigure, în special, componenta de informații privind serviciul (în conformitate cu punctul 4 de mai sus), permite prezentarea de informații complementare în extensii de informații privind serviciul pentru a compensa situațiile în care în certificatul calificat nu sunt disponibile suficiente informații (care pot fi prelucrate de calculator) cu privire la statutul său „calificat", eventualul suport din partea unui SSCD și mai ales pentru a aborda faptul suplimentar că majoritatea CSP-urilor (din domeniul comercial) apelează la o singură autoritate de certificare (CA) emitentă pentru a emite diferite tipuri de certificate, atât calificate, cât și necalificate, pentru entitățile finale.

În contextul serviciilor de generare de certificate (CA), numărul de intrări de servicii în lista pentru un CSP poate fi redus în cazul în care în infrastructura cu cheie publică (*Public Key Infrastructure* – PKI) a CSP există unul sau mai multe servicii CA superioare (de exemplu, în contextul unei ierarhii de CA-uri dintr-o autoritate de certificare de bază (Root CA) în sens descendent până la mai multe CA emitente) prin includerea în listă a unor astfel de servicii CA superioare și nu a serviciilor CA care eliberează certificate pentru entitățile finale (de exemplu, menționând în listă doar Root CA a CSP). Cu toate acestea, în astfel de cazuri, informațiile despre statut se aplică întregii ierarhii de servicii CA de sub serviciul inclus în listă, fiind necesar să se mențină și să se asigure respectarea principiului de garantare a unei legături neechivoce între un serviciu de certificare al unui CSP_{QC} și setul de certificate care urmează să fie identificate ca QC.

2.1. *Descrierea informațiilor din fiecare categorie*

1. Eticheta listei sigure

2. Informații privind lista sigură și sistemul de publicare a acesteia

Această categorie va cuprinde, printre altele, următoarele informații:

— un **identificator al versiunii formatului** listei sigure;

— un **număr de secvență (sau de publicare)** al listei sigure;

— **informații privind tipul** listei sigure (de exemplu, pentru a identifica dacă lista sigură în cauză furnizează informații cu privire la statutul supravegherii/acreditării aferent serviciilor de certificare furnizate de CSP supravegheate/acreditate de statul membru de referință în vederea conformității cu dispozițiile Directivei 1999/93/CE);

— **informații privind operatorul (proprietarul) programului** listei sigure (de exemplu, numele, adresa, informațiile de contact etc. ale organismului din statul membru responsabil pentru crearea, publicarea în condiții de siguranță și menținerea listei sigure);

— **informații cu privire la programul (programele) de bază de supraveghere/acreditare** cu care este asociată lista sigură, inclusiv, printre altele:

  — țara în care se aplică;

  — informații despre sau trimiteri la locația unde sunt disponibile informațiile cu privire la program(e) (modelul, regulile, criteriile, comunitatea în care se aplică, tipul programului etc.);

  — perioada de păstrare a informațiilor (istorice).

— **politica și/sau avizul juridic, obligațiile și responsabilitățile aferente** listei sigure;

— **data și ora publicării** listei sigure;

— **următoarea actualizare prevăzută** a listei sigure.

3. Informații de identificare neechivoce cu privire la fiecare CSP supravegheat/acreditat în cadrul programului

Acest set va cuprinde cel puțin următoarele informații:

— denumirea organizației CSP, astfel cum este utilizată în înregistrările juridice oficiale (inclusiv codul unic de identificare – UID – al organizației CSP în conformitate cu practicile statului membru);

— adresa și informațiile de contact ale CSP;

— informații suplimentare cu privire la CSP, fie menționate direct, fie indicate printr-o trimitere la adresa de unde acestea pot fi descărcate.

4. Pentru fiecare CSP inclus pe listă, o secvență de câmpuri cuprinzând informații neechivoce de identificare privind un serviciu de certificare furnizat de CSP și supravegheat/acreditat în cadrul Directivei 1999/93/CE

Acest set de informații include pentru fiecare serviciu de certificare furnizat de un CSP de pe listă cel puțin următoarele detalii:

— identificator al tipului de serviciu (*Service type identifier*): un identificator al tipului de serviciu de certificare (de exemplu, un identificator care să indice că serviciul de certificare supravegheat/acreditat furnizat de CSP este o autoritate de certificare care eliberează QC);

— denumirea (comercială) a serviciului [*Service (trade) name*]: denumirea (comercială) a serviciului de certificare respectiv;

— identitatea digitală a serviciului (*Service digital identity*): un identificator unic neechivoc al serviciului de certificare;

— statutul curent al serviciului (*Service current status*): un identificator al statutului curent al serviciului;

— data și ora la care s-a trecut la statutul curent (*Current status starting date and time*);

— extensia de informații privind serviciul (*Service information extension*), atunci când este cazul: informații suplimentare cu privire la serviciu (de exemplu, menționate direct sau indicate printr-o trimitere la adresa de unde pot fi descărcate): informații privind definiția serviciului furnizate de către operatorul programului, informații de acces cu privire la serviciu, informații privind definiția serviciului furnizate de către CSP și extensii de informații privind serviciul. De exemplu, pentru serviciile CA/QC, o secvență opțională de tupluri cu informații, fiecare dintre acestea furnizând:

  — criterii care vor fi utilizate la identificarea (filtrarea) mai precisă în cadrul serviciului sigur identificat a setului precis de rezultate ale serviciului [de exemplu, set de certificate (calificate)] pentru care sunt solicitate/furnizate informații suplimentare cu privire la statutul acestuia, indicarea dacă se bazează sau nu pe un SSCD și/sau eliberarea către o persoană juridică; precum și

  — „calificativele" asociate care furnizează informații indicând dacă setul de rezultate ale serviciului identifică sau nu certificate pentru a fi considerate calificate și/sau dacă certificatele calificate identificate provenite de la acest serviciu se bazează sau nu pe un SSCD și/sau informații referitoare la eventualitatea ca astfel de QC să fie eliberate pentru persoane juridice (acestea sunt considerate implicit ca fiind eliberate persoanelor fizice).

5. Pentru fiecare serviciu de certificare inclus în listă, informațiile istorice cu privire la statutul acestuia

6. O semnătură computerizată pentru autentificare pe toate câmpurile aferente TL, cu excepția valorii semnăturii

3. **Orientări privind editarea intrărilor în Lista sigură**

3.1. *Informații privind statutul serviciilor de certificare supravegheate/acreditate și furnizorii acestora, într-o listă unică*

Lista sigură a unui stat membru este definită drept „Lista privind statutul supravegherii/acreditării serviciilor de certificare furnizate de prestatorii de servicii de certificare care sunt supravegheați/acreditați de către statul membru în cauză în vederea conformității cu dispozițiile relevante ale Directivei 1999/93/CE".

O astfel de listă sigură este instrumentul unic care trebuie să fie utilizat de către statul membru în cauză pentru a furniza informații cu privire la statutul de supraveghere/acreditare a serviciilor de certificare și la furnizorii acestora:

— **toți prestatorii de servicii de certificare**, astfel cum sunt definiți la articolul 2 punctul 11 din Directiva 1999/93/CE, și anume „orice entitate sau persoană fizică sau juridică ce eliberează certificate sau prestează alte servicii referitoare la semnăturile electronice";

— **care sunt supravegheați/acreditați** în vederea conformității cu dispozițiile relevante ale Directivei 1999/93/CE.

