Acest document reprezintă un instrument de documentare, iar instituțiile nu își asumă responsabilitatea pentru conținutul său.

►B ►C1 **DECIZIA 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

[notificată cu numărul C(2009) 7806]

(Text cu relevanță pentru SEE)

(2009/767/CE) ◄

(JO L 274, 20.10.2009, p. 36)

Astfel cum a fost modificată prin:

		Jurnalul Oficial		
		NR.	Pagina	Data
►M1	Decizia 2010/425/UE Comisiei din 28 iulie 2010	L 199	30	31.7.2010
►M2	Regulamentul (UE) nr. 519/2013 al Comisiei din 21 februarie 2013	L 158	74	10.6.2013

rectificată prin:

►C1 Rectificare, JO L 299, 14.11.2009, p. 18 (2009/767/CE)
►C2 Rectificare, JO L 4, 7.1.2011, p. 6 (2009/767/CE)

▼B
▼C1

DECIZIA 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

[notificată cu numărul C(2009) 7806]

(Text cu relevanță pentru SEE)

(2009/767/CE)

COMISIA COMUNITĂȚILOR EUROPENE,

având în vedere Tratatul de instituire a Comunității 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) Obligațiile de simplificare administrativă impuse statelor membre prin capitolul II din Directiva 2006/123/CE, în special articolele 5 și 8, includ obligația de a simplifica procedurile și formalitățile aplicabile accesului la o activitate de servicii și exercitării acesteia și obligația de a garanta că procedurile și formalitățile pot fi îndeplinite cu ușurință de către prestatorii de servicii, la distanță și prin mijloace electronice prin intermediul „ghișeelor unice”.

(2) Îndeplinirea procedurilor și formalităților prin intermediul „ghișeelor unice” trebuie să fie posibilă între statele membre, în conformitate cu articolul 8 din Directiva 2006/123/CE.

(3) Pentru a respecta obligația de a simplifica procedurile și formalitățile și pentru a facilita utilizarea transfrontalieră a „ghișeelor unice”, procedurile prin mijloace electronice trebuie să se bazeze pe soluții simple, inclusiv în ceea ce privește utilizarea semnăturilor electronice. În cazurile în care, în urma evaluării adecvate a riscurilor în legătură cu proceduri și formalități concrete, se consideră că este necesar un nivel ridicat de siguranță sau echivalența cu o semnătură de mână, prestatorilor de servicii li s-ar putea solicita, pentru anumite proceduri și formalități, să prezinte semnături electronice avansate, bazate pe un certificat calificat, cu sau fără un dispozitiv securizat de creare a semnăturii.

([1]) JO L 376, 27.12.2006, p. 36.

▼C1

(4) Cadrul comunitar pentru semnăturile electronice a fost stabilit în Directiva 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice ([1]). Pentru a facilita utilizarea transfrontalieră eficace a semnăturilor electronice avansate bazate pe un certificat calificat, este necesar ca încrederea în aceste semnături electronice să fie ameliorată, indiferent de statul membru în care este stabilit semnatarul sau prestatorul de servicii de certificare care eliberează certificatul calificat. Acest obiectiv poate fi atins prin facilitarea accesului la o formă fiabilă a informațiilor necesare pentru validarea semnăturilor electronice, în special a informațiilor referitoare la prestatori de servicii de certificare care sunt supravegheați/acreditați într-un stat membru și la serviciile furnizate de aceștia.

(5) Este necesar să se garanteze că statele membre publică aceste informații folosind un model comun, pentru a facilita utilizarea lor și pentru a asigura un nivel adecvat de detaliere care permite destinatarului să valideze semnătura electronică,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Utilizarea și acceptarea semnăturilor electronice

(1) Dacă se justifică pe baza unei evaluări adecvate a riscurilor implicate și în conformitate cu articolul 5 alineatele (1) și (3) din Directiva 2006/123/CE, statele membre pot solicita, pentru îndeplinirea anumitor proceduri și formalități prin intermediul ghișeelor unice prevăzute la articolul 8 din Directiva 2006/123/CE, utilizarea de către prestatorul de servicii a unor semnături electronice avansate bazate pe un certificat calificat, cu sau fără un dispozitiv securizat de creare a semnăturii, în conformitate cu definițiile și dispozițiile Directivei 1999/93/CE.

(2) Statele membre acceptă toate semnăturile electronice avansate bazate pe certificate calificate, cu sau fără un dispozitiv securizat de creare a semnăturii, pentru îndeplinirea procedurilor și formalităților menționate la alineatul (1), fără a aduce atingere posibilității statelor membre de a limita această acceptare la semnăturile electronice avansate bazate pe un certificat calificat și create printr-un dispozitiv securizat de creare a semnăturii, dacă o astfel de măsură este în conformitate cu evaluarea riscurilor menționată la alineatul (1).

(3) Statele membre nu impun pentru acceptarea semnăturilor electronice avansate bazate pe un certificat calificat, cu sau fără un dispozitiv securizat de creare a semnăturii, condiția respectării unor cerințe care creează obstacole în calea utilizării de către prestatorii de servicii a procedurilor prin mijloace electronice prin intermediul ghișeelor unice.

([1]) JO L 13, 19.1.2000, p. 12.

▼C1

(4) Dispozițiile de la alineatul (2) nu împiedică statele membre să accepte semnături electronice, altele decât semnăturile electronice avansate bazate pe un certificat calificat, cu sau fără un dispozitiv securizat de creare a semnăturii.

Articolul 2

Crearea, păstrarea și publicarea listelor sigure

(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.

▼M1

(2) Statele membre creează și publică atât o formă lizibilă pentru om, cât și o formă care poate fi procesată de calculator a listei sigure, în conformitate cu specificațiile prevăzute în anexă.

(2a) Statele membre semnează electronic forma care poate fi procesată de calculator a listelor sigure respective și publică, cel puțin, forma lizibilă pentru om a listei sigure, printr-un mijloc securizat, pentru asigurarea autenticității și integrității acesteia.

(3) Statele membre notifică următoarele informații Comisiei:

(a) organismul sau organismele responsabile pentru crearea, păstrarea și publicarea formei lizibile pentru om și a formei care poate fi procesată de calculator a listei sigure;

(b) locațiile unde forma lizibilă pentru om și forma care poate fi procesată de calculator a listei sigure sunt publicate;

(c) certificatul de cheie publică utilizat pentru implementarea canalului securizat prin care este publicată forma lizibilă pentru om a listei sigure sau, dacă lista lizibilă pentru om este semnată electronic, certificatul de cheie publică utilizat pentru semnarea acesteia;

(d) certificatul de cheie publică utilizat pentru semnarea electronică a formei care poate fi procesată de calculator a listei sigure;

(e) orice modificări ale informațiilor de la literele (a)-(d).

(4) Comisia pune la dispoziția statelor membre, printr-un canal securizat către un server web autentificat, informațiile menționate la alineatul (3), astfel cum sunt notificate de statele membre, atât în formă lizibilă pentru om, cât și într-o formă semnată, care poate fi procesată de calculator.

▼C1

Articolul 3

Aplicare

Prezenta decizie se aplică de la 28 decembrie 2009.

Articolul 4

Destinatari

Prezenta decizie se adresează statelor membre.

▼C1

ANEXĂ

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

PREFAȚĂ

1. **Aspecte generale**

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 din Directiva 1999/93/CE. Aceasta include furnizarea de informații istorice cu privire la statutul supravegherii/acreditării serviciilor de certificare supravegheate/acreditate.

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

Informațiile suplimentare privind alți CSP supravegheați/acreditați care nu eliberează QC, dar prestează servicii referitoare la semnăturile electronice (de exemplu, CSP care prestează servicii de marcare temporală și care eliberează jetoane de marcare temporală, CSP care eliberează certificate necalificate etc.) pot fi incluse pe lista sigură la nivel național în mod voluntar.

Aceste informații au ca scop principal susținerea validării semnăturilor electronice calificate (QES) și a semnăturilor electronice avansate (AdES) ([4]) bazate pe un certificat calificat ([5]) ([6]).

Modelul comun propus este compatibil cu o punere în aplicare pe baza specificațiilor din ETSI TS 102 231 ([7]) care sunt utilizate pentru a gestiona crearea, publicarea, localizarea, accesarea, autentificarea și fiabilitatea acestui tip de liste.

([1]) Conform definiției de la articolul 2 punctul 11 din Directiva 1999/93/CE.
([2]) Conform definiției de la articolul 2 punctul 10 din Directiva 1999/93/CE.
([3]) Conform definiției de la articolul 2 punctul 6 din Directiva 1999/93/CE.
([4]) Conform definiției de la articolul 2 punctul 2 din Directiva 1999/93/CE.
([5]) Pentru o AdES bazată pe un QC, se va folosi pe parcursul prezentului document acronimul „$AdES_{QC}$”.
([6]) Este de 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 care susțin respectiva semnătură (de exemplu, eliberarea unui certificat necalificat) să facă parte din serviciile supravegheate/acreditate incluse de un stat membru pe lista sigură, printre informațiile furnizate în mod voluntar.
([7]) ETSI TS 102 231 – Semnături și infrastructuri electronice (*Electronic Signatures and Infrastructures* – ESI): Furnizarea de informații armonizate privind statutul serviciilor de încredere (*Provision of harmonized Trust-service status information*).

▼C1

2. **Linii directoare privind editarea intrărilor din TL**

2.1. *O listă sigură care include în special servicii de certificare supravegheate/acreditate*

Servicii de certificare și prestatori de servicii de certificare relevanți într-o singură listă

Lista sigură a unui stat membru este definită ca „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 trebuie să includă:

— **toți prestatorii de servicii de certificare**, astfel cum sunt definiți la articolul 2 punctul 11 din Directiva 1999/93/CE, respectiv „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 din Directiva 1999/93/CE.

În ceea ce privește definițiile și dispozițiile Directivei 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, respectiv 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 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 în cauză.

— 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 stipulate la articolul 3 alineatul (3), articolul 8 alineatul (1), articolul 11 și considerentul (13) [respectiv articolul 2 punctul 13, articolul 3 alineatul (2), articolul 7 alineatul (1) litera (a), articolul 8 alineatul (1), articolul 11, considerentul (4) și considerentele (11)-(13)].

— **CSP care nu eliberează QC**

— Aceștia pot intra sub incidența unui sistem de „acreditare voluntară” (în conformitate cu definiția și cu prevederile 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 directivă].

— 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 o astfel de „calificare” va rămâne probabil semnificativă numai la nivel național.

▼C1

Lista sigură a unui stat membru trebuie să furnizeze un minimum de informații privind CSP supravegheați/acreditați care eliberează certificate calificate pentru public în conformitate cu dispozițiile Directivei 1999/93/CE [articolul 3 alineatele (2) și (3) și articolul 7 alineatul (1) litera (a)], informații privind QC care atestă semnătura electronică, precum și dacă o semnătură este sau nu creată printr-un dispozitiv securizat de creare a semnăturii.

Informațiile suplimentare cu privire la alte servicii supravegheate/acreditate furnizate de CSP care nu eliberează QC pentru public (de exemplu CSP care prestează servicii de marcare temporală și eliberează jetoane de marcare temporală, CSP care eliberează certificate necalificate etc.) pot fi incluse pe lista sigură la nivel național în mod voluntar.

Lista sigură are următoarele scopuri:

— includerea pe listă și furnizarea de informații fiabile privind statutul supravegherii/acreditării serviciilor de certificare furnizate de prestatorii de servicii de certificare care sunt supravegheați/acreditați de către statul membru responsabil pentru crearea și menținerea listei în vederea conformității cu dispozițiile relevante ale Directivei 1999/93/CE;

— facilitarea validării semnăturilor electronice atestate de serviciile supravegheate/acreditate incluse pe listă, prestate de CSP incluși pe listă.

Un singur set de valori pentru statutul supravegherii/acreditării

În fiecare stat membru trebuie creată și menținută o singură TL pentru a indica statutul supravegherii și/sau acreditării acelor servicii de certificare furnizate de acei CSP certificați/acreditați de către statul membru.

Faptul că un serviciu este la momentul actual fie supravegheat, fie acreditat face parte din statutul actual al serviciului respectiv. În plus, statutul de supraveghere sau de acreditare poate fi „în curs”, „în curs de a fi suspendat”, „suspendat” sau chiar „revocat”. Pe parcursul existenței sale, același serviciu de certificare poate trece de la statutul de supraveghere la cel de acreditare și invers ([1]).

Următoarea figură 1 descrie fluxul preconizat, pentru un serviciu de certificare, între eventualele stadii 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 mod analog, 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.