În ceea ce privește definițiile și dispozițiile prevăzute în Directiva 1999/93/CE, în special cele referitoare la CSP relevanți și la sistemele lor de supraveghere/acreditare voluntară, se pot distinge două categorii de CSP, și anume CSP care eliberează QC pentru public (CSP_{QC}) și CSP care nu eliberează QC pentru public, însă prestează „alte servicii (auxiliare) referitoare la semnăturile electronice":

— **CSP care eliberează QC**:

  — aceștia trebuie să fie supravegheați de statul membru în care sunt stabiliți (dacă sunt stabiliți într-un stat membru) și pot fi și acreditați în vederea conformității cu dispozițiile Directivei 1999/93/CE, inclusiv cerințele din anexa I (cerințe privind QC) și din anexa II (cerințe privind CSP care eliberează QC). CSP care eliberează QC și sunt acreditați într-un stat membru trebuie să facă totuși obiectul unui sistem adecvat de supraveghere al statului membru în cauză, cu excepția cazului în care nu sunt stabiliți în statul membru respectiv;

— sistemul aplicabil de „supraveghere” (respectiv sistemul de „acreditare voluntară”) este definit în Directiva 1999/93/CE și trebuie să îndeplinească cerințele relevante ale acesteia, în special cele prevăzute la articolul 3 alineatul (3), articolul 8 alineatul (1), articolul 11, considerentul 13 [respectiv, articolul 2 punctul 13, articolul 3 alineatul (2), articolul 7 alineatul (1) litera (a), articolul 8 alineatul (1), articolul 11 și considerentele 4, 11, 12, 13].

— **CSP care nu eliberează QC**:

— aceștia pot intra sub incidența unui sistem de „acreditare voluntară” (în conformitate cu definiția și cu dispozițiile din Directiva 1999/93/CE) și/sau a unui „program de aprobare recunoscut” definit și pus în aplicare la nivel național în vederea supravegherii conformității cu dispozițiile directivei și eventual cu dispozițiile naționale în ceea ce privește prestarea serviciilor de certificare (în sensul articolului 2 punctul 11 din Directiva 1999/93/CE);

— unele dintre obiectele fizice sau binare (logice) generate sau eliberate ca urmare a prestării unui serviciu de certificare pot avea dreptul la o „calificare” specifică pe baza conformității lor cu dispozițiile și cerințele stabilite la nivel național, însă semnificația unei astfel de „calificări” este probabil să fie limitată numai la nivel național.

În fiecare stat membru trebuie creată și menținută o singură listă sigură pentru a indica statutul supravegherii și/sau acreditării serviciilor de certificare furnizate de CSP certificați/acreditați de către statul membru. Lista sigură trebuie să includă cel puțin CSP care eliberează QC. Lista sigură poate indica, de asemenea, statutul altor servicii de certificare supravegheate sau acreditate în cadrul unui program de aprobare definit la nivel național.

3.2. *Un set unic de valori pentru statutul supravegherii/acreditării*

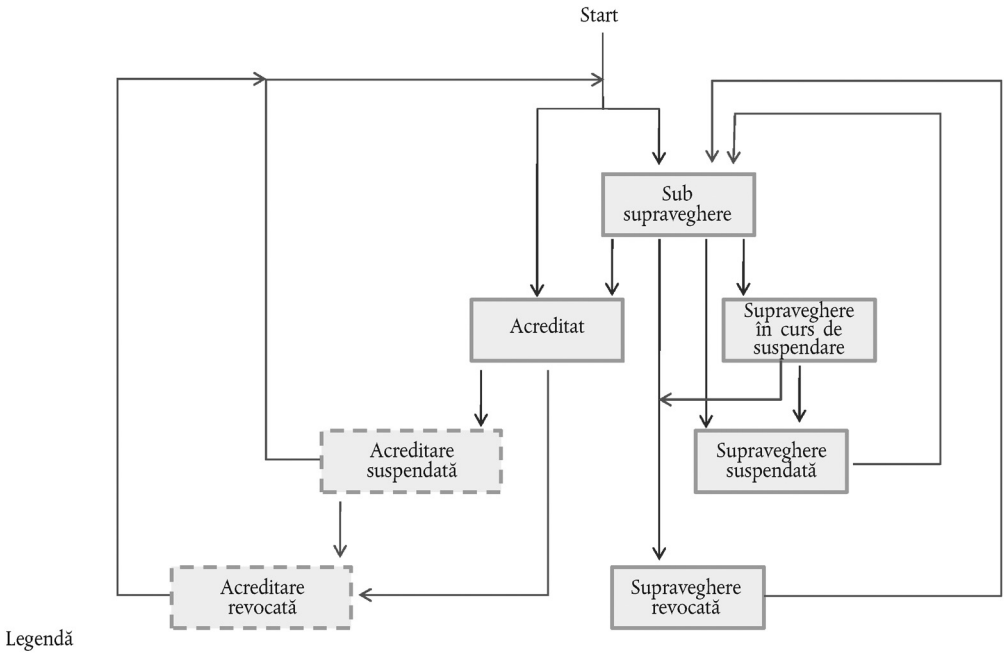
În lista sigură, faptul că un serviciu este la un moment „supravegheat” sau „acreditat” este dat de valoarea statutului său actual. În plus, statutul de supraveghere sau de acreditare poate fi pozitiv („sub supraveghere”, „acreditat”, „supraveghere în curs de suspendare”), suspendat („supraveghere suspendată”, „acreditare suspendată”), sau chiar revocat („supraveghere revocată”, „acreditare revocată”) și poate fi stabilit la valoarea corespunzătoare. Pe parcursul existenței sale, același serviciu de certificare poate trece de la statutul de supraveghere la cel de acreditare și invers ([1]).

Figura 1 de mai jos descrie fluxul preconizat, pentru un singur serviciu de certificare, între posibile statute de supraveghere/acreditare:

([1]) De exemplu, un prestator de servicii de certificare stabilit într-un stat membru, care furnizează un serviciu de certificare supravegheat inițial de statul membru (organism de supraveghere), poate decide, după o anumită perioadă de timp, să adopte o acreditare voluntară pentru serviciul de certificare supravegheat la momentul respectiv. În schimb, un prestator de servicii de certificare dintr-un alt stat membru poate decide să nu sisteze un serviciu de certificare acreditat, trecând în schimb de la statutul de acreditare la statutul de supraveghere, de exemplu din motive comerciale și/sau economice.

Figura 1

Flux prevăzut al statutului de supraveghere/acreditare al unui serviciu furnizat de CSP



Legendă

Statut de tranzit atunci când există un model de supraveghere asociat (de exemplu, pentru un CSP care eliberează QC acreditat și supravegheat în statul membru în care este stabilit),
Statut curent posibil arunci când nu există nici un model de supraveghere asociat (de exemplu, pentru un CSP acreditat într-un stat membru în care acesta nu este stabilit)

Statut curent posibil

Atunci când este stabilit într-un stat membru, un serviciu de certificare care eliberează QC trebuie supravegheat (de către statul membru în care este stabilit) și poate fi acreditat voluntar. Valoarea statutului unui astfel de serviciu atunci când figurează pe o listă sigură trebuie să fie una dintre valorile statutului descrise mai sus ca „valoare a statutului curent", în conformitate cu statutul său curent și trebuie să se schimbe, atunci când este cazul, în funcție de fluxul statutului descris mai sus. Cu toate acestea, atât „acreditarea suspendată", cât și „acreditarea revocată" trebuie să fie valori de „statute de tranzit" atunci când serviciul CSP_{QC} corespunzător este inclus pe lista sigură a statului membru în care este stabilit, întrucât un astfel de serviciu trebuie să fie supravegheat în mod implicit (inclusiv atunci când nu este sau nu mai este acreditat); în cazul în care serviciul respectiv este inclus pe listă (acreditat) într-un alt stat membru decât cel în care este stabilit, valorile respective pot fi valori finale.

Statele membre care instituie sau au instituit „un program (programe) recunoscut(e) de aprobare" definit(e) și pus(e) în aplicare la nivel național în vederea supravegherii conformității serviciilor furnizate de CSP care **nu** eliberează QC cu dispozițiile Directivei 1999/93/CE și cu eventualele dispoziții naționale privind prestarea de servicii de certificare [în sensul articolului 2 alineatul (11) din Directiva 1999/93/CE] trebuie să clasifice programul (programele) de aprobare în următoarele două categorii:

— „acreditare voluntară", astfel cum este definită și reglementată de Directiva 1999/93/CE [articolul 2 punctul 13, articolul 3 alineatul (2), articolul 7 alineatul (1) litera (a), articolul 8 alineatul (1), articolul 11, considerentele 4, 11, 12 și 13];

— „supraveghere" în conformitate cu cerințele Directivei 1999/93/CE, pusă în aplicare prin dispozițiile și cerințele naționale, în conformitate cu legislația națională.

În consecință, un serviciu de certificare care nu eliberează QC poate fi supravegheat sau acreditat voluntar. Atunci când este introdus pe o listă sigură, valoarea statutului unui astfel de serviciu trebuie să fie una dintre valorile statutului descrise mai sus ca „valoare a statutului curent" (a se vedea figura 1), în conformitate cu statutul curent al acestuia și trebuie să evolueze, atunci când este cazul, în conformitate cu fluxul statutului descris mai sus.

Lista sigură trebuie să conțină informații cu privire la programul (programele) de bază de supraveghere/acreditare, în special:

— informații cu privire la sistemul de supraveghere aplicabil oricărui CSP_{QC};

— atunci când este cazul, informații cu privire la programul național de „acreditare voluntară" aplicabilă oricărui CSP_{QC};

— atunci când este cazul, informații cu privire la sistemul de supraveghere aplicabil oricărui CSP care nu eliberează QC;

— atunci când este cazul, informații cu privire la programul național de „acreditare voluntară" aplicabil oricărui CSP care nu eliberează QC.

Ultimele două seturi de informații au o importanță esențială pentru ca părțile care se bazează pe certificat să poată evalua nivelul de calitate și siguranță al sistemelor de supraveghere/acreditare aplicate la nivel național pentru CSP care nu eliberează QC. Atunci când în lista sigură sunt furnizate informații privind statutul supravegherii/acreditării serviciilor furnizate de CSP care nu eliberează QC, seturile de informații menționate anterior vor fi furnizate în lista sigură utilizând „Scheme information URI" (dispoziția 5.3.7 – informații furnizate de statele membre), „Scheme type/community/rules" (dispoziția 5.3.9 – prin utilizarea unui text comun pentru toate statele membre și informații specifice opționale furnizate de un stat membru) și „TSL policy/legal notice" (dispoziția 5.3.11 – un text comun pentru toate statele membre care face trimitere la Directiva 1999/93/CE, fiecare stat membru având posibilitatea de a adăuga texte/referințe care îi sunt specifice).

Informațiile suplimentare privind „calificarea" definite la nivelul sistemelor naționale de supraveghere/acreditare pentru CSP care nu eliberează QC pot fi furnizate la nivelul fiecărui serviciu dacă este cazul și dacă este necesar (de exemplu, pentru a distinge între mai multe niveluri de calitate/siguranță) prin utilizarea extensiei „additionalServiceInformation" (dispoziția 5.5.9.4) ca parte din extensia „Service information" (dispoziția 5.5.9). Informațiile suplimentare privind specificațiile tehnice corespunzătoare sunt cuprinse în specificațiile detaliate din capitolul I.

Cu toate că responsabilitatea pentru supravegherea și acreditarea serviciilor de certificare dintr-un stat membru poate fi deținută de organisme separate ale statului membru în cauză, se preconizează că o singură intrare va fi utilizată pentru un serviciu de certificare unic și că statutul de supraveghere/acreditare aferent acestuia va fi actualizat în mod corespunzător.

3.3. *Intrări în lista sigură pentru facilitarea validării QES și* $AdES_{QC}$

Cel mai critic aspect în crearea unei liste sigure este stabilirea părții obligatorii a acesteia, și anume „Lista de servicii" pentru fiecare CSP care eliberează QC, cu scopul de a reflecta corect situația exactă a fiecărui serviciu de eliberare a QC și pentru a garanta că informațiile furnizate la fiecare intrare sunt suficiente pentru a facilita validarea QES și a $AdES_{QC}$ (atunci când sunt combinate cu conținutul QC pentru o entitate finală furnizat de CSP în baza serviciului de certificare introdus pe listă la această intrare).

Informațiile necesare pot include alte informații în afară de identitatea digitală a serviciului („Service digital identity") a unei autorități de certificare de bază [(*Root*) CA] unice, în special informații care permit identificarea statutului QC al certificatelor emise de un astfel de serviciu CA și informații privind utilizarea eventuală a unui SSCD pentru crearea semnăturilor atestate. Organismul dintr-un stat membru desemnat să creeze, să editeze și să mențină lista sigură trebuie, prin urmare, să ia în considerare profilul curent și conținutul certificatului în cazul fiecărui QC eliberat, pentru fiecare serviciu CSP_{QC} inclus în lista sigură.

În mod ideal, fiecare QC eliberat ar trebui să cuprindă declarația de QcCompliance [1] definită de ETSI dacă se afirmă că este un QC și declarația QcSSCD definită de ETSI dacă se afirmă că acesta se bazează pe un SSCD pentru a crea semnături electronice și/sau că fiecare QC eliberat include unul dintre identificatorii de obiecte (OID) ai politicii de certificare QCP/QCP + definiți în ETSI EN 319 411-2 [2]. Utilizarea de către CSP care eliberează QC a unor standarde diferite drept referință, diferențele de interpretare a standardelor respective, precum și lipsa cunoștințelor legate de existența și prioritatea anumitor specificații tehnice sau standarde normative au avut drept rezultat diferențe apărute în conținutul real al QC eliberate în prezent (de exemplu, utilizarea sau nu a QcStatements definite de ETSI), ceea ce împiedică destinatarii să se bazeze pur și simplu pe certificatul semnatarului (și pe lanțul/traseul asociat) atunci când trebuie să evalueze, cel puțin într-o formă care poate fi citită de calculator, dacă se afirmă sau nu că certificatul care atestă o semnătură electronică este un QC și dacă acesta este sau nu asociat cu un SSCD prin care a fost creată semnătura electronică.

[1] A se vedea ETSI EN 319 412-5 Semnături și infrastructuri electronice (*Electronic Signatures and Infrastructures* – ESI); Profiluri pentru prestatori de servicii sigure care emit certificate (*Profiles for Trust Service Providers issuing certificates*); Partea 5: Extensie pentru profilul certificatului calificat pentru definirea unei astfel de declarații (*Extension for Qualified Certificate profile for the definition of such a statement*).

[2] ETSI EN 319 411-2 - Semnături și infrastructuri electronice (*Electronic Signatures and Infrastructures* – ESI); Cerințe de politică și de securitate pentru prestatorii de servicii de încredere care eliberează certificate (*Policy and security requirements for Trust Service Providers issuing certificates*); Partea 2: Cerințe pentru autoritățile de certificare care eliberează certificate calificate (*Policy requirements for certification authorities issuing qualified certificates*).

Completarea câmpurilor privind serviciul „Service type identifier" („Sti"), „Service name" („Sn") și „Service digital identity" („Sdi") din lista sigură cu informațiile furnizate în câmpul „Service information extensions" („Sie") permite determinarea în mod integral a unui anumit tip de certificat calificat eliberat de un serviciu de certificare al unui CSP introdus pe listă care eliberează QC și furnizează informații privind eventualitate ca acesta să se bazeze pe un SSCD (dacă informațiile nu sunt incluse în QC eliberat). O informație specifică despre un „Service current status" („Scs") este asociată acestei intrări. Figura 2 de mai jos ilustrează acest aspect.