▼C1

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

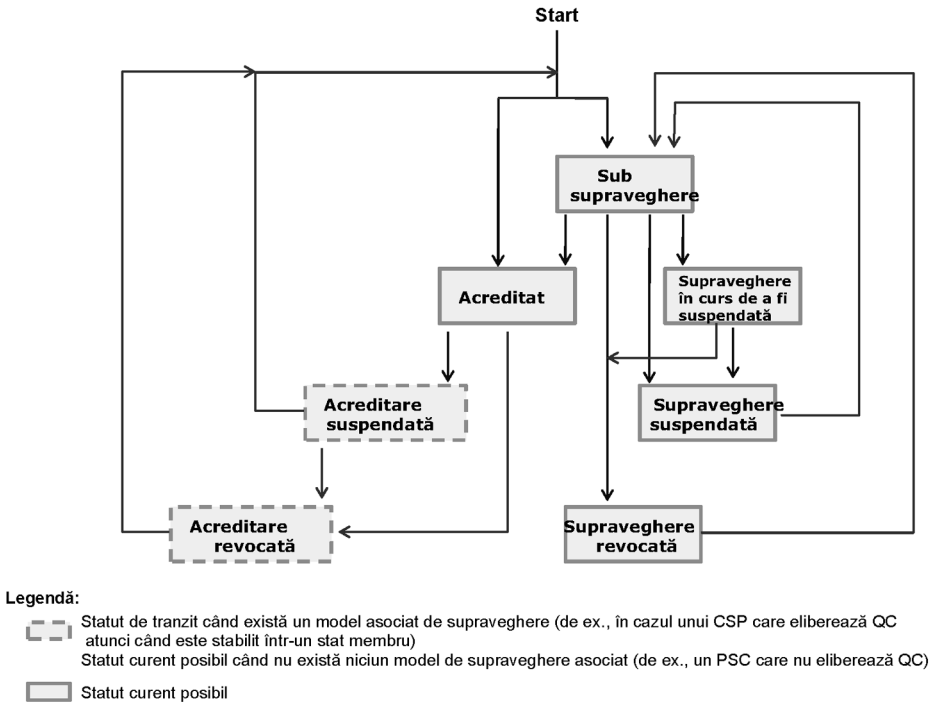


Figura 1

Un serviciu de certificare care eliberează QC trebuie supravegheat (dacă este stabilit într-un stat membru) și poate fi acreditat voluntar. Atunci când este inclus pe lista sigură, statutul unui serviciu poate avea ca „valoare a statutului curent” oricare dintre valorile de statut prezentate mai sus. Cu toate acestea, trebuie să se rețină că atât „acreditare suspendată”, cât și „acreditare revocată” trebuie să fie valori ale „statutului de tranzit” doar în cazul serviciilor CSP_{QC} stabiliți într-un stat membru, întrucât aceste servicii trebuie să fie implicit supravegheate (chiar și atunci când nu sunt sau când nu mai sunt acreditate).

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 punctul 11 din directivă] trebuie să clasifice programul (programele) de aprobare în următoarele două categorii:

— „acreditare voluntară”, în conformitate cu definiția și dispozițiile Directivei 1999/93/CE [articolul 2 punctul 13, articolul 3 alineatul (2), articolul 7 alineatul (1) litera (a), articolul 8 alineatul (1), articolul 11, considerentul (4) și considerentele (11)-(13)];

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

▼C1

În consecință, un serviciu de certificare care nu eliberează QC poate fi supravegheat sau acreditat voluntar. Atunci când este introdus pe o listă sigură, statutul acestui serviciu poate avea ca „valoare a statutului curent” oricare dintre valorile de statut prezentate anterior (a se vedea figura 1).

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

— informații privind sistemul de supraveghere aplicabil oricărui CSP_{QC};

— atunci când este cazul, informații privind programul național de „acreditare voluntară” aplicabilă 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.

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 acestor sisteme de supraveghere/acreditare aplicate la nivel național acelor CSP care nu eliberează QC. Atunci când în TL sunt furnizate informații privind statutul supravegherii/acreditării serviciilor furnizate de un CSP care nu eliberează QC, seturile de informații menționate anterior vor fi furnizate în TL 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 referire 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 5.8.2) ca parte din „Service information extension” (dispoziția 5.5.9). Informațiile suplimentare privind specificațiile tehnice corespunzătoare sunt cuprinse în specificațiile detaliate din capitolul I.

În ciuda faptului 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 anumit serviciu de certificare (identificat prin „Service digital identity”, în conformitate cu ETSI TS 102 231 [1]) și că statutul acreditării/supravegherii aferent acestuia va fi actualizat în mod corespunzător. Înțelesul stadiilor prezentate mai sus este descris în dispoziția 5.5.4 din specificațiile tehnice detaliate cuprinse în capitolul I.

2.2. *Intrări în TL pentru facilitarea validării QES și $AdES_{QC}$*

Cel mai critic aspect în crearea unei TL este elaborarea părții obligatorii a acesteia, anume a „Listei de servicii” pentru fiecare CSP care eliberează QC, pentru a reflecta corect situația exactă, în ceea ce privește eliberările, a fiecărui serviciu de eliberare a QC de acest tip 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).

[1] ETSI TS 102 231 – Semnături și infrastructuri electronice (*Electronic Signatures and Infrastructures* – ESI): Furnizarea de informații armonizate privind statutul serviciilor de încredere (*Provision of harmonized Trust-service status information*).

▼C1

În măsura în care nu există un profil cu adevărat interoperabil și transfrontalier pentru QC, informațiile necesare pot include alte date în afara „Service digital identity” a unei singure (Root) CA (Autoritate de certificare de bază), în special informații care permit identificarea statutului QC al certificatului eliberat și acele informații privind utilizarea eventuală a unui SSCD pentru crearea semnăturilor atestate. Organismul dintr-un stat membru desemnat să creeze, să editeze și să mențină TL (adică operatorul programului în conformitate cu ETSI TS 102 231) trebuie, prin urmare, să ia în considerare profilul curent și conținutul certificatului în cazul fiecărui QC eliberat, pentru fiecare CSP_{QC} inclus în TL.

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 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 TS 101 456 ([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 diferențele apărute în conținutul real al QC eliberate în prezent (de exemplu, utilizarea sau nu a acelor 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 calculatoare, 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.

Completarea câmpurilor „Service type identifier” („Sti”), „Service name” („Sn”) și „Service digital identity” („Sdi”) ([3]) cu informațiile furnizate în câmpul „Service information” („Sie”) permite modelului comun propus pentru TL să determine în mod integral un anumit tip de certificat calificat eliberat de un serviciu de certificare al unui CSP introdus pe listă care eliberează QC și să determine dacă acesta se bazează pe un SSCD sau nu (dacă aceste informații nu sunt incluse în QC eliberat). O informație specifică despre un „Service current status” („Scs”) este, desigur, 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 orice certificat pentru o entitate finală eliberat în cadrul acestei (ierarhii) (Root) CA conține suficiente informații definite de ETSI și care pot fi procesate de calculator pentru a evalua dacă certificatul este sau nu un QC și dacă se bazează pe un SSCD. În cazul în care, de exemplu, ultima afirmație nu este adevărată (de exemplu, în QC nu există indicații standardizate conform ETSI și având o formă care poate fi procesată de calculator pentru a determina dacă certificatul se bazează sau nu pe un SSCD), prin introducerea pe listă doar a „Sdi” a acelei (Root) CA, se poate presupune doar că QC eliberate în cadrul acestei ierarhii a (Root) CA nu se bazează pe niciun SSCD. Pentru a putea considera acele QC ca bazându-se pe un SSCD, ar trebui să se utilizeze „Sie” pentru a indica acest aspect (ceea ce indică, de asemenea, că este garantat de CSP care eliberează QC și supravegheat/acreditat de organismul de supraveghere sau de acreditare).

([1]) A se vedea ETSI TS 101 862 – Semnături și infrastructuri electronice (*Electronic Signatures and Infrastructures* – ESI): Profilul certificatului calificat (*Qualified Certificate Profile*).

([2]) ETSI TS 101 456 – Semnături și infrastructuri electronice (*Electronic Signatures and Infrastructures* – ESI); Cerințe pentru autoritățile de certificare care emit certificate calificate (*Policy requirements for certification authorities issuing qualified certificates*).

([3]) Adică cel puțin un certificat X.509 v3 al QCA emitente sau al unei upper CA (Autoritate de supraveghere superioară) de pe traseul de certificare.

▼C1

Principii generale – Reguli de editare – Intrări CSP^{QC} (servicii de pe listă)

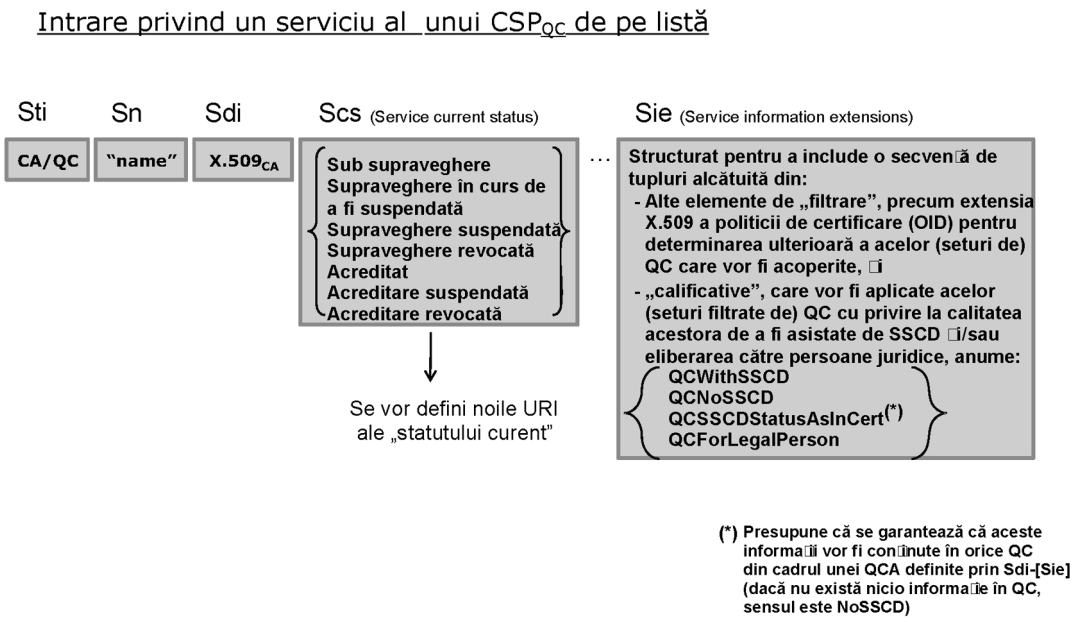


Figura 2

Intrare în TL implementată în formatul TSL privind un serviciu al unui CSP care eliberează QC

Specificațiile tehnice actuale pentru modelul comun de TL 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 CA care eliberează QC („CA/QC");

— „Service Name" („Sn");

— „Service digital identity" („Sdi"), informații care identifică un serviciu introdus pe listă, de exemplu certificatul X.509v3 (ca o cerință minimă) al unei CA care eliberează QC;

— pentru serviciile CA/QC, informații opționale privind „Service information extensions" („Sie") care permit includerea unei secvențe de unul sau mai multe tupluri, fiecare tuplu conținând:

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

  — informațiile asociate („calificative") care să indice dacă acest set de certificate calificate al serviciului identificat în mod mai precis se bazează sau nu pe un SSCD sau dacă aceste informații asociate fac parte din QC într-o formă standardizată care poate fi procesată de un calculator și/sau informații cu privire la faptul că aceste QC sunt eliberate către persoane juridice (acestea vor fi considerate implicit ca eliberate exclusiv persoanelor fizice);

▼C1

— informații privind „statutul curent” al acestui serviciu care indică:

— dacă este un serviciu supravegheat sau acreditat; și

— statutul propriu-zis de supraveghere/acreditare.

2.3. *Linii directoare privind editarea și utilizarea intrărilor privind serviciile CSP_{QC}*

Liniile directoare generale privind editarea sunt:

1. Dacă 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” 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. Dacă 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 este creat astfel încât să nu conțină 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. Dacă 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 aceste QC sunt destinate a se baza pe SSCD, iar altele nu (de exemplu această diferență 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, cu posibilitate de procesare de către calculatoare sau nu), însă nu conține NICI declarația QcSSCD, NICI QCP OID(+) definit de ETSI, atunci utilizarea unei „Sdi” adecvate poate să nu fie suficientă ȘI câmpul „Sie” trebuie folosit pentru a indica informațiile explicite privind generarea prin SSCD, precum și eventuala extensie a informațiilor pentru a identifica setul acoperit de certificate. Probabil că în acest caz va fi necesar ca acesta să se includă diferitele „valori ale informațiilor privind suportul SSCD” pentru aceeași „Sdi” atunci când se utilizează câmpul „Sie”.

4. Dacă 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 această „Sdi” sunt proiectate să devină QC și/sau să se bazeze pe SSCD, iar altele nu (de exemplu această diferențiere 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, cu posibilitate de procesare de către calculatoare sau nu), atunci utilizarea unei „Sdi” adecvate nu va fi suficientă ȘI câmpul „Sie” trebuie folosit pentru a include informații explicite privind generarea prin SSCD. 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”.