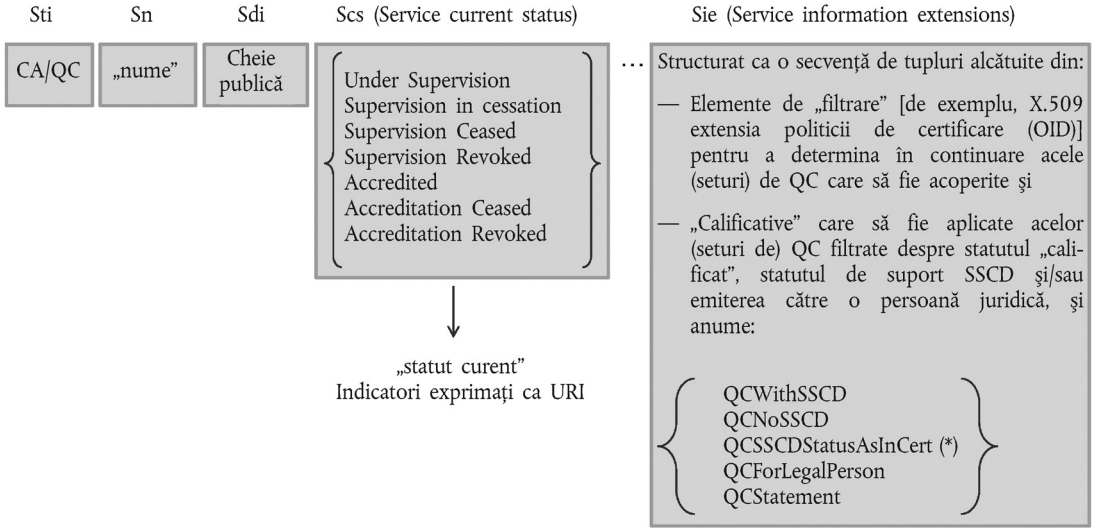
Introducerea pe listă a unui serviciu doar prin furnizarea „Sdi" a unei (*Root*) CA ar presupune că se garantează (de către CSP care eliberează QC, dar și de către organismul de supraveghere/acreditare responsabil pentru supravegherea/acreditarea respectivului CSP) că oricare certificat pentru o entitate finală eliberat în cadrul respectivei (ierarhii) (*Root*) CA conține suficiente informații definite de ETSI care pot fi prelucrate de calculator pentru a evalua dacă certificatul este sau nu un QC și dacă se bazează sau nu pe un SSCD. În cazul în care, de exemplu, ultima afirmație nu este adevărată (de exemplu, în QC nu există indicații standardizate conform ETSI având o formă care poate fi prelucrată de calculator pentru a determina dacă certificatul se bazează sau nu pe un SSCD), prin introducerea pe listă doar a „Sdi" a (*Root*) CA se poate presupune doar că QC eliberate în cadrul respectivei ierarhii a (*Root*) CA nu se bazează pe niciun SSCD. Pentru a indica că acele QC trebuie să fie considerate ca bazându-se pe un SSCD, ar trebui să se utilizeze câmpul „Sie" (ceea ce indică, de asemenea, că informațiile sunt garantate de CSP care eliberează QC și supravegheate/acreditate de organismul de supraveghere sau de acreditare).

Figura 2

Intrare în lista sigură privind un serviciu de pe listă al unui CSP care eliberează QC

Principii generale – Reguli de editare – intrări CSP_{QC} (servicii de pe listă)

Intrare privind un serviciu pentru un CSP_{QC} inclus pe listă:



(*) în sensul că se garantează că astfel de informații sunt conținute în orice QC în cadrul CA/QC definite prin Sdi-[Sie] (în cazul în care nu este nimic în QC, atunci sensul este NoSSCD)

Specificațiile tehnice actuale pentru prezentul modelul comun de listă sigură permit utilizarea unei combinații de cinci categorii principale de informații în intrarea privind un serviciu:

— „Service type identifier" („Sti"), de exemplu elementul de identificare a unei CA care eliberează QC („CA/QC");

— „Service Name" („Sn");

— „Service digital identity" („Sdi"), informații care identifică un serviciu introdus pe listă, de exemplu cheia publică (ca o cerință minimă) a unei CA care eliberează QC;

— pentru serviciile CA/QC, informații opționale „Service information extension” („Sie”), care permit includerea unui număr de informații specifice legate de serviciu cu privire la statutul de revocare a certificatelor expirate, caracteristicile suplimentare ale QC, preluarea CSP de către un alt CSP și alte informații suplimentare privind serviciul. De exemplu, caracteristicile suplimentare ale QC sunt reprezentate de o secvență de unul sau mai multe tupluri, fiecare tuplu furnizând:

— criterii care să fie utilizate pentru identificarea mai precisă (filtrarea) în cadrul serviciului de certificare identificat printr-o „Sdi” a setului de certificate calificate pentru care sunt solicitate/furnizate informații suplimentare pentru a indica statutul „calificat”, dacă se bazează pe un SSCD sau nu și/sau eliberarea către o persoană juridică; precum și

— informații asociate („calificative”) care să indice dacă acest set de certificate calificate trebuie considerat drept „calificat”, dacă se bazează sau nu pe un SSCD sau dacă informațiile asociate fac parte din QC într-o formă standardizată care poate fi prelucrată de un calculator și/sau informații cu privire la faptul că astfel de QC sunt eliberate către persoane juridice (acestea sunt considerate implicit ca fiind eliberate exclusiv persoanelor fizice);

— informații privind „statutul curent” al serviciului care indică:

— dacă este un serviciu supravegheat sau acreditat; și

— statutul propriu-zis de supraveghere/acreditare.

3.4. *Orientări referitoare la editarea și utilizarea intrărilor privind serviciile CSP_{QC}*

Orientări generale privind editarea

1. În cazul în care se asigură [garanție oferită de CSP_{QC} și supravegheată/acreditată de organismul de supraveghere (SB)/organismul de acreditare (AB)] că, pentru un serviciu inclus pe listă și identificat printr-o „Sdi”, orice QC care se bazează pe un SSCD conține declarația QcCompliance definită de ETSI și declarația QcSSCD și/sau un identificator de obiecte (OID) al QCP+, atunci utilizarea unei „Sdi” adecvate este suficientă, iar câmpul „Sie” poate fi utilizat ca o opțiune și nu va fi necesar să conțină informații cu privire la suportul SSCD.

2. În cazul în care se asigură (garanție oferită de CSP_{QC} și supravegheată/acreditată de SB/AB) că, pentru un serviciu introdus pe listă și identificat printr-o „Sdi”, orice QC care nu se bazează pe un SSCD conține declarația QcCompliance și/sau QCP OID și nu conține declarația QcSSCD sau QCP + OID, atunci utilizarea unei „Sdi” adecvate este suficientă, iar câmpul „Sie” poate fi utilizat ca opțiune și nu va fi necesar ca acesta să conțină informații cu privire la suportul SSCD (însemnând că nu se bazează pe un SSCD).

3. În cazul în care se asigură (garanție oferită de CSP_{QC} și supravegheată/acreditată de SB/AB) că, pentru un serviciu introdus pe listă și identificat printr-o „Sdi”, orice QC conține declarația QcCompliance și unele dintre QC sunt destinate a se baza pe SSCD, iar altele nu (de exemplu, diferențierea poate fi făcută de diferiți OID specifici ai politicilor de certificare ale CSP sau de alte informații specifice ale CSP conținute în QC, în mod direct sau indirect, care pot fi prelucrate sau nu de calculator), dar un certificat care se bazează pe un SSCD nu conține NICI declarația QcSSCD, NICI QCP OID(+) definit de ETSI, atunci utilizarea unei „Sdi” adecvate poate să nu fie suficientă ȘI trebuie folosit câmpul „Sie” pentru a indica informațiile explicite privind suportul SSCD, precum și eventuala extensie a informațiilor pentru a identifica setul acoperit de certificate. Probabil că în acest caz va fi necesar să se includă diferite „valori ale informațiilor privind suportul SSCD” pentru aceeași „Sdi” atunci când se utilizează câmpul „Sie”.

4. În cazul în care se asigură (garanție oferită de CSP_{QC} și supravegheată/acreditată de SB/AB) că, pentru un serviciu introdus pe listă și identificat printr-o „Sdi”, niciun QC nu conține declarația QcCompliance, QCP OID, declarația QcSSCD sau QCP + OID, dar se asigură că unele dintre aceste certificate pentru entitățile finale eliberate cu respectiva „Sdi” sunt destinate să devină QC și/sau să se bazeze pe SSCD, iar altele nu (de exemplu diferențierea poate fi făcută de diferiți OID specifici ai politicilor de certificare ale CSP_{QC} sau de alte informații specifice CSP_{QC} conținute în QC, în mod direct sau indirect, care pot fi prelucrate de calculator sau nu), atunci utilizarea unei „Sdi” adecvate nu va fi suficientă ȘI trebuie folosit câmpul „Sie” pentru a include informații explicite privind calificarea. Probabil că în acest caz va fi necesar să se includă diferite „valori ale informațiilor privind suportul SSCD” pentru aceeași „Sdi” atunci când se utilizează câmpul „Sie”.

Ca un principiu general implicit, pentru un CSP inclus pe lista sigură trebuie să existe o singură intrare privind serviciul pentru fiecare cheie publică pentru un serviciu de certificare de tip CA/QC, și anume pentru o autoritate de certificare care eliberează (direct) QC. În anumite circumstanțe excepționale și în anumite condiții atent coordonate, organismul de supraveghere sau de acreditare al statului membru poate decide să utilizeze ca „Sdi” a unei singure intrări din lista de servicii din CSP inclus pe listă, cheia publică a unei *Root* CA (autoritate de certificare de bază) sau *Upper level* CA (autoritate de certificare superioară) în cadrul PKI CSP (de exemplu, în contextul unei ierarhii a CSP de AC de la o

Root CA în sens descendent până la mai multe CA emitente) în loc să includă pe listă toate serviciile CA subordonate emitente (și anume, o autoritate de certificare care nu eliberează direct QC pentru entitățile finale, dar certifică o ierarhie de autorități de certificare în sens descendent până la autoritățile de certificare ce eliberează QC către entitățile finale). Consecințele (avantajele și dezavantajele) utilizării unei astfel de chei publice *Root* CA sau *Upper* CA ca valoare „Sdi" într-o intrare de serviciu din lista sigură trebuie să fie analizate cu atenție atunci când este pusă în aplicare de către statele membre. În plus, dacă utilizează această excepție autorizată de la principiul implicit, statul membru trebuie să prezinte documentația necesară pentru a facilita crearea și verificarea căii de certificare. De exemplu, în cazul unui CSP_{QC} care folosește o *Root* CA în cadrul căreia mai multe CA eliberează certificate calificate și certificate necalificate, însă pentru care QC conțin doar declarația de QcCompliance fără a indica dacă se bazează sau nu pe un SSCD, introducerea pe listă a „Sdi" pentru *Root* CA ar presupune doar că, în temeiul regulilor explicate anterior, niciun QC eliberat în cadrul respectivei ierarhii *Root* CA nu se bazează pe un SSCD. Dacă există QC care se bazează de fapt pe un SSCD, dar în certificate nu este inclusă nicio declarație care poate fi prelucrată de calculator care să indice un astfel de suport, ar fi recomandat să se facă uz pe viitor de declarația QcSSCD în QC eliberate. Între timp (până la expirarea ultimului QC care nu conține această informație), lista sigură trebuie să utilizeze câmpul „Sie" și extensia asociată „Qualifications Extension", de exemplu furnizând informații pentru filtrare pentru a identifica set(uri) de certificate prin utilizarea unui/unor OID specific(e) definit(e) de CSP_{QC} utilizate eventual de CSP_{QC} pentru a distinge între diferite tipuri de QC (unele pe bază de SSCD, altele nu) care asociază „SSCD support information" explicite cu privire la setul(urile) de certificate filtrate identificate prin intermediul „calificativelor (Qualifiers)".

Orientările generale privind utilizarea aplicațiilor, a serviciilor sau a produselor legate de semnături electronice bazate pe o listă sigură în conformitate cu prezentele specificații tehnice sunt următoarele:

O intrare „Sti"„CA/QC" (în mod similar o intrare a CA/QC calificată ulterior ca fiind o „*Root*CA/QC" prin utilizarea extensiei *additionalServiceInformation* „Sie"):

— indică faptul că începând cu CA identificată prin „Sdi" (în mod similar în cadrul ierarhiei CA începând de la *Root* CA identificată prin „Sdi"), toate certificatele eliberate pentru entitățile finale sunt QC **cu condiția** să se afirme acest lucru în certificat prin utilizarea unei *QcStatement* adecvate care poate fi prelucrată de calculator (și anume, *QcCompliance*) și/sau QCP(+) OID definiți de ETSI (acest aspect fiind garantat de organismul de supraveghere/acreditare, a se vedea mai sus „orientările generale privind editarea");

Notă: Dacă nu există informații privind calificarea („Qualifications Extension") în „Sie" sau dacă un certificat al unei entități finale care este considerat un QC nu este identificat mai precis printr-o „Qualifications Extension" aferentă „Sie", atunci informațiile care pot fi prelucrate de calculator cuprinse în QC sunt supravegheate/acreditate ca fiind exacte. Aceasta presupune că utilizarea (sau neutilizarea) *QcStatements* adecvate (anume *QcCompliance*, QcSSCD) și/sau QCP(+) OID definiți de ETSI este garantată ca fiind în conformitate cu afirmațiile CSP_{QC}.

— **și DACĂ** există informații privind calificarea („Qualifications Extension") în „Sie", atunci, în plus față de regula sus-menționată de interpretare implicită, certificatele care sunt identificate prin utilizarea acestor informații privind calificarea („Qualifications Extension") din „Sie", create pe baza principiului unei secvențe de filtre care identifică mai precis un set de certificate, trebuie să fie considerate în funcție de calificativele asociate care furnizează informații suplimentare cu privire la statutul calificării, „suportul SSCD" și/sau „persoana juridică în calitate de subiect" (de exemplu, certificatele care conțin un OID specific în extensia politicii de certificare și/sau au un model specific de „Key usage" (utilizarea cheii) și/sau care sunt filtrate prin utilizarea unei valori specifice care apare într-un anumit câmp sau într-o anumită extensie a certificatului etc.). Calificativele respective fac parte din următorul set de „calificative" utilizate pentru a compensa lipsa informațiilor din QC corespunzător și care sunt folosite respectiv:

— pentru a indica statutul calificat: „QCStatement" care presupune că certificatul (certificatele) identificat(e) este (sunt) calificat(e);

ȘI/SAU

— pentru a indica natura suportului SSCD:

— „QCWithSSCD" – valoare a calificativului care presupune că „QC se bazează pe un SSCD"; sau

— „QCNoSSCD" – valoare a calificativului care presupune că „QC nu se bazează pe un SSCD"; sau

— „QCSSCDStatusAsInCert" – valoare a calificativului care presupune că se garantează că informațiile privind suportul SSCD sunt conținute în orice QC în cadrul informațiilor „Sdi"-„Sie" furnizate în această intrare CA/QC;

ȘI/SAU

— pentru a indica eliberarea către o persoană juridică:

— „QCForLegalPerson” – valoare a calificativului care presupune că „certificatul este eliberat către o persoană juridică”.