▼C1

Ca un principiu general implicit, pentru un CSP inclus pe lista sigură trebuie să existe o singură intrare privind serviciul pentru fiecare certificat X.509v3 pentru un serviciu de certificare de tip CA/QC, însemnând o autoritate de certificare care eliberează (direct) QC. În anumite circumstanțe atent definite și în anumite condiții atent coordonate, un organism de supraveghere sau de acreditare dintr-un stat membru poate decide să utilizeze certificatul X.509v3 al unei Root CA sau Upper level CA (autoritate de certificare superioară) (adică 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 care eliberează QC către entitățile finale) ca „Sdi" pentru o singură intrare din lista de servicii furnizate de un CSP inclus pe listă. Consecințele (avantajele și dezavantajele) utilizării acestui certificat X.509v3 al Root CA sau Upper CA ca valori „Sdi" ale intrărilor privind serviciile din TL trebuie să fie analizate cu atenție și aprobate de 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.

Pentru a ilustra liniile directoare generale privind editarea, se poate oferi următorul exemplu: în cazul unui CSP_{QC} care folosește o Root CA în cadrul căreia mai multe autorități de certificare 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, orice QC eliberat în cadrul acestei ierarhii Root CA NU se bazează pe un SSCD. Dacă acele QC se bazează de fapt pe un SSCD, se recomandă cu insistență utilizarea declarației QcSSCD în QC eliberate pe viitor. Între timp (până la expirarea ultimului QC care nu conține această informație), TSL trebuie să utilizeze câmpul „Sie" și extensia asociată „Qualifications", de exemplu filtrarea certificatelor prin intermediul 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 includ „SSCD suport information" explicite cu privire la acele certificate filtrate prin intermediul „Calificativelor".

Liniile directoare generale privind utilizarea aplicațiilor, serviciilor sau produselor legate de semnături electronice bazate pe implementarea TSL a unei TL 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 „RootAC/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 QcStatements adecvate (de exemplu, QcC, QcSSCD) și/sau QCP(+) OID definiți de ETSI (acest aspect fiind garantat de organismul de supraveghere/acreditare, a se vedea mai sus „liniile directoare generale privind editarea")

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

▼C1

— **și DACĂ** există informații privind „Qualification” în „Sie”, atunci în plus față de regula sus-menționată de interpretare implicită, acele certificate care sunt identificate prin utilizarea acestei intrări „Qualification” din „Sie”, create pe baza principiului unei secvențe de „filtre” care identifică mai precis un set de certificate și furnizează informații suplimentare cu privire la „suportul SSCD” și/sau „persoana juridică în calitate de subiect” [de exemplu acele certificate 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.], vor fi luate în considerare în funcție de următorul set de „calificative”, compensând astfel lipsa informațiilor din QC corespunzător, și anume:

— pentru a indica suportul 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

  — „StatutDSCSCCconformCert” – 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”.

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

Trebuie să fie, de asemenea, incluse cazurile în care CRL (listele certificatelor revocate) și răspunsurile OCSP (*Online Certificate Status Protocol* – protocol online privind statutul certificatelor) sunt semnate cu chei diferite de cele ale unei CA care eliberează QC („CA/QC”). Aceasta se poate realiza prin introducerea pe listă a acelor servicii ca atare în implementarea TSL a TL (respectiv cu un „Service type identifier” calificat ulterior printr-o „AdditionalServiceInformation” care indică faptul că un serviciu OCSP sau CRL este parte componentă a furnizării de QC, de exemplu printr-un tip de serviciu precum „OCSP/QC”, respectiv „CRL/QC”), întrucât aceste servicii pot fi considerate ca parte componentă a serviciilor „calificate” supravegheate/acreditate asociate prestării serviciilor de certificare a 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 prevedere asemănătoare se poate aplica serviciilor de certificare care eliberează certificate necalificate (de tip „CA/PKC” – autoritate de certificare care folosește criptografia cu chei publice) folosind tipurile implicite de servicii OCSP și CRL definite de ETSI TS 102 231.

Trebuie reținut faptul că implementarea TSL a unei TL TREBUIE să includă servicii de revocare dacă informațiile aferente nu sunt prezente în câmpul AIA al certificatelor finale sau dacă certificatul nu este semnat de o CA inclusă pe listă.

2.5. *Evoluția către un profil QC interoperabil*

În general, trebuie să se încerce o simplificare (reducere) pe cât posibil a numărului de intrări de servicii („Sdi” diferite). Această acțiune trebuie compensată,însă, prin identificarea corectă a acelor servicii legate de eliberarea de QC și cu furnizarea informațiilor de încredere cu privire la suportul SSCD al unui QC, dacă aceste informații nu apar în QC eliberat.

▼C1

În mod ideal, utilizarea câmpului „Sie” și a extensiei „Qualification” trebuie limitată (strict) la acele cazuri specifice care trebuie soluționate în acest mod, întrucât QC trebuie să conțină informații suficiente cu privire la afirmațiile privind statutul de certificat calificat și suportul SSCD sau inexistența acestuia.

Statele membre ar trebui să impună, pe cât posibil, adoptarea și utilizarea profilurilor QC interoperabile.

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

Modelul comun propus pentru lista sigură a unui stat membru va fi structurat pe următoarele categorii de informații:

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

2. o secvență de câmpuri care să conțină informații de identificare neechivoce cu privire la fiecare CSP supravegheat/acreditat din cadrul programului (această secvență este opțională, ceea ce presupune că, dacă nu este utilizată, lista va fi considerată goală, adică niciun CSP nu este supravegheat sau acreditat în statul membru asociat în contextul domeniului listei sigure);

3. pentru fiecare CSP inclus pe listă, o secvență de câmpuri care conțin informații de identificare neechivoce privind un serviciu de certificare supravegheat/acreditat furnizat de CSP (această secvență trebuie să conțină minimum o intrare);

4. pentru fiecare serviciu de certificare supravegheat/acreditat inclus pe listă, identificarea statutului curent al serviciului și istoricul statutului său.

În contextul unui CSP care eliberează QC, identificarea neechivocă a unui serviciu de certificare supravegheat/acreditat care urmează să fie introdus pe listă trebuie să ia în considerare acele situații în care nu sunt disponibile suficiente informații în certificatul calificat cu privire la statutul de „certificat calificat” și la eventualul suport SSCD și în special să abordeze un alt aspect, respectiv faptul că majoritatea CSP (din domeniul comercial) apelează la o singură CA calificată emitentă pentru a emite diferite tipuri de certificate, atât calificate, cât și necalificate, pentru entitățile finale.

Numărul de intrări din listă pentru fiecare CSP recunoscut ar putea fi redus dacă există unul sau mai multe servicii ale Upper CA, de exemplu în contextul unei ierarhii comerciale de autorități de certificare de la o Root CA în sens descendent la autoritățile de certificare emitente. Cu toate acestea, chiar și în aceste cazuri, trebuie să se păstreze 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.

1. *Informații privind lista sigură și sistemul de publicare a acesteia*

Această categorie va cuprinde, printre altele, următoarele informații:

— o **etichetă** a listei sigure care să faciliteze identificarea listei sigure în timpul căutărilor electronice și care să confirme, de asemenea, obiectivele acesteia atunci când este creată într-o formă lizibilă pentru om;

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

— un **număr de secvență (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);

▼C1

— **informații privind proprietarul** 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 incluzând, printre altele:

  — țara în care se aplică;

  — informații despre sau referințe 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 și următoarea actualizare prevăzută a** listei sigure.

2. *Informații de identificare neechivoce cu privire la fiecare CSP recunoscut de program*

Acest set de informații va cuprinde cel puțin următoarele:

— denumirea organizației CSP, astfel cum este utilizată în înregistrările juridice oficiale (poate include 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 pot fi descărcate.

3. *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 va include pentru fiecare serviciu de certificare furnizat de un CSP de pe listă cel puțin următoarele detalii:

— 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 de certificare respectiv;

— un identificator unic neechivoc al serviciului de certificare;

— informații suplimentare cu privire la serviciul de certificare (de exemplu, informații menționate direct sau prin trimitere la o adresă de unde se pot descărca, informații de acces referitoare la serviciu);

— pentru serviciile CA/QC, o secvență opțională de tupluri cu informații, fiecare dintre acestea conținând

  (i) criterii care vor fi utilizate la identificarea mai precisă (filtrarea) în cadrul serviciilor de certificare identificate prin „Sdi” a acelui serviciu (respectiv set de certificate calificate) pentru care sunt solicitate/furnizate informații suplimentare pentru a indica dacă se bazează pe un SSCD sau nu (și/sau eliberarea către o persoană juridică); și

  (ii) „calificative” asociate care să furnizeze informații care să indice dacă acest set de certificate calificate al serviciului identificat în mod mai precis se bazează sau nu pe un SSCD și/sau informații cu privire la faptul că aceste QC sunt eliberate sau nu către persoane juridice (acestea vor fi considerate implicit ca eliberate exclusiv persoanelor fizice).

▼C1

4. *Pentru fiecare serviciu de certificare inclus pe listă, identificarea statutului curent al serviciului și istoricul statutului său*

Acest set de informații va cuprinde cel puțin următoarele:

— un identificator al statutului curent;

— data și ora la care s-a trecut la statutul curent;

— informații istorice cu privire la acest statut.

4. **Definiții și abrevieri**

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

Termen	Abreviere	Definiție
Prestator de servicii de certificare	CSP	Așa cum este definit la articolul 2 punctul 11 din Directiva 1999/93/CE
Autoritate de certificare	CA	O CA este un CSP și poate utiliza diferite chei tehnice private de semnare ale autorităților de certificare cu scopul de a elibera certificate pentru entitățile finale. O CA este o autoritate căreia unul sau mai mulți utilizatori îi încredințează crearea și repartizarea certificatelor. Opțional, autoritatea de certificare poate crea chei pentru utilizatori [ETSI TS 102 042]. Se consideră că CA este identificată prin informațiile de identificare completate în câmpul Issuer (al emitentului) din certificatul CA aferent cheii publice (de certificare) care este asociată cu cheia de semnare privată a CA, care este utilizată efectiv de CA pentru a elibera certificate pentru entități. O CA poate dispune de mai multe chei de semnare. Fiecare cheie de semnare a CA este identificată în mod unic printr-un identificator unic din câmpul Authority Key Identifier din certificatul CA.
Autoritate de certificare care 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	Așa cum este definit la articolul 2 punctul 9 din Directiva 1999/93/CE
Certificat calificat	QC	Așa cum este definit la articolul 2 punctul 10 din Directiva 1999/93/CE
Semnatar	Semnatar	Așa cum este definit la articolul 2 punctul 3 din Directiva 1999/93/CE
Supraveghere	Supraveghere	Termenul „supraveghere” este utilizat în sensul Directivei 1999/93/CE [articolul 3 alineatul (3)]. Directiva impune statelor membre să creeze un sistem adecvat care să permită supravegherea CSP stabiliți pe teritoriul lor și eliberarea de certificate calificate pentru public, asigurând supravegherea respectării dispozițiilor directivei.
Acreditare voluntară	Acreditare	Așa cum este definită la articolul 2 punctul 13 din Directiva 1999/93/CE
Listă sigură	TL	Desemnează lista care indică statutul 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.

▼C1

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 102 231.
Serviciu de încredere		Serviciu care sporește încrederea în tranzacțiile electronice (folosind în general, dar nu obligatoriu tehnici criptografice sau implicând materiale confidențiale) (ETSI TS 102 231).
Prestator de servicii de încredere	TSP	Organism care prestează unul sau mai multe servicii (electronice) de încredere (acest termen 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. Exemplele de TrST binare includ certificatele, CRL, jetoane de marcare temporală și răspunsurile OCSP.
Semnătură electronică calificată	QES	O AdES confirmată de un QC și creată de un SSCD, în conformitate cu definiția de la articolul 2 din Directiva 1999/93/CE.
Semnătură electronică avansată	AdES	Așa 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 în conformitate cu definiția de la articolul 2 din Directiva 1999/93/CE.
Dispozitiv securizat de creare a semnăturii	SSCD	Așa cum este definit la articolul 2 punctul 6 din Directiva 1999/93/CE.

CAPITOLUL I

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

În următoarea secțiune a documentului cuvintele cheie „TREBUIE” (din engleză MUST), „NU TREBUIE” (din engleză MUST NOT), „OBLIGATORIU” (din engleză REQUIRED), „ESTE/NU ESTE” și timpul prezent în general (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]).

►**M1** Prezentele specificații se bazează pe specificațiile și cerințele prevăzute în ETSI TS 102 231 v.3.1.2. Atunci când în prezentele specificații nu există cerințe specifice, SE APLICĂ în întregime cerințele din ETSI TS 102 231 v.3.1.2. ◄ Dacă în cuprinsul prezentelor specificații se menționează cerințe specifice, acestea PREVALEAZĂ asupra cerințelor corespunzătoare din ETSI TS 102 231 și vor fi completate de specificațiile privind formatul din ETSI TS 102 231. În cazul în care apar discrepanțe între prezentele specificații și specificațiile cuprinse în ETSI TS 102 231, prezentele specificații SUNT cele cu caracter normativ.

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

▼C1

Suportul lingvistic ESTE implementat și oferit cel puțin în limba engleză (EN) și eventual în una sau mai multe limbi naționale.

Indicarea datei și a orei RESPECTĂ dispoziția 5.1.4 din ETSI TS 102 231.

Utilizarea URI RESPECTĂ dispoziția 5.1.5 din ETSI TS 102 231.

Informații privind sistemul de publicare a listei sigure

Tag

TLS tag (dispoziția 5.2.1)

Câmpul este OBLIGATORIU și RESPECTĂ dispoziția 5.2.1 din ETSI TS 102 231.

▼M1

———————

▼C1

Scheme information

TLS version identifier (dispoziția 5.3.1)

Acest câmp este OBLIGATORIU și SE SETEAZĂ la „3” (număr întreg).

TSL sequence number (dispoziția 5.3.2)

▼M1

Acest câmp este OBLIGATORIU. Acesta SPECIFICĂ numărul secvențial al TSL. Începând de la „1”, la prima publicare a TSL, valoarea acestui număr întreg CREȘTE la fiecare publicare ulterioară a TSL. Valoarea NU ESTE readusă la „1” atunci când crește „TSL version identifier” de mai sus.

▼C1

TSL type (dispoziția 5.3.3)

▼M1

Acest câmp este OBLIGATORIU pentru a specifica tipul TSL. Acesta ESTE setat la http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic).

▼C1

Notă: Pentru a respecta ETSI TS 102 231, dispoziția 5.3.3, și pentru a indica tipul specific al TSL făcând referire la existența prezentelor specificații care reglementează organizarea implementării TSL a listelor sigure a statelor membre ([1]) și permițând unui program de analiză să determine ce formă a oricăruia dintre câmpurile următoare ([2]) este preconizată, în cazul în care acele câmpuri au sensuri specifice (sau alternative) în funcție de tipul de TSL reprezentat (în acest caz, o listă sigură a unui stat membru), URI specific sus-menționat SE ÎNREGISTREAZĂ și SE DESCRIE după cum urmează:

([1]) Adică „o listă cuprinzând statutul de supraveghere/acreditare a serviciilor de certificare furnizate de prestatorii de servicii de certificare care sunt supravegheați/acreditați de statul membru în vederea conformității cu dispozițiile relevante din Directiva 1999/93/CE” (pe scurt, „lista sigură”).

([2]) Respectiv câmpurile specificate de ETSI TS 102 231 – Semnături și infrastructuri electronice (*Electronic Signatures and Infrastructures* – ESI): Furnizarea de informații armonizate privind statutul serviciilor de încredere (*Provision of harmonized Trust-service status information*) și „adaptate” de prezentele specificații cu scopul de a specifica elaborarea listelor sigure ale statelor membre.

▼M1

URI: (Generic) http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic.

▼C1

Descriere: O implementare TSL a unei liste cuprinzând statutul supravegherii/acreditării aferent serviciilor de certificare furnizate de prestatorii de servicii de certificare care sunt supravegheați/acreditați de statul membru de referință care este proprietarul implementării TSL, în vederea conformității cu dispozițiile relevante din Directiva 1999/93/CE, prin intermediul unui proces de monitorizare directă (fie voluntară sau normativă).

Scheme operator name (dispoziția 5.3.4)

Acest câmp este OBLIGATORIU. Câmpul SPECIFICĂ denumirea organismului statului membru responsabil pentru crearea, publicarea și menținerea listei sigure naționale. Acesta SPECIFICĂ denumirea oficială sub care operează entitatea juridică sau autorizată prin mandat (de exemplu pentru agențiile administrative guvernamentale) asociată acestui organism. Denumirea TREBUIE să fie cea utilizată în actele oficiale de înregistrare sau de autorizare, căreia trebuie să i se adreseze toate comunicările oficiale. Denumirea ESTE alcătuită dintr-o secvență de șiruri de caractere multilingve și ESTE implementată în limba engleză (EN) ca limbă obligatorie și eventual în una sau mai multe limbi naționale.

Notă: O țară POATE avea organisme de supraveghere și acreditare separate și chiar și organisme suplimentare pentru diferite activități operaționale aferente. ►M1 Statele membre sunt cele care desemnează Scheme operator pentru implementarea TSL a TL a statului membru. ◄ Se preconizează că organismul de supraveghere, organismul de acreditare și operatorul programului (atunci când este vorba de organisme separate) vor avea responsabilități și obligații proprii.

Orice situație în care mai multe organisme poartă răspunderea pentru supraveghere, acreditare sau alte aspecte operaționale ESTE REFLECTATĂ cu exactitate și IDENTIFICATĂ ca atare în informațiile privind programul care fac parte din TL, inclusiv în informațiile specifice de program indicate de „Scheme information URI” (dispoziția 5.3.7).

▼M1

Scheme Operator desemnat (dispoziția 5.3.4) este entitatea care va semna TSL.

▼C1

Scheme operator address (dispoziția 5.3.5)

Acest câmp este OBLIGATORIU. Câmpul SPECIFICĂ adresa entității juridice sau a organizației autorizate prin mandat identificate în câmpul „Scheme operator name” (dispoziția 5.3.4) pentru comunicații prin poștă, precum și pentru cele electronice. Acesta INCLUDE atât „PostalAddress” (respectiv strada, localitatea, [statul sau provincia], [codul poștal] și codul țării ISO 3166-1 alpha-2) în conformitate cu dispoziția 5.3.5.1, cât și „ElectronicAddress” (respectiv adresa e-mail și/sau URI al site-ului web) în conformitate cu dispoziția 5.3.5.2.

Scheme name (dispoziția 5.3.6)

Acest câmp este OBLIGATORIU și specifică denumirea programului. Denumirea CONSTĂ într-o secvență de șiruri de caractere multilingve (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale) definite după cum urmează:

▼C1

— Versiunea EN CONSTĂ într-un șir de caractere organizat după cum urmează:

CC:EN_name_value

unde:

— „CC” = codul țării ISO 3166-1 alpha-2 folosit în câmpul „Scheme territory” (dispoziția 5.3.10);

— „:” = este folosit ca separator;

▼M1

— „EN_name_value” = Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State’s laws.

▼C1

— Orice versiune în limba națională a statului membru CONSTĂ într-un șir de caractere organizat după cum urmează:

CC:name_value

unde:

— „CC” = codul țării ISO 3166-1 alpha-2 folosit în câmpul „Scheme territory” (dispoziția 5.3.10);

— „:” = este folosit ca separator;

— „denumire_valoare” = traducerea oficială în limba națională a șirului de caractere „EN_name_value” sus-menționat, adică, pentru limba română: „Lista cuprinzând statutul supravegherii/acreditării serviciilor de certificare furnizate de prestatorii de servicii de certificare supravegheați/acreditați de statul membru de referință al operatorului desemnat al programului în vederea conformității cu dispozițiile relevante din Directiva 1999/93/CE”.

Denumirea programului trebuie să identifice în mod unic, prin nume, programul la care face referire „Scheme information URI” și să garanteze că, în cazul în care un operator de program gestionează mai multe programe, fiecăruia dintre acestea i se atribuie o denumire diferită.

Statele membre și operatorii de program SE VOR ASIGURA că, în cazul în care un stat membru sau un operator de program gestionează mai multe programe, fiecăruia dintre acestea i se atribuie o denumire diferită.

Scheme information URI (dispoziția 5.3.7)

Acest câmp este OBLIGATORIU și SPECIFICĂ URI (unul sau mai mulți) unde utilizatorii (părțile care se bazează pe certificat) pot obține informații specifice programului (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale). Acest câmp CONSTĂ într-o secvență de indicatori multilingvi (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale). URI de referință (unul sau mai mulți) TREBUIE să furnizeze o cale către „informațiile corespunzătoare despre program”.

„Informațiile corespunzătoare despre program” INCLUD 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 este următorul:

▼C1

The present list is the TSL implementation of [*name of the relevant Member State*] „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;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)], including 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 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 Art. 3.3, Art. 8.1, Art. 11 (respectively, Art. 2.13, Art. 3.2, Art. 7.1(a), Art. 8.1, Art. 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 and the present TSL implementation 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};

([1]) Ultimele două seturi de informații prezintă o importanță esențială pentru a permite părților care se bazează pe certificate să evalueze nivelul de calitate și siguranță al acestor sisteme de supraveghere/acreditare. Aceste seturi de informații vor fi furnizate în LS 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).

▼C1

— 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.

— Aceste informații specifice INCLUD pentru fiecare program de bază enumerat 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.

Informațiile suplimentare specifice statului membru cu privire la program POT fi furnizate în mod voluntar. Acestea INCLUD:

— 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.

Status determination approach (dispoziția 5.3.8)

Acest câmp este OBLIGATORIU și SPECIFICĂ identificatorul metodei de determinare a statutului. SE FOLOSEȘTE următorul URI specific, înregistrat și descris după cum urmează:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/appropriate

Descriere: Statutul serviciilor este determinat de operatorului programului sau în numele acestuia în baza unui sistem adecvat pentru un stat membru de referință care permite „supravegherea” (și „acreditarea voluntară”, dacă este cazul) a prestatorilor de servicii de certificare care sunt stabiliți pe teritoriul statului în cauză (sau care sunt stabiliți într-o țară terță în cazul „acreditării voluntare”) și eliberează certificate calificate pentru public în conformitate cu articolul 3 alineatul (3) [respectiv articolul 3 alineatul (2) sau articolul 7 alineatul (1) litera (a)] din Directiva 1999/93/CE și care, dacă este cazul, permite „supravegherea”/„acreditarea voluntară” a prestatorilor de servicii de certificare care nu eliberează certificate calificate, în conformitate cu „un program (mai multe programe) recunoscut (recunoscute)” definit (definite) și stabilit (stabilite), precum și pus (puse) în aplicare la nivel național în vederea supravegherii respectării de către serviciile furnizate de CSP care nu eliberează QC a dispozițiilor din Directiva 1999/93/CE și completate eventual cu dispozițiile naționale referitoare la prestarea acestor servicii de certificare.

▼C1

Scheme type/community/rules (dispoziția 5.3.9)

Acest câmp este OBLIGATORIU și CONȚINE cel puțin următorii URI înregistrați:

— Un URI comun tuturor listelor sigure ale statelor membre care indică un text descriptiv care SE APLICĂ tuturor TL:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

— care informează cu privire la participarea programului statului membru [identificat prin „TSL type” (dispoziția 5.3.3) și „Scheme name” (dispoziția 5.3.6)] într-o schemă a tuturor programelor (adică o TSL care indică spre toate statelor membre care publică și mențin o TL sub forma unei TSL);

— unde utilizatorii pot obține politica/regulile CARE SE APLICĂ la evaluarea serviciilor incluse pe listă și prin care se poate determina tipul TSL (a se vedea dispoziția 5.3.3);

— unde utilizatorii pot obține o descriere a modului de utilizare și interpretare a conținutului implementării TSL a listei sigure. Aceste reguli privind utilizarea SUNT comune tuturor listelor sigure ale statelor membre indiferent de tipul serviciului de pe listă și de sistemul (sistemele) de supraveghere/acreditare.

Textul 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 TSL implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's TSL implementation of their 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 a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 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.

▼C1

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 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 Art. 3.3, Art. 8.1, Art. 11 (respectively, Art. 2.13, Art. 3.2, Art. 7.1(a), Art. 8.1, Art. 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 and the present TSL implementation 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 Art. 2.11 of the Directive). 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 TSL implementation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision 2009/767/EC 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 ETSI TS 101 862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101 456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C1

Note: if no „Sie”„Qualification” information is present or if an end-entity certificate that is claimed to be a QC is not „further identified” through a related „Sie” entry, 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. QcC, QcSSCD) 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”„Qualification” information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this „Sie”„Qualification” entry, 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 „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 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 TSL implementation of the Member States' Trusted Lists.

▼C1

— Un URI specific pentru fiecare listă sigură a unui stat membru care trimite la un text descriptiv care SE APLICĂ respectivei TL a statului membru respectiv:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC

unde CC = codul țării ISO 3166-1 alpha-2 utilizat în câmpul „Scheme territory” (dispoziția 5.3.10)

— unde utilizatorii pot obține politica/regulile specifice ale statului membru de referință care SE APLICĂ 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 implementării TSL a listei sigure în ceea ce privește serviciile de certificare care nu se raportează la 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” în acest scop.

Statele membre POT defini URI suplimentari pornind de la URI specific al statului membru menționat mai sus (respectiv URI definiți pornind de la acest URI ierarhic specific).

Scheme territory (dispoziția 5.3.10)

În contextul prezentelor specificații, acest câmp este OBLIGATORIU și SPECIFICĂ țara unde este stabilit programul (codul țării ISO 3166-1 alpha-2).