3.5. *Servicii pe care se bazează serviciile „CA/QC”, dar care nu sunt incluse în „Sdi” al „CA/QC”*

Serviciile privind statutul de valabilitate a certificatului legate de QC și pentru care informațiile privind statutul de valabilitate a certificatului (de exemplu, CRL-uri și răspunsurile OCSP) sunt semnate de către o entitate a cărei cheie privată nu este autorizată în cadrul unei căi de certificare ce duce la o CA inclusă pe listă care eliberează QC („CA/QC”) vor fi incluse în lista sigură prin enumerarea serviciilor privind statutul de valabilitate a certificatului ca atare în TL (și anume, cu un tip de serviciu „OCSP/QC” sau „CRL/QC”) deoarece astfel de servicii pot fi considerate ca făcând parte din serviciile supravegheate/acreditate „calificate” legate de furnizarea de servicii de certificare QC. În mod evident, respondenții OCSP sau emitenții CRL ale căror certificate sunt semnate de autorități de certificare în cadrul ierarhiei unui serviciu CA/QC introdus pe listă vor fi considerați drept „valabili” și în conformitate cu valoarea statutului serviciului CA/QC de pe listă.

O dispoziție asemănătoare se poate aplica serviciilor de certificare ce eliberează certificate necalificate (de tip serviciu „CA/PKC”).

Lista sigură trebuie să includă serviciile privind starea de valabilitate a certificatului în cazul în care certificatele pentru entități finale cărora li se aplică serviciile privind starea de valabilitate a certificatului nu conțin informații legate de locație pentru astfel de servicii.

4. **Definiții și abrevieri**

În sensul prezentului document, se utilizează următoarele definiții și abrevieri:

Termen	Abreviere	Definiție
Prestator de servicii de certificare	CSP	Astfel cum este definit la articolul 2 punctul 11 din Directiva 1999/93/CE
Autoritate de certificare	CA	1. un prestator de servicii de certificare care creează și repartizează certificate cu cheie publică; sau 2. un serviciu tehnic de generare de certificate, care este utilizat de către un prestator de servicii de certificare care creează și repartizează certificate cu cheie publică. *NOTĂ:* A se vedea dispoziția 4 din EN 319 411-2 [1] pentru explicații suplimentare privind conceptul de autoritate de certificare.
Autoritate de certificare are eliberează certificate calificate	CA/QC	O CA care îndeplinește cerințele stipulate în anexa II la Directiva 1999/93/CE și eliberează certificate calificate în conformitate cu cerințele stipulate în anexa I la Directiva 1999/93/CE.
Certificat	Certificat	Astfel cum este definit la articolul 2 punctul 9 din Directiva 1999/93/CE.
Certificat calificat	QC	Astfel cum este definit la articolul 2 punctul 10 din Directiva 1999/93/CE.
Semnatar	Semnatar	Astfel cum este definit la articolul 2 punctul 3 din Directiva 1999/93/CE.
Supraveghere	Supraveghere	Se referă la supraveghere astfel cum este prevăzută la articolul 3 alineatul (3) din Directiva 1999/93/CE. Directiva impune statelor membre să creeze un sistem adecvat care să permită supravegherea prestatorilor de servicii de certificare stabiliți pe teritoriul lor și eliberarea de certificate calificate pentru public, asigurând supravegherea respectării dispozițiilor directivei respective.
Acreditare voluntară	Acreditare	Astfel cum este definită la articolul 2 punctul 13 din Directiva 1999/93/CE.
Listă sigură	TL	Desemnează lista care indică statutul de supraveghere/acreditare aferent serviciilor de certificare furnizate de prestatorii de servicii de certificare care sunt supravegheați/acreditați de statul membru de referință în vederea conformității cu dispozițiile Directivei 1999/93/CE.

Termen	Abreviere	Definiție
Lista statutelor serviciilor de încredere	TSL	Formă a unei liste semnate utilizată ca bază pentru prezentarea informațiilor privind statutul unui serviciu de încredere în conformitate cu specificațiile prevăzute în ETSI TS 119 612.
Serviciu de încredere		Serviciu care sporește încrederea în tranzacțiile electronice (folosind în general, dar nu obligatoriu, tehnici criptografice sau implicând materiale confidențiale) (ETSI TS 119 612). *NOTĂ:* Termenul are aplicabilitate mai mare comparativ cu serviciul de certificare care eliberează certificate sau prestează alte servicii legate de semnături electronice.
Prestator de servicii de încredere	TSP	Organism care prestează unul sau mai multe servicii (electronice) de încredere (termenul are aplicabilitate mai mare comparativ cu CSP).
Jeton al serviciului de încredere	TrST	Un obiect fizic sau binar (logic) generat sau eliberat ca urmare a utilizării unui serviciu de încredere. Exemple de TrST binare sunt certificatele, listele certificatelor revocate (CRL), jetoane de marcare temporală (TST) și răspunsurile OCSP (*Online Certificate Status Protocol* – protocol online privind statutul certificatelor).
Semnătură electronică calificată	QES	O AdES confirmată de un QC și creată de un dispozitiv securizat de creare a semnăturii, astfel cum este definită la articolul 2 din Directiva 1999/93/CE.
Semnătură electronică avansată	AdES	Astfel cum este definită la articolul 2 punctul 2 din Directiva 1999/93/CE.
Semnătură electronică avansată confirmată de un certificat calificat	$AdES_{QC}$	Desemnează o semnătură electronică care îndeplinește criteriile pentru o AdES și este confirmată de un QC, astfel cum este definit la articolul 2 din Directiva 1999/93/CE.
Dispozitiv securizat de creare a semnăturii	SSCD	Astfel cum este definit la articolul 2 punctul 6 din Directiva 1999/93/CE.

([1]) EN 319 411-2: Semnături și infrastructuri electronice (*Electronic Signatures and Infrastructures* – ESI); Cerințe de politică și de securitate pentru prestatorii de servicii de încredere care eliberează certificate (*Policy and security requirements for Trust Service Providers issuing certificates*); Partea 2: Cerințe pentru autoritățile de certificare care eliberează certificate calificate (*Policy requirements for certification authorities issuing qualified certificates*).

În următoarele capitole, cuvintele cheie „TREBUIE” (din engleză *MUST*), „NU TREBUIE” (din engleză *MUST NOT*), „OBLIGATORIU” (din engleză *REQUIRED*), „TREBUIE/NU TREBUIE” (din engleză *SHALL/SHALL NOT*), „AR TREBUI” (din engleză *SHOULD*), „NU AR TREBUI” (din engleză *SHOULD NOT*), „SE RECOMANDĂ” (din engleză *RECOMMENDED*), „ESTE POSIBIL” sau „POATE” (din engleză (*MAY*) și „OPȚIONAL” (din engleză *OPTIONAL*) și variantele lor gramaticale trebuie interpretate în sensul echivalentelor lor din limba engleză, în conformitate cu RFC 2119 ([1]).

CAPITOLUL I

SPECIFICAȚII DETALIATE PRIVIND MODELUL COMUN PENTRU „LISTA SIGURĂ A PRESTATORILOR DE SERVICII DE CERTIFICARE SUPRAVEGHEAȚI/ACREDITAȚI”

Prezentele specificații se bazează pe specificațiile și cerințele prevăzute în ETSI TS 119 612 v1.1.1 (denumite în continuare ETSI TS 119 612).