TSL policy/legal notice (dispoziția 5.3.11)

În contextul prezentelor specificații, acest câmp este OBLIGATORIU și SPECIFICĂ politica programului sau furnizează un aviz cu privire la statutul juridic al programului sau la cerințele legale respectate de program în jurisdicția în care este stabilit programul și/sau orice constrângeri și condiții aplicate la menținerea și publicarea TL.

Acesta CONSTĂ într-un șir de caractere multilingv (text) alcătuit din două părți:

— O primă parte obligatorie, comună tuturor TL ale statelor membre (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale), conform căreia cadrul legal aplicabil este Directiva 1999/93/CE și formele corespunzătoare de implementare a acesteia din legislația statului membru indicat la câmpul „Scheme territory”.

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 the 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.”

▼C1

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

Cadrul legal aplicabil pentru prezenta implementare 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 implementarea acesteia în dreptul [numele statului membru relevant].

— O a doua parte opțională, specifică fiecărei TL (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale), care face referire la cadrul juridic național specific aplicabil (de exemplu, în special când se raportează la programele naționale de supraveghere/acreditare pentru CSP care nu eliberează QC).

Historical information period (dispoziția 5.3.12)

Acest câmp este OBLIGATORIU și SPECIFICĂ durata (număr întreg) de păstrare a informațiilor istorice în TSL. Această valoare întreagă trebuie să fie indicată sub forma unui număr de zile și, în contextul prezentelor specificații, ESTE mai mare decât sau egală cu 3 653 (ceea ce înseamnă că implementarea TSL a TL a statelor membre TREBUIE să păstreze informațiile istorice timp de minimum zece ani). În cazul unor valori mai mari, trebuie să se acorde atenția cuvenită cerințelor legale privind păstrarea datelor aplicabile în statul membru indicate în „Scheme Territory” (dispoziția 5.3.10).

Pointers to other TSLs (dispoziția 5.3.13)

În contextul prezentelor specificații, acest câmp este OBLIGATORIU și INCLUDE, dacă este disponibil, indicatorul către o formă conformă cu ETSI TS 102 231 a listei întocmite de CE cuprinzând linkuri (indicatori) către toate implementările TSL ale listelor sigure din statele membre. Se aplică specificațiile din ETSI TS 102 231, dispoziția 5.3.13, dacă se impune utilizarea identității digitale opționale, reprezentând emitentul TSL desemnată de indicator, formatată conform dispoziției 5.5.3.

Notă: În așteptarea implementării în conformitate cu ETSI TS 102 231 a listei întocmite de CE cuprinzând linkurile către implementările TSL ale TL ale statelor membre, acest câmp NU ESTE UTILIZAT.

List issue date and time (dispoziția 5.3.14)

Acest câmp este OBLIGATORIU și SPECIFICĂ data și ora (UTC exprimat ca Zulu) la care a fost publicată TSL folosind valoarea data-oră conform specificațiilor din ETSI TS 102 231, dispoziția 5.1.4.

Next update (dispoziția 5.3.15)

Acest câmp este OBLIGATORIU și SPECIFICĂ data și ora (UTC exprimat ca Zulu) cele mai recente la care se va publica următoarea TSL sau va fi nul pentru a indica o TSL închisă (folosind valoarea dată-oră conform specificațiilor din ETSI TS 102 231, dispoziția 5.1.4).

În cazul în care nici un TSP sau serviciu acoperit de program nu este modificat între timp, TSL TREBUIE să fie republicată până la data expirării ultimei TSL publicate.

În contextul prezentelor specificații, diferența dintre data și ora „Next update” și „List issue date and time” NU TREBUIE să depășească **șase (6)** luni.

▼C1

Distribution points (dispoziția 5.3.16)

Acest câmp este OPȚIONAL. Dacă este utilizat, acesta SPECIFICĂ locațiile unde se va publica implementarea actuală TSL a TL și unde pot fi găsite actualizările TSL curente. Dacă se specifică mai multe puncte de distribuire, toate acestea TREBUIE să furnizeze copii identice ale TSL curente sau ale versiunii actualizate a acesteia. Dacă este utilizat, acest câmp este formatat ca o secvență nevidă de șiruri, fiecare dintre acestea fiind în conformitate cu RFC 3986 ([1]).

Scheme extensions (dispoziția 5.3.17)

Acest câmp este OPȚIONAL și nu se utilizează în contextul prezentelor specificații.

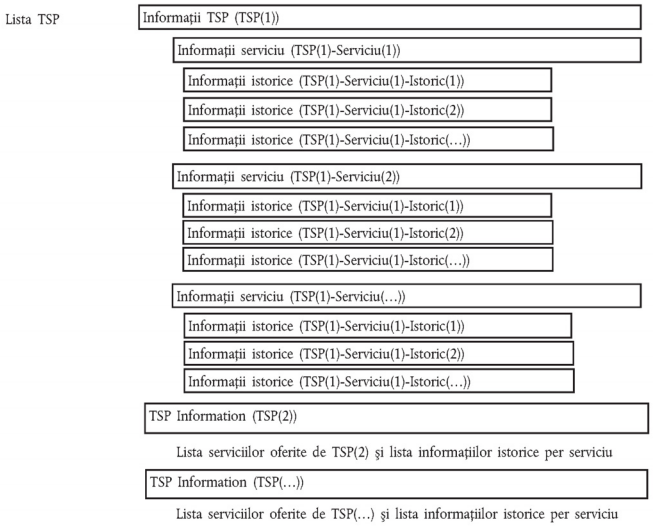
List of Trust Service Providers

Acest câmp este OPȚIONAL.

În cazul în care niciun CSP nu este sau nu a fost supravegheat/acreditat în contextul programului într-un stat membru, acest câmp ESTE ABSENT. S-a convenit, cu toate acestea, ca și în situația în care într-un stat membru nu există CSP supravegheat sau acreditat în cadrul programului, statele membre să IMPLEMENTEZE o TSL în care acest câmp să fie absent. Absența oricărui CSP din listă PRESUPUNE că nu există niciun CSP supravegheat/acreditat în țara menționată specificat la „Scheme territory”.

În cazul în care unul sau mai multe servicii ale CSP sunt sau au fost supravegheate/acreditate în cadrul programului, atunci câmpul CONȚINE o secvență de identificare a fiecărui CSP care furnizează unul sau mai multe servicii dintre cele supravegheate/acreditate, precum și detalii despre statutul de serviciu supravegheat/acreditat și despre istoricul statutului pentru fiecare dintre serviciile furnizate de CSP (TSP = CSP în imaginea de mai jos).

▼C2



([1]) IETF RFC 3986: „Identificatorii uniformi de resurse (URI): Sintaxă generică” (*Uniform Resource Identifiers (URI): Generic syntax*).

▼C1

Lista TSP este organizată conform reprezentării din imaginea de mai sus. Pentru fiecare TSP, există o secvență de câmpuri care cuprind informații privind TSP („TSP Information”), urmată de o listă de servicii. Pentru fiecare dintre aceste servicii, lista cuprinde o secvență de câmpuri conținând informații privind serviciul („Service Information”) și o secvență de câmpuri privind istoricul statutului aprobării aferent serviciului („Service approval history”).

TSP Information

TSP(1)

T S P n a m e (dispoziția 5.4.1)

Acest câmp este OBLIGATORIU și SPECIFICĂ denumirea **entității juridice** responsabile pentru serviciile furnizate de CSP care sunt sau au fost supravegheate sau acreditate în cadrul programului. Acesta este o secvență de șiruri de caractere multilingve (în EN ca limbă obligatorie și eventual în una sau mai limbi naționale). Această denumire TREBUIE să fie denumirea folosită în actele oficiale de înregistrare și cea căreia trebuie să i se adreseze toate comunicările oficiale.

T S P t r a d e n a m e (dispoziția 5.4.2)

Acest câmp este OPȚIONAL și, dacă este prezent, SPECIFICĂ o denumire alternativă prin care CSP se identifică în contextul specific al prestării acelor servicii, dintre cele pe care le furnizează, care sunt incluse în această TSL la intrarea „TSP name” (dispoziția 5.4.1).

Notă: Dacă o singură entitate juridică CSP furnizează servicii sub denumiri comerciale diferite sau în contexte specifice diferite, există posibilitatea să se includă un număr de intrări CSP egal cu numărul contextelor specifice (de exemplu, intrări denumire/denumire comercială). Alternativa ar consta în introducerea pe listă a fiecărui CSP (entitate juridică) o singură dată și în furnizarea informațiilor specifice privind serviciul. Operatorului de program al statului membru îi revine rolul de discuta și de a stabili, împreună cu CSP, cea mai potrivită abordare.

T S P a d d r e s s (dispoziția 5.4.3)

Acest câmp este OBLIGATORIU și SPECIFICĂ adresa entității juridice sau organizației autorizate prin mandat identificate în câmpul „TSP name” (dispoziția 5.4.1) atât pentru comunicarea prin poștă, cât și pentru cea pe cale electronică. Acest câmp INCLUDE atât „PostalAddress” (respectiv strada și numărul, localitatea, [statul sau provincia], [codul poștal] și codul țării ISO 3166-1 alpha-2) în conformitate cu dispoziția 5.3.5.1, precum și „ElectronicAddress” (respectiv adresa de e-mail și/sau URI al site-ului web) în conformitate cu dispoziția 5.3.5.2.

T S P i n f o r m a t i o n U R I (dispoziția 5.4.4)

Acest câmp este OBLIGATORIU și SPECIFICĂ URI (unul sau mai mulți) unde utilizatorii (de exemplu, părțile care se bazează pe certificat) pot obține informații specifice despre CSP. Câmpul CONSTĂ într-o secvență de indicatori multilingvi (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale). URI de referință (unul sau mai mulți) TREBUIE să furnizeze o cale către informațiile care descriu termenii și condițiile generale ale CSP, practicile sale, aspectele juridice aferente, politicile sale privind serviciile pentru clienți și alte informații cu caracter general care se aplică tuturor serviciilor acestuia incluse în intrarea CSP din TSL.

Notă: Dacă o singură entitate juridică CSP furnizează servicii sub denumiri comerciale diferite sau în contexte specifice diferite, situație reflectată în numărul de intrări TSP egal cu numărul de contexte specifice, acest câmp SPECIFICĂ informații referitoare la setul specific de servicii introduse pe listă la o anumită intrare TSP/denumire comercială.

▼C1

TSP information extensions (dispoziția 5.4.5)

Acest câmp este OPȚIONAL și, dacă este prezent, POATE fi utilizat de către operatorul de program în conformitate cu specificațiile ETSI TS 102 231 (dispoziția 5.4.5), cu scopul de a furniza informații specifice care urmează a fi interpretate în conformitate cu regulile programului respectiv.

List of Services

Acest câmp este OBLIGATORIU și CONȚINE o secvență care identifică fiecare serviciu recunoscut furnizat de CSP și statutul aprobării (precum și istoricul statutului respectiv) serviciului respectiv. Cel puțin un serviciu trebuie introdus pe listă (chiar dacă toate informațiile existente sunt istorice).

Întrucât păstrarea informațiilor istorice despre serviciile introduse pe listă este OBLIGATORIE în temeiul prezentelor specificații, informațiile istorice respective TREBUIE păstrate chiar dacă statutul curent al serviciului ar presupune în mod normal introducerea acestora pe listă (de exemplu, serviciul este retras). Prin urmare un CSP TREBUIE să fie inclus chiar și atunci când singurul serviciu furnizat de acesta, este introdus pe listă, are un stadiu care nu modifică istoricul.

Service Information

TSP(1) Service(1)

Service type identifier (dispoziția 5.5.1)

▼M1

Acest câmp este OBLIGATORIU și SPECIFICĂ identificatorul tipului de serviciu în conformitate cu actualele specificații TSL (respectiv „/eSigDir-1999-93-EC-TrustedList/TSLType/generic”).

▼C1

Dacă serviciul introdus pe listă are legătură cu eliberarea certificatelor calificate, URI menționat ESTE http://uri.etsi.org/TrstSvc/Svctype/CA/QC (o autoritate de certificare care eliberează certificate calificate).

Dacă serviciul introdus pe listă are legătură cu eliberarea jetoanelor serviciilor de încredere care nu sunt QC și pe care nu se bazează eliberarea de QC, URI menționat ESTE unul dintre URI definiți în ETSI 102 231 și figurând pe listă la dispoziția D.2, corespunzătoare acestui câmp. Această situație SE APLICĂ și acelor jetoane ale serviciilor de încredere care sunt supravegheate/acreditate în vederea îndeplinirii anumitor calificări specifice în conformitate cu legislația națională a statelor membre (de exemplu, așa-numitul jeton calificat de marcare temporală în DE sau HU); URI menționat ESTE unul dintre URI definiți în ETSI 102 231 și figurând pe listă la dispoziția D.2, corespunzătoare acestui câmp (de exemplu, TSA pentru jetoanele calificate de marcare temporală definite la nivel național). Dacă este cazul, aceste calificări naționale specifice ale jetoanelor serviciilor de încredere POT fi incluse în intrarea serviciului; în acest scop SE FOLOSEȘTE extensia additionalServiceInformation (dispoziția 5.8.2) din dispoziția 5.5.9 („Service information extension”).

▼C1

Ca un principiu implicit general, fiecare certificat X.509v3 BENEFICIAZĂ de o singură intrare (de exemplu pentru un serviciu de certificare de tip CA/QC) în cadrul serviciilor de certificare de pe listă furnizate de un CSP inclus pe lista sigură [de exemplu, o autoritate de certificare care eliberează (direct) QC]. În anumite circumstanțe luate în considerare cu atenție și în anumite condiții coordonate și aprobate cu mare atenție, un organism de supraveghere/acreditare al unui stat membru POATE decide să folosească certificatul X.509v3 al unei Root CA sau Upper level CA (de exemplu, o autoritate de certificare care nu eliberează direct QC pentru entități finale, dar care certifică o ierarhie de CA în mod descendent până la CA care eliberează QC către entitățile finale) ca „Sdi" a unei singure intrări din lista de servicii furnizate de un CSP de pe listă. Consecințele (avantajele și dezavantajele) utilizării acestui certificat X.509v3 al unei Root CA sau Upper CA ca valoare „Sdi" a intrărilor pentru servicii din TL trebuie să fie analizate cu atenție și aprobate de statele membre [1]. În plus, la aplicarea unei asemenea excepții autorizate de la principiul implicit, statele membre TREBUIE să prezinte documentația necesară pentru a facilita crearea și verificarea căii de certificare.

Notă: Acei TSP cum ar fi respondenții OCSP și emitenții CRL care fac parte din serviciile de certificare CSP_{QC} și care folosesc perechi separate de chei pentru a semna răspunsurile OCSP, respectiv CRL, POT fi, de asemenea, introduși pe listă în modelul TSL actual folosind următoarea combinație de URI:

— Valoarea „Service type identifier" (dispoziția 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

combinată cu următoarea valoare a extensiei additionalServiceInformation (dispoziția 5.8.2) din „Service information extension" (dispoziția 5.5.9):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Descriere: un furnizor de informații privind statutul certificatelor care operează un server OCSP ca parte a unui serviciu furnizat de un CSP care eliberează certificate calificate.

— Valoarea „Service type identifier" (dispoziția 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

combinată cu următoarea valoarea a extensiei additionalServiceInformation (dispoziția 5.8.2) din „Service information extension" (dispoziția 5.5.9):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Descriere: un furnizor de informații privind statutul certificatelor care operează o CRL ca parte a unui serviciu furnizat de un CSP care eliberează certificate calificate.

— Valoarea „Service type identifier" (dispoziția 5.5.1):

http://uri.etsi.org/JSIvc/Svctype/AC/CC

[1] Folosirea unui certificat X.509v3 al unei Root CA în calitate de valoare „Sdi" al unui serviciu inclus pe listă va obliga operatorul de program să ia în considerare întregul set de servicii de certificare din cadrul unei astfel de Root CA în ceea ce privește „statutul de supraveghere/acreditare". De exemplu, orice modificare a statutului solicitată de o singură CA din ierarhia de bază de pe listă va obliga întreaga ierarhie să transpună acea modificare a statutului.

▼C1

combinată cu următoarea valoare a extensiei additionalServiceInformation (dispoziția 5.8.2) din „Service information extension” (dispoziția 5.5.9):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Descriere: o autoritate de certificare de bază de la care se poate stabili traseul certificării până la o autoritate de certificare care eliberează certificate calificate.

— Valoarea „Service type identifier” (dispoziția 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/TSA

combinată cu următoarea valoare a extensiei additionalServiceInformation (dispoziția 5.8.2) din „Service information extension” (dispoziția 5.5.9):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Descriere: un serviciu de marcare temporală ca parte a unui serviciu furnizat de un prestator de servicii de certificare care eliberează certificate calificate care eliberează TST care pot fi utilizate în procesul de verificare a semnăturii calificate cu scopul de a stabili și extinde valabilitatea semnăturii în cazul în care QC este revocat sau a expirat.

Service name (dispoziția 5.5.2)

Acest câmp este OBLIGATORIU și SPECIFICĂ denumirea în baza căreia CSP identificat la „TSP name” (dispoziția 5.4.1) furnizează serviciul identificat la „Service type identifier” (dispoziția 5.5.1). Câmpul CONSTĂ într-o secvență de șiruri de caractere multilingve (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale).

Service digital identity (dispoziția 5.5.3)

Acest câmp este OBLIGATORIU și SPECIFICĂ cel puțin o reprezentare a identificatorului digital unic pentru serviciul al cărui tip este specificat la „Service type identifier” (dispoziția 5.5.1) prin care se poate identifica neechivoc serviciul.

În prezentele specificații, identificatorul digital utilizat în acest câmp ESTE certificatul X.509v3 relevant ca reprezentare a cheii (cheilor) publice utilizate de CSP pentru furnizarea serviciului al cărui tip este specificat de „Service type identifier” (dispoziția 5.5.1) (respectiv cheia utilizată de o RootCA/QC, cheia utilizată la semnarea certificatelor ([1]) sau la eliberarea jetoanelor de marcare temporală, semnarea CRL sau a răspunsurilor OCSP). Acest certificat X.509v3 asociat ESTE UTILIZAT ca identificator digital minim necesar [ca reprezentare a cheii (cheilor) publice utilizate de CSP pentru furnizarea serviciului de pe listă]. Identificatorii suplimentari POT fi utilizați după cum urmează, însă toți TREBUIE să se raporteze la aceeași identitate (respectiv la certificatul X.509v3 asociat):

([1]) Acesta poate fi un certificat al unei CA care eliberează certificate pentru entitățile finale (de exemplu, CA/PKC, CA/QC) **sau** certificatul unei Root CA de încredere de la care se stabilește o cale până la certificatele calificate pentru entități finale, de pe poziția inferioară. În funcție de existența unei posibilități de a utiliza aceste informații și informațiile cuprinse în fiecare certificat pentru entități finale eliberat în temeiul acestei baze de încredere cu scopul de a determina neechivoc caracteristicile corespunzătoare ale oricărui certificat calificat, poate fi necesar ca aceste informații („Service digital identity”) să fie completate de datele din „Service information extensions” (a se vedea dispoziția 5.5.9).

▼C1

(a) numele distinctiv (DN) al certificatului care poate fi folosit pentru a verifica semnăturile electronice ale serviciului CSP specificat la „Service type identifier” (dispoziția 5.5.1);

(b) identificatorul cheii publice asociate (respectiv SubjectKeyIdentifier X.509v3 sau valoarea SKI);

(c) cheia publică asociată.

Ca un principiu implicit general, identificatorul digital (respectiv certificatul X.509v3 asociat) NU TREBUIE să fie inclus pe lista sigură decât o singură dată, adică fiecare certificat X.509v3 BENEFICIAZĂ de o singură intrare pentru un serviciu de certificare dintre cele introduse pe listă prestate de un CSP cuprins pe lista sigură. În mod reciproc, SE FOLOSEȘTE un singur certificat X.509v3 într-o singură intrare a serviciului ca valoare „Sdi”.

Nota 1: Singurul caz în care nu poate fi aplicat principiul implicit general sus-menționat este situația în care se folosește un singur certificat X.509v3 la eliberarea diferitelor tipuri de jetoane ale serviciilor de încredere pentru care se aplică diferite programe de supraveghere/acreditare; de exemplu un singur certificat X.509v3 este folosit de către un CSP pe de o parte la eliberarea QC în cadrul unui sistem corespunzător de supraveghere și pe de altă parte la eliberarea certificatelor necalificate sub un statut diferit de supraveghere/acreditare. În acest caz și exemplu, se vor folosi două intrări cu valori „Sti” diferite (de exemplu CA/QC, respectiv CA/PKC în exemplul dat) și cu aceeași valoare „Sdi” (certificatul asociat X.509v3).

Formele de implementare depind de ASN.1 sau XML și RESPECTĂ specificațiile ETSI TS 102 231 (pentru ASN.1 a se consulta anexa A la ETSI TS 102 231 iar pentru XML a se consulta anexa B la ETSI TS 102 231).

Nota 2: Dacă trebuie să se furnizeze informații suplimentare despre „calificare” în legătură cu intrarea privind serviciul identificat, atunci operatorul de program IA ÎN CONSIDERARE, dacă este cazul, utilizarea extensiei „additionalServiceInformation” (dispoziția 5.8.2) din câmpul „Service information extension” (dispoziția 5.5.9) în funcție de scopul furnizării acestor informații suplimentare despre „calificare”. În plus, operatorul de program are opțiunea de a aplica dispoziția 5.5.6 („Scheme service definition URI”).

Service current status (dispoziția 5.5.4)

Acest câmp este OBLIGATORIU și SPECIFICĂ identificatorul statutului serviciului prin intermediul unuia dintre următorii URI:

▼C2

— **Under supervision (sub supraveghere)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision);

— **Supervision of Service in Cessation (supravegherea serviciului în curs de a fi suspendată)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

— **Supervision Ceased (supraveghere suspendată)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— **Supervision Revoked (supraveghere revocată)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked);

— **Accredited (acreditat)** (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited);

— **Accreditation Ceased (acreditare suspendată)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— **Accreditation Revoked (acreditare revocată)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

În contextul prezentelor specificații ale listei sigure, statutele sus-menționate SE INTERPRETEAZĂ după cum urmează:

— ***Sub supraveghere:*** Serviciul identificat la „Service digital identity” (dispoziția 5.5.3) furnizat de prestatorul de servicii de certificare (CSP) identificat la „TSP name” (dispoziția 5.4.1) se află în prezent sub supravegherea statului membru identificat la „Scheme territory” (dispoziția 5.3.10) în care este stabilit CSP, în vederea conformității cu dispozițiile Directivei 1999/93/CE.

▼M1

— ***Supravegherea serviciului în curs de a fi suspendată:*** Serviciul identificat la „Service digital identity” (dispoziția 5.5.3) furnizat de CSP identificat la „TSP name” (dispoziția 5.4.1) este în prezent în curs de a fi suspendat însă este încă supravegheat până în momentul în care supravegherea este suspendată sau revocată. În cazul în care o altă persoană juridică în afara celei identificate la „TSP name” preia responsabilitatea asigurării acestei etape de suspendare, identificarea acestei persoane juridice noi sau de rezervă (CSP de rezervă) ESTE prevăzută la „Scheme service definition URI” (dispoziția 5.5.6) și în extensia „TakenOverBy” (dispoziția L.3.2) a intrării serviciului.

▼C1

— ***Supraveghere suspendată:*** Perioada de valabilitate a evaluării în vederea supravegherii a expirat fără ca serviciul identificat la „Service digital identity” (dispoziția 5.5.3) să fie reevaluat. În prezent, serviciul nu s-a mai aflat sub supraveghere de la data de trecere la statutul curent, întrucât se consideră că nu se mai prestează serviciul respectiv.

— ***Supraveghere revocată:*** Fiind supravegheat anterior, serviciul furnizat de CSP sau chiar CSP nu a mai reușit să respecte în continuare dispozițiile Directivei 1999/93/CE, potrivit constatării statului membru identificat la „Scheme territory” (dispoziția 5.3.10) în care este stabilit CSP. În consecință, s-a solicitat să nu se mai presteze serviciul respectiv și se consideră că acesta nu mai este prestat din motivul menționat anterior.

Nota 1: Valoarea statutului „Supraveghere revocată” poate constitui un statut definitiv, chiar dacă CSP își încetează complet activitatea; în acest caz, nu este necesară trecerea la statutul „Supravegherea serviciului în curs de a fi suspendată” sau „Supraveghere suspendată”. În realitate, singura posibilitate de a modifica statutul „Supraveghere revocată” este restabilirea conformității cu dispozițiile Directivei 1999/93/CE potrivit sistemului adecvat de supraveghere în vigoare în statul membru care este proprietarul TL și redobândirea statutul „Sub supraveghere”. Statutul „Supravegherea serviciului în curs de suspendare” sau „Supraveghere suspendată” este atribuit doar dacă un CSP își încetează direct serviciile asociate aflate sub supraveghere, și nu dacă s-a revocat supravegherea.

— ***Acreditat:*** Organismul de acreditare a efectuat o evaluare în vederea acreditării în numele statului membru identificat la „Scheme territory” (dispoziția 5.3.10) și se constată că serviciul identificat la „Service digital identity” (dispoziția 5.5.3) furnizat de CSP [1] identificat la „TSP name” (dispoziția 5.4.1) este conform cu dispozițiile Directivei 1999/93/CE.

[1] Trebuie reținut că acest CSP acreditat poate fi stabilit într-un stat membru diferit de cel identificat la „Sheme territory” din implementarea TSL a LS sau într-o țară terță [a se vedea articolul 7 alineatul (1) litera (a) din Directiva 1999/93/CE].