Atunci când în prezentele specificații nu există cerințe specifice, TREBUIE SĂ SE APLICE în întregime cerințele din ETSI TS 119 612 dispozițiile 5 și 6. Dacă în cuprinsul prezentelor specificații se menționează cerințe specifice, acestea TREBUIE SĂ PREVALEZE asupra cerințelor corespunzătoare din ETSI TS 119 612. În cazul în care apar discrepanțe între prezentele specificații și specificațiile cuprinse în ETSI TS 119 612, prezentele specificații TREBUIE SĂ FIE specificațiile cu caracter normativ.

Scheme operator name (dispoziția 5.3.4)

Acest câmp TREBUIE SĂ FIE PREZENT și SĂ RESPECTE specificațiile din TS 119 612 dispoziția 5.3.4.

([1]) IETF RFC 2119: „Cuvinte cheie destinate utilizării în RFC-uri pentru a indica nivelul cerințelor” („Key words for use in RFCs to indicate Requirements Levels”).

O țară POATE avea organisme de supraveghere și acreditare separate și chiar organisme suplimentare pentru diferite activități operaționale aferente. Fiecare stat membru este responsabil cu desemnarea operatorului programului listei sigure a statului membru. Se preconizează că organismul de supraveghere, organismul de acreditare și operatorul programului (atunci când este vorba despre organisme separate) vor avea responsabilități și obligații proprii.

Orice situație în care mai multe organisme poartă răspunderea pentru supraveghere, acreditare sau alte aspecte operaționale TREBUIE SĂ FIE reflectată cu exactitate și identificată ca atare în informațiile privind programul care fac parte din lista sigură, inclusiv în informațiile specifice de program indicate de „Scheme information URI" (dispoziția 5.3.7).

Scheme name (dispoziția 5.3.6)

Acest câmp TREBUIE să fie prezent și să respecte specificațiile din TS 119 612 dispoziția 5.3.6, unde pentru program TREBUIE să se folosească următorul nume:

„EN_name_value" = „Lista statutului privind supravegherea/acreditarea serviciilor de certificare oferite de furnizori de servicii de certificare, care sunt supravegheați/acreditați de statul membru de referință operator al programului în vederea respectării dispozițiilor relevante prevăzute în Directiva 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice".

Scheme information URI (dispoziția 5.3.7)

Acest câmp TREBUIE SĂ FIE prezent și să respecte specificațiile din TS 119 612 dispoziția 5.3.7, unde „informațiile corespunzătoare despre program" TREBUIE să includă cel puțin:

— informații introductive cu caracter general care sunt comune pentru toate statele membre în ceea ce privește domeniul și contextul listei sigure, precum și programul (programele) de supraveghere/acreditare de bază. 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:

„The present list is the „Trusted List of supervised/accredited Certification Service Providers" providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— allowing for a trusted validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)], including, when this is not part of the QCs, information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including compliance with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Article 3(3), Article 8.(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List at a national level on a voluntary basis.";

— informații specifice privind programul (programele) de supraveghere/acreditare de bază, în special ([1]):

  — informații cu privire la sistemul de supraveghere aplicabil oricărui CSP_{QC};

  — atunci când este cazul, informații privind programul național de acreditare voluntară aplicabil oricărui CSP_{QC};

  — atunci când este cazul, informații privind sistemul de supraveghere aplicabil oricărui CSP care nu eliberează QC;

  — atunci când este cazul, informații privind programul național de acreditare voluntară aplicabil oricărui CSP care nu eliberează QC;

  Informațiile specifice TREBUIE să includă pentru fiecare program de bază menționat mai sus:

  — descrierea generală;

  — informații despre procesul parcurs de organismul de supraveghere/acreditare pentru a supraveghea/acredita CSP și de către CSP pentru a fi supravegheat/acreditat;

  — informații cu privire la criteriile aplicate la supravegherea/acreditarea CSP;

— atunci când este cazul, informații specifice cu privire la „calificările" specifice care ar putea fi atribuite unor obiecte fizice sau binare (logice) generate sau eliberate ca urmare a prestării unui serviciu de certificare ca urmare a conformității lor cu dispozițiile și cerințele stipulate la nivel național, inclusiv sensul unei asemenea „calificări" și dispozițiile și cerințele naționale asociate.

Informații suplimentare specifice statului membru cu privire la program POT fi furnizate în mod voluntar, de exemplu:

— informații privind criteriile și regulile aplicate în vederea selectării supraveghetorilor/auditorilor și care definesc modul de supraveghere (verificare)/acreditare (auditare) a CSP de către aceștia;

— alte informații de contact și generale care se aplică funcționării programului.

Scheme type/community/rules (dispoziția 5.3.9)

Acest câmp TREBUIE să fie prezent și să respecte specificațiile din TS 119 612 dispoziția 5.3.9 și TREBUIE să includă cel puțin doi URI:

— un URI comun tuturor listelor sigure ale statelor membre care indică un text descriptiv care TREBUIE să se aplice 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 of supervised/accredited Certification Service Providers" providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

  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

  The Trusted List of a Member State must provide, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)], including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

([1]) Ultimele două seturi de informații au o importanță esențială pentru ca părțile care se bazează pe certificat să poată evalua nivelul de calitate și de siguranță al sistemelor de supraveghere/acreditare aplicabile CSP care nu eliberează QC. Aceste seturi de informații vor fi furnizate în lista sigură utilizând actualele „Scheme information URI" (dispoziția 5.3.7 – informații furnizate de statul membru), „Scheme type/community/rules" (dispoziția 5.3.9 – prin utilizarea unui text comun tuturor statelor membre) și „TSL policy/legal notice" (dispoziția 5.3.11 – un text comun tuturor statelor membre care face referire la Directiva 1999/93/CE, fiecare stat membru având posibilitatea de a adăuga texte/referințe care îi sunt specifice). Informațiile suplimentare privind sistemele naționale de supraveghere/acreditare aplicate în cazul CSP care nu eliberează QC pot fi furnizate la nivelul fiecărui serviciu, atunci când este cazul și în funcție de necesitate (de exemplu, pentru a distinge între mai multe niveluri de calitate/siguranță), prin utilizarea „Scheme service definition URI" (dispoziția 5.5.6).

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including compliance with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Article 3(3), Article 8)(1), Article 11 (respectively, Article2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a 'voluntary accreditation' system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined „recognised approval scheme" implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Article 2(11) of Directive 1999/93/EC). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific „qualification" on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a „qualification" is likely to be limited solely to the national level.

Interpretation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a Trusted List according to the Annex of Commission Decision [reference to the present Decision] are as follows:

A „CA/QC" „Service type identifier" („Sti") entry (similarly a CA/QC entry further qualified as being a „RootCA/QC" through the use of „Service information extension" („Sie") additionalServiceInformation Extension):

— indicates that from the „Service digital identifier" („Sdi") identified CA (similarly within the CA hierarchy starting from the „Sdi" identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) **provided** that it is claimed as such in the certificate through the use of appropriate EN 319 412-5 defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or EN 319 411-2 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

Note: if no „Sie" „Qualifications Extension" information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related „Sie" „Qualifications Extension" information, then the „machine-processable" information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs;

— **and IF** „Sie" „Qualifications Extension" information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this „Sie" „Qualifications Extension" information, which is constructed on the principle of a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing some additional information regarding the qualified status, the „SSCD support" and/or „Legal person as subject" (e.g. those 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.). Those qualifiers are part of the following set of „Qualifiers" used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

— to indicate the qualified status: „QCStatement" meaning the identified certificate(s) is(are) qualified;

AND/OR

— to indicate the nature of the SSCD support:

— „QCWithSSCD" qualifier value meaning „QC supported by an SSCD", or

— „QCNoSSCD" qualifier value meaning „QC not supported by an SSCD", or

— „QCSSCDStatusAsInCert" qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the „Sdi"-„Sie" provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

— „QCForLegalPerson" qualifier value meaning „Certificate issued to a Legal Person".