▼C1

Nota 2: Atunci când sunt folosite în cazul unui CSP care eliberează QC stabilit în „Scheme territory” (dispoziția 5.3.10), statutele „Acreditare revocată” și „Acreditare suspendată” TREBUIE să fie considerate drept „statute de tranzit” și NU TREBUIE să fie utilizate ca o valoare pentru „Service current status” deoarece, în cazul în care sunt folosite, acestea TREBUIE să fie urmate imediat în „Service approval history information” sau în „Service current status” de un statut „Sub supraveghere”, și eventual de un alt statut de supraveghere definit mai sus și ilustrat în figura 1. Dacă este utilizat în cazul unui CSP care nu eliberează QC în condițiile în care nu există decât un program asociat de „acreditare voluntară” fără niciun program asociat de supraveghere sau în cazul unui CSP care eliberează QC fără ca CSP respectiv să fie stabilit în „Scheme territory” (dispoziția 5.3.10) (de exemplu, într-o țară terță), statutele „Acreditare revocată” și „Acreditare suspendată” POT fi folosite ca valoare pentru „Service current status”:

— ***Acreditare suspendată:*** Perioada de valabilitate a evaluării în vederea acreditării s-a încheiat fără ca serviciul identificat la „Service digital identity” (dispoziția 5.5.3) să fie reevaluat.

— ***Acreditare revocată:*** Stabilindu-se în prealabil îndeplinirea criteriilor programului de către serviciul identificat la „Service digital identity” (dispoziția 5.5.3) furnizat de prestatorul de servicii de certificare (CSP) identificat la „TSP name” (dispoziția 5.4.1), serviciul în cauza sau chiar CSP nu au mai reușit să respecte în continuare dispozițiile Directivei 1999/93/CE.

Nota 3: Pentru CSP care eliberează QC și pentru CSP care nu eliberează QC (de exemplu, prestatori de servicii de marcare temporală care eliberează TST, CSP care eliberează certificate necalificate etc.) trebuie să se folosească exact aceleași valori pentru statute. „Service Type identifier” (dispoziția 5.5.1) VA FI FOLOSIT pentru a face diferența între sistemele de supraveghere/acreditare aplicabile.

Nota 4: Informațiile suplimentare despre „calificare” aferente statutului și 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). Operatorii de program UTILIZEAZĂ extensia „additionalServiceInformation” (dispoziția 5.8.2) a câmpului „Service information extension” (dispoziția 5.5.9) în funcție de scopul furnizării acestor informații suplimentare privind „calificarea”. În plus, operatorul de program are opțiunea de a utiliza dispoziția 5.5.6 („Scheme service definition URI”).

Current status starting date and time (dispoziția 5.5.5)

Acest câmp este OBLIGATORIU și SPECIFICĂ data și ora la care intră în vigoare statutul de aprobare curent (valoarea datei și orei conform definiției din ETSI TS 102 231 dispoziția 5.1.4).

Scheme service definition URI (dispoziția 5.5.6)

Acest câmp este OPȚIONAL și, dacă este prezent, SPECIFICĂ URI (unul sau mai mulți) unde părțile care se bazează pe certificat pot obține informații specifice serviciului furnizate de operatorul de program sub forma unei secvențe de indicatori multilingvi (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale).

Dacă este (sunt) utilizat (utilizați), URI de referință TREBUIE să furnizeze o cale către informațiile care descriu serviciul în conformitate cu indicațiile programului. Dacă este cazul, acestea POT include în special:

(a) URI care indică identitatea CSP de rezervă în cazul supravegherii în curs de a fi suspendate a unui serviciu care implică un CSP de rezervă (a se vedea „Service current status” – dispoziția 5.5.4);

▼C1

(b) URI care fac trimitere la documente care prezintă informații suplimentare cu privire la utilizarea unei calificări specifice definite la nivel național pentru un serviciu supravegheat/acreditat care eliberează jetoane al serviciilor de întrecere în conformitate cu utilizarea câmpului „Service information extension” (dispoziția 5.5.9) cu o extensie „additionalServiceInformation” definită conform dispoziției 5.8.2.

Service supply points (dispoziția 5.5.7)

Acest câmp este OPȚIONAL și, dacă este prezent, SPECIFICĂ URI (unul sau mai mulți) unde părțile care se bazează pe certificat pot accesa serviciul printr-o secvență de șiruri de caractere a căror sintaxă TREBUIE să fie în conformitate cu RFC 3986.

TSP service definition URI (dispoziția 5.5.8)

Acest câmp este OPȚIONAL și, dacă este prezent, SPECIFICĂ URI (unul sau mai mulți) de unde părțile care se bazează pe certificat pot obține informații specifice serviciilor furnizate de TSP sub forma unei secvențe de indicatori multilingvi (în EN ca limbă obligatorie și eventual în una sau mai multe limbi naționale). URI de referință (unul sau mai mulți) TREBUIE să ofere o cale de obținere a informațiilor care descriu serviciul conform indicațiilor TSP.

Service information extensions (dispoziția 5.5.9)

În contextul prezentelor specificații, acest câmp este OPȚIONAL, dar ESTE prezent în cazul în care informațiile furnizate la „Service digital identity” (dispoziția 5.5.3) nu sunt suficiente pentru a identifica în mod neechivoc certificatele calificate eliberate de acest serviciu și/sau în cazul în care informațiile cuprinse în certificatele calificate asociate nu permit identificarea prin procesare computerizată a eventualei utilizări a unui SSCD ca suport pentru QC ([1]).

În contextul prezentelor specificații, dacă utilizarea acestui câmp este OBLIGATORIE, de exemplu pentru serviciile CA/QC, SE UTILIZEAZĂ și SE STRUCTUREAZĂ un câmp opțional de informații privind „Service information extensions” („Sie”), în conformitate cu extensia „Qualifications” definită la ETSI TS 102 231 anexa L.3.1, sub forma unei secvențe de unul sau mai multe tupluri, fiecare dintre acestea cuprinzând:

— (filtre) Informații care vor fi utilizate la identificarea mai precisă a unui serviciu anume, din rândul serviciilor de certificare identificate prin „Sdi” (respectiv un set de certificate calificate), pentru care sunt solicitate/furnizate informații suplimentare pentru a indica dacă se bazează pe un SSCD sau nu (și/sau dacă au fost eliberate către o persoană juridică); și

— Informații asociate („calificative”) care să indice dacă acest set de certificate calificate ale serviciului identificat mai precis se bazează pe un SSCD sau nu (dacă informațiile au „QCSSCDStatusAsInCert”, aceasta presupune că aceste informații asociate fac parte din QC într-o formă care poate fi procesată computerizat conform standardelor ETSI ([2]) și/sau informații cu privire la faptul că aceste QC sunt eliberate către o persoană juridică (acestea vor fi considerate implicit ca eliberate exclusiv persoanelor fizice).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD) înseamnă că se garantează de către CSP și se verifică (model de supraveghere) sau se auditează (model de acreditare) de către statul membru (respectiv organismul de supraveghere sau organismul de acreditare al acestuia) că orice QC eliberat în cadrul serviciului (QCA) identificat la „Service digital identity” (dispoziția 5.5.3) și identificat mai precis prin informațiile sus-menționate (filtre) utilizate pentru a identifica mai precis în cadrul serviciului de certificare identificat prin „Sdi” acel set de certificate calificate pentru care sunt necesare aceste informații suplimentare cu privire la prezența sau absența SSCD, **SE BAZEAZĂ** pe un SSCD (respectiv cheia privată asociată cu cheia publică din certificat este stocată într-un dispozitiv securizat de creare a semnăturii conform anexei III la Directiva 1999/93/CE).

([1]) A se vedea secțiunea 2.2 din prezentul document.

([2]) Se face referire la o combinație corespunzătoare între declarația de QcCompliance definită de ETSI, declarațiile QcSSCD [ETSI TS 101 862] sau un QCP/QCP + OID definit de ETSI [ETSI TS 101 456].

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD) înseamnă că se garantează de către CSP și se verifică (model de supraveghere) sau se auditează (model de acreditare) de către statul membru (respectiv organismul de supraveghere sau organismul de acreditare al acestuia) că orice QC eliberat în cadrul serviciului (RootCA/QC sau CA/QC) identificat la „Service digital identity" (dispoziția 5.5.3) și identificat mai precis prin informațiile sus-menționate (filtre) utilizate pentru a identifica mai precis în cadrul serviciului de certificare identificat prin „Sdi" acel set de certificate calificate pentru care sunt necesare aceste informații suplimentare cu privire la prezența sau absența SSCD, **NU ESTE** bazat pe un SSCD (respectiv cheia privată asociată cu cheia publică din certificat **nu este** stocată într-un dispozitiv securizat de creare a semnăturii conform anexei III la Directiva 1999/93/CE).

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert) înseamnă că se garantează de către CSP și se verifică (model de supraveghere) sau se auditează (model de acreditare) de către statul membru (respectiv organismul de supraveghere sau organismul de acreditare al acestuia) că orice QC eliberat în cadrul serviciului (CA/QC) identificat la „Service digital identity" (dispoziția 5.5.3) și identificat mai precis prin informațiile sus-menționate (filtre) utilizate pentru a identifica mai precis în cadrul serviciului de certificare identificat prin „Sdi" acel set de certificate calificate pentru care sunt necesare aceste informații suplimentare cu privire la prezența sau absența SSCD, CONȚINE informații care pot fi procesate computerizat indicând dacă QC se bazează sau nu pe un SSCD.

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson) presupune că se garantează de către CSP și se verifică (model de supraveghere) sau se auditează (model de acreditare) de către statul membru (respectiv organismul de supraveghere sau organismul de acreditare al acestuia) că orice QC eliberat în cadrul serviciului (QCA) identificat la „Service digital identity" (dispoziția 5.5.3) și identificat mai precis prin informațiile sus-menționate (filtre) utilizate pentru a identifica mai precis în cadrul serviciului de certificare identificat prin „Sdi" acel set de certificate calificate pentru care sunt necesare aceste informații suplimentare cu privire la eliberarea către o persoană juridică **ESTE** eliberat către persoane juridice.

Aceste calificative trebuie utilizate doar ca extensie dacă tipul serviciului este http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Acest câmp este specific formei de implementare (ASN.1 sau XML) și TREBUIE să respecte specificațiile prevăzute la ETSI TS 102 231, anexa L.3.1.

▼M1

În contextul unei implementări XML, conținutul specific al acestor informații suplimentare trebuie să fie codificat utilizând fișierele xsd prevăzute în anexa C la ETSI TS 102 231.

▼C1

Service Approval History

Acest câmp este OPȚIONAL, dar TREBUIE să fie prezent dacă „Historical information period" (dispoziția 5.3.12) este diferită de zero. Prin urmare, în contextul prezentelor specificații, programul TREBUIE să păstreze informațiile istorice. În cazul în care se intenționează să se păstreze informațiile istorice, dar serviciul nu dispune de un istoric anterior statutului curent (adică statutul înregistrat inițial sau informațiile istorice nu au fost păstrate de operatorul de program) acest câmp ESTE gol. În caz contrar, pentru fiecare modificare adusă statutului curent al serviciului furnizat de TSP care a avut loc în perioada de păstrare a informațiilor istorice conform specificațiilor din ETSI TS 102 231 dispoziția 5.3.12, informațiile cu privire la statutul anterior al aprobării SUNT furnizate în ordinea descrescătoare datei și orei de modificare a statutului (respectiv data și ora la care următorul statut al aprobării intră în vigoare).

▼C1

Acest câmp CONSTĂ într-o secvență de informații istorice conform definițiilor următoare.

TSP(1) Service(1) History(1)

Service type identifier (dispoziția 5.6.1)

Acest câmp este OBLIGATORIU și SPECIFICĂ identificatorul tipului serviciului, cu formatul și sensul folosite la „TSP Service Information – Service type identifier” (dispoziția 5.5.1).

Service name (dispoziția 5.6.2)

Acest câmp este OBLIGATORIU și SPECIFICĂ denumirea folosită de CSP în vederea furnizării serviciului identificat la „TSP Service Information – Service type identifier” (dispoziția 5.5.1), precum și formatul și sensul folosite în „TSP Service Information – Service name” (dispoziția 5.5.2). Această dispoziție nu necesită ca denumirea să fie identică cu cea specificată la dispoziția 5.5.2. Modificarea denumirii POATE fi una dintre situațiile care impun un nou statut.

▼M1

Service digital identity (dispoziția 5.6.3)

Acest câmp este OBLIGATORIU și SPECIFICĂ cel puțin o reprezentare a identificatorului digital (respectiv certificatul X.509v3) utilizat în „TSP Service Information – Service digital identity” (dispoziția 5.5.3) cu formatul și sensul definite în ETSI TS 102 231, dispoziția 5.5.3.

Notă: Pentru o valoare a certificatului X.509v3 utilizată în „Sdi”, dispoziția 5.5.3, a unui serviciu, trebuie să existe doar o singură intrare privind serviciul într-o listă sigură, per valoare „Sti:Sie/additionalServiceInformation”. Informațiile „Sdi” (dispoziția 5.6.3) utilizate în informațiile privind statutul aprobării aferent serviciului, asociate unei intrări privind serviciul, precum și informațiile „Sdi” (dispoziția 5.5.3) utilizate în această intrare privind serviciul TREBUIE să fie asociate aceleiași valori a certificatului X.509v3. Atunci când un serviciu inclus în listă își modifică „Sdi” (respectiv reînnoire sau stabilirea unei alte chei pentru acest certificat X.509v3 pentru, de exemplu, CA/PKC sau CA/QC) sau creează un „Sdi” nou pentru un astfel de serviciu, chiar și cu valori identice pentru „Sti”, „Sn”, and [„Sie”] asociate, aceasta înseamnă că Scheme Operator TREBUIE să creeze o intrare diferită privind serviciul față de cea anterioară.

▼C1

Service previous status (dispoziția 5.6.4)

Acest câmp este OBLIGATORIU și SPECIFICĂ identificatorul statutului anterior al serviciului, cu formatul și sensul folosite în „TSP Service Information – Service current status” (dispoziția 5.5.4).

Previous status starting date and time (dispoziția 5.6.5)

Acest câmp este OBLIGATORIU și SPECIFICĂ data și ora la care statutul anterior respectiv a intrat în vigoare, cu formatul și sensul folosite în „TSP Service Information – Service current status starting date and time” (dispoziția 5.5.5).

Service information extensions (dispoziția 5.6.6)

Acest câmp este OPȚIONAL și POATE fi utilizat de către operatorii de program pentru a furniza informații specifice referitoare la servicii cu formatul și sensul folosite în „TSP Service Information – Service information extensions” (dispoziția 5.5.9).

▼C1

TSP(1) Service(1) History(2)

Idem pentru TSP(1) Service(1) History(2) (anterior lui History 1)

…

TSP(1) Service(2)

Idem pentru TSP(1) Service 2 (după caz)

TSP(1)Service(2)History(1)

…

TSP(2) Information

Idem pentru TSP 2 (după caz)

Idem pentru TSP 2 Service 1

Idem pentru TSP 2 Service 1 History 1

…

▼M1

Signed TSL

Implementarea TSL în formă lizibilă pentru om a listei sigure, creată în conformitate cu prezentele specificații, în special capitolul IV, AR TREBUI să fie semnată de „Scheme operator name” (dispoziția 5.3.4) pentru a se asigura autenticitatea și integritatea acesteia ([1]). Formatul semnăturii AR TREBUI să fie PAdES part 3 [ETSI TS 102 778-3 ([2])] însă POATE fi PAdES part 2 [ETSI TS 102 778-2 ([3])] în contextul modelului sigur specific creat prin publicarea certificatelor utilizate pentru semnarea listelor sigure.

Implementarea TSL care poate fi procesată de calculator a listei sigure, creată în conformitate cu prezentele specificații ESTE SEMNATĂ de „Scheme operator name” (dispoziția 5.3.4) pentru a asigura autenticitatea și integritatea acesteia. Formatul implementării TSL care poate fi procesată de calculator a listei sigure, creată în conformitate cu prezentele specificații ESTE XML și ESTE CONFORMĂ cu specificațiile prevăzute în anexele B și C la ETSI TS 102 231.

Formatul semnăturii ESTE XAdES BES sau EPES, în conformitate cu definițiile din specificațiile ETSI TS 101 903 pentru implementările XML. Această implementare a semnăturii electronice ÎNDEPLINEȘTE cerințele, după cum se menționează în anexa B la ETSI TS 102 231 ([4]). Cerințele generale suplimentare cu privire la această semnătură sunt prevăzute în următoarele secțiuni.

▼C1

Scheme identification (dispoziția 5.7.2)

Acest câmp este OBLIGATORIU și SPECIFICĂ o referință asociată de operatorul de program care identifică în mod unic programul descris în prezentele specificații și în TSL creată și care TREBUIE să fie inclusă în calcularea semnăturii. În principiu, acesta este un șir de caractere sau un șir de biți.

([1]) În cazul în care implementarea TSL lizibilă pentru om a listei sigure nu este semnată, autenticitatea și integritatea acesteia TREBUIE să fie garantate printr-un canal de comunicare adecvat, cu un nivel echivalent de securitate. Utilizarea TLS (IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2”) este recomandată în acest scop, iar amprenta certificatului canalului TLS TREBUIE să fie pusă la dispoziția utilizatorilor în afara benzii de către statele membre.

([2]) ETSI TS 102 778-3 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic – Profile based on ISO 32000-1.

([4]) Este obligatoriu să se protejeze operatorul de program care semnează certificatele folosind semnătura în unul dintre modurile prevăzute de ETSI TS 101 903, iar ds:keyInfo ar trebui să conțină lanțul aferent certificatului, dacă este cazul.

▼M1

În contextul prezentelor specificații, referința desemnată INCLUDE „TSL type” (dispoziția 5.3.3), „numele programului” (dispoziția 5.3.6) și valoarea extensiei SubjectKeyIdentifier a certificatului utilizat de operatorul de program pentru semnarea electronică a TSL.

▼C1

Signature algorithm identifier (dispoziția 5.7.3)

Acest câmp este OBLIGATORIU și SPECIFICĂ algoritmul criptografic utilizat pentru a crea semnătura. În funcție de algoritmul utilizat, acest câmp POATE necesita parametri suplimentari. Acest câmp TREBUIE să fie inclus în calcularea semnăturii.

Signature value (dispoziția 5.7.4)

Acest câmp este OBLIGATORIU și CONȚINE valoarea reală a semnăturii digitale. Toate câmpurile aferente TSL (cu excepția valorii semnăturii) TREBUIE să fie incluse în calcularea semnăturii.

TSL extensions (dispoziția 5.8)

Extensia **expiredCertsRevocationInfo** (dispoziția 5.8.1)

Această extensie este OPȚIONALĂ. Dacă este utilizată, ea TREBUIE să respecte specificațiile ETSI TS 102 231, dispoziția 5.8.1.

Extensia **additionalServiceInformation** (dispoziția 5.8.2)

Această extensie OPȚIONALĂ, dacă este utilizată, TREBUIE să fie utilizată exclusiv la nivelul serviciului și doar în câmpul definit la dispoziția 5.5.9 („Service information extension”). Aceasta este utilizată pentru a furniza informații suplimentare cu privire la un serviciu. Extensia ESTE constituită dintr-o secvență de unul sau mai multe tupluri, fiecare dintre acestea conținând:

(a) un URI care identifică informațiile suplimentare, de exemplu:

— un URI care indică o anumită calificare specifică definită la nivel național pentru un jeton supravegheat/acreditat al serviciului de încredere care prestează un serviciu, de exemplu,

— un nivel specific de granularitate al siguranței/calității referitor la un program național de supraveghere/acreditare pentru CSP care nu eliberează QC (de exemplu, RGS */**/*** în FR, statut specific „de supraveghere” stabilit de legislația națională pentru anumiți CSP care eliberează QC în DE), a se vedea nota 4 „Service current status” – dispoziția 5.5.4;

— sau o formă juridică specifică pentru furnizarea supravegheată/acreditată a unui jeton al serviciului de încredere (de exemplu, un „TST calificat” definit la nivel național precum în DE sau HU);

— sau sensul unui identificator specific al politicii prezent într-un certificat X.509v3 furnizat în câmpul „Sdi”;

— sau un URI înregistrat specificat la „Service type identifier”, dispoziția 5.5.1, cu scopul de a specifica mai precis participarea serviciului identificat prin „Sti” ca fiind unul dintre serviciile componente ale prestatorului de servicii de certificare care eliberează QC (de exemplu, OCSP-QC, CRL-QC și RootCA-QC);

(b) un șir opțional care conține valoarea serviceInformation, cu sensul prevăzut în program (de exemplu, *, ** sau ***);

(c) orice informații suplimentare opționale furnizate într-un format specific programului.

▼**M1**

Dereferirea URI AR TREBUI să aibă drept rezultat informații lizibile pentru om (cel puțin în EN și eventual în una sau mai multe limbi naționale) care să fie considerate adecvate și suficiente pentru ca un beneficiar să înțeleagă extensia și, în special, care să explice sensul URI-urilor respective, specificând valorile posibile pentru serviceInformation și sensul fiecărei valori.

Qualifications Extension (dispoziția L.3.1)

Descriere: Acest câmp este OPȚIONAL dar ESTE prezent atunci când utilizarea sa este OBLIGATORIE, de exemplu, pentru servicii RootCA/QC sau CA/QC, și atunci când:

— informațiile prevăzute în „Service digital identity” nu sunt suficiente pentru a identifica fără echivoc certificatele calificate emise de acest serviciu;

— informațiile prezente în certificatele calificate aferente nu permit identificarea care poate fi procesată de calculator a datelor privind existența sau inexistența unui SSCD la baza QC.

Atunci când este utilizată, această extensie a nivelului serviciului TREBUIE să fie utilizată doar în câmpul definit în „Service information extension” (dispoziția 5.5.9) și ESTE conformă cu specificațiile prevăzute în anexa L.3.1 la ETSI TS 102 231.

TakenOverBy Extension (dispoziția L.3.2)

Descriere: Această extensie este OPȚIONALĂ dar ESTE prezentă atunci când un serviciu care anterior se afla sub responsabilitatea legală a unui CSP este preluat de un alt TSP și este destinat specificării oficiale a responsabilității legale privind un serviciu și facilitării afișării de către software-ul de verificare a unui detaliu juridic utilizatorului. Informațiile furnizate în această extensie SUNT conforme cu utilizarea aferentă a dispoziției 5.5.6 și SUNT conforme cu specificațiile din anexa L.3.2 la ETSI TS 102 231.

▼M1

CAPITOLUL II

În momentul creării listelor sigure, statele membre vor utiliza:

codurile lingvistice cu litere minuscule și codurile naționale cu litere majuscule;

codurile lingvistice și codurile naționale în conformitate cu tabelul prevăzut mai jos.

Atunci când este prezent alfabetul latin (cu codul său lingvistic propriu) se adaugă o transliterație în alfabetul latin cu codurile lingvistice aferente specificate în tabelul de mai jos.

Nume scurt (limba sursă)	Nume scurt (limba engleză)	Cod de țară	Cod lingvistic	Note	Transliterație în alfabetul latin
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	Cod de țară recomandat de UE	el-Latn
España	Spain	ES	es	inclusiv catalană (ca), bască (eu), galiciană (gl)	
France	France	FR	fr		
▼M2 Hrvatska	Croatia	HR	hr		
▼M1 Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼M1

Nume scurt (limba sursă)	Nume scurt (limba engleză)	Cod de țară	Cod lingvistic	Note	Transliterație în alfabetul latin
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Cod de țară recomandat de UE	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Transliterație în alfabetul latin: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

CAPITOLUL IV

SPECIFICAȚII PRIVIND FORMA LIZIBILĂ PENTRU OM A IMPLEMENTĂRII ÎN TSL A LISTEI SIGURE

Forma lizibilă pentru om (*Human Readable* – HR) a implementării în TSL a listei sigure TREBUIE să fie disponibilă public și accesibilă prin mijloace electronice. Aceasta AR TREBUI să fie prezentată sub forma unui document PDF (*Portable Document Format*) conform ISO 32000 care TREBUIE formatat conform profilului PDF/A (ISO 19005).

Conținutul formei HR bazată pe PDF/A a implementării TSL a listei sigure AR TREBUI să respecte următoarele cerințe:

▼M1

— titlul formei lizibile pentru om a listelor sigure este elaborat sub forma unei concatenații a următoarelor elemente:

  — opțional, imaginea drapelului național al statului membru;

  — spațiu liber;

  — numele scurt al țării în limba (limbile) sursă (astfel cum se prevede în prima coloană a tabelului din capitolul II);

  — spațiu liber;

  — „(”;

  — numele scurt al țării în limba engleză (astfel cum se prevede în a doua coloană a tabelului din capitolul II) între paranteze;

  — „):” ca închidere de paranteză și separator;

  — spațiu liber;

  — „Trusted List”;

  — opțional, logoul operatorului de program din statul membru;

▼C1

— structura formei HR AR TREBUI să reflecte modelul logic descris la secțiunea 5.1.2 din ETSI TS 102 231;

— 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 și în special în conformitate cu anexa D la ETSI TS 102 231 sau cu prezentele specificații referitoare la URI înregistrați (de exemplu, „O autoritate de certificare care eliberează certificate cu chei publice.”);

  — versiuni în mai multe limbi naturale conform mențiunilor aferente implementării TSL a listei sigure, dacă este cazul;

— în forma HR 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

▼C1

— 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 HR AR TREBUI să poată fi imprimată cu ușurință;

— forma HR POATE fi semnată electronic. Dacă este semnată, aceasta TREBUIE să fie semnată de operatorul programului în conformitate cu aceleași specificații privind semnătura aplicabile implementării TSL a listei sigure.