The general interpretation rule for any other „Sti" type entry is that the listed service named according to the „Sn" field value and uniquely identified by the „Sdi" field value has a current supervision/accreditation status according to the „Scs" 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 Technical specifications for a Common Template for the „Trusted List of supervised/accredited Certification Service Providers" in the Annex of Commission Decision 2009/767/EC for further details on the fields, description and meaning for the Member States' Trusted Lists."

— un URI specific pentru fiecare listă sigură a unui stat membru care trimite la un text descriptiv care TREBUIE să se aplice respectivei TL 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" (dispoziția 5.3.10):

— unde utilizatorii pot obține politica/regulile specifice ale statului membru de referință care TREBUIE să se aplice la evaluarea serviciilor incluse pe listă în conformitate cu sistemul de supraveghere și programele de acreditare voluntară corespunzătoare din statul membru;

— unde utilizatorii pot obține o descriere specifică oferită de statul membru de referință cu privire la modul de utilizare și de interpretare a conținutului listei sigure în ceea ce privește serviciile de certificare ce nu sunt legate de eliberarea de QC. Acesta poate fi utilizat pentru a indica o eventuală divizare în cadrul sistemelor naționale de supraveghere/acreditare în ceea ce privește CSP care nu eliberează QC și modul în care se utilizează „Scheme service definition URI" (dispoziția 5.5.6) și câmpul „Service information extension" (dispoziția 5.5.9) în acest scop.

Statele membre POT defini și utiliza URI suplimentari pornind de la URI specific al statului membru menționat mai sus (și anume, URI definiți pornind de la URI ierarhic specific).

TSL policy/legal notice (dispoziția 5.3.11)

Acest câmp TREBUIE să fie prezent și să respecte specificațiile din TS 119 612 dispoziția 5.3.11, unde politica/avizul juridic privind statutul juridic al programului sau cerințele legale respectate de program în temeiul jurisdicției în care este stabilit și/sau orice constrângeri și condițiile în care lista sigură este actualizată și publicată TREBUIE să fie un șir de caractere multilingv (text) alcătuit din două părți:

1. o primă parte obligatorie, comună tuturor listelor sigure ale statelor membre (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale), care să precizeze că Directiva 1999/93/CE și formele corespunzătoare de punere în aplicare a acesteia din legislația statului membru indicat la câmpul „Scheme territory" reprezintă cadrul legal aplicabil.

   Versiunea în limba engleză a textului comun:

   The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.

([1]) ISO 3166-1:2006: „Coduri pentru reprezentarea numelor țărilor și a subdiviziunilor acestora – Partea 1: Codurile țărilor" („Codes for the representation of names of countries and their subdivisions Part 1: Country codes").

Textul în limba națională a (limbile naționale ale) unui stat membru: [traducerea/traducerile oficială/oficiale ale textului în limba engleză de mai sus, și anume pentru limba română:]

Cadrul legal aplicabil pentru prezenta punere în aplicare TSL a listei sigure a prestatorilor de servicii de certificare supravegheați/acreditați din [numele statului membru relevant] este Directiva 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice și legislația de punere în aplicare a acesteia în dreptul [numele statului membru relevant].

2. o a doua parte, opțională, specifică fiecărei listei sigure (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale), care face referire la cadrul legal național specific aplicabil (de exemplu, în special când este legat de programele naționale de supraveghere/acreditare pentru CSP care nu eliberează QC).

CAPITOLUL II

CONTINUITATEA LISTELOR SIGURE

Certificate care vor fi notificate Comisiei în conformitate cu articolul 3 litera (c) din prezenta decizie TREBUIE să se elibereze astfel încât acestea:

— să aibă minimum trei luni între datele lor de valabilitate;

— să fie create pe noi perechi de chei deoarece nicio pereche de chei utilizată anterior nu trebuie să fie certificată din nou.

În cazul compromiterii sau desființării UNEIA dintre cheile private corespunzătoare cheii publice care ar putea fi utilizată pentru a valida semnătura listei sigure și care a fost notificată Comisiei și este publicată în listele centrale de indicatori ale Comisiei, statele membre TREBUIE:

— să elibereze din nou, fără nici o întârziere, o nouă listă sigură semnată cu o cheie privată necompromisă în cazul în care lista sigură publicată a fost semnată cu o cheie privată compromisă sau desființată;

— să notifice prompt Comisiei noua listă de certificate cu chei publice care corespund cheilor private care ar putea fi utilizate pentru a semna lista sigură.

În cazul compromiterii sau desființării TUTUROR cheilor private care corespund cheilor publice care ar putea fi utilizate pentru a valida semnătura listei sigure și care au fost notificate Comisiei și sunt publicate în listele centrale de indicatori ale Comisiei, statele membre TREBUIE:

— să genereze noi perechi de chei care ar putea fi utilizate pentru a semna lista sigură și certificatele lor corespunzătoare cu chei publice;

— să elibereze din nou, fără nici o întârziere, o nouă listă sigură semnată cu una dintre aceste chei private noi și al căror certificat cu cheie publică corespunzător urmează a fi notificat;

— să notifice prompt Comisiei noua listă de certificate cu chei publice care corespund cheilor private care ar putea fi utilizate pentru a semna lista sigură.

CAPITOLUL III

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 AR TREBUI să fie prezentată sub forma unui document PDF (*Portable Document Format*) conform ISO 32000 ([1]) care TREBUIE formatat conform profilului PDF/A (ISO 19005 ([2])).

Conținutul formei lizibile pentru om bazată pe PDF/A a listei sigure AR TREBUI să respecte următoarele cerințe:

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

— fiecare câmp existent AR TREBUI să fie vizibil și să cuprindă:

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

  — valoarea câmpului (de exemplu, „CA/QC”);

  — sensul (descrierea) valorii câmpului, atunci când este cazul (de exemplu, „Autoritate de certificare care eliberează certificate cu chei publice.”);

  — versiuni în mai multe limbi naturale, astfel cum sunt prevăzute în lista sigură, dacă este cazul.

([1]) ISO 32000-1:2008: Gestionare de documente –Format de document portabil – Part 1: PDF 1.7
([2]) ISO 19005-2:2011: Gestionare de documente – Format de document electronic pentru păstrare pe termen lung – Partea 2: Utilizarea ISO 32000-1 (PDF/A-2)

— în forma lizibilă pentru om AR TREBUI să fie vizibile cel puțin următoarele câmpuri și valori corespunzătoare ale certificatelor digitale disponibile în câmpul „Service digital identity”:

  — versiune;

  — număr de serie;

  — algoritmul semnăturii;

  — emitent;

  — valabil de la …;

  — valabil până la …;

  — subiect;

  — cheie publică;

  — politici de certificare;

  — identificatorul cheii subiectului;

  — puncte de distribuire a CRL;

  — identificatorul cheii autorității;

  — utilizarea cheii;

  — restricții de bază;

  — algoritmul amprentei;

  — amprentă;

— forma lizibilă pentru om AR TREBUI să poată fi imprimată cu ușurință;

— forma lizibilă pentru om TREBUIE să fie semnată de operatorul programului în conformitate cu profilul situației inițiale a semnăturilor PAdES (PAdES *Signatures baseline profile*) ([1]).

([1]) ETSI TS 103 172 (martie 2012) – Semnături și infrastructuri electronice (*Electronic Signatures and Infrastructures* – ESI); Profil al situației inițiale PAdES (PAdES Baseline Profile